INFORME DE LA PONENCIA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES

SENADO
2014

INFORME DE LA PONENCIA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES

SENADO
2014

Supervisión del texto a cargo del Letrado de las Cortes Generales don Eugenio de Santos Canalejo.

Secretaría General del Senado
Dirección de Estudios
Departamento de Publicaciones.

ISBN: 987-84-96451-51-3
Depósito legal: M. 2.049-2015

Preimpresión, impresión y encuadernación:
Grafo Industrias Gráficas
Avda. de Cervantes, 51. Pol. Denac
48970 Basauri (Bizkaia). España.

ÍNDICE

1. PRESENTACIÓN

Pocos avances científicos y técnicos ha habido con tanta repercusión en nuestras vidas cotidianas como la revolución de las tecnologías de la información y la comunicación. La red no cesa de expandirse, de incrementar su capacidad de interconexión y su complejidad, de tal manera que hoy nos resulta prácticamente imposible concebir cualquier tipo de actividad económica, social, cultural o sencillamente lúdica que pueda ser desarrollada sin alguna relación con internet.

Internet ya no es un nuevo mundo paralelo al mundo real, como algunos teorizaban no hace muchos años, sino que tiene un valor de centralidad absoluta. Es decir, el digital no es un sector más entre otros: el ciberespacio es una malla por la que ya se mueven e interactúan todos los sectores y tipos de actividades humanas. De ese modo, en mayor medida que ninguna otra innovación, internet nos proporciona fortalezas y nos abre oportunidades de progreso y libertad.

Pero, al mismo tiempo, no es menos cierto que, por su carácter abierto y su dimensión global, internet también lleva aparejado un reverso de nuevos problemas y amenazas contra nuestra seguridad, entre ellas, de forma destacada, las que afectan a un sector de la población tan especialmente vulnerable y por tanto protegible como son los menores de edad.

El Senado de España siempre ha concedido una atención muy señalada a todas las cuestiones relacionadas con el desarrollo de la Sociedad de la Información y el Conocimiento, incluso, podríamos decir, desde una posición tan pionera como la de aquella Comisión Especial sobre Redes Informáticas creada en 1998.

Continuadora de la trayectoria trazada por aquella Comisión, ha sido esta Ponencia de estudio sobre los riesgos derivados del uso de la red por parte de los menores, cuya buena labor ha hecho posible la redacción del informe que el lector tiene ahora a su disposición y en el que podrá

encontrar resumidas las interesantes aportaciones de todos los expertos, procedentes de muy distintos ámbitos, que han participado en sus trabajos, así como las conclusiones y recomendaciones finales desprendidas de ellos.

Confío, por tanto, que este informe sirva al propósito esencial que ha motivado la labor de la ponencia de estudio y que no ha sido otro que el de contribuir al refuerzo de la seguridad de los menores en el acceso a la red.

Pío García-Escudero Márquez
Presidente del Senado

2. INTRODUCCIÓN

La sociedad en la que vivimos está marcada profundamente por la realidad de Internet, que ha configurado un escenario revolucionario para las relaciones humanas y sociales, caracterizado por la conectividad, la interactividad y la convergencia de los medios audiovisuales, en una dimensión hasta hace poco insospechada y de evolución vertiginosa.

En este contexto, los menores ocupan un lugar propio, en el que el mundo digital constituye parte natural de sus vidas, con unas necesidades específicas, tanto desde el punto de vista de las oportunidades que ofrece Internet como desde el de los riesgos que entraña.

El Senado de España ha querido sumarse a los esfuerzos manifestados en esta dirección, mediante la creación de una **Ponencia de estudio sobre los riesgos derivados del uso de la Red por parte de los menores**. Este grupo de trabajo, que inició su andadura en los primeros meses de 2013, lo hemos integrado diez Senadores, responsables de la elaboración del Informe objeto de esta publicación. A todos ellos quiero agradecer el acierto en las propuestas, su dedicación y las facilidades otorgadas a este Coordinador. Y añado que esta referencia no estaría completa si olvidara mencionar a D. Eugenio de Santos, letrado de las Cortes Generales, que asumió la tarea de dar orden y forma a las propuestas de los Senadores y que tiene tanta responsabilidad como los integrantes de la Ponencia en el buen fin de este empeño.

Nuestra convicción de que las necesidades de los menores en la red debían ser objeto de estudio de manera integral, teniendo en cuenta la diversidad de enfoques, partes interesadas y niveles de acción concurrentes, determinó un ambicioso plan de trabajo, en el que han colaborado destacados representantes de entidades públicas y privadas y reconocidos expertos, procedentes de muy distintos ámbitos: poderes públicos, organizaciones de protección de menores y representativas de intereses

en los sectores afectados y especialistas en diversas disciplinas, como la ciberseguridad, la psicología o la comunicación digital. A todos ellos, nuestro reconocimiento por la abundante y valiosa información aportada, y sincero agradecimiento por su disposición y entusiasmo. También a cuantos, fuera del marco formal de estas comparecencias, han manifestado su interés por este reto y remitido a la misma estudios, artículos, o sencillas notas con interesantes aportaciones.

Los valores esenciales de nuestra sociedad y las alianzas público-privadas son premisas fundamentales para las claves de la acción política que proponemos, porque tanto en el mundo físico como en el digital deben regir los valores que encarnan los derechos fundamentales de la persona, reconocidos en la Constitución Española y en los tratados internacionales, que en el caso de los menores garantizan además el «interés superior» de los mismos como «consideración primordial». También porque la existencia de actores muy diferentes, con intereses relevantes en la materia, reclama una responsabilidad compartida, en la que las alianzas público-privadas, desde un liderazgo gubernamental con visión estratégica, y acento en la coordinación y coherencia, constituye una palanca fundamental para la acción. A ella hay que añadir la cooperación internacional, derivada de la naturaleza dinámica y global de Internet, que exige que los objetivos y acciones a nivel nacional no puedan prescindir de los que se plantean a nivel europeo e internacional.

El texto concluye en la enumeración de veintiuna Conclusiones y nueve Recomendaciones, de las que son medulares, en primer lugar, la alfabetización digital y mediática de los menores, con la escuela como piedra angular de la misma, la doble protección que debe procurar al menor la existencia de un nivel aceptable de seguridad en el propio entorno en línea y, finalmente, un sistema normativo y de aplicación de la ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red.

Cobra, asimismo, singular importancia para los países miembros de la Unión Europea, como España, una posición decidida en el proceso de revisión en curso del marco regulador europeo de protección de datos de carácter personal. Creemos necesario que se contemplen las necesidades específicas de los menores, a través, entre otras medidas, de la implantación de mecanismos de verificación de la edad, la elección por defecto de la opción más exigente en cuanto a privacidad, robustas herramientas de denuncia, y mecanismos ágiles de coordinación con las organizacio-

nes de protección de menores y con las fuerzas policiales. Además de otras propuestas relevantes, como la regulación del «agente encubierto», figura reclamada por muchos y cualificados representantes de todos los sectores, o un Adjunto del Defensor del Pueblo especializado en esta materia, entre otras.

Para finalizar, debe subrayarse que la unanimidad reflejada en la firma por todos los grupos parlamentarios de la moción que originó la constitución de esta Ponencia y la colaboración fluida de todos sus miembros concluyeron en el voto unánime de la Ponencia al acordar, en sesión del 30 de septiembre, aprobar y elevar al Pleno de la Cámara el Informe elaborado, siendo respaldado por el voto unánime de todos los Senadores.

TOMÁS PEDRO BURGOS BETETA
Senador
Coordinador de la Ponencia conjunta de estudio sobre los riesgos derivados del uso de la Red por parte de los menores

3. INFORME DE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES[*]

[*] Boletín Oficial de las Cortes Generales, Senado, X Legislatura, núm. 410, de 3 de octubre de 2014.

La Ponencia conjunta de estudio sobre los riesgos derivados del uso de la Red por parte de los menores, constituida en el seno de la Comisión conjunta de las Comisiones de Interior, de Educación y Deporte, y de Industria, Energía y Turismo e integrada por los Excmos. Sres. D. Emilio Álvarez Villazán (GPS); D. Iñaki Mirena Anasagasti Olabeaga (GPV); D. José María Ángel Batalla (GPS); Dª. Carmen Azuara Navarro (GPP); D. Francisco Boya Alós (GPEPC); D. Tomás Pedro Burgos Beteta (GPP); D. José María Chiquillo Barber (GPP); D. Andrés Gil García (GPS); Dª. Amalur Mendizabal Azurmendi (GPMX) y D. Jordi Miquel Sendra Vellvè (GPCIU) ha aprobado el siguiente informe:

I. *Introducción: constitución, composición y actividad de la ponencia*

De resultas de una moción[1] firmada por todos los grupos parlamentarios de la Cámara (Grupo Parlamentario Popular en el Senado, Grupo Parlamentario Socialista, Grupo Parlamentario Catalán en el Senado Convergència i Unió, Grupo Parlamentario Entesa pel Progrés de Catalunya, Grupo Parlamentario Vasco en el Senado (EAJ-PNV) y Grupo Parlamentario Mixto), el Pleno del Senado, en su sesión número 24 de la X Legislatura, celebrada el día 19 de diciembre de 2012, acordó por unanimidad de los Senadores presentes, la creación de una Ponencia conjunta de las Comisiones de Interior, de Educación y Deporte y de Industria, Energía y Turismo, que abordase el estudio de determinados ámbitos relacionados con el uso de Internet por parte de los menores, a saber:

[1] Moción por la que el Senado acuerda la creación de una Ponencia conjunta entre las Comisiones de Interior, de Educación y Deporte y de Industria, Energía y Turismo, que aborde el estudio de diversos ámbitos relacionados con la prevención y la lucha contra los nuevos delitos cibernéticos (BOCG, Senado, n.º 142, de 27 de diciembre de 2012).

«a. Las medidas de prevención contra los riesgos derivados del uso de las redes sociales por parte de los menores. Estas medidas han de ser aplicables desde los centros escolares y en el ámbito educativo en general, atendiendo a la formación de los profesores y educadores. Así como a la determinación de responsabilidades de los centros en el control de estos riesgos.

b. La determinación de las responsabilidades y el autocontrol de las empresas gestoras de las redes sociales en relación con el acceso de los menores y la utilización de la información personal y privada.

c. Los instrumentos de que disponen las fuerzas y cuerpos de seguridad del Estado para abordar la lucha contra los nuevos delitos cibernéticos. Así como la formación de profesionales y de unidades especializadas para la lucha contra este tipo de delitos.»[2]

La Mesa del Senado, en su reunión celebrada el día 29 de enero de 2013, acordó la constitución de la Comisión conjunta de las mencionadas Comisiones, integrada por los miembros de las mismas y presidida por el Presidente del Senado. En su sesión celebrada el día 5 de febrero de 2013, la Comisión Conjunta de las Comisiones de Interior, de Educación y Deporte y de Industria, Energía y Turismo acordó designar como miembros de la Ponencia conjunta creada por el Pleno de la Cámara a los siguientes Senadores:

— Excmo. Sr. D. Emilio Álvarez Villazán (GPS).

— Excmo. Sr. D. Iñaki Mirena Anasagasti Olabeaga (GPV).

— Excmo. Sr. D. José María Ángel Batalla (GPS).

— Excma. Sra. Dª. Carmen Azuara Navarro (GPP).

— Excmo. Sr. D. Francisco Boya Alós (GPEPC).

— Excmo. Sr. D. Tomás Pedro Burgos Beteta (GPP).

— Excmo. Sr. D. José María Chiquillo Barber (GPP).

— Excmo. Sr. D. Andrés Gil García (GPS).

— Excma. Sra. Dª. Amalur Mendizabal Azurmendi (GPMX).

— Excmo. Sr. D. Jordi Miquel Sendra Vellvé (GPCIU).

[2] Diario de Sesiones del Pleno n.º 47, de 19 de diciembre de 2012.

La coordinación de la Ponencia ha estado a cargo del Senador Excmo. Sr. D. Tomás Pedro Burgos Beteta, y su asistencia y apoyo lo han estado del Letrado de las Cortes Generales D. Eugenio de Santos Canalejo y de la Secretaria de las Comisiones de Interior e Industria, Energía y Turismo Dª. Isabel Jalvo García.

La Ponencia celebró entre los meses de febrero y abril de 2013 cuatro reuniones preparatorias de sus trabajos, en las que esclareció varios aspectos relevantes:

— Estableció como título idóneo de sí misma el de «Ponencia conjunta de estudio sobre los riesgos derivados del uso de la Red por parte de los menores».

— Formuló como premisa fundamental de sus trabajos la consideración de los menores como grupo con unas necesidades específicas en Internet, que deben ser objeto de estudio de manera integral, teniendo en cuenta la diversidad de enfoques, partes interesadas y niveles de acción concurrentes.

— Estableció un límite temporal a sus trabajos, situado en el mes de septiembre de 2014, y un plan de trabajo basado fundamentalmente en la comparecencia de destacados representantes de entidades públicas y privadas y reconocidos expertos, designados por su relación con las materias objeto de estudio, entre las propuestas presentadas por los Senadores integrantes de la Ponencia. En concreto delineó cuatro ámbitos relevantes en tal designación:

  • El ámbito de los poderes públicos, en concreto de los sectores con un ámbito competencial relacionado, desde diferentes ángulos, con la materia objeto de estudio.

  • El ámbito de las organizaciones privadas con una específica vocación en la protección de menores o representativas de asociaciones educativas y de usuarios de Internet.

  • El ámbito de expertos de distintas disciplinas como las nuevas tecnologías y la ciberseguridad, la psicología o la comunicación digital.

  • El ámbito de la industria y de los creadores de contenidos digitales.

— Impulsó, previa autorización de la Mesa del Senado, una novedosa práctica, conforme a la cual, no obstante celebrarse sus sesiones

sin una publicidad directa, como es habitual en el funcionamiento de este tipo de órganos, se incorporaría a la página web del Senado el texto de las disertaciones de los comparecientes, previo su consentimiento para ello.

La Ponencia ha celebrado un total de treinta y tres sesiones, de ellas diecinueve para la celebración de comparecencias, siendo un total de cincuenta y tres las personas invitadas al efecto, que se relacionan a continuación, siguiendo el orden cronológico de las sesiones en que intervinieron[3]:

Sesión de 9 de mayo de 2013

— D. Víctor Calvo-Sotelo Ibáñez-Martín, Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

— D. Borja Adsuara Varela, Director General de Red.es.

— D. Manuel Escalante García, Director General del Instituto Nacional de Tecnologías de la Comunicación (INTECO).

Sesión de 16 de mayo de 2013

— D. Ignacio Cosidó Gutiérrez, Director General de la Policía.

— D. Juan Miguel Manzanas Manzanas, Comisario Jefe de la Brigada de Investigación Tecnológica de la Comisaría General de la Policía Judicial de la Dirección General de la Policía.

— Dª. Carolina González García, Inspectora Jefa de Sección de Prensa y Redes Sociales de la Oficina de Prensa y Relaciones Informativas de la Dirección General de la Policía.

Sesión de 20 de mayo de 2013

— D. Arsenio Fernández de Mesa Díaz del Río, Director General de la Guardia Civil.

— D. Óscar de la Cruz Yagüe, Comandante Jefe del Grupo de Delitos Telemáticos de la Unidad Central Operativa (UCO) de la Guardia Civil.

---

[3] Para las intervenciones de los comparecientes publicadas en la web del Senado: http://www.senado.es/web/actividadparlamentaria/sesionescomision/detallecomisiones/ponenciasdeestudio/index.html?id=S030001&id2=S020009&legis=10&tab=t

En Anexo 1 a este informe se incluye una relación de los comparecientes por orden alfabético.

— D. Carlos Igual Garrido, Capitán del Grupo de Menores y Explotación Sexual Infantil de la Unidad Técnica de Policía Judicial (UTPJ) de la Guardia Civil.

Sesión de 6 de junio de 2013

— D. Alfonso González Hermoso de Mendoza, Director General de Evaluación y Cooperación Territorial.

— Dª. Ana María Román Riechman, Directora del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF).

Sesión de 17 de junio de 2013

— D. Manuel Viota Maestre, Jefe de la Sección Central de Delitos en Tecnologías de la Información de la Unidad de Investigación Criminal y Policía Judicial de la Ertzaintza.

— D. Joaquim Bayarri i Nogueras, Jefe de la División Técnica de Planificación de la Seguridad Ciudadana de los Mossos d'Esquadra.

Sesión de 27 de junio de 2013

— Dª. Elvira Tejada de la Fuente, Fiscal de Sala Coordinadora contra la Criminalidad Informática.

— Dª. Consuelo Madrigal Martínez-Pereda, Fiscal de Sala Coordinadora de Menores.

— Dª. María Salomé Adroher Biosca, Directora General de Servicios para la Familia y la Infancia.

Sesión de 12 de septiembre de 2013

— D. Guillermo Cánovas Gaillemín, Presidente del Centro de Seguridad en Internet de la Asociación Protégeles.

— D. Francisco Javier Martos Mota, Director Ejecutivo de UNICEF Comité Español.

— D. Jorge Flores Fernández, Director de PantallasAmigas.

Sesión de 26 de septiembre de 2013

— Dª. Liliana Orjuela López, Coordinadora de los derechos de la infancia de «Save the children».

— D. Miguel Comín Hernández, Director de Fundación Alia2.

— D. Luis Carbonell Pintanel, Presidente de la Confederación Católica Nacional de Padres de Familia y Padres de Alumnos (CONCAPA).

Sesión de 10 de octubre de 2013

— D. Josep Manuel Prats Moreno, Presidente de la Federació d'Associacions de Pares i Mares d'Escoles Lliures de Catalunya (FAPEL).

— D. Jesús Salido Navarro, Vicepresidente de la Confederación Española de Asociaciones de Padres y Madres de Alumnos (CEAPA).

— D. José Luis Rodríguez Álvarez, Director de la Agencia Española de Protección de Datos (AEPD).

Sesión de 24 de octubre de 2013

— D. Carlos Represa Estrada, Director del Centro de Seguridad TIC Escolar (CTIC) y Director en la Fundación UNIR (Universidad Internacional de La Rioja) del Área de Seguridad en Internet y protección de menores.

— D. Miguel Pérez Subías, Presidente de la Asociación de Usuarios de Internet (AUI).

— D. Miguel Errasti Argal, Presidente de la Asociación Nacional de Empresas de Internet (ANEI).

Sesión de 4 de noviembre de 2013

— D. Javier Urra Portillo, Primer Defensor del Menor de la Comunidad de Madrid.

— D. Juan María Martínez Otero, Vocal del Consejo Asesor de la Federación de Asociaciones de Consumidores y Usuarios de los Medios (iCmedia).

— D. José Miguel Rosell Tejada, socio-Director de S2 Grupo.

Sesión de 27 de noviembre de 2013

— D. Antoni Gutiérrez Rubí, Asesor de comunicación y analista de las redes sociales.

— D. Mariano Chóliz Montañés, Profesor Titular de la Facultad de Psicología de la Universidad de Valencia.

Sesión de 30 de enero de 2013

— D. Eugenio Fontán Oñate, Presidente del Colegio Oficial de Ingenieros de Telecomunicación.

— Dª. Dolors Reig Hernández, Psicóloga Social experta en Sociedad - red y responsable del espacio El caparazón.

— D. Félix Brezo Fernández, Ingeniero Informático e Ingeniero en Organización Industrial.

Sesión de 10 de febrero de 2013

— D. Francisco Ruiz Antón, Mánager de Políticas Públicas y Asuntos Institucionales de Google España y Portugal.

— Dª. Natalia Basterrechea Oñate, Directora de Asuntos Públicos de Facebook de España y Portugal.

— D. Jesús Guijarro Valladolid, Mánager de Responsabilidad Social Corporativa de Orange.

Sesión de 24 de febrero de 2014

— D. Héctor Sánchez Montenegro, Director de Tecnología de Microsoft Ibérica.

— D. Sebastián Muriel Herrero, Director General de Operaciones de Tuenti.

Sesión de 10 de marzo de 2014

— D. José Miguel Tourné Alegre, Director General de la Federación para la Protección de la Propiedad Intelectual (FAP).

— D.ª Salud Martínez Monreal, experta en innovación para la seguridad de la información.

— Dª. Sofía Fernández de Mesa Echeverría, Directora de Responsabilidad e Innovación Social Corporativas de Telefónica.

Sesión de 2 de abril de 2014

— D. José Luis Casal Castro, Cofundador y Director de Marketing de Talk2Us Comunicación.

— D. José Manuel Sedes García, Mánager de Sostenibilidad y Calidad de Vodafone España.

— Dª. Carlota Navarrete Barreiro, Directora General de la Coalición de creadores e industrias de contenidos digitales.

Sesión de 7 de abril de 2014

— D. Íñigo Polo González, Director de Relaciones Institucionales de Ono.

— D. Francisco Javier Santos Ortega, Gerente de Seguridad Corporativa de Ono.

— D. Joan Taulé Valdeperas, Director General de Symantec España.

— Dª. María José Gallego Morales, Responsable de consumidores y usuarios e interceptación legal de las comunicaciones de Jazztel.

Sesión de 5 de mayo de 2014

— Dª. Sinéad McSweeney, Directora de Políticas Públicas, EMEA, de Twitter.

— Dª. Patricia Cartes, Directora de Seguridad de Twitter.

De forma complementaria a las sesiones informativas de los comparecientes, la Ponencia realizó dos visitas institucionales. La primera visita, a invitación del Director General de la Policía, D. Ignacio Cosidó Gutiérrez, al complejo policial de Canillas, en Madrid, el 3 de julio de 2013, con ocasión de la cual la Ponencia conoció las instalaciones de la Comisaría General de Policía Científica y asistió a una presentación de la Unidad de Investigación Tecnológica. La segunda visita se realizó el 8 de julio de 2013, a invitación del Director General del Instituto Nacional de Tecnologías de la Comunicación (INTECO), D. Manuel Escalante García, para mantener una jornada de trabajo en la sede en León de dicho organismo, durante la que se presentaron las líneas estratégicas de éste, se visitó el centro de respuesta a incidentes de seguridad INTECO-CERT y fueron presentadas tecnologías de seguridad de INTECO.

En el curso de los trabajos de la Ponencia, en concreto el 11 de febrero de 2014, se celebró el «Día para una Internet más segura», evento que, bajo los auspicios de la red europea de centros de seguridad en Internet (INSAFE), se desarrolla cada año desde 2003, y en el que participan un número creciente de países. Con ocasión de esta jornada, la Ponencia aprobó una Declaración de adhesión a la misma,

saludando en particular la celebración del «III Congreso nacional Joven y en Red», organizado por el Centro de Seguridad en Internet para menores en España (Protégeles/Cesicat), como acto central de aquel Día. El contenido de dicha Declaración se adjunta como Anexo 2 a este Informe.

El Informe recoge a continuación el análisis de la Ponencia sobre la materia objeto de estudio, a la luz de las aportaciones de los comparecientes y de la documentación complementaria consultada, estructurado sistemáticamente en cinco títulos principales, encabezados por las siguientes rúbricas:

— Uso de la Red por los menores.

— Riesgos existentes en el uso de la Red por los menores.

— ¿Qué hacer?: los menores como centro de una estrategia de ciudadanía digital.

— Conclusiones.

— Recomendaciones.

Una precisión de carácter metodológico debe hacerse. Sin perjuicio de la bibliografía existente relacionada con la materia objeto de estudio, el presente Informe se ha basado, en el apartado documental, en la de origen institucional, que es por ello la citada a lo largo de sus páginas. Como excepción, se citan determinados trabajos de naturaleza estadística que, por corresponderse con iniciativas financiadas por la Unión Europea y ofrecer una base de comparación entre varios países europeos, incluida España, la Ponencia ha juzgado de especial interés[4].

---

[4] Livingston, S., Haddon, L., Görzig, A, Ólafsson. (2010). «Risks and safety for children on the internet: The perspective of European children. Full Findings». LSE London. EU Kids Online, 2011. Disponible en:http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf

También de los mismos autores, «Final Report, EU Kids Online II», 2011. Disponible en: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

La lectura de los resultados entre menores españoles, en Maialen Garmendia, Carmelo Garitaonandia, Gemma Martínez y Miguel Ángel Casado, «Riesgos y seguridad en Internet: los menores españoles en el contexto europeo». Universidad del País Vasco, Bilbao, 2011. Disponible en: http://www.prentsa.ehu.es/p251-content/es/contenidos/

El Informe fue aprobado por la Ponencia en su sesión del día 30 de septiembre de 2014.

II. *Uso de la red por los menores*

1. Escenario global

La seguridad de los menores en la Red no puede analizarse con rigor fuera del escenario global que representa Internet y la evolución tecnológica.

La frase de Churchill en un discurso de 1943 a la Cámara de los Comunes, «nosotros damos forma a nuestros edificios y después nuestros edificios nos dan forma a nosotros», en cita recordada por José Miguel Rosell, en su intervención ante la Ponencia, bien puede aplicarse a la evolución de Internet.

Desde ARPAnet (la red de colaboración surgida en los años sesenta del pasado siglo entre el Departamento de Defensa de Estados Unidos y algunas de las mejores universidades de ese país) hasta la adopción en 1973 del protocolo TCP/IP (que marca el inicio de Internet, al permitir la conexión de los ordenadores conectados a ARPAnet y los de otras redes por entonces existentes), y la posterior generalización de Internet entre el gran público, y de ahí hasta la aparición en los primeros años del nuevo milenio de la web 2.0 (esto es, de la época de la interactividad) y la irrupción de las redes sociales (en 2004 el nacimiento de Facebook), en el umbral ya de la época del «Big Data» y del «Internet de las cosas» (almacenamiento, procesamiento e intercambio masivo de información y conexión de los objetos a Internet), el hombre ha configurado a golpe de avances tecnológicos de rapidez vertiginosa, un escenario, el de Internet y el mundo digital, de consecuencias revolucionarias en las relaciones humanas y sociales.

---

noticia/20110328_internet_kids/es_interkid/adjuntos/Informe_Espa%C3%B1a_completo_red.pdf

Tsitsika, A., Tzavela, E. y Mavromati, F. (ed.). «Investigación sobre conductas adictivas a Internet entre los adolescentes europeos». EU NET ADB Consortium, 2011-2012.

Disponible en: www.eunetadb.eu

Algunas de las características principales del contexto en el que actualmente nos encontramos son la conectividad, la interactividad y la convergencia de medios.

Como señaló a la Ponencia Antoni Gutiérrez, el concepto clave ya no es el de acceso a Internet, sino el de conectividad. Ello es así, como consecuencia de la difusión de las redes de alta velocidad (banda ancha y fibra en las fijas, y banda ancha mediante tecnología UMTS y LTE —tercera y cuarta generación, respectivamente— en las redes de telefonía móvil) y de la irrupción de los nuevos dispositivos móviles (fundamentalmente «tablets» y «smartphones»), que han permitido a capas cada vez más amplias de la población, un acceso y conexión potencialmente continuo a la Red, y lo que es más importante, a los servicios avanzados que ofrece la misma (redes sociales, entre otros), con una ubicuidad total (Internet en el bolsillo, con el «Smartphone»), y a escala planetaria.

Internet es, en palabras de Eugenio Oñate en su disertación a la Ponencia, «la herramienta de la pancomunicación».

Los datos son elocuentes, con altas tasas de crecimiento a nivel mundial en el acceso a Internet, los accesos de banda ancha y la telefonía móvil. A finales de 2012, alrededor de 2.500 millones de personas estaban conectadas a la Red, con un crecimiento a lo largo de dicho año del 10,70% en todo el mundo, estimándose en un 40% la población mundial conectada a Internet en 2013[5].

Por otro lado, los dispositivos portátiles inteligentes, especialmente «tablets» y «smartphones», se han convertido en los terminales principales de conectividad (más de 1.000 millones de «smartphones» vendidos en 2013 en todo el mundo y, asociado al anterior fenómeno, se estima un crecimiento del consumo de aplicaciones móviles desde los aproximadamente 1.200 millones de usuarios de estas aplicaciones en 2012 a 4.400 millones en 2017[6]).

España no es una excepción en este escenario. Según datos del INE[7] referidos a 2013:

---

[5] Fundación Telefónica. «La Sociedad de la Información en España 2013», p. 34. Disponible en: http://www.fundacion.telefonica.com/es/arte_cultura/publicaciones/sie/sie2013.htm

[6] Ibídem, p. 42.

[7] Instituto Nacional de Estadística (INE). Encuesta sobre equipamiento y uso de las tecnologías de la información y comunicación en los hogares 2013.

— El 69,8% de viviendas disponen de acceso a Internet (casi tres puntos porcentuales de aumento respecto a 2012), y un porcentaje similar de viviendas (68,9%) tiene conexión de banda ancha (ADSL, red de cable, etc.).

— En cuanto a la población (16 a 74 años) un 71,6% ha usado Internet en 2013 (24,8 millones de personas, con un aumento de casi dos puntos porcentuales respecto a 2012), constituyendo la edad un factor diferenciador significativo, en el sentido de aumentar la extensión en el uso de Internet a menor edad del segmento considerado, siendo la franja de menor edad analizada (de 16 a 24 años) en donde se produce un uso casi universal (97,4%) (4 millones de personas, un incremento de casi dos puntos porcentuales respecto a 2012).

— A su vez, del total de usuarios de Internet, un 75,1% lo hace diariamente (lo que sumado al 16,9% que lo hace semanalmente, aunque no sea de forma diaria, arroja un porcentaje del 92% de uso frecuente de Internet), siendo de nuevo la franja de 16 a 24 años la que arroja el mayor porcentaje de uso diario de Internet (un 88,5%).

— El uso del teléfono móvil es prácticamente universal (96,1% de viviendas con un teléfono móvil y 94,2% de personas que lo usan), dato que cabe relacionar con el de venta de «smartphones», que ya suponían en diciembre de 2012 el 80% de los teléfonos móviles, lo que convierte la migración del teléfono móvil tradicional al «Smartphone» en un hecho asentado[8].

— Entre los usuarios de Internet, el tipo de dispositivo principal a través del cual se accede a Internet fuera de la vivienda o centro de trabajo, es el teléfono móvil (63,2% de internautas, porcentaje que se eleva hasta el 82,7% en la franja de edad entre 16 y 24 años).

En suma, la conectividad a través de Internet y la movilidad de la misma, forma parte de la vida de los españoles y de una manera especialmente intensa entre los más jóvenes.

Una segunda característica del momento actual es la interactividad, esto es, la potencialidad de los usuarios de actuar como creadores de contenido y en compartirlo en línea con los demás usuarios. Un ejemplo extraído

[8] Fundación Telefónica, op. cit., p. 42.

del Libro verde de la Comisión Europea sobre la convergencia del mundo audiovisual: cada minuto se introducen en YouTube 72 horas de vídeo[9].

En esta perspectiva las denominadas redes sociales ocupan un primer plano. El Instituto Nacional de Tecnologías de la Comunicación (INTECO) y la Agencia Española de Protección de Datos (AEPD) definieron en un estudio de 2009 las redes sociales «online» como «servicios prestados a través de Internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles» [10].

Sebastián Muriel propuso, en su comparecencia ante la Ponencia, un concepto de red social adaptado a la irrupción del fenómeno de los «smartphones» y de la movilidad: «cualquier aplicación que permita la comunicación entre los usarios y el intercambio de información y contenidos entre los mismos», concepto que incluye las aplicaciones móviles del tipo WhatsApp, Line, WeChat, etc., y que tiene su trascendencia desde el punto de vista de la realidad que deben manejar los marcos reguladores y de autorregulación.

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) destacaba, en un estudio de Diciembre de 2011, el dinamismo de la penetración de las redes sociales en España, situándose entonces dos décimas porcentuales por encima de la media de penetración de las redes sociales en Europa[11].

Según datos del INE referidos a 2013, entre los servicios más utilizados por los usuarios de Internet en España se encuentra la participación en redes sociales: un 64,1%, que se eleva a un 94,5% en la franja de edad entre 16 y 24 años[12].

---

[9] Comisión Europea. «Libro Verde. Prepararse para la convergencia plena del mundo audiovisual: crecimiento, creación y valores». COM(2013) 231 final, p. 5.

[10] INTECO/AEPD, «Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online», 2009. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf

[11] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información. «Las redes sociales en Internet», 2011, p. 27. Disponible en: http://www.ontsi.red.es/ontsi/sites/default/files/redes_sociales-documento_0.pdf

[12] INE, encuesta citada.

Otra característica del entorno tecnológico actual es la convergencia del mundo audiovisual, entendida como «la fusión progresiva de los servicios de radiodifusión tradicionales y de Internet»[13]. La divisoria entre servicios de radiodifusión lineal recibida en televisores y servicios a petición prestados por Internet recibidos en ordenadores se difumina. Se espera que de aquí a 2016 la mayoría de hogares de la Unión Europea con televisión estén equipados con un aparato híbrido, que permitirá la recepción de contenidos lineales y de contenidos ofrecidos a través de Internet. También se espera que en el mismo período la mayor parte del volumen de tráfico en Internet de los consumidores sea de vídeo y que la mayor parte de aquel tráfico se canalice principalmente a través de dispositivos móviles.

2. Los menores y el uso de la Red

Los menores no son ajenos a este escenario de uso de la Red y de impacto de las TIC. A los efectos de este Informe, y siguiendo el criterio de la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989, ratificada por España, se consideran menores los de edad inferior a 18 años, aunque los análisis estadísticos disponibles utilizan rangos de edad variables, lo que supone una dificultad para la comparación y el diagnóstico.

Es un lugar común atribuir a los menores la condición de «nativos digitales», pero el significado de esta expresión debe aclararse.

Lo son en el sentido más directo que se deduce de la literalidad de la expresión. Como ponía de manifiesto un estudio de INTECO de 2009[14], mientras los adultos utilizan Internet para algo, con una finalidad concreta, para los niños Internet es una realidad vital, simplemente están y viven en ella, y por eso su perspectiva es —como señaló Héctor Sánchez ante la Ponencia— la de estar siempre conectados («always on»). En este sentido, es preciso arrumbar una falsa creencia propia del mundo de los adultos, la de la existencia de un mundo virtual diferente del real. Sólo hay una realidad, de la que el mundo digital forma parte, y los menores viven esta afirmación con naturalidad.

---

[13] Comisión Europea, «Libro verde …», documento citado, p. 3.

[14] INTECO. «Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres», 2009, p. 46. Disponible en: http://www.inteco.es/guias_estudios/Estudios/Estudio_ninos

De lo anterior se desprende un segundo sentido de la expresión de nativos digitales. Los menores son usuarios intensivos de las nuevas tecnologías, variando esta intensidad según la franja de edad.

Así lo reflejan los datos ya manejados más arriba en relación con la franja de edad entre 16 y 24 años.

Por su ámbito (25 países europeos) y vinculación al programa de la Comisión Europea «Internet más segura» («Safer Internet Programme»), tiene interés reproducir a continuación algunos de los resultados de la última encuesta realizada en el marco del proyecto EU Kids Online (II fase de este proyecto) entre menores europeos de 9 a 16 años[15]. Tales resultados, aunque obtenidos en 2010 y presentados en 2011, apuntan tendencias que en conjunto mantendrían su validez.

a) Edad de inicio y frecuencia de uso de Internet

Tanto en España como a nivel europeo la tendencia es el descenso en la edad de inicio del uso de Internet. En concreto, la edad media de conexión por primera vez a Internet de los menores españoles se situaba entonces en la misma media europea (esto es, 9 años, dato complementado con la manifestación del grupo más joven —9-10 años— de haberse iniciado en la conexión a Internet con 7 años, mientras que los de 15-16 años dijeron hacerlo con 11 años).

En la frecuencia de uso de Internet los menores españoles se situaba ligeramente por debajo de la media europea. Así, un 58% manifestaba usar Internet todos o casi todos los días (60% en el conjunto de Europa) y un 34% utilizarlo una o dos veces por semana (33% en Europa), porcentajes que sumados arrojaban un alto porcentaje (92%) de menores usuarios frecuentes de Internet.

Las diferencias según segmentos de edad eran marcadas. Mientras que en el grupo más joven (9-10), un tercio (33%) accedía a Internet diariamente, entre los mayores (15-16 años), el acceso diario alcanzaba el 82%, diferencia muy similar a la existente a nivel europeo (33% y 80%, respectivamente, de media).

[15] Vid. cita 4.

El estudio también midió el tiempo diario de uso de Internet, aun reconociendo la dificultad de tal medición debido, entre otros factores, al hecho de que los menores simultanean diferentes actividades («multitarea»), sin desconectarse del todo de Internet, considerado lo cual, el tiempo medio de uso diario de Internet de los menores españoles era de 71 minutos (por debajo de la media europea, 88 minutos), apreciándose una diferencia importante según los rangos de edad (45 minutos en el de 9-10 años frente a 97 minutos en el de 15-16 años, que en la media europea eran 58 y 118, respectivamente).

En conclusión, el uso de Internet presentaba ya en 2010 un alto grado de presencia en la vida diaria de los menores españoles y europeos.

b) Lugar de conexión

El hogar era el principal lugar donde los menores usaban Internet (84% de los menores españoles, cifra muy cercana a la media europea, un 87%) seguido de la escuela (70% de los menores españoles, cifra superior a la media europea, 63%).

Situados en el escenario del hogar, los porcentajes respectivos de menores españoles que utilizaban Internet en su propia habitación y los que lo hacían en cualquier otra habitación de la casa eran los mismos (42%, lo que reflejaba una diferenciación con la media europea, en la que dichos porcentajes eran de media 49% y 38%, respectivamente).

La edad constituía también un nítido factor de diferenciación, en el sentido de que el uso «privado», en la propia habitación, se producía con más frecuencia entre los adolescentes que entre los de menor edad.

Si hasta hace poco el acceso a Internet se limitaba a los ordenadores de sobremesa, y ello explicaba el consejo generalizado a los padres de situar el ordenador en un lugar común del hogar, con la irrupción de los dispositivos móviles, el lugar y los medios de acceso a Internet se han visto modificados.

c) Actividades online

Las actividades principales para las que usaban Internet los menores eran: para tareas escolares (83% España, 85% Europa), juegos (por

ejemplo videojuegos contra el ordenador, 80% España, 83% Europa), ver videoclips (78% España, 76% Europa), y comunicarse (a través de mensajería instantánea, redes sociales o correo electrónico, con porcentajes de 68%, 59% y 62% respectivamente; porcentajes ligeramente diferentes en Europa, con 62%, 62% y 61%, respectivamente, de media). También realizaban otras actividades que tienen que ver con la creación de contenidos en porcentajes inferiores y variables.

Se ha señalado que los datos en este punto apoyarían la idea de la «escalera de oportunidades», según la cual ciertas actividades básicas tienden a hacerse primero y por más niños, mientras que las más creativas y participativas vienen más tarde y son realizadas por menos jóvenes.

En todo caso, la participación en redes sociales es considerada la de más rápido crecimiento entre las actividades «online» de los jóvenes.

El 56% de los menores españoles encuestados afirmaba tener un perfil propio en una red social (59%, de media en Europa). La variable de la edad era de nuevo un factor diferenciador en un abanico entre el 11% y el 42% en los segmentos de 9-10 años y 11-12 años, respectivamente, y entre el 74% y 89% de presencia en las redes en la franja superior, de 13-14 años y 15-16 años, respectivamente.

Los anteriores datos, considerado el umbral legal existente en España para prestar consentimiento para ceder datos personales y, por tanto, para tener un perfil en una red social (14 años), permiten pensar que esta restricción de edad no se cumple.

Los datos hasta aquí mencionados, en cuanto reflejo de tendencias a nivel europeo y de otros países (acceso a Internet a edades cada vez más tempranas; uso progresivamente intensivo según edad; hogar y escuela como entornos principales de conexión «online»; pluralidad de actividades «online», con presencia destacada de las comunicativas e irrupción de las redes sociales) seguramente mantengan su validez significativa.

Hay, sin embargo, un factor, referido a los dispositivos utilizados para conectarse «online», en particular el uso de dispositivos móviles, que probablemente convierte en desfasados los datos del estudio manejado.

En efecto, en dicho estudio, mientras los porcentajes entre menores españoles de acceso a Internet a través de un PC eran cercanos a la media europea (59% a través de un PC compartido, 30% a través de

un PC personal, frente a porcentajes del 58% y 35%, respectivamente, de media en Europa), el uso de dispositivos móviles por los menores españoles para acceso a Internet era entonces (2010) sustancialmente inferior al resto de países de Europa, aunque en un nivel más similar a los países del sur y algunos del este de Europa (9% uso de teléfono móvil u otro dispositivo portátil, frente a un 34% de uso de tales dispositivos, de media en Europa).

La difusión del teléfono móvil y en particular de «smartphones», particularmente intenso en España en los últimos tiempos, pone en cuestión la vigencia de esas cifras.

Según datos del INE referidos a 2013[16], el 91,8% de la población infantil entre 10 y 15 años usa Internet, y el 63% dispone de teléfono móvil (en una escala creciente que va del 26,1% entre los niños de 10 años, al 90,2% entre los adolescentes de 15 años). Y aunque la encuesta se refiere a la disposición de teléfono móvil, el dato de ventas de «smartphones» (8 de cada 10 móviles) sugiere una presencia destacada de los mismos como vía de acceso a Internet entre los menores. En palabras de Jesús Guijarro ante la Ponencia, el escenario actual aparece definido por un acceso a edades cada vez más tempranas a dispositivos móviles que convergen en cuanto a prestaciones con pequeños ordenadores personales. Estos dispositivos proporcionan a los padres una sensación de seguridad y control sobre los hijos, y a éstos de libertad y autonomía.

Si dos de los sentidos de la expresión «nativos digitales» parecen incuestionables (Internet como realidad natural para el menor y conexión «online» intensiva), hay un tercer sentido que constituiría un mito, no sustentado en evidencias empíricas. Es el que se refiere a las competencias digitales. En afirmación plausible de Jorge Flores ante la Ponencia, los menores no son usuarios avanzados, son intensivos y a veces compulsivos. En la misma línea, se ha afirmado que hablar de nativos digitales obscurece la necesidad de prestar apoyo a los niños en el desarrollo de sus habilidades digitales.

En la encuesta antes considerada se preguntaba a menores entre 11 y 16 años acerca de determinadas competencias digitales, centradas en capacidades de examen crítico y de seguridad.

---

[16] INE, encuesta citada.

La mayoría de los consultados en España afirmaron saber marcar una página web entre favoritos (76%), bloquear mensajes de alguien con quien no se quiere contactar (70%), encontrar información de cómo usar Internet de forma segura (63%) o comparar diferentes webs para contrastar información (61%), porcentajes algo mayores que los correspondientes de media europea (64%, 64%, 63% y 56%), respectivamente.

En cambio, en torno a la mitad o menos afirmaron saber cambiar los parámetros de privacidad del perfil de una red social (55%), borrar el historial de páginas visitadas (45%), bloquear anuncios o spam indeseados (52%) o cambiar las preferencias de los filtros de contenido (27%) (porcentajes similares a los de media en Europa).

Las diferencias según edad son relevantes. Los adolescentes (13-16 años) afirman tener más habilidades que los más jóvenes (11-12 años).

Adicionalmente la población comprendida entre 9 y 16 años fue preguntada acerca del nivel de su conocimiento en relación con el que consideraban que tenían sus padres. Cerca de la mitad, un 47%, afirmó ser «muy cierta» la afirmación de saber más que sus padres (superior al de media europea, un 36%). Las diferencias de edad son en este punto muy marcadas, mostrándose el menor más de acuerdo con aquella afirmación a medida que aumenta la edad.

Otro dato relevante es el uso de los parámetros de privacidad en las redes sociales.

Entre los menores usuarios de redes sociales en España, manifestaron mantener un perfil privado (accesible sólo a los amigos), parcialmente privado (pueden verlo amigos de amigos y redes) o público (accesible a cualquiera), un 67%, 17% y 14% respectivamente (porcentajes superiores a los de media europea, 43%, 28% y 26% respectivamente). Aunque se ha apuntado que estos datos reflejarían un mayor nivel de concienciación de los menores españoles, quizás se expliquen por la prevalencia, entre las redes en las que participan aquéllos, de la red española Tuenti, en la que el perfil privado está configurado por defecto.

Datos complementarios son el relativamente bajo porcentaje de menores que muestran su dirección o número de teléfono (9% en España, 14% de media en Europa), aunque sea común colgar algún tipo de in-

formación que pueda identificarlos dentro de su perfil (en España, una media de 2,4 datos —entre un total de seis, por los que se les preguntó, foto, apellido, dirección, teléfono, colegio, edad correcta—, ligeramente por debajo de la media europea, 2,8), y el relativamente alto porcentaje de menores españoles que han declarado una edad incorrecta en su perfil, el más alto de los países de la Unión (un 27%, frente al 16% de media en Europa), probablemente como consecuencia de una mayor restricción en cuanto a la edad para tener un perfil en las redes en España.

III. *Riesgos existentes en el uso de la red por los menores*

1. Oportunidades y riesgos. Tipología de riesgos

Incontrovertido, y como tal lo han subrayado todos los comparecientes ante la Ponencia, es el hecho de que en el uso de la Red concurren oportunidades y riesgos. Es más, para ser exactos, unas y otros son *a priori* sólo posibilidades, de las que pueden derivar beneficios o perjuicios, respectivamente, dependiendo de muy variadas circunstancias, bien referidas a la naturaleza misma de ciertas situaciones (pues si algunas, por ejemplo el acoso, se perfilan claramente como factores de riesgo, otras, por ejemplo la visita de páginas que alojan vídeos, presentan una naturaleza ambigua, pudiendo representar oportunidades o riesgos), bien a factores externos: factores individuales (edad, género, factores psicológicos), entorno social más cercano (padres, escuela, amigos) y entorno social amplio (factores económicos, sociales y culturales).

Además, las relaciones entre oportunidades y riesgos son complejas, porque van de la mano, lo que quiere decir que, como en otras facetas de la vida, la asunción de un cierto grado de riesgo es inevitable para alcanzar las oportunidades, y el reto consiste en encontrar el equilibrio adecuado, sin que un énfasis excesivo en las oportunidades, sin medidas de protección, incremente las posibilidades de riesgo, ni un énfasis excesivo en estas medidas ahogue aquéllas.

En este contexto los menores presentan necesidades específicas, que vienen reclamando una creciente atención, tanto desde la perspectiva de las oportunidades como desde la perspectiva de los riesgos, enfoque que está presente a nivel europeo tanto en la «Agenda Digital para Europa»

como en la «Estrategia europea en favor de una Internet más adecuada para los niños»[17].

Los menores reclaman en efecto necesidades especiales en relación con el juego, la formación y el conocimiento, la creatividad, la comunicación y la participación, acorde con su edad, en tareas de grupo o comunitarias. Y desde este punto de vista las tecnologías de la información y comunicación ofrecen enormes oportunidades, como destacaron todos los comparecientes en la Ponencia.

Así, Alfonso González se refirió a Internet como «la gran ciudad del siglo XXI», una ciudad basada en el uso intensivo de las tecnologías de la información y comunicación, global, abierta y en cambio permanente, constituyendo el reto el de integrar la escuela (en sí misma «la tecnología más potente que ha desarrollado la humanidad para alcanzar cotas más altas de justicia y prosperidad»), con las posibilidades de aprendizaje que ofrecen las nuevas tecnologías, puestas así al servicio tanto de los niños (en condiciones de igualdad, para que nadie quede al margen de la adquisición de las competencias básicas digitales, e integrando a quienes tienen inteligencias distintas, a veces las más creativas) como de los profesores («el gran descubrimiento de la transformación educativa»), para los que, como señaló Ana María Román, aquéllas constituyen un recurso clave en la dirección de la mejora de la calidad educativa, al permitir fomentar una cultura colaborativa y abierta en el entorno escolar, facilitar la educación personalizada y, en general, apoyar la tarea de mediación en la transmisión del conocimiento y en el interés por el mismo.

Salomé Adroher, Francisco Javier Martos y Liliana Orjuela subrayaron la doble perspectiva (oportunidades y riesgos) en el marco de la Convención de las Naciones Unidas sobre los Derechos del Niño.

Dolors Reig, por su parte, enfatizó la virtualidad de las tecnologías de la información y la comunicación (TIC) como tecnologías de empoderamiento y participación (TEP), en la medida en que estarían propiciando determinados cambios en las capacidades intelectivas y relacionales, de carácter positivo, como el desarrollo de la inteligencia fluida (frente a la cristalizada), la diversidad, y las actividades colaborativas y participativas.

---

[17] «Una Agenda Digital para Europa». COM(2010) 245 final y «Estrategia europea en favor de una Internet más adecuada para los niños». COM(2012) 196 final.

Los menores constituyen un grupo con especiales necesidades en el mundo digital también desde el punto de vista de los riesgos. Además de encontrarse en proceso de formación, sus propias características de desarrollo físico y psicológico les hace particularmente vulnerables. Como recordó ante la Ponencia Mariano Chóliz refiriéndose a los adolescentes, en ellos no están desarrolladas las áreas del córtex prefrontal responsables del control del comportamiento, la planificación y la valoración de las consecuencias de sus actos, mostrándose proclives a reacciones afectivas extremas, entre la excitación y el aburrimiento, el placer y la frustración, y a la impulsividad.

Los estudios realizados en el marco del proyecto ya mencionado EU Kids Online han extendido una tipología de riesgos que distingue entre riesgos de contenidos (en los que el papel del menor es de receptor), riesgos de contacto (en los que el niño tiene de algún modo un papel activo, aunque sea involuntario, en una actividad en la que interviene un adulto) y riesgos de conducta (en los que el niño es autor o víctima de una conducta dada en una relación entre iguales).

Más allá de la utilidad académica de esta clasificación, a los efectos de este informe y considerada la nutrida información aportada por todos los comparecientes en la Ponencia, emerge una división primaria que permitiría distinguir entre riesgos de Internet y riesgos en Internet. Los riesgos de Internet serían riesgos intrínsecos a Internet, no en el sentido de que sean inevitables sino en el de que su existencia es inseparable de la de Internet, mientras que los riesgos en Internet serían aquellos asociados a situaciones que encuentran en este medio un soporte idóneo para producirse, aunque existían y existen también fuera del mismo.

A su vez entre los riesgos de Internet, pueden distinguirse entre, por un lado, aquellos de carácter general que afectan a la forma en que recibimos y aprehendemos la información y a la forma en que nos relacionamos con los demás (cambios cognitivos y relacionales) y al uso mismo de Internet (uso excesivo), y, por otro, aquellos riesgos específicos que tienen que ver con situaciones en las que los sistemas o herramientas informáticos son en sí mismos objeto de conductas maliciosas, que pueden llegar a ser constitutivas de delito y servir o no, a su vez, de medio para la comisión de otros delitos (actos maliciosos que tienen por objeto los sistemas o herramientas informáticos).

Entre los riesgos en Internet cabe distinguir, simplificando la tipología de EU Kids Online, entre riesgos derivados de la circulación de contenidos en Internet (riesgos de contenidos), asociados a comportamientos de particular gravedad (pornografía infantil) o a comportamientos en general nocivos para el menor (exposición a pornografía de adultos o a otros contenidos inapropiados), y riesgos derivados de determinadas conductas en las que el menor tiene una u otra participación, voluntaria o involuntaria (riesgos de contacto), entre los que a su vez puede hacerse una clasificación principal entre aquellos que afectan de uno u otro modo a la integridad física o psíquica del menor («ciberbullying», «cibergrooming», violencia de género digital, juego «online»), los que afectan a la privacidad y a la protección de los datos de carácter personal («sexting», problemas a largo plazo para la imagen, cosificación de la identidad digital, uso malicioso de la información personal) y los asociados a la propiedad intelectual (piratería digital).

Antes de proseguir con el examen individualizado de los riesgos de y en Internet para los menores, importa subrayar la dificultad de tal examen, tanto por razón de que los riesgos son «dinámicos y evolucionan constantemente, empujados por las nuevas posibilidades técnicas que surgen casi a diario»[18], como por la dificultad de sustentar tal examen en términos objetivos generalmente reconocidos.

Las diferencias de percepción y evaluación se advierten entre los propios padres e hijos. En la investigación citada del proyecto EU Kids Online, realizada entre menores europeos de 9 a 16 años, algo más de la mitad (un 55%) de los menores europeos usuarios de Internet manifestaron que hay situaciones en Internet que molestan a los de su propia edad, percepción compatible con la de una vasta mayoría (90%) que consideraba ser algo o muy cierto que hay muchas situaciones de Internet positivas para los menores de su propia edad. Minoritario, aunque no desdeñable, era, a su vez, el porcentaje (uno de cada ocho, 12%), de los menores europeos que afirmaron encontrar en Internet situaciones que les molestaron personalmente (un 14% en España).

Por otra parte, aunque los análisis más antiguos revelaban, en paralelo a la «brecha digital», diferencias relevantes en la percepción entre padres

[18] INTECO. «Estudio sobre hábitos seguros …», 2009, op. cit., p. 71.

e hijos, tales diferencias tenderían a reducirse. El estudio citado mostraba un 8% de padres que pensaban que sus hijos habían sido molestados por alguna situación «online», en contraste con el porcentaje del 12% de los menores que afirmaron haber encontrado situaciones que les molestaron, lo que reflejaba una cierta proclividad de los padres a subestimar las experiencias de daño de sus hijos.

Más allá de la percepción sobre los riesgos de los usuarios de Internet, entre ellos los menores y sus padres, es posible destacar, en términos objetivos, dos géneros de amenazas o riesgos, por la preocupación que suscitan a nivel global, reflejada en los análisis de la Unión Europea.

Por un lado aquellos que, intrínsecos a Internet o valiéndose de este medio como plataforma, forman parte del fenómeno de la ciberdelincuencia, un fenómeno que, a tenor de lo afirmado en la Estrategia de Ciberseguridad de la Unión Europea, «es una de las formas de delincuencia de crecimiento más rápido, con más de un millón de víctimas diarias en todo el mundo»[19] y que genera grandes beneficios. Según informó Ignacio Cosidó a la Ponencia, el cibercrimen es «actualmente el delito más lucrativo a nivel mundial después de la prostitución y el tráfico de drogas».

Este género de delincuencia presenta (como señalaron a la Ponencia I. Cosidó, Manuel Escalante, Elvira Tejada y Óscar de la Cruz) determinadas características, a saber: desde el lado de los autores, el constituir una actividad de bajo riesgo, hasta el punto de haberse profesionalizado y haber generado un modelo de negocio basado en «plataformas multicrimen», el uso de medios técnicos sofisticados que facilitan el anonimato, y la dificultad para luchar contra el mismo, derivada de la dimensión global de internet (víctima y autor del delito pueden estar en países diferentes separados por miles de kilómetros) y la inadaptación de los ordenamientos penales y procesales (Óscar de la Cruz: la ciberdelincuencia «es una de las amenazas más asimétricas que hay hoy día»); y, desde el lado de las víctimas, el tratarse de una amenaza que puede afectar a la generalidad de la población y sobre todo la vulnerabilidad en la que los usuarios de la Red se encuentran, en función de la ausencia de cultura de seguridad y la amplificación que Internet supone de las consecuencias del delito.

[19] «Estrategia de ciberseguridad de la Unión Europea». JOIN(2013) 1 final, p. 10.

El segundo fenómeno de riesgo que acapara buena parte de la atención y preocupación, con incidencia en toda la población, es el que planea sobre la intimidad y los datos personales. José Luis Rodríguez destacó que la combinación de las memorias digitales (que permiten conservar todo tipo de informaciones a un coste reducido), de Internet (que permite conectar todas esas memorias con independencia de la ubicación geográfica y transmitir y compartir la información en tiempo real) y de los motores de búsqueda (que permiten recopilar y proporcionar acceso a la información con extraordinaria capacidad) ha derrumbado las dos barreras, espacio y tiempo, que hasta ahora habían sido muy eficaces en la protección de la privacidad.

A este escenario tecnológico se añade la característica autocomposición de intereses que gobierna Internet, ámbito sin regulación, salvo en determinadas cuestiones técnicas, del que ha quedado en lo fundamental orillado el ordenamiento jurídico, centrado en los medios de comunicación tradicionales, y en el que, como recordó Eugenio Fontán, la gratuidad añade un factor de riesgo adicional, al poder servir de excusa al prestador de servicios «online» para no ofrecer unos parámetros de calidad.

En este contexto, la protección de los datos de carácter personal, transmutada en el mundo digital como protección de la identidad digital, se convierte en un reto fundamental, como destacaron de modo particular José Luis Rodríguez (la protección de los datos de carácter personal es un derecho fundamental, conectado con otros, pero con propia autonomía, reconocido en la Carta de Derechos Fundamentales de la Unión Europea, y cuyo respeto debe asegurarse), Eugenio Fontán («Europa debe pugnar por proteger nuestro derecho a poseer los datos que nos conciernen»; «para lograr una sociedad justa en la era de los datos, debemos alcanzar un nuevo acuerdo sobre datos, cuya clave es tratar los datos personales como un activo, sobre el que los individuos tienen derecho de propiedad» —citando a Alex Pentland—), o Antoni Gutiérrez y José Luis Casal (al subrayar la importancia del aprendizaje sobre el valor de la identidad digital).

Las encuestas a nivel europeo y español muestran una percepción extendida del público de desinformación y desconfianza en relación con los datos personales suministrados en la Red.

Según el Eurobárometro especial 390, «Cybersecurity», a un 40% de los usuarios les inquieta el riesgo que pueden correr sus datos personales en línea.

En el barómetro del CIS del mes de mayo de 2013, en el que se incluyeron preguntas relacionadas con la protección de datos personales, son significativos algunos datos: un 66% manifiesta que la seguridad de Internet en torno a la protección de datos personales es baja o muy baja; un 70,3% afirma estar poco o nada de acuerdo con que las políticas de privacidad y de información que se ofrecen en los sitios de Internet sobre el tratamiento de datos son claras y sencillas de entender (aunque al propio tiempo, un 13,8% afirma leer siempre o casi siempre las políticas de privacidad de las páginas que visita); un 65,5% señala estar muy de acuerdo o bastante de acuerdo con que los sitios web intentan que no sepamos qué van a hacer con nuestros datos personales o un 76,5% indica estar bastante o muy de acuerdo con que las políticas de privacidad que publican lo sitios web buscan evitar problemas legales más que informar correctamente; el 74,6% muestra estar poco o nada de acuerdo con que las redes sociales cuidan de la seguridad de los datos personales de sus usuarios; un 69,2% afirma estar bastante o muy de acuerdo con que es difícil controlar quien ve la información que introduzco en mi perfil; un 89,1% señala estar bastante o muy de acuerdo con que las redes sociales no deberían cambiar sus políticas de privacidad sin el consentimiento de los usuarios; un 94,8% afirma estar bastante o muy de acuerdo con que las redes sociales no deberían comunicar datos personales a terceros.

En todo caso, la seguridad y la confianza se revelan como presupuestos necesarios para el efectivo desarrollo de la sociedad de la información, y así, figuran como eje estratégico en dos iniciativas de la Unión Europea, complementarias desde tal perspectiva: la Agenda Digital para Europa, adoptada en agosto de 2010 y revisada en diciembre de 2011 (los europeos no adoptarán una tecnología en la que no confíen; «la era digital no es ni el «Gran hermano» ni el «salvaje oeste cibernético»»[20]; «la Unión Europea debe ser una zona puntera en el mundo en términos de seguridad de las redes y de la información, la seguridad en línea y la protección de la privacidad en línea.»[21]) y la Estrategia de Ciberseguri-

[20] COM(2010) 245 final, p. 18.

[21] «La Agenda Digital para Europa - Motor del crecimiento europeo». COM(2012) 784 final.

dad de la Unión Europea adoptada en febrero de 2013 (que parte, entre otras premisas, de que «los valores esenciales de la Unión Europea lo son tanto en el mundo físico como en el digital» y que plantea entre sus prioridades la de «reducir drásticamente la ciberdelincuencia»[22].)

2. Los cambios cognitivos y relacionales

Un factor intrínseco a las nuevas tecnologías, sobre el que no hay perspectiva temporal de estudio, es el relativo a la forma en que los usuarios obtienen y asimilan la información que el medio digital facilita, factor del que no parece haber duda que ocasionará cambios cognitivos, incluso a nivel físico, de incierto diagnóstico y evaluación, sobre los que llamaron la atención de la Ponencia Guillermo Cánovas, Dolors Reig y Miguel Pérez. El primero ejemplificó estos cambios con algunas referencias, como la presunta capacidad «multitarea» que los propios jóvenes, en los paneles en los que participan, destacan, y que alude al despliegue de diferentes tareas a la vez, la sobrecarga cognitiva que el exceso de información de la Red produciría o el nuevo modo de lectura en «f» que propicia la información «online», cuestiones, éstas y otras, cuyo balance, positivo o negativo, resulta prematuro obtener, pero que en todo caso conducen, a juicio de G. Cánovas, no ya a una brecha digital, ni siquiera generacional, sino evolutiva.

Para D. Reig el acento de los cambios en los procesos cognitivos estaría en el desarrollo de la memoria de trabajo, muy vinculada a la inteligencia fluida y a la imaginación. Por su parte, Miguel Pérez abogó por fomentar actividades alternativas que de algún modo compensen las lagunas que el uso de las nuevas tecnologías pueda generar.

Además de los cambios cognitivos, las nuevas tecnologías estarían originando cambios profundos en la forma en que nos relacionamos con los demás, afectando, como señaló D. Reig, a aquellos niveles de necesidades del ser humano de la conocida pirámide de Maslow que se refieren a la afiliación, al reconocimiento y a la autorrealización.

En este plano, Internet provocaría una especial atracción entre los adolescentes al facilitar las necesidades de información, socialización y ocio de esta etapa de crecimiento. Según el estudio citado del proyecto

[22] JOIN(2013) 1 final, p. 4.

EU Kids Online, un 50% de los menores europeos entre 11-16 años dijeron encontrar más fácil ser ellos mismos en Internet que en una relación cara a cara, porcentaje algo superior al mostrado en España (40%).

Una de las preocupaciones mayores relativa a la seguridad de los menores en Internet se refiere a los contactos que mantienen a través de este medio, dada la ausencia de señales de advertencia de tiempo, lugar y contexto que caracteriza Internet, en contraste con el mundo físico.

A este respecto el mismo estudio citado reveló que la gran mayoría de los menores europeos entre 11 y 16 años (87%, que en España fue del 94%) afirmó estar en contacto «online» con personas ya conocidas del mundo exterior (lo que mostraría que la comunicación a través de Internet complementaría la entablada en los círculos sociales preexistentes), si bien un porcentaje minoritario pero significativo (39%, igual en España) señaló comunicarse con personas que conocieron en Internet pero con conexión con familiares o amigos del mundo exterior, y una proporción menor (25%; en España 19%) manifestaron estar en contacto a través de Internet con personas con las que no tenían conexión en su círculo social preexistente.

A su vez, considerado el espectro mayor de edades analizado por el mismo estudio (entre 9 y 16 años), el 30% de menores europeos (21% en el caso de España) señaló haber tenido contactos en Internet con alguien no conocido en una relación preexistente, y el 9% (idéntica proporción en España) manifestó haber acudido a una cita con alguien que conocieron en Internet, si bien dentro de este último porcentaje la mayoría (un 57%, 67% en España) afirmó que la persona con la que se reunió formaba parte de su círculo social —amigo o pariente de alguien conocido en persona—. También entre el 9% de menores que manifestó haber tenido algún encuentro con alguien que conoció por medio de Internet, el 11% (17% en España) afirmaron sentirse molestos por lo sucedido, porcentajes que, aun reducidos en relación con el total de menores encuestados, son los que más preocupación pueden generar.

Por último se habría observado que, considerados los menores que mantuvieron algún encuentro con contactos «online», el 61% de los padres (70% en España), no fueron conscientes de este suceso.

El análisis en torno a los contactos con desconocidos a través de Internet revela una característica de este entorno que constituye un factor

de riesgo en sí misma, que es la relativa a la descontextualización de las situaciones y relaciones, sobre la que llamaron la atención de la Ponencia algunos comparecientes (Consuelo Madrigal, Antoni Gutiérrez o Dolors Reig). La descontextualización no sólo tiene trascendencia en relación con aquellos posibles contactos, al dificultar la obtención de una imagen cabal de los demás usuarios con los que los menores interactúan, al no permitir la mediación de la pantalla contar con los signos de advertencia que en el mundo físico previenen de ciertos riesgos, sino también en relación con la imagen del menor que el entorno digital difunde en el espacio y perpetúa en el tiempo, al ser una imagen necesariamente distorsionada. La existencia de un largo historial de información vertido en Internet por los menores, desconectado de las circunstancias concretas en que tal información se ofreció en cada momento, puede tener involuntarias consecuencias negativas a largo plazo.

La descontextualización afecta en suma a la forma de relacionarnos con los demás, al igual que la influencia que las nuevas tecnologías tiene sobre ciertos sesgos del comportamiento humano, como la polarización, sobre el que tendrían un efecto multiplicador.

A este respecto algunos de los comparecientes se refirieron a la importancia de educar en el valor del silencio (Javier Urra) o de la desconexión (Dolors Reig), y en las reglas básicas de comunicación en el entorno de la Red, en lo que constituiría, en palabras de Consuelo Madrigal, una «semiología virtual».

3. El uso excesivo de Internet

Un factor de riesgo intrínseco a Internet de creciente preocupación, en su incidencia sobre los menores, es el uso excesivo. Se va abriendo paso la opinión de que el uso excesivo puede provocar un trastorno adictivo y así lo mantuvo en particular ante la Ponencia el profesor Mariano Chóliz (aunque la mención a las tecnoadicciones estuvo también presente en otros comparecientes —Salomé Adroher, Juan María Martínez, Luis Carbonel, Antoni Gutiérrez, Guillermo Cánovas, Jorge Flores o Dolors Reig—). Se habla a este respecto de «conducta adictiva a Internet» (CAI), definida por una investigación realizada entre 2011 y 2012, con entrevistas a adolescentes entre 14-17 años de siete países europeos, entre ellos España, como «un patrón de comportamiento caracterizado por

la pérdida de control sobre el uso de Internet»[23]. La misma investigación distingue entre la conducta adictiva a Internet (CAI) y la situación de riesgo de dicha conducta, englobando ambas bajo la expresión «conducta disfuncional en Internet (CDI)».

Mariano Chóliz indicó como manifestaciones de la pérdida de control que supondría la conducta adictiva, aplicables a este tipo adictivo, la tolerancia (necesidad de consumir cada vez más), la abstinencia (malestar cuando se lleva un tiempo sin consumo), el consumo a pesar de saber el perjuicio, la incapacidad para dejar el consumo a pesar de desearlo, el empleo de excesivo tiempo en actividades relacionadas con el consumo y el abandono o descuido de otras actividades.

Entre los países objeto de estudio, España presenta la mayor prevalencia de conducta disfuncional en Internet, si bien la ratio mayor dentro de dicha conducta corresponde a la situación de riesgo —21,3%— y no a la CAI propiamente dicha, situada en el 1,5% (la media de los países estudiados fue de 12,7% y 1,2%, respectivamente).

El mismo estudio revela una mayor proclividad a este trastorno entre los chicos, los adolescentes mayores y aquellos de padres con menor nivel educativo, y una mayor asociación a dicho trastorno de ciertas actividades, como los juegos de azar con apuestas «online» (que triplican el riesgo de CDI), el uso de las redes sociales (el uso de estas redes durante más de dos horas al día o tener más de 500 «amigos» «online» se vincula con la CDI) y los juegos de ordenador (jugar más de 2,6 horas/día se vincula a CDI).

Como señaló Dolors Reig la adicción lo es no tanto a Internet como tal cuanto a determinadas actividades que se realizan a través de este medio.

Este factor de riesgo mostraría una relación curvilínea entre el uso de Internet y el beneficio, de modo que un mayor uso es beneficioso hasta un punto, a partir del cual podría tornarse problemático.

Juan María Martínez citó ante la Ponencia las recomendaciones hechas públicas en octubre de 2013 por la Asociación Americana de Pediatría para fomentar un uso saludable de las herramientas digitales por los

[23] «Investigación sobre conductas adictivas a Internet entre los adolescentes europeos», vid. cita 4.

menores, entre ellas la necesidad de establecer normas claras sobre dicho uso, para asegurar aspectos como la capacidad de concentración del menor, su adecuada alimentación o el correcto desarrollo de sus ciclos de sueño. En la misma línea, recordó el Sr. Martínez, se habría manifestado el Departamento de Salud del Gobierno británico.

M. Chóliz, a partir de la premisa de que la adolescencia es un período crítico en la prevención de adicciones, explicó ante la Ponencia el desarrollo de un «programa de prevención de las adicciones tecnológicas», adoptado por la Generalidad Valenciana, basado en tres principios básicos: debe aplicarse antes de que aparezca la conducta problemática; debe aplicarse con carácter universal, y por tanto en el ámbito escolar, porque todos los adolescentes utilizan las tecnologías; y debe basarse en la información, sensibilización y pautas de acción.

4. Actos maliciosos que tienen por objeto los sistemas y herramientas informáticos

El uso de la Red puede suponer la exposición al ataque de virus y otros tipos de programas informáticos maliciosos («malware») con finalidades inmediatas de interferencia o intrusión en los sistemas o herramientas informáticos, y finalidad última diversa: funcionamiento difícil del equipo o incluso pérdida de información; obstaculización del acceso legítimo de usuarios a un ordenador o red (denegación de servicio —DoS—); intrusión para tomar el control de un ordenador o un conjunto de ordenadores («botnets» o «redes zombies»), o la activación remota de la «webcam» u obtención de contraseñas.

Por otro lado, están las falsificaciones y fraudes informáticos, en los que la actuación sobre sistemas y herramientas informáticos persigue, respectivamente, la creación de datos falsos que puedan ser considerados y utilizados como auténticos, o la obtención fraudulenta de un beneficio económico y un correlativo perjuicio patrimonial de la víctima.

Los menores, como usuarios de la Red, pueden verse afectados por estas situaciones, siendo, según INTECO[24], los virus, el bloqueo del ordenador, o la pérdida de información más frecuentes, y muy reducidas, las tasas declaradas de fraudes (entre los menores europeos de 11 a 16

[24] INTECO. «Estudio sobre hábitos seguros...», op. cit., p. 81.

años encuestados dentro del proyecto citado de EU Kids Online, sólo un 1% manifestó haber perdido dinero por ser estafado en Internet).

Desde el punto de vista normativo, España ratificó en 2010 (en concreto el 20 de mayo, Boletín Oficial del Estado número 226, de 17 de septiembre), el Convenio sobre la ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, promovido por el Consejo de Europa, que contempla en su tipología de la «ciberdelincuencia» dos categorías en las que se encuadrarían muchas de las situaciones referidas: los «delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos», referidos a las situaciones de intrusión, interceptación e interferencia de o en sistemas y datos informáticos, y los «delitos informáticos», que comprenden las falsificaciones y fraudes informáticos.

5. Pornografía infantil

Los abusos sexuales y la explotación sexual de menores, incluida la pornografía infantil, constituyen graves manifestaciones de violencia contra los niños que concitan un repudio universal, reflejado en diferentes instrumentos internacionales como la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989, cuyo artículo 34 obliga a los Estados parte a proteger al niño contra todas las formas de explotación y abusos sexuales, el Protocolo facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño de 2000 relativo a la venta de menores, la prostitución infantil y la utilización de los menores en la pornografía, el Convenio del Consejo de Europa sobre la ciberdelincuencia de 2001 (Convenio de Budapest) y el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual de 2007 (Convenio de Lanzarote), todos ellos ratificados por España.

En línea con tales instrumentos la Unión Europea aprobó en 2011 la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil (Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, que sustituye a la Decisión Marco 2004/68/JAI del Consejo), que constituye un notable impulso para la adaptación del Derecho penal y procesal de los Estados miembros de forma que contemplen la incidencia de las TIC en la comisión de los delitos relativos al abuso y explotación sexual de

menores, y se articulen instrumentos eficaces y consistentes en la lucha contra los mismos. El plazo fijado por la Directiva para su incorporación al Derecho nacional de los Estados miembros finalizó el 18 de diciembre de 2013.

Por lo que se refiere en concreto a la pornografía infantil, su gravedad deriva tanto del tipo de imágenes que comprende, con frecuencia representaciones de delitos reales (imágenes de abusos sexuales a menores efectuados por adultos, incluso de atroces violaciones, como relató elocuentemente ante la Ponencia Carlos Igual; imágenes de menores participantes en conductas sexuales explícitas, reales o simuladas, o de sus órganos sexuales, con fines sexuales; o incluso imágenes realistas de menores participantes en conductas sexualmente explícitas, o de sus órganos sexuales, aunque no reflejen una realidad sucedida), como de las consecuencias perversas que origina, a las que se refirió C. Igual, tales como distorsiones cognitivas en los consumidores, utilización como medio para acosar y corromper a menores, y creación de un círculo de oferta y demanda de tal forma que a medida que más gente demanda estas imágenes mayor oferta se crea, especialmente en determinados países donde los niños están más desfavorecidos socialmente.

Aunque el término de «pornografía infantil» es de uso común, las organizaciones que trabajan en la protección de menores señalan (y así lo hizo ante la Ponencia Liliana Orjuela) su preferencia por la expresión «imágenes de abuso sexual infantil», porque describe mejor la situación de vulneración de derechos, evita toda comparación con las imágenes de la pornografía para adultos y niega a los pedófilos cualquier margen en el fomento y legitimación de sus actividades delictivas. En este mismo sentido se pronuncia el informe sobre «Seguridad en línea» de la Comisión de Cultura, Medios de Comunicación y Deporte de la Cámara de los Comunes, aprobado en marzo de 2014[25].

Es difícil estimar la magnitud de las imágenes de abuso sexual a menores en Internet debido al anonimato que envuelve esta actividad criminal pero, según UNICEF, el número de imágenes de abuso de menores ronda los millones y el número de niños víctimas se cuenta probablemente en

[25] House of Commons. Culture, Media and Sport Committee. Report «Online safety», 2014, p. 6. Disponible en: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/729/729.pdf

decenas de millares[26]. Una de las prioridades a este respecto de los cuerpos policiales es precisamente (como señalaron Juan Miguel Manzanas y Carlos Igual) la identificación de las víctimas, pues hasta que no se las identifica, el abuso continúa y las víctimas no pueden recibir asistencia.

Según comentó a la Ponencia Óscar de la Cruz, en la actualidad la mayor parte de los intercambios de pornografía infantil se produce en el ámbito de las redes entre pares («peer-to-peer»), que formaría la base de una pirámide en la que su parte más estrecha la constituirían foros cerrados (la Internet oculta), donde se producen los intercambios de contenidos más violentos y graves y donde actúan redes organizadas que mueven dinero.

En España, el artículo 189 del Código Penal tipifica como delito, producir, vender, distribuir, exhibir, ofrecer o facilitar la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad (o incapaces), o su posesión para estos fines, así como poseer para uso propio dicho material. Asimismo, el producir, vender, distribuir, exhibir o facilitar por cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores (o incapaces), se emplease su voz o imagen alterada o modificada. Según informó a la Ponencia Elvira Tejada, asistimos a un incremento de esta tipología delictiva por la incidencia de las tecnologías de la información y la comunicación. Según la Memoria de la Fiscalía General del Estado correspondiente al año 2011, un 12,52% de los procedimientos judiciales incoados en España por conductas asociadas al uso de las TIC tuvieron por objeto delitos de pornografía infantil o en relación con personas discapacitadas y el número de acusaciones presentadas por el Ministerio Fiscal por hechos ilícitos de esta naturaleza fue de 368 en el mismo período anual.

En la actualidad se encuentra en tramitación en las Cortes Generales un Proyecto de Ley Orgánica de modificación del Código Penal, que en esta materia ofrece algunas novedades, que fueron valoradas positivamente por Liliana Orjuela y Elvira Tejada. En concreto, esta última se refirió a la incorporación de una definición de pornografía infantil, tomada de la Directiva 201/93/UE, a su vez basada en la incluida en las

[26] UNICEF. «Child Safety Online. Global Challenges and Strategies», 2011, p. 1. Disponible en: http://www.unicef.es/sites/www.unicef.es/files/Child_Safety_online_-_Global_challenges_and_strategies.pdf

Convenciones de Budapest y de Lanzarote del Consejo de Europa, y la tipificación como delito, siguiendo también la Directiva citada, del acceso en línea a archivos con pornografía infantil, lo que incluye el visionado en «streaming», aunque no haya una descarga efectiva, circunstancia que hasta ahora viene exigiendo la jurisprudencia para que concurra el supuesto de posesión para propio uso.

Un aspecto relevante que atañe en parte a las autoridades encargadas de la aplicación de la Ley, en particular a los jueces y en esta medida afecta al Derecho procesal, pero que concierne también a la responsabilidad de las empresas que operan en Internet, es el relativo a la retirada de imágenes de pornografía infantil o al bloqueo del acceso a las mismas. Se trata de un aspecto crucial en la consecución del objetivo de reducir de forma drástica la circulación de estas imágenes en Internet.

Hay dos principales obstáculos en el logro de este objetivo. Uno está constituido, por un lado, por el principio de general aplicación, de exención de responsabilidad en cuanto a los contenidos, de aquellas empresas prestadoras de servicios en Internet que suelen calificarse de «intermediación»: es el caso de los operadores de redes de telecomunicaciones y proveedores de acceso (en cuanto se limitan a la prestación de un servicio de intermediación consistente en la transmisión de datos por una red de telecomunicaciones o en facilitar el acceso a ésta), de los prestadores de servicios de alojamiento, entre los que se incluirían las redes sociales (en cuanto se limitan al almacenamiento de datos) y de los prestadores de servicios que facilitan enlaces a contenidos o instrumentos de búsqueda (los llamados «motores de búsqueda»). Según la Ley española de servicios de la sociedad de la información y de comercio electrónico (Ley 34/2002, de 11 de julio), que adopta aquel principio, estos dos últimos tipos de prestadores de servicios en Internet no son responsables por la información almacenada o por la información a la que dirijan al usuario, siempre que «no tengan conocimiento efectivo de que la actividad o la información almacenada (a la que remiten) es ilícita», o si lo tienen, «actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos» (o «para suprimir o inutilizar el enlace correspondiente») (artículos 16 y 17 de la Ley 34/2002).

En la práctica «el conocimiento efectivo» que hace responsable al proveedor del servicio dependerá, bien de la correspondiente resolución del órgano competente que ordene la retirada de la información ilícita o

el bloqueo del acceso, por tanto de un impulso exterior, bien de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios, esto es, de la autorregulación.

El otro obstáculo en la consecución del objetivo de reducir la circulación en Internet de pornografía infantil o de limitar el acceso a la misma, lo constituye la dimensión global de Internet, en relación con el principio de territorialidad de las legislaciones nacionales. Es comúnmente el lugar de establecimiento del prestador de servicios, el punto de conexión que determina la Ley aplicable y las autoridades competentes para el control de su cumplimiento, por lo que no son iguales las posibilidades de respuesta de las autoridades de un país en relación con los contenidos alojados en el mismo que en relación con los alojados fuera del mismo[27]. Así sucede también en España, donde la Ley 34/2002, de 11 de julio, parte del mismo principio de conexión (aplicación «a los prestadores de servicios de la sociedad de la información establecidos en España» y a los servicios ofrecidos «a través de un establecimiento permanente situado en España», precisándose que «la utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador» —artículo 2—), lo que condiciona no sólo las posibilidades de respuesta frente a los responsables de los contenidos ilícitos, sino también el alcance del deber de colaboración de los prestadores de servicios de «intermediación», limitado como tal deber a los establecidos en España (artículo 11 de la Ley precitada), dependiendo la que puedan prestar los radicados fuera de España, de los canales de cooperación internacional, y del mayor o menor grado de compromiso del prestador de servicios.

6. Otros riesgos de contenidos

Además de la pornografía infantil y de otros contenidos de carácter delictivo (como por ejemplo la incitación al odio o al terrorismo) existe un amplio abanico de contenidos a los que los menores están expuestos en Internet, que aun siendo lícitos y considerados amparados por la libertad de expresión, resultan nocivos para los menores, en cuanto pueden causarles un perjuicio físico, psíquico o moral (pornografía para adultos,

[27] Vid. «Online Safety», op. cit., p. 12.

páginas pro anorexia o bulimia, páginas de apología de la pedofilia, de apología de la «autolesión» —«self-injuring»— o del suicidio, etc).

Una distinción preliminar se hace necesaria, teniendo en cuenta que en la actualidad cualquiera con un dispositivo conectado a Internet es un editor potencial, entre los contenidos autogenerados y los ofrecidos por un programador o editor como objeto de una actividad comercial. Si los primeros escapan prácticamente a todo control, sobre los segundos, el reto lo constituye la dificultad de trasladar al mundo virtual las restricciones que por razón de edad operan en el mundo exterior para el acceso a contenidos de adultos.

El material pornográfico ilustra probablemente mejor que ningún otro tales dificultades. Las disposiciones administrativas sobre clasificación o venta de dicho tipo material y la generalmente aceptada sanción penal de ciertas conductas (así en España, el Código Penal castiga como delito la venta, difusión, o exhibición de material pornográfico entre menores de edad —o incapaces— «por cualquier medio directo» —artículo 186—) ofrecen un eficaz sistema de restricciones de acceso de los menores a dicho material en el mundo físico.

Tales restricciones se muestran sin embargo de difícil aplicación en Internet.

En primer lugar por la posibilidad de modelos de negocio a través de Internet para el ofrecimiento de contenidos pornográficos que escapan al teórico control que puede ejercerse sobre los servicios «online» que por su similitud con los televisivos caen en el ámbito de aplicación de la legislación sobre comunicación audiovisual.

Así, por ejemplo, los llamados servicios de comunicación audiovisual «a petición» (también llamados «a la carta»), que se diferencian de los servicios televisivos tradicionales «lineales» (basados en un horario de programación) en posibilitar el visionado de programas en el momento elegido por el espectador y a petición propia sobre la base de un catálogo previamente seleccionado por el editor, están comprendidos en el ámbito de aplicación de la legislación comunitaria (Directiva 2010/13/UE, de 10 de marzo de 2010, conocida como Directiva de servicios de comunicación audiovisual) y de las correspondientes legislaciones nacionales (en el caso de España, la Ley 7/2010, de 31 de marzo, general de la comunicación audiovisual). Según el artículo 12 de aquella Directiva, los Estados miembros deben velar porque los

servicios de programación a petición que puedan dañar gravemente el desarrollo físico, mental o moral de los menores «se faciliten únicamente de manera que se garantice que, normalmente, los menores no verán ni escucharán dichos servicios». La Ley española general de comunicación audiovisual dedica un extenso artículo (artículo 7) a la protección del menor y, aunque parte de una declaración general aparentemente aplicable a todos los contenidos audiovisuales, de prohibición de «la emisión de aquellos que puedan perjudicar seriamente el desarrollo físico, mental o moral de los menores, y, en particular, la de aquellos programas que incluyan escenas de pornografía, maltrato, violencia de género o violencia gratuita» (apartado 1), más allá de la efectividad de tal declaración, de la regulación contenida en dicho apartado (centrada en el establecimiento de franjas horarias de protección) se desprende que está concebida para los servicios de comunicación televisiva tradicionales o lineales, existiendo no obstante determinadas referencias explícitas en el artículo citado a los servicios de programas a petición, en particular la contenida en su apartado 5, que prescribe la obligación de los prestadores de tales servicios de «elaborar catálogos separados para aquellos contenidos que puedan perjudicar seriamente el desarrollo físico, mental o moral de los menores» y de establecer «dispositivos, programas o mecanismos eficaces, actualizables y fáciles de utilizar que permitan el control parental a través del bloqueo a los contenidos perjudiciales para los menores». A este respecto, todos los productos audiovisuales ofrecidos por un editor, también los a petición, deben contar con una clasificación por edades, basada en una codificación digital que permita el ejercicio del control parental, homologada por la autoridad audiovisual (apartados 2 y 6 del artículo 7 de la LGCA).

Existen, sin embargo, otros modelos de negocio en Internet, a través de los que se muestran contenidos pornográficos, como es el basado en el modelo de YouTube (por eso, se les suele denominar sitios «Tube») que ofrecen vídeos de pornografía dura gratuita y sin restricciones como escaparate que sirve de acceso a los espectadores a otros servicios pornográficos de pago o de espacio publicitario para otros servicios[28], que escapan a las obligaciones y controles de la legislación del sector de la comunicación audiovisual.

[28] Vid. «Online Safety», op. cit., p. 21.

A este factor se añade otro obstáculo ya señalado en relación con la pornografía infantil, que es el referido a la dimensión global de Internet que, en el caso de los contenidos para adultos y nocivos para menores, tiene consecuencias en un doble aspecto. Por un lado, en el de que ya se trate de servicios de programación a la carta, ya de otros servicios prestados en línea, las posibilidades de actuación de las autoridades nacionales se limitan a los establecidos dentro de sus fronteras, siendo así que los radicados allende las mismas escapan al control nacional (véase en este sentido el ámbito territorial de aplicación de la LGCA, artículo 3). Por otro lado, uno de los mecanismos principales en un sistema de restricción de acceso de los menores a contenidos audiovisuales perjudiciales «online» sería el del etiquetado digital que, basado en metadatos, realizaran los proveedores de contenido y que funcionara con independencia del medio a través del cual se ofreciesen (televisión o Internet), pero que, como señalaron Borja Adsuara o Miguel Errasti, a la vez que destacaron su relevancia como acción de futuro, sólo sería realmente eficaz en una dimensión global, al modo de un «protocolo de Internet para el etiquetado de contenidos» (B. Adsuara).

7. Riesgos de contacto: «ciberbullying», «cibergrooming», violencia de género digital, juego en internet, «sexting», problemas a largo plazo para la imagen, cosificación de la identidad digital, uso malicioso de la información personal y piratería digital

Dentro de los riesgos presentes en Internet, esto es, de aquellos asociados a situaciones que se valen de este medio para producirse pero que se daban y se dan también fuera del mismo, distinguíamos dos grandes categorías, los riesgos de contenidos (a los que nos hemos referido en los dos epígrafes anteriores) y los riesgos de contacto, que son aquellos derivados de determinadas conductas en las que el menor tiene una u otra participación, voluntaria o involuntaria, y que pueden a su vez adscribirse a tres categorías principales, según el bien jurídico afectado.

En la categoría de los riesgos de contacto que afectan a la integridad física o psíquica del menor, uno de los tipos que más preocupación y alarma social ha suscitado es el «ciberbullying», que es una manifestación concreta del genérico ciberacoso cuando se produce entre los menores, referida tal conducta a las amenazas, hostigamiento, humillación

y otro tipo de molestias realizadas por medio de tecnologías telemáticas de comunicación[29].

Tomados en conjunto los menores europeos entre 9 y 16 años que fueron consultados en el marco del citado proyecto EU Kids Online, un 6% manifestó haber sido acosado «online» (4% en España), y un 5% (igual en España) confesó haber perpetrado este tipo de conducta, proporción que aumentaba en relación con los que señalaron ser víctima o autor de esta conducta tanto en Internet como fuera de este medio (19% —16% en España— y 12% —9% en España—, respectivamente). Pero quizás el dato más relevante sea la percepción de los menores en relación con esta situación, siendo, entre los que la sufrieron, la sentida como más perjudicial. También es relativamente alta la proporción de padres, entre aquellos menores que manifestaron haber sido víctimas de «bullying», que no conocían esta situación (56% de media en Europa, 67% en España).

Elvira Tejada llamó la atención de la Ponencia sobre el incremento de las amenazas, coacciones, humillaciones y en general de los actos que suponen un trato degradante de menores a través de las nuevas tecnologías.

Este incremento se atribuye a la relajación de los resortes psicológicos de control social y al velo del anonimato e impunidad que se asocian a Internet, por más que el acoso a través de este medio y fuera de él no están separados, ni hay una migración del patio escolar al «patio virtual», sino que más bien se hallan conectados, formando una especie de vínculo vicioso en el que los autores de estas conductas persiguen a las víctimas a través de medios diferentes y las víctimas encuentran difícil escapar de esta situación.

Las consecuencias, no obstante, no son las mismas, pues Internet amplifica el daño en un doble sentido, como señaló a la Ponencia Manuel Viota, por un lado al borrar la separación de los grupos sociales de pertenencia del menor, que antes existía en el mundo exterior, y, por otro, al «democratizar» el acoso, produciéndose en muchas ocasiones además una victimización secundaria, como es el abandono del centro escolar.

---

[29] Definición tomada de INTECO. «Guía de actuación contra el ciberacoso», 2012. Disponible en: http://www.chaval.es/chavales/sites/default/files/editor/guia_lucha_ciberacoso_menores_osi.pdf

Los medios a través de los cuales tienen lugar las situaciones de acoso son mayoritariamente la mensajería instantánea y las redes sociales, y las acciones concretas, como señaló E. Tejada, muy variadas: mensajes de contenido humillante o degradante, grabaciones de la víctima en situaciones comprometidas o que ofenden a su dignidad que son luego difundidas, suplantación de la identidad de la víctima para atribuirle determinadas expresiones o conductas con la intención de perjudicar sus relaciones con terceros, etc. Estas conductas pueden llegar a tener carácter delictivo, encajando en diferentes tipos penales, según las circunstancias concretas de cada caso, y de hecho así lo está haciendo el Ministerio Fiscal, como explicó E. Tejada: delitos de amenazas o coacciones (artículos 169 a 172 del Código Penal), delitos de descubrimiento o revelación de secretos (artículo 197 del Código Penal), e incluso, en los casos más graves, delitos contra la integridad moral (artículo 173 del Código Penal).

Una manifestación de ciberacoso de particular gravedad es el conocido como «cibergrooming» (también se utiliza, aunque de un modo impreciso en cuanto no contiene una referencia al uso de Internet, la expresión «child grooming»), que puede definirse como «aquellas acciones (a través de Internet) realizadas deliberadamente (por un adulto) para establecer una relación y control emocional sobre un niño o una niña con el fin de preparar el terreno para el abuso sexual del menor»[30].

El «modus operandi» en estas acciones es diverso, pudiendo consistir, como señaló M. Viota, en apropiarse de la cuenta de correo electrónico de un menor, a través de la que accede a su vida digital, y con la que puede obtener el control de más cuentas, o adoptar la identidad de un adolescente y buscar el «enamoramiento» de la víctima.

El «cibergrooming» fue objeto de una tipificación específica mediante una reforma del Código Penal llevada a cabo en 2010, desarrollando en este sentido el Convenio de Lanzarote del Consejo de Europa (artículo 23), y se contiene en el artículo 183 bis de aquel cuerpo legal, que castiga al que «a través de Internet, del teléfono o de cualquier tecnología de la información y de la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento».

---

[30] INTECO. «Guía de actuación…», ibídem, p. 11.

Elvira Tejada informó a la Ponencia, en línea con lo manifestado por la Fiscalía General del Estado en su memoria referida al año 2011, sobre la rígida articulación de este tipo penal, que ha limitado considerablemente las posibilidades de su aplicación, de un lado, por la circunstancia de que el tipo penal contemple únicamente como víctimas a los menores de trece años (lo que se explica por ser esta edad la fijada actualmente en España para prestar el consentimiento sexual), y de otro, por la exigencia de que la propuesta de mantener un encuentro con el niño deba acompañarse de «actos materiales encaminados al acercamiento». Esta exigencia deja fuera de este tipo penal, y ha de reconducirse, en su caso, a otros preceptos penales, el supuesto frecuente de que el autor no pretenda un encuentro físico con el menor, sino un encuentro virtual a los fines de lograr material pornográfico obtenido directamente o bien de inducir al menor a realizar ante la «webcam» actos de contenido sexual.

El proyecto de Ley Orgánica de reforma del Código Penal en curso de tramitación en las Cortes Generales superaría ambas limitaciones, pues, por un lado, al elevar la edad de consentimiento sexual, amplía el ámbito de aplicación del precepto en cuestión, y por otro, se tipifica también la conducta cuando el agresor no pretende el acercamiento físico sino la obtención de material pornográfico.

Por su parte, Consuelo Madrigal llamó la atención sobre el hecho de que el Código Penal, en lo que es la definición de conductas, también se aplica a los menores cuando son ellos los autores de las mismas, aunque las consecuencias son distintas. De ahí que en la reforma de tipos penales como el de abuso sexual, debiera considerarse, cuando se aplican a menores, una disimetría de edad, que a juicio de la Sra. Madrigal, debería ser como mínimo de cinco años.

Además de las situaciones de ciberacoso descritas, algunos comparecientes han manifestado su preocupación por lo que Jorge Flores denominó «violencia de género digital», consecuencia de la cual la condición de menor y mujer puede suponer una doble victimización. Patrones patriarcales y estereotipos de género que parecían estar en retroceso resurgen, favorecidos por los nuevos medios de conectividad, que, como señaló Antoni Gutiérrez, permiten «el uso vigilante, el uso inquisidor, el uso protector, el uso propietario de las relaciones humanas».

Otro de los factores de riesgo de creciente preocupación es el del juego «online», una actividad que en España se halla regulada desde 2011

(Ley 13/2011, de 27 de mayo, de regulación del juego), y que desde entonces muestra una tendencia al alza (en 2012, es la única de las modalidades de juego que sube, estimándose el gasto en la misma en torno a los cinco mil millones de euros, casi duplicando el gasto del año anterior).

El riesgo asociado al juego reside en su potencialidad para convertirse en adicción. El profesor M. Chóliz explicó a la Ponencia que la denominada ludopatía o juego patológico es considerada como un trastorno adictivo, categorizado por la Asociación Americana de psiquiatría como drogodependencia, al haberse encontrado «evidencias consistentes de que el juego activa el sistema cerebral de recompensa de forma similar a como lo hacen las drogas de abuso y de que los síntomas clínicos de los trastornos provocados por el juego son similares a los que provocan las drogas». Desde esta perspectiva, según M. Chóliz, el juego «online» ya es la segunda modalidad de juego en provocar adicción, sólo detrás de las tragaperras. Ello es así porque el juego «online» presenta unas características que estructuralmente lo hacen muy peligroso: accesibilidad (se puede jugar con móviles), inmediatez del premio y aprovechamiento de todos los recursos que ofrecen las nuevas tecnologías (por ejemplo, los «bonos de bienvenida», que funcionan como lo que en psicología se llama «muestra de reforzamiento», estrategia que se utiliza para alentar una conducta reforzándola de antemano).

A diferencia de los juegos tradicionales, propios de adultos, el juego «online» tiene en los adolescentes y jóvenes un preocupante nicho de mercado.

Es cierto que el juego está prohibido para los menores de edad, y que la protección de los mismos está presente en la Ley 13/2011, de 27 de mayo, de regulación del juego, en virtud de la cual y de sus normas de desarrollo, las casas de juego, incluidas las «online», tienen que articular mecanismos de identificación y verificación de la edad, pero a juicio del profesor Chóliz, la identificación debería ser fehaciente y sería preciso, además, profundizar por vía reglamentaria en aquella protección, desde el punto de vista de regular los tipos de juego y la publicidad.

En sentido similar se manifestó Félix Brezo, que identificó como principales grietas del marco regulador puesto en pie por la Ley 13/2011, la existencia de plataformas radicadas fuera de España, que escapan a sus controles, y la incesante publicidad del juego «online» a través de los sitios web de noticias deportivas y, lo que es más llamativo, a través de

la radio, publicidad que puede llegar fácilmente a los menores, porque a menudo incluyen aquellos sitios entre sus páginas de consulta diaria. Según F. Brezo este problema podría afrontarse por vía legislativa en términos similares a como se ha hecho con el tabaco o el alcohol.

Internet ha propiciado el surgimiento de otras modalidades de juego que caen fuera del marco regulador, como los videojuegos con multijugador «online», que según Jorge Flores cumplen una función de redes sociales, ajenas a todo escrutinio y que, por su finalidad lúdica, atraen a pedófilos, ya que por su naturaleza los jugadores y sus padres bajan la guardia, o los videojuegos con micropagos o los nuevos entornos de realidad aumentada, del tipo «Second Life», o juegos sociales en los que el manejo de criptodivisas genera, como alertó ante la Ponencia F. Brezo, intercambios especulativos al margen del control estatal y de la normativa fiscal, y que pueden dar lugar a mercados de servicios o productos ilícitos.

Un segundo grupo de riesgos de contacto tiene que ver con la intimidad y más específicamente con la protección de datos de carácter personal. En páginas anteriores se ha hablado con carácter general sobre el interés creciente que esta última suscita. Ahora se trata de descender a un plano más concreto, el de determinados riesgos que pueden tener una especial incidencia entre los menores.

Si se atiende a los resultados de determinadas encuestas, entre los riesgos a que se exponen los menores considerados más habituales por la población adulta se encuentra la difusión de fotos o vídeos comprometidos. Según el barómetro del CIS del mes de mayo de 2013, es éste, seguido del riesgo de dar demasiada información de sí mismos a desconocidos, los riesgos a que se exponen los menores en Internet destacados por un mayor número de encuestados (39,6% y 22,9% respectivamente), a los que seguirían el ser acosado con el fin de obtener concesiones sexuales —17,1%—, el ciberacoso —6,7%—, el perjuicio futuro derivado de los datos subidos a la red —4,5%— y la suplantación de identidad —2,4%—.

Por «sexting» (término inglés resultante de la combinación de los términos «sex» y «texting») se conoce precisamente la práctica del intercambio de textos o imágenes autogenerados, de contenido sexual; práctica que, aun realizada con frecuencia en el contexto de relaciones privadas, puede tener imprevistas consecuencias negativas por la alta

probabilidad de que tales datos o imágenes desborden el marco de tales relaciones, haciéndose públicas, con el efecto difusor y de perdurabilidad que tiene Internet.

El daño que la publicidad de este tipo de contenidos, aun generado por la propia víctima, puede provocar ha exagerado sin embargo en ocasiones la prevalencia de este tipo de conducta (a tenor de los resultados de la citada encuesta EU Kids Online, entre los menores europeos de 11 a 16 años, un 15% de media manifestaron haber visto o recibido a través de Internet mensajes de contenido sexual, y un 3% habrían enviado o subido tal tipo de mensajes, siendo en particular España uno de los países con menor incidencia declarada de esta práctica, con porcentajes, respectivamente del 9% y del 1%).

El proyecto de reforma del Código Penal en curso de tramitación en las Cortes Generales incluye entre sus novedades la tipificación de aquellas conductas en que, obtenidas imágenes o grabaciones de otra persona, voluntariamente emitidas por ésta en el ámbito personal, son luego difundidas sin su consentimiento, lesionando gravemente su intimidad. Con independencia de la valoración que esta propuesta legislativa merezca, debe examinarse cuidadosamente, como apuntó J. M. Martínez ante la Ponencia, en relación con la específica problemática que el «sexting» plantea cuando tiene lugar entre menores de edad.

Aun sin incurrir en prácticas de intercambio de contenidos autogenerados particularmente problemáticos, el rastro que las personas dejan en Internet de muy diversas formas y con diversos motivos (captura automática o casi automática a través de «cookies» al visitar sitios web, datos facilitados al cumplimentar formularios «online» o al acceder a determinados servicios, información volcada en los perfiles de las redes sociales, en blogs u otras aplicaciones interactivas, etc.) puede entrañar ciertos riesgos de gran calado que cada vez suscitan mayor preocupación y que tienen una especial incidencia entre los menores, por la temprana edad en que empiezan a formar su historial digital y por su vulnerabilidad.

Uno de tales riesgos es el constituido por los problemas a largo plazo para la imagen o reputación propia que puede ocasionar la información personal vertida en Internet, teniendo en cuenta por ejemplo que la selección para un trabajo por una empresa puede basarse en la previa búsqueda de la biografía digital del candidato, y que dicha búsqueda puede sacar a la luz textos, fotografías o vídeos de los que pueda inferirse un

juicio negativo sobre la personalidad de aquél, aun cuando no responda a la realidad por presentarse aquellos datos descontextualizados de las circunstancias concretas en que se crearon.

En relación con este factor de riesgo, cobra gran relevancia el llamado «derecho al olvido», que no es sino una particular proyección en Internet de la facultad de cancelación, que forma parte del núcleo del derecho fundamental a la protección de datos de carácter personal, y que consiste en la facultad de las personas de obtener la supresión de los datos personales que obrasen a disposición de un tercero responsable de su tratamiento.

La efectividad de este derecho se ha visto sin embargo hasta ahora cuestionada no ya por la ubicuidad de la información, personal o no, que circula en Internet, sino en concreto como consecuencia de las dudas que en el ámbito europeo, y derivadamente en España, ha planteado la aplicación a determinadas empresas prestadoras de servicios en Internet, bien por la naturaleza de su actividad, bien por la radicación de su matriz, del marco regulador de protección de datos de carácter personal, constituido, a nivel europeo, por la Directiva 95/46/CE, y, a nivel español, por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal, que recoge de forma exigente los estándares contenidos en aquella Directiva, y el Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de la citada Ley.

Una reciente sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, que resuelve diferentes cuestiones prejudiciales planteadas por la Audiencia Nacional de España, en el marco de un litigio entre Google, por un lado, y la Agencia Española de Protección de Datos y un particular, por otro, en relación con una resolución de dicha Agencia por la que estimó la reclamación de dicho particular y se ordenó a Google la adopción de las medidas necesarias para retirar determinados datos personales de su índice e imposibilitara el acceso futuro a los mismos, contiene manifestaciones de interés. Entre ellas, que las empresas que gestionan motores de búsqueda (cuya actividad consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y por último ponerla a disposición de los internautas según un orden de preferencia determinado), en cuanto dicha actividad se refiera a datos personales, son responsables del tratamiento de dichos datos y, por tanto, dicha ac-

tividad es materialmente incardinable en el marco regulador europeo (y español) de protección de datos de carácter personal, y, asimismo que, aunque la matriz del motor de búsqueda y la actividad de tratamiento de datos estén radicados fuera de la Unión Europea, la existencia en uno de sus Estados miembros de un establecimiento, como, en el caso de autos, uno destinado a una actividad de promoción y venta de espacios publicitarios entre los habitantes de dicho Estado, determina, en la medida en que ambas actividades se hallan indisociablemente ligadas, la aplicación del marco regulador de protección de datos del Estado afectado. Esta doble consideración conduce a que el motor de búsqueda no pueda sustraerse a las obligaciones y garantías establecidas en dicho marco regulador, entre ellas, la de eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona, vínculos a páginas web publicadas por terceros y que contengan información relativa a esta persona, incluso en el supuesto de que esta información no se borre de estas páginas web y aunque la publicación en éstas pueda ser en sí misma lícita.

Esta sentencia tendrá indudablemente eco en los términos que finalmente adopte la propuesta de Reglamento de la Unión Europea relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)[31] (sobre la que ya se ha pronunciado el Parlamento Europeo en «primera lectura» mediante resolución adoptada el 12 de marzo de 2014) que, entre otras novedades, respecto de la Directiva vigente (además de su propia naturaleza como instrumento normativo), incorpora un criterio amplio en cuanto a su ámbito de aplicación territorial, al incluir en el mismo, con independencia de la ubicación principal de la empresa, las actividades de tratamiento de datos que supongan «la oferta de bienes y servicios a ciudadanos de la Unión Europea» o esté relacionada con el «control de su comportamiento», y reconoce de forma expresa el «derecho al olvido», con una explícita mención a su relevancia para los menores (artículo 17 y considerando 53 —«Este derecho es particularmente pertinente si los interesados hubieran dado su consentimiento siendo niños, cuando no se es plenamente consciente de los riesgos que implica el tratamiento y más tarde quisiera suprimir tales datos personales especialmente en Internet»—).

[31] COM(2012) 11 final.

Otro de los riesgos que, aunque desconocido o insuficientemente medido hasta ahora en los análisis de base estadística[32], cobra cada vez mayor atención, es el que en este Informe denominaremos como cosificación de la identidad digital, derivado del cambio de paradigma que Internet ha supuesto para la actividad comercial y publicitaria, que ha convertido los datos de carácter personal en codiciada materia prima para el trazado de perfiles cada vez más precisos al servicio de una publicidad personalizada.

La falta de conciencia suficiente acerca del modelo de negocio de muchos servicios de Internet, entre ellos los de motores de búsqueda o las redes sociales, aparentemente gratuitos, pero que realmente se pagan con información personal, afecta de un modo particular a los menores que, desde muy temprana edad, pueden convertirse, involuntariamente, en objeto de prácticas invasivas de monitorización, perfilado y publicidad conductual, de las que alertaron en la Ponencia distintos comparecientes, entre ellos, Alfonso González (para quien el reto fundamental de integrar la escuela con las posibilidades de aprendizaje que ofrecen las nuevas tecnologías debe hacerse conjurando el peligro de convertir el aprendizaje «en una mercancía de información para los gigantes de la red»), Josep Manuel Prats («Hemos cedido la imagen nuestra y de nuestros hijos sin limitación alguna y sin el derecho al olvido»), o Consuelo Madrigal (que utilizó el contundente símil de «golpe de estado virtual», para referirse a las amenazas que para la libertad suponen las solicitaciones de la industria de lo imaginario, la publicidad y el mercado).

La propuesta de Reglamento de la Unión Europea antes mencionada sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales acoge el derecho de las personas a oponerse al tratamiento de sus datos de carácter personal con fines de mercadotecnia directa, y a no ser objeto de medidas basadas en la elaboración de perfiles por medio de tratamiento automatizado (artículos 19 y 20, y considerandos 57 y 58).

Un tercer tipo de riesgo es el que deriva del uso malicioso que otras personas pueden hacer de la información personal de los menores exis-

[32] Entre las excepciones, puede citarse, como ejemplo, el informe de la OCDE, «The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them», *OECD Digital Economy Papers*, No. 179, 2011, p. 27. Disponible en: http://dx.doi.org/10.1787/5kgcjf71pl28-en

tente en Internet, facilitado tanto por ciertas prácticas confiadas y habituales de éstos (como la de facilitar su contraseña a sus amigos, para que estos puedan acceder a sus cuentas de correo y perfiles en las redes sociales) como de la abundancia de aquella información, que no es sólo de sí mismos sino que se extiende a su grupo familiar y de amistades, y que puede llegar no sólo por iniciativa del propio menor, sino también de otros (a través de la conocida práctica del «etiquetado» de las fotos —«tagging»—) e incluso inadvertidamente como consecuencia de la huella de geolocalización que habitualmente acompaña a las fotos digitales o de la funcionalidad del mismo tipo que incorporan hoy día los «smartphones», y que permiten conocer el paradero del menor o la ruta que sigue.

El uso malicioso puede traducirse en comportamientos delictivos de distinta valoración jurídico-penal, tales como coacciones, delitos contra el honor o delitos contra la integridad moral ya aludidos, o también de descubrimiento y revelación de secretos, si pueden reconducirse a las circunstancias tipificadas en el artículo 197 del Código Penal, o puede, pese a la alarma que genera, no disponer de una tipificación específica, como sucede con la suplantación de identidad.

Refiriéndose a esta última situación, en efecto, Elvira Tejada señaló ante la Ponencia que, salvo que puede atraer la tipificación derivada de otras conductas en atención, por ejemplo, a su contenido infamante o injurioso, la suplantación de la identidad de otra persona en la Red y en general a través de medios electrónicos, carece de tipificación propia, al no encajar en la figura que podría considerarse más próxima de «usurpación de estado civil» (artículo 401 Código Penal), por no reunir los requisitos que exige dicho tipo tal y como vienen siendo interpretados por la jurisprudencia del Tribunal Supremo. Sin embargo, en línea con lo señalado por la Memoria de la Fiscalía General del Estado referida al año 2011, E. Tejada defendió que suplantar la identidad de otro en ciertas condiciones, como hacerlo con carácter de permanencia y de forma que induzca realmente a error, puede implicar un atentado grave contra la privacidad y puede tener una seria incidencia en las relaciones de la víctima con terceros, por lo que merecería una respuesta penal específica. La suplantación puede utilizarse también para perjudicar al menor en sus relaciones con terceros, y puede también tener como objeto acceder a información o datos íntimos del menor, pudiendo proceder tal propósito de un adulto, como antesala de una situación de acoso sexual.

Aludiremos finalmente en este capítulo de los riesgos de contacto, a los que pueden afectar a la propiedad intelectual, derivados de la actividad ilícita de determinados sitios web desde los que se permite a los usuarios bien descargar directamente películas, series, música, o videojuegos o bien la posibilidad de enlazar o compartir enlaces con servidores desde los cuales pueden efectuarse dichas descargas. Los perniciosos efectos de la actividad de estos sitios web se proyectan en varias vertientes, como señalaron ante la Ponencia José Manuel Tourné y Carlota Navarrete.

La vertiente quizás más evidente es la propia infracción de los derechos de autor que tal actividad supone, y lo que es más grave, la erosión de la conciencia colectiva sobre el valor de la propiedad intelectual, no sólo como un bien individual sino en términos de riqueza general y empleo. En este sentido, los datos aportados por Carlota Navarrete, al pasar del uso de la Red por los menores para consumo de contenidos digitales al consumo de adultos en el mercado ilegal de estos contenidos, apuntan una tendencia sobre este consumo preocupante.

Otra vertiente menos conocida es la del negocio mismo, altamente lucrativo, que hay detrás de esta actividad, realizada con infracción de las normas que rigen para el establecimiento de cualquier proveedor de servicios en Internet (en particular las contenidas en el artículo 10 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico) y por tanto ejercida con competencia desleal en relación con el sector legal de contenidos en Internet.

Tampoco son irrelevantes las implicaciones en cuanto a los riesgos colaterales a que se exponen los menores que visitan estos sitios web, como puede ser la exposición a contenidos para adultos (enlaces a contenidos pornográficos, películas de violencia extrema), a publicidad de casas de juego «online» o incluso el riesgo de ser víctimas de estafas.

La materia de la infracción de la propiedad intelectual, en la que desde el campo del ordenamiento penal, y en palabras de la Memoria de la Fiscalía General del Estado referida al año 2011, «no existe sino una jurisprudencia menor muy dispersa y en buena medida contradictoria», se ha visto afectada por la entrada en vigor del Reglamento aprobado por Real Decreto 1889/2011, de 30 de diciembre, que desarrolló la disposición final cuadragésimo tercera de la Ley 2/2011, de Economía Sostenible, que regula el funcionamiento de la Comisión de Propiedad Intelectual,

una de cuyas secciones tiene como función actuar en vía administrativa en los supuestos de «vulneración de los derechos de propiedad intelectual, por el responsable de un servicio de la sociedad de la información, siempre que dicho responsable directa o indirectamente actúe con ánimo de lucro o haya causado o sea susceptible de causar un daño patrimonial al titular de tales derechos».

La relevancia de las redes sociales como plataformas privilegiadas de comunicación de personas y grupos las sitúa en el centro de la atención en relación con el enfoque adoptado por las mismas para afrontar algunos de los factores de riesgo de contacto examinados.

La Ponencia ha podido contar con el testimonio de tres importantes redes sociales, Tuenti, Facebook y Twitter.

Tuenti es una empresa tecnológica española que, según Sebastián Muriel, cuenta con cerca de doscientos empleados de alta cualificación, y un modelo de negocio centrado en las herramientas de comunicación social, cuyo centro de gravedad ha evolucionado del servicio web inicial al «Smartphone». En la actualidad tiene 16 millones de usuarios registrados y entre 5 y 6 millones de usuarios activos en la parte de operador móvil, de los que un 75% son mayores de edad.

En relación con Facebook, Natalia Basterrechea señaló que hay más de 1.200 millones de usuarios activos en esta plataforma, en los que están incluidos aproximadamente 18 millones de España, y que en torno a la mitad se conectan diariamente y muchos a través del teléfono móvil.

En cuanto a Twitter, según los datos aportados por Sinéad McSweeney y Patricia Cartes en su comparecencia ante la Ponencia, cuenta con 400 millones de visitantes al mes, alcanzándose la cifra de 1.000 millones de «tuits» cada dos días.

Ya se ha visto no sólo que la interacción a través de mensajería instantánea y de redes sociales se encuentra entre las actividades principales de los menores a través de Internet, sino también que con frecuencia no se cumplen los umbrales de edad establecidos para estar presentes en las mismas, umbrales comúnmente coincidentes con la edad mínima exigida por la legislación aplicable para consentir la cesión de datos personales.

A este respecto debe tenerse presente el marco regulador general en materia de protección de los datos de carácter personal, constituido, en el caso español, por la Ley Orgánica 15/1999, de 13 de diciembre, de pro-

tección de los datos de carácter personal, y el Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de aquella Ley. En concreto, el artículo 13 de este Reglamento establece en los catorce años la edad por debajo de la cual se requiere el consentimiento de los padres o tutores para consentir el tratamiento de datos de carácter personal y, por tanto, los menores de catorce años no pueden prestar su consentimiento por sí solos para crear un perfil en una red social. Además, corresponde al «responsable del fichero o tratamiento» (en su caso de la red social), «articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales» (apartado 4 del artículo 13 citado).

La empresa española Tuenti fija en catorce años el umbral para que los menores puedan darse de alta por sí solos en esta red social, mientras que la edad fijada en las redes sociales de matriz norteamericana es de trece años, edad que es justamente la fijada en EE.UU. en la «Child Online Privacy Protection Act» (COPPA), y que, por cierto, es también la establecida en la propuesta de Reglamento de la Unión Europea, en curso de tramitación, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[33].

En el caso de Facebook, José Luis Rodríguez informó que en España, a requerimiento de la Agencia Española de Protección de Datos, ha elevado la edad de acceso de 13 a 14 años para adecuarla a la normativa española.

El problema reside en la articulación de algún procedimiento de verificación de la edad en el momento del alta en una red social, procedimiento que «de facto» no existe en ninguna red social, arbitrando sólo las principales, mecanismos reactivos «a posteriori», basados comúnmente en denuncias procedentes de la propia comunidad de usuarios. La red social que llega más lejos en este punto es Tuenti, cuyo protocolo de verificación y borrado de perfiles de menores de catorce años incluye el DNI electrónico (DNIe) como mecanismo de verificación («a posteriori») de la identidad.

Sinéad McSweeney y Patricia Cartes de Twitter informaron a la Ponencia que la edad mínima para estar en Twitter es de trece años, y que la

[33] COM(2012) 11 final, art. 8.

plataforma se basa en un principio de «minimización de la colecta de datos», de suerte que para abrir una cuenta real no se piden datos de edad, lugar o de otro tipo, y confía a un mecanismo de denuncia la advertencia y eventual retirada de las cuentas de menores de trece años.

Tuenti, Facebook y Twitter informaron a la Ponencia de sus políticas «comunitarias» para dar respuesta, entre otras, a las situaciones de acoso en sentido amplio. El denominador común de todas estas políticas, basadas en la autorregulación, es confiar a los propios usuarios la detección y denuncia, a través de los mecanismos habilitados al efecto, de los contenidos o conductas inapropiados que se produzcan en la red social.

En concreto, Sebastián Muriel, en nombre de Tuenti, explicó que el compromiso de esta compañía con la protección de menores se basa en tres pilares: facilitar a menores, padres y educadores herramientas (disponibles en su «Centro de ayuda y seguridad») para que puedan informar (denunciar) cualquier contenido o perfil que no cumpla los términos de uso, y que pueden desembocar en el bloqueo o eliminación de la cuenta denunciada; adopción de acuerdos con los cuerpos y fuerzas de seguridad y con las organizaciones de protección del menor; e información y educación a menores, padres y educadores sobre todas las herramientas puestas a su disposición. Además, la estrategia de seguridad de Tuenti incluye un mecanismo para verificar el cumplimiento del principio de que sólo se admiten identidades reales, consistente en asociar la creación de un perfil en esta red bien a una previa invitación de otro usuario, bien a una dirección de email o teléfono.

Natalia Basterrechea, en nombre de Facebook, explicó que las normas de comportamiento en esta plataforma están basadas en la «Declaración de derechos y responsabilidades» y en las «Normas comunitarias», que, en concreto, prohíben el «bullying», la intimidación o el acoso a un usuario, compartir y actualizar contenido relativo a un discurso que incite al odio, amenazas, contenido pornográfico, contenido que incite a la violencia, y contenido que contenga desnudos o violencia gráfica. Está prohibida cualquier actividad ilícita, engañosa, maliciosa o discriminatoria.

Para garantizar el efectivo cumplimiento de estas normas, cuenta con una pluralidad de herramientas, entre ellas las denominadas de «denuncia social», basada en una innovadora línea de investigación («Compassion Research») que busca diseñar una interfaz más compasiva y humanizada que permita a los usuarios de Facebook tener conexiones más significa-

tivas y resolver conflictos de manera eficaz. Así la «denuncia social» es una herramienta que intenta conducir una situación conflictiva entre dos personas, con la ayuda de una tercera persona del entorno, hacia una solución amistosa, sin necesidad de plantear una denuncia propiamente tal. En un 85% de casos, este sistema habría permitido resolver la situación planteada.

El canal de denuncias, a disposición de los usuarios, sería otra herramienta, en la que el examen de la situación se confía a un equipo de operaciones, cuya dedicación es a cualquier hora de cualquier día, con capacidad para dar soporte en más de 24 idiomas y que cuenta al efecto con cuatro oficinas repartidas entre Estados Unidos, Irlanda y la India.

La Sra. Basterrechea completó la descripción de la política de seguridad de Facebook con la referencia al «Centro de Seguridad para Familias», disponible incluso en abierto, que contiene numerosos materiales educativos e informativos, con orientaciones específicas para adolescentes, y a la profusa colaboración que mantiene Facebook con múltiples actores, bien a través del llamado «Consejo asesor de seguridad global», que forman cinco grandes organizaciones americanas y europeas, y cuya misión es asesorar a Facebook en cuestiones relacionadas con la seguridad de la Red, bien a través de relaciones específicas con muy diversas organizaciones y con fuerzas de seguridad estatales.

Sinéad McSweeney y Patricia Cartes explicaron que Twitter cuenta con dos equipos principales, el de «Trust & Safety», con diferentes áreas de especialización (entre ellas la de derechos del usuario y privacidad —responsable del asunto de los menores de trece años que están en la Red y de los elementos de privacidad—, la de seguridad del usuario —encargado de situaciones relacionadas con abusos, acoso, autolesiones, suicidio—, la de solicitudes legales —que se encarga de las relaciones con las fuerzas de seguridad— y la de explotación de menores —que se encarga junto con el equipo de seguridad del usuario, no sólo de examinar cualquier denuncia en esta materia, sino también de la colaboración activa para combatir los contenidos relacionados con la explotación del menor), y el de atención al usuario (encargado de un soporte más genérico, y que incluye el centro de ayuda, y la solución de problemas técnicos derivados de «spam» o «malware»). Entre los dos equipos, que están tanto en San Francisco como en Dublín, se da soporte al usuario veinticuatro horas al día, siete días a la semana.

El procedimiento para asegurar el cumplimiento de las normas de uso es el de la denuncia, que puede canalizarse a través del centro de ayuda, o a través del propio «tuit» que, pulsando en el botón de «Más», conduce a la opción de «bloquear» o «reportar» y dentro de esta última, existen a su vez diferentes opciones.

La Sra. Cartes se refirió en particular a dos tipos de situaciones. Por un lado, a las situaciones de abuso y acoso que, desde la premisa de su prohibición y tras la evaluación de la correspondiente denuncia, puede dar lugar desde el simple envío de advertencias para recordar las reglas, a las que en la gran mayoría de los casos, los usuarios reaccionan positivamente, hasta la suspensión temporal de la cuenta y, en los casos más severos, a la suspensión de la cuenta de forma permanente, incluyendo el caso de amenazas, la recomendación de contactar con las fuerzas de seguridad. Por otro lado, las situaciones de explotación al menor, frente a las que la política de Twitter es de tolerancia cero, estando comprometida la compañía no sólo en la denuncia de cualquier contenido de este tipo al «National Center for Missing and Exploited Children» (NCMEC), con el que la Guardia Civil tiene una conexión VPN, que es la forma de obtener los datos específicos de un usuario que esté compartiendo este tipo de contenidos, sino en una colaboración activa, reflejada en la adopción de la tecnología PhotoDNA. Asimismo, la Sra. Cartes se refirió a la regla que prohíbe la suplantación de identidad, en relación con la cual también puede activarse el mecanismo de la denuncia y que puede originar la suspensión de la cuenta.

En materia de privacidad, con frecuencia los menores (como también muchos adultos) tienden a pasar por alto las declaraciones, condiciones o términos de uso de los servicios ofrecidos en Internet, incluidas las redes sociales, y estas declaraciones, a su vez, no tienen con frecuencia presentes las especiales características de este grupo de usuarios ni en los términos formales de claridad adecuados de sus políticas de información, ni en la adopción de otros aspectos de configuración del servicio, que dotarían a la experiencia de los menores en la Red de mayores niveles de seguridad.

La empresa española Tuenti muestra un alto grado de compromiso en esta materia, derivado de los siguientes elementos principales, mencionados por Sebastián Muriel:

- Máximo nivel de privacidad por defecto para sus usuarios, principio que, como comentó José Luis Rodríguez, vienen recomen-

dando las autoridades de protección de datos y que supone que la apertura del acceso a la información a terceros se hace depender de la decisión consciente y voluntaria del usuario.

- No indexación de los datos e información personal de los usuarios en los buscadores.
- Encriptado y cifrado de las conversaciones de chat (protocolo SSL).
- Distinción entre «contactos» (sólo para chatear) y «amigos» (para chatear y compartir información, contenidos, tablón, etc.), de manera que el usuario puede agregar a otro usuario eligiendo una u otra categoría.
- Los anteriores elementos se completan con una política de privacidad, que, desde el punto de vista informativo, se propone ser comprensible a los destinatarios, así como con un panel de privacidad sencillo, con el que poder configurar el grado de privacidad y un centro de ayuda y seguridad, «tuenti.com/privacidad», con recursos de ayuda, informativos y formativos, incluyendo espacios audiovisuales y recomendaciones de uso responsable para padres, educadores y usuarios.

Por lo que se refiere a Facebook, como declaró Natalia Basterrechea, reconoce su sometimiento al marco europeo de protección de datos, a través de su establecimiento radicado en Irlanda, del que deriva su sometimiento a la supervisión ejercida por la autoridad de protección de datos correspondiente a dicho establecimiento, que es la autoridad irlandesa.

En relación con Twitter, Sinéad McSweeney y Patricia Cartes subrayaron la naturaleza pública de esta plataforma, en cuanto a los contenidos (los «tuits» son en su conjunto públicos o privados, sin que exista la posibilidad de elegir la audiencia de cada contenido concreto), compatible con la privacidad del usuario, en cuyo contexto situaron la posibilidad del uso anónimo de cuentas, o el principio de minimización de los datos que se recogen, reflejo del cual es la decisión temprana de la compañía de eliminar de las fotos que se suben a la plataforma, la información sobre su localización geográfica.

IV. *¿Qué hacer?: Los menores como centro de una estrategia de ciudadanía digital*

1. Cinco ideas clave

En un informe como el presente, cuya naturaleza es la de un informe para la acción política, es éste un capítulo decisivo, cuya finalidad hay que situar en el contexto de las potestades de una Cámara parlamentaria como el Senado de orientación política general sobre el Gobierno, lo que comporta un enfoque particular sobre la materia de estudio, diferente del que pueda adoptarse desde otras instancias.

De la información aportada por todos los comparecientes y de la documentación examinada, se desprenden cinco ideas clave:

— Aunque Internet ofrece, desde muchos puntos de vista, enormes oportunidades, al propio tiempo presenta una serie de riesgos, de mayor o menor entidad, constituyendo precisamente un reto para las políticas públicas encontrar el equilibrio adecuado entre unas y otros. En este contexto los menores presentan necesidades específicas, desde una y otra perspectiva.

— Los valores que encarnan los derechos fundamentales de la persona, reconocidos en la Constitución española y en los tratados internacionales, deben regir tanto en el mundo físico como en el mundo digital, y, en el caso de los menores, garantizan el «interés superior» de éstos como «consideración primordial» para autoridades públicas o instituciones privadas en todos los actos que les conciernan (artículo 3 de la Convención de Naciones Unidas sobre los Derechos del Niño de 1989 y artículo 24 de la Carta de los Derechos Fundamentales de la Unión Europea).

— La existencia de diferentes actores con intereses relevantes en la materia objeto de estudio (poderes públicos, niños y padres, escuela y educadores, organizaciones privadas del sector de acción social, empresas de distinta índole relacionadas con la sociedad de información) plantea la cuestión básica del papel respectivo que corresponde a los dos círculos principales en los que aquellos actores se encuadran, Estado y sociedad, que se corresponden con dos enfoques normativos diferentes (regulación y autorregulación, respectivamente), apuntando la respuesta a dicha cuestión a un sistema de responsabilidad compartida.

— La existencia de una pluralidad de actores y de enfoques normativos (regulación y autorregulación) demanda una estrategia a nivel nacional en relación con las necesidades de los menores en Internet.

— La naturaleza dinámica y global de Internet hace que los objetivos y acciones a nivel nacional no puedan prescindir de los que se plantean a nivel internacional, tanto en el plano de decisión política y normativo como en el plano operacional.

2. Autorregulación y regulación en la protección de los menores en Internet: las alianzas público-privadas

La propia evolución de Internet ha otorgado un protagonismo indiscutible a la autocomposición de intereses, o si se prefiere, a la autorregulación, quedando el Estado en un papel menor, desbordado por la rapidez de la evolución tecnológica y la naturaleza internacionalmente accesible de la Red, situación que tiene su reflejo en la general inadaptación del ordenamiento jurídico al entorno digital, que han puesto de relieve varios de los comparecientes en la Ponencia.

Esta afirmación no contiene una valoración negativa de la autorregulación, a la que comúnmente se reconoce un importante papel en la protección de los menores en este ámbito, sino que tan sólo busca preguntarse por la posición que idealmente debería corresponder al Estado, y más en concreto al engarce adecuado entre dos enfoques, el de la autorregulación y el de la regulación.

El espectro mismo de iniciativas de autorregulación y co-regulación es muy amplio y las fronteras entre estos dos términos no son claras, pareciendo querer referirse el segundo a una combinación de regulaciones, pública y privada, y el primero a un compromiso puramente voluntario del sector privado sin ningún componente gubernamental. Las fórmulas que gozan de mayor aceptación en la actualidad son las alianzas («partenariados» según el anglicismo derivado del término inglés «partnership») público-privadas, que se encuentran en la intersección de la co-regulación y de la autorregulación, en cuanto el Gobierno toma parte activa en la negociación de compromisos planteados para su voluntaria adopción por las empresas privadas participantes. En estas fórmulas, el resultado mantiene las características de la autorregulación, pero el proceso conducente al mismo es catalizado en el seno de la alianza público-privada.

La Unión Europea y sus Estados miembros suelen adscribirse a un modelo que combina diferentes enfoques, de regulación y de autorregulación o co-regulación, poniendo el acento en unos u otros en función de las categorías de riesgos.

La autorregulación ha ocupado y ocupa en la Unión Europea un lugar relevante, en atención a su capacidad de adaptación al desarrollo tecnológico y a las tendencias sociales, con destacadas iniciativas como las producidas en los ámbitos de las comunicaciones por telefonía móvil, las redes sociales y los juegos «online». Así, en 2007, la Comisión Europea auspició un acuerdo entre las principales operadoras europeas de telefonía y proveedores de contenidos, el denominado «Marco europeo para un uso más seguro de los teléfonos móviles por parte de niños y adolescentes» («European Framework for Safer Mobile Use by Younger Teenagers and Children»[34]), que describe principios y medidas, agrupados en cuatro bloques (clasificación de contenidos, mecanismos de control de acceso, educación y concienciación y colaboración con las fuerzas policiales y jueces en la lucha contra los contenidos ilegales), que debían ser desarrollados a nivel nacional, trasunto de los cuales se adoptó en España por las principales operadoras de telefonía, antes de finalizar el mismo año, un código de conducta que, como recordó Sofía Fernández de Mesa, continúa vigente y ha permitido, entre otras iniciativas, el desarrollo de un icono común para la denuncia de contenidos ilegales, disponible no sólo en las «webs» de las compañías, sino también descargable en «smartphones» y tabletas.

No mucho tiempo después, en 2009, vieron la luz los «Principios de la Unión Europea para unas redes sociales más seguras» («Safer Social Networking Principles for the European Union»[35]), propuestos por las principales redes sociales operantes en Europa, después de un proceso de consultas con la Comisión Europea y organizaciones no gubernamentales, y que se centran en recomendaciones en siete áreas (aumentar la concienciación; promover una oferta de servicios apropiada en razón de la edad; capacitar en el uso de la tecnología; facilitar mecanismos de fácil uso para denunciar los contenidos o conductas que violen las condicio-

[34] Disponible en: http://www.gsma.com/gsmaeurope/wp-content/uploads/2012/04/saferchildren.pdf

[35] Disponible en: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf

nes de uso; responder eficazmente a las anteriores denuncias; evaluar los procedimientos de revisión de las denuncias sobre contenidos o conductas ilegales o prohibidas).

El Código de seguridad en línea PEGI, Información Paneuropea sobre juegos («Pan-European Game Information»), adoptado en 2003, es otro ejemplo notable de esquema de autorregulación de marca europea con un alcance más amplio que el representado por la Unión Europea como tal organización, a través del cual los firmantes del Código se adhieren, entre otros compromisos, a un sistema de clasificación de contenidos.

No son las anteriores las únicas iniciativas de autorregulación de ámbito europeo centradas en la protección de los menores en Internet, pudiendo citarse también la Coalición en torno a los «Principios para un uso seguro de los dispositivos con conexión a Internet y los servicios en línea en la Unión Europea por parte de los niños y los jóvenes», promovida por el denominado sector TIC ampliado —operadores de telecomunicación, proveedores de contenidos, motores de búsqueda, fabricantes de dispositivos—[36], o la «Coalición para hacer de Internet un lugar mejor para los niños»[37], que responde a una convocatoria de la Comisión Europea entre los CEO de las grandes empresas involucradas en el sector de las TIC.

El enfoque de autorregulación se ha ido entrelazando en la Unión Europea con marcos normativos que identifican la protección de los menores en Internet entre sus principios básicos. Es el caso de la adopción en 2010 de la Directiva, ya mencionada, de servicios de comunicación audiovisual (Directiva 2010/13/UE), que extiende la protección de los menores respecto a contenidos inapropiados a la comunicación comercial o a los servicios audiovisuales a la carta («a petición») ofrecidos por Internet, o en 2011 de la Directiva, también mencionada, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil (Directiva 2011/92/UE).

En España, la Ley incorpora el fomento de la autorregulación como una obligación de las Administraciones Públicas. Así, según el artículo 18 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la in-

[36] Disponible en: www.ictcoalition.eu

[37] Disponible en: http://ec.europa.eu/digital-agenda/self-regulation-better-internet-kids

formación y de comercio electrónico, aquéllas «impulsarán (…) códigos de conducta voluntarios», para su adopción por «corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores», y «que tendrán especialmente en cuenta la protección de los menores», y «estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos».

En este último apartado, los principales canales de televisión suscribieron en 2004 un Código de Autorregulación de Contenidos Televisivos e Infancia, que la Ley 7/2010, de 31 de marzo, general de comunicación audiovisual reconoce expresamente para la puesta en práctica de las obligaciones que dicha Ley impone a todos los prestadores de servicios de comunicación audiovisual televisiva, incluidos los de a petición, de clasificación y etiquetado de sus contenidos (artículos 7 y 12).

Por otro lado, la Ley 34/2002 establece también determinadas obligaciones de la industria, de información a los usuarios sobre herramientas técnicas para aumentar la seguridad en Internet, incluidas «las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios de Internet no deseados o que puedan resultar nocivos para la juventud y la infancia», así como sobre la responsabilidad del usuario «por el uso de Internet con fines ilícitos, en particular para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial», si bien estas obligaciones están limitadas a los proveedores de acceso a Internet (artículo 12 bis de la Ley citada).

3. Las palancas para la acción: estrategia, coordinación, coherencia y cooperación internacional

En la «Estrategia europea en favor de una Internet más adecuada para los niños», elaborada en 2012, la Comisión Europea parte del reconocimiento de que las diferentes políticas emprendidas hasta el momento a nivel europeo en favor de los menores no se han combinado en un marco coherente, y proclama que «Europa necesita una estrategia que evite la fragmentación del mercado y cree un entorno en línea más seguro y enriquecedor para todos los niños de la Unión Europea»[38].

[38] COM(2012) 196 final.

La adopción de una estrategia constituye también a nivel nacional un instrumento, una palanca imprescindible de las políticas públicas referidas a las necesidades de los menores en un entorno como el de Internet, en el que confluye una pluralidad de actores, de enfoques normativos (autorregulación y regulación) y de niveles de acción (nacional e internacional).

Varios de los comparecientes ante la Ponencia han subrayado el valor de la estrategia como palanca para afrontar los retos que las necesidades de los menores en Internet plantean.

Así lo hicieron, desde el campo gubernamental, Víctor Calvo-Sotelo, Manuel Escalante y Salomé Adroher al referirse a los principales instrumentos aprobados por el Gobierno con incidencia en esta materia, por un lado, la Agenda Digital para España, aprobada por el Consejo de Ministros el 15 de febrero de 2013, cuyos objetivos 4.1 y 4.2 se refieren, respectivamente, a «impulsar el mercado de servicios de confianza» y a «reforzar las capacidades para la confianza digital», y, por otro, al «II Plan Estratégico nacional para la infancia y la adolescencia 2013-2016 (II PENIA)», aprobado por Acuerdo del Consejo de Ministros de 5 de abril de 2013, cuyo objetivo 3 es «Impulsar los derechos y la protección de la infancia con relación a los medios de comunicación y a las tecnologías de la información en general».

Con una proyección particular, también Ignacio Cosidó y Arsenio Fernández de Mesa subrayaron la importancia de la estrategia en la lucha contra el cibercrimen, estrategia que debe ser transversal, en atención a las especiales características que tiene la comisión de delitos en la Red.

Desde el campo de las organizaciones de protección de la infancia, se refirieron de modo particular al valor de la adopción de una estrategia nacional, Liliana Orjuela y Jorge Flores.

Liliana Orjuela defendió que tal estrategia debía enmarcarse en una más general de protección de los niños contra la violencia, en línea con las «Directrices del Consejo de Europa sobre las estrategias nacionales integrales para la protección de los niños contra la violencia», aprobadas en 2009 mediante Recomendación del Comité de Ministros de dicha organización (REC(2009) 10), y en el marco más amplio de los compromisos para los Estados firmantes derivados de la Convención de las Naciones Unidas sobre los Derechos del Niño.

Jorge Flores subrayó la importancia del diseño de un plan integral, eficiente y flexible a la vez, que reúna tres condiciones: determinación y constancia en el tiempo; coordinación y optimización de recursos, como condiciones de eficacia; y rapidez de adaptación. En este sentido alentó a los poderes públicos a superar sus limitaciones operativas y anticiparse.

En efecto, las claves conceptuales de una estrategia, también en la materia examinada, son la coordinación y la coherencia. La coordinación persigue aunar los procesos de decisión y gestión de los diferentes actores en este campo, y la coherencia busca evitar tanto las contradicciones internas en las acciones individualmente consideradas en relación con los objetivos que cada una de ellas persigue, como alinear el conjunto de las acciones de todos los sectores en vista de los objetivos trazados.

Coordinación y coherencia deben propiciarse a través de concretas fórmulas organizativas que traduzcan un paso decidido desde la mera agregación de múltiples iniciativas públicas y privadas a una visión estratégica con alto liderazgo y compromisos a largo plazo, idea que puede considerarse uno de los hilos conductores de prácticamente todos los comparecientes ante la Ponencia, concretado por alguno (Óscar de la Cruz) en la creación de un «centro nacional de coordinación» que aglutine a todos los órganos con competencias en la materia e integre también al sector privado y que permita un flujo de información de todos para todos.

Un ejemplo interesante lo ofrece el Reino Unido que, sobre la base de las recomendaciones de un informe independiente (el conocido como «Informe Byron») estableció el denominado «Consejo del Reino Unido para la Seguridad de los menores en Internet» (UKCCIS, según las siglas inglesas), una organización en la que están representados más de dos centenares de actores, públicos y privados, cuya función es diseñar y desarrollar la Estrategia de seguridad de los menores en Internet, cuya primera versión fue publicada en 2009.

Más común suele ser la creación de grupos de trabajo, con liderazgo gubernamental o en los que el gobierno participa con las demás partes interesadas, como sucede en España donde, además de la coordinación bilateral para temas específicos, por ejemplo entre dos Departamentos Ministeriales, existen algunos grupos de trabajo generales. Borja Adsuara, Manuel Escalante y Salomé Adroher se refirieron al grupo «Internet y Menores», creado en mayo de 2013 y dirigido por el Instituto Nacional

de Tecnologías de la Comunicación (INTECO), que coordina, a nivel de la Administración Central, los trabajos de los distintos organismos implicados.

La cuestión que se plantea es la de si este grado de articulación es suficiente o debe darse algún paso más en la dirección de las exigencias inherentes a las ideas de estrategia, coordinación y coherencia. Cuestión que, a su vez, cabe plantear desde la óptica específica de las necesidades de los menores en Internet, o subsumida ésta en la perspectiva más amplia del modelo organizativo que a nivel gubernamental debe adoptarse en las materias relacionadas con Internet.

Sobre esta última cuestión existe un debate abierto, con opiniones diversas, como la de quienes defienden un Alto Comisionado Digital, en la estela del «Chief Digital Officer» (CDO) existente en algunas Administraciones del mundo anglosajón, aludida en la intervención de Antoni Gutiérrez ante la Ponencia, o la de quienes abogan por fórmulas organizativas más prototípicas de la Administración española.

En la actualidad, el modelo español sitúa las competencias públicas relacionadas con Internet en la órbita ministerial, en concreto a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, incardinada en el Ministerio de Industria, Energía y Turismo (con el apoyo de Red.es —a la que le corresponde entre otras funciones, la de actuar de «observatorio del sector de las telecomunicaciones y de la sociedad de la información», «la elaboración de estudios e informes y, en general, el asesoramiento de la Administración General del Estado en todo lo relativo a la sociedad de la información», y «el fomento y desarrollo de la sociedad de la información», según establece la disposición adicional decimosexta de la Ley 9/2014, de 9 de mayo, de telecomunicaciones— y del Instituto Nacional de Tecnologías de la Comunicación, INTECO, identificado por la Agenda Digital para España como centro de referencia en confianza digital y ciberseguridad), a cuyas acciones se unen las de la Secretaría de Estado de Educación, la Secretaría de Estado de Asuntos Sociales, la Secretaría de Estado de Seguridad, a través de los Cuerpos y Fuerzas de Seguridad del Estado, y el Ministerio de Justicia, complementándose con las que corresponden, desde distintos ángulos, a la Comisión Nacional de los Mercados y la Competencia (creada por Ley 3/2013, de 4 de junio, que agrupó las funciones de distintos organismos reguladores, entre ellos la Comisión del Mercado de las Telecomuni-

caciones y el Consejo Estatal de Medios Audiovisuales) y a la Agencia Española de Protección de Datos (regulada en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal). A este conjunto organizativo se suma la previsión relativa al «Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información», contenida en la citada Ley 9/2014 (disposición adicional quinta).

Una última palanca para la acción, imprescindible en todo lo relacionado con Internet, y por tanto también en lo que se refiere a las necesidades de los menores, es la cooperación internacional, tanto en el nivel de decisión político —normativa o de influencia en el mismo (nivel que para los países miembros de la Unión Europea tiene en las instituciones de ésta la plataforma natural de acción, sin olvidar otras, bien regionales como el Consejo de Europa, o de ámbito más amplio —OCDE, UIT, o el mismo Foro para la Gobernanza de Internet—) como en el nivel operacional, nivel este último en el que la importancia de la cooperación se proyecta en varias vertientes: la armonización de los marcos estadísticos nacionales, para medir de forma consistente los aspectos de acceso, uso y prevalencia de riesgos de Internet en los menores; la cooperación transfronteriza de las autoridades policiales en la persecución y lucha contra el delito; la actividad de las redes de líneas de ayuda y centros de seguridad en Internet, respectivamente, INHOPE e INSAFE, originariamente europeas, pero hoy convertidas en modelos de cooperación internacional; las actividades de concienciación y sensibilización, de las que constituye un notable ejemplo el «Día para una Internet más segura» («Safer Internet Day»), organizada por INSAFE, cuya convocatoria cobra cada año mayor importancia; o las iniciativas que promueven estándares internacionales para la interoperabilidad de muchas técnicas, como los controles parentales en plataformas o dispositivos.

4. Objetivos y acciones

La «Estrategia europea en favor de una Internet más adecuada para los niños» plantea cuatro objetivos básicos, en torno a los cuales se articulan las acciones concretas:

1) Estimular los contenidos en línea de calidad para los jóvenes.

2) Intensificar la sensibilización y la capacitación.

3) Crear un entorno en línea seguro para los niños.

4) Luchar contra los abusos sexuales y la explotación sexual de los niños.

Este informe seguirá en lo esencial este esquema, si bien, teniendo en cuenta las aportaciones de los comparecientes, que unánimemente han situado en la educación, el enfoque prioritario para abordar las necesidades específicas de los menores en Internet, tanto desde el punto de vista de las oportunidades como de los riesgos, propone la capacitación de los menores en competencias digitales y la sensibilización como objetivo primario, objetivo con el que guarda relación el fomento de contenidos en línea de calidad para los menores y que debe complementarse con la doble protección externa que debe procurar al menor la existencia de un nivel aceptable de seguridad en el propio entorno en línea y de un sistema normativo y de aplicación de la Ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red.

Así, la Ponencia enuncia los siguientes objetivos para una estrategia de oportunidades y uso seguro y responsable de Internet para los menores:

1) Capacitación en competencias digitales y sensibilización.

2) Fomento de contenidos en línea de calidad para niños y jóvenes.

3) Protección a través de un nivel de seguridad aceptable de Internet.

4) Protección a través de un sistema normativo y de aplicación de la Ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red.

4.1. Capacitación en competencias digitales y sensibilización

Uno de los ejes de la «Agenda Digital para Europa» lo constituye precisamente «fomentar la alfabetización, la capacitación y la inclusión digitales», y en relación con él se afirma que «la competencia digital es una de las ocho competencias clave que resultan fundamentales para las personas en una sociedad basada en el conocimiento…», y como parte de ella se encuentra la de «garantizar la propia seguridad cuando se está en línea»[39].

[39] COM(2010) 245 final, p. 28.

Asume así esta Agenda el planteamiento sobre «competencias clave para el aprendizaje permanente» contenido en la Recomendación del Parlamento Europeo y del Consejo de 18 de diciembre de 2006, que define tales competencias como «aquéllas que todas las personas precisan para su realización y desarrollo personales, así como para la ciudadanía activa, la inclusión social y el empleo», entre las cuales se encuentra la «competencia digital», que «entraña el uso seguro y crítico de las tecnologías de la sociedad de la información para el trabajo, el ocio y la comunicación» y «se sustenta en las competencias básicas en materia de TIC: el uso de ordenadores para obtener, evaluar, almacenar, producir, presentar e intercambiar información, y comunicarse y participar en redes de colaboración a través de Internet».[40]

En el mismo sentido, pero con mayor alcance aún, para la «Estrategia europea en favor de una Internet más adecuada para niños», «la alfabetización digital y mediática y las correspondientes aptitudes son cruciales para el uso de Internet por los niños», y para el futuro de la sociedad misma, pues, en definitiva, «la forma de comportarse hoy en línea de los niños contribuirá a definir el mundo digital del mañana»[41].

La alfabetización digital (que incluye la seguridad digital, pero no se agota en este aspecto) y la alfabetización mediática, que amplía el alcance de aquélla, apuntan a un concepto nuevo, el de ciudadanía digital, que enfatiza las oportunidades creativas y de participación de Internet para los menores.[42]

Si la coordinación para aunar objetivos y acciones, traducible en fórmulas organizativas coherentes con las exigencias de tal principio, fue uno de los principales hilos conductores de todos los comparecientes en la Ponencia, otra idea expuesta recurrentemente fue la de la importancia del aprendizaje escolar del uso seguro y responsable de las nuevas tecnologías, que algunos comparecientes conectaron con la idea de ciudadanía y la condición de los menores como sujetos de derechos, entre ellos y de modo particular el derecho a la intimidad o privacidad y a la protección de los datos de carácter personal (Francisco Javier Martos, Liliana Orjuela, Jorge Flores; con especial énfasis en la necesidad de

[40] Recomendación del Parlamento Europeo y del Consejo de 18 de diciembre de 2006 sobre las competencias clave para el aprendizaje permanente (2006/962/CE).

[41] COM(2012) 196 final, pp. 9 y 18.

[42] OCDE, op. cit., p. 73.

aprender a proteger y gestionar la identidad digital, José Luis Rodríguez, Eugenio Oñate, Antoni Gutiérrez, José Luis Casal, Consuelo Madrigal, Joaquim Bayarri), con las capacidades comunicativas en general (Josep Manuel Prats, Javier Urra, Consuelo Madrigal, quien se refirió incluso a una «semiología virtual», referida a las destrezas de comunicación en el entorno digital) o con las capacidades que suelen adscribirse a las denominadas «competencias sociales y cívicas», que incluyen recursos psicológicos, como la resiliencia (o capacidad de hacer frente a la adversidad —de la que ya se habla también en relación con los factores de riesgo en Internet—), el respeto y la empatía, o los valores cívicos que integran a la persona en la comunidad (Dolors Reig, Javier Urra, José Luis Casal, Joaquim Bayarri, Jorge Flores; con énfasis particular en el respeto a la propiedad intelectual Miguel Pérez, José Manuel Tourné, Carlota Navarrete).

Este aprendizaje, sin embargo, plantea distintas posibilidades en cuanto a la forma de llevarse a efecto, pudiendo vertebrarse en el currículo educativo en forma de asignatura o módulo específico, o como un elemento transversal (variando en este aspecto, al menos en los términos genéricos en que se formuló, la opinión de los comparecientes), y a su vez, en una u otra forma, incluirse desde la enseñanza primaria o en una etapa educativa posterior (siendo en este punto generalizada la opinión favorable a la inclusión desde la primera etapa de la enseñanza obligatoria).

La Ley Orgánica 2/2006, de 3 de mayo, de Educación señala que tanto el respeto a los valores y las normas de convivencia como el uso adecuado de las tecnologías de la información constituyen objetivos prioritarios de las distintas etapas de la educación básica y del bachillerato (como se desprende de los artículos 17.a) e i), para la Educación Primaria, 23.a) y e), para la Educación Secundaria, y 33 a) y g), para el Bachillerato). Esta idea se reitera en el Preámbulo de la Ley Orgánica 8/2013, de 9 de diciembre, de mejora de la calidad educativa («el uso responsable y ordenado de estas nuevas tecnologías por parte de los alumnos y alumnas debe estar presente en todo el sistema educativo» —apartado IX del Preámbulo—), si bien esta Ley no contiene modificación alguna en relación con la articulación de este aprendizaje en el currículo (pues el nuevo artículo 111 bis que esta Ley introduce en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, se refiere a las tecnologías de la información y las comunicaciones desde el ángulo de su utilización como herramienta

educativa), debiéndose estar a este respecto a lo que disponen las normas de rango reglamentario que establecen los currículos básicos de las distintas etapas educativas.

De estas normas (constituidas en la actualidad por los Reales Decretos 126/2014, de 28 de febrero, 1631/2006, de 29 de diciembre, y 1467/2007, de 2 de noviembre, referidos a la educación primaria, educación secundaria y bachillerato, respectivamente) se desprende un enfoque primario del aprendizaje en el uso de las tecnologías de la información y la comunicación (al igual que de los valores cívicos) como un aprendizaje transversal, que debe estar presente en todas las asignaturas, sin perjuicio de su tratamiento específico en algunas de las asignaturas de cada etapa educativa.

A priori, la transversalidad parece inherente al concepto de «competencias clave» a que se refiere la mencionada Recomendación del Parlamento Europeo y del Consejo, y ésta resulta ser la línea argumental recogida en el significativo Preámbulo del Real Decreto 126/2014, por el que se establece el currículo básico de la Educación Primaria (primero —y hasta ahora único— de los que, para el desarrollo de los currículos básicos de las etapas educativas, habían de venir tras la entrada en vigor de la Ley Orgánica 8/2013, de mejora de la calidad educativa), que declara basarse, «en línea con la Recomendación 2006/962/EC, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2006, sobre las competencias clave para el aprendizaje permanente, en la potenciación del aprendizaje por competencias», la cual «se caracteriza por su transversalidad, su dinamismo y su carácter integral».

Cuestión diferente y que probablemente sea la que deba ser objeto de detenido análisis, es la del grado de plasmación efectiva, a lo largo del itinerario que atraviesa las distintas etapas educativas, de la proclamada declaración de la competencia digital como competencia básica o clave del currículo.

La vertebración en el currículo de las competencias digitales (de las que buscar, jerarquizar, almacenar, utilizar, producir y compartir información, comunicarse y participar en redes de colaboración, gestionar la identidad digital y conocer los riesgos de y en Internet y ser capaz de afrontar los mismos, son componentes básicos), constituye, según opinión prácticamente unánime, el epicentro de las acciones encaminadas a capacitar a los menores en tales competencias, pero en torno a ella

aparecen otras acciones, como presupuesto o complemento necesario de la misma.

Presupuesto necesario, como señalaron en particular comparecientes procedentes del campo educativo y de las organizaciones de protección de la infancia, es la formación de maestros y profesores, que debe comenzar en las propias escuelas universitarias, cuyos planes de estudio deben revisarse (José Miguel Rosell), sobre todo desde la perspectiva de arrumbar las barreras todavía existentes no ya en el aprendizaje de las TIC, sino en cuanto a la formación continua (Miguel Comín, Carlos Represa), que capacite para adaptarse a la evolución tecnológica.

Complemento necesario lo constituye la formación de los padres que, como en otras actividades que comportan riesgos, «dan la mano, enseñan las normas y acompañan». (Antoni Gutiérrez, Luis Carbonel, Josep Manuel Prats, Jesús Salido).

Si las acciones que tienen que ver con el currículo escolar o los planes de estudio universitarios, en cuanto constitutivos de un aprendizaje reglado, remiten a medidas normativas, el resto de acciones se adscriben a un aprendizaje informal, de interés no sólo para padres, sino también para los niños y adolescentes (como complemento de su formación reglada) y para sus profesores (como parte de su formación continua) y forman parte de las acciones de sensibilización general.

Puede decirse que en buena medida los esfuerzos de capacitación de los menores en el uso seguro y responsable de las TIC han venido gravitando en este tipo de acciones de sensibilización, con iniciativas múltiples, bien de origen público, a su vez procedentes de organismos de diferentes ámbitos, bien de origen privado, desplegadas tanto por organizaciones del sector de acción social como por las empresas del sector de las TIC, como parte de su responsabilidad social corporativa (quienes comparecieron ante la Ponencia en representación de estas empresas, informaron de sus iniciativas al respecto).

El reto que en este campo se plantea es el de enmarcar todas estas iniciativas en una estrategia que, partiendo del aprendizaje formal como epicentro de las acciones de capacitación en las competencias digitales, lo complemente con aquéllas, coordinándolas y alineándolas, valiéndose de alianzas público-privadas, que involucren también a los medios de comunicación (Salomé Adroher y Antoni Gutiérrez), de manera que el

objetivo de sensibilización de todos (niños, padres, profesores y educadores) se consiga de modo eficaz. La coordinación debe tener en cuenta también los esfuerzos desplegados a nivel europeo, especialmente a través de los programas de la Comisión, y de eventos como el «Día para una Internet más segura», organizado cada año en el mes de febrero, bajo el impulso de INSAFE, la red europea de centros de seguridad en Internet, y que tiene lugar en un número de países cada vez mayor.

Dos aspectos relevantes para la eficacia de las iniciativas de sensibilización se refieren a la necesidad de tener en cuenta las diferencias de edad entre los menores y a la participación misma de los jóvenes.

Así, la «Estrategia europea en favor de una Internet más adecuada para los niños» señala que «las estrategias de sensibilización deben tener en cuenta los diferentes niveles de desarrollo de los niños más pequeños y los adolescentes, prestando especial atención a los más jóvenes y vulnerables, incluidos los que presentan discapacidades intelectuales y de aprendizaje», así como que «la educación por iguales constituye una estrategia valiosa para que niños de todas las edades conozcan sus derechos y responsabilidades en línea»[43].

En relación con la participación de los jóvenes en las actividades de sensibilización, algunos comparecientes informaron de algunas interesantes experiencias, bien en entornos virtuales (plataforma «ciberresponsables», mencionada por Salomé Adroher; iniciativa «cybermanagers», señalada por Jorge Flores, los menores como «agentes activos de la solución»), o bien a través de talleres o actividades presenciales en la escuela (Joaquim Bayarri, formar a alumnos que hagan de formadores de alumnos de cursos inferiores).

Algunos comparecientes insistieron también en la importancia de que los contenidos utilizados en las iniciativas de sensibilización sean de calidad y atractivos (Manuel Escalante), y se apuntó también la utilidad de abordar temas específicos («cápsulas», Joaquim Bayarri; «píldoras informativas», José Miguel Rosell, basándose en casos reales, siguiendo el ejemplo de las campañas de Tráfico).

Una particular dimensión de las acciones de capacitación y sensibilización que tienen en la escuela su espacio natural de desenvolvimiento

[43] COM(2012) 196 final, p. 10.

se refiere a las situaciones en las que los niños son los agresores, como ocurre con el «ciberbulling», situaciones que requieren de protocolos de actuación claros, cuya definición debe promoverse, como pusieron de manifiesto Manuel Escalante y Carlos Represa. Este último apuntó incluso, con un alcance más general, el fomento de la figura del «Director de Seguridad», que requeriría una formación específica, como una traslación al ámbito de la escuela de la figura del «Delegado de protección de datos» contemplada en la propuesta de Reglamento de la Unión Europea relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales[44].

4.2. Fomento de contenidos en línea de calidad para niños y jóvenes

Uno de los objetivos de la «Estrategia europea en favor de una Internet más adecuada para niños», estrechamente relacionado con el de capacitación en competencias digitales, lo constituye el fomento de contenidos en Internet de alta calidad para niños y jóvenes, lo que dicha Estrategia concreta en dos líneas de actuación entrelazadas, referida una al estímulo de contenidos digitales instrumentales de la enseñanza, destinados, según la edad, al juego y a la educación y que favorezcan la creatividad y el pensamiento crítico, y otra al estímulo de la iniciativa de los propios niños y adolescentes, fomentando en ellos una actitud no limitada al consumo sino al uso positivo de Internet y a la creatividad. Ambas líneas de actuación redundarán también a favor del mercado único digital europeo y de la innovación tecnológica.

Las acciones en este capítulo a nivel nacional deben fomentar la innovación y los desarrollos destinados a la creación de este tipo de contenidos, y las iniciativas de los propios jóvenes, y deben coordinarse con las promovidas a nivel europeo.

4.3. Protección a través de un nivel de seguridad aceptable de Internet

Aun cuando la alfabetización digital y mediática de los menores, con la escuela como eje central de la misma, complementada con las acciones de formación de profesores y padres, y de sensibilización, así como

[44] COM (2012) 11 final, arts. 35 y ss.

con el fomento de su experiencia positiva en este entorno, constituye (vuelve a reiterarse) el núcleo de una estrategia sobre las necesidades de los menores en Internet, es opinión general que la protección de los mismos debe provenir también de un nivel de seguridad aceptable de la Red.

En este plano, las medidas que pueden adoptarse son fundamentalmente de carácter técnico, y habitualmente confiadas a la autorregulación, reservándose el poder público un margen mayor o menor de intervención, que va desde una acción de fomento, con o sin apoyo financiero, a una acción normativa que obligue a las empresas afectadas a establecer unas u otras medidas.

Atendiendo al tipo de riesgos que las medidas técnicas intentarían reducir o mitigar, adquieren especial importancia las herramientas de filtrado para bloquear el acceso a contenidos ilícitos (en particular las imágenes de abuso sexual infantil) o contenidos nocivos para los menores.

Las técnicas de filtrado pueden basarse en «listas negras» («blacklists», que permiten con carácter general el acceso a los contenidos «web» excepto en aquellos identificados como rechazables) o «listas blancas» («whitelists», que bloquean con carácter general el acceso, excepto para los identificados como admisibles) y pueden operar en los distintos niveles del proceso técnico de comunicación (bien en el de la infraestructura, que puede ser ya en el acceso a la red facilitado por el proveedor, ya en el de acceso a una red local, o en el de acceso al servidor de una plataforma determinada, bien en el del terminal del usuario).

Aunque los filtros no son una panacea, pues presentan fallos en su efectividad, bien por bloqueo en exceso (bloqueo accidental de sitios que no son para adultos) bien de bloqueo por defecto (no bloquean todos los sitios para adultos), y muchos jóvenes se muestran renuentes a los mismos, cuando no en ocasiones —filtros instalados en el terminal— los eluden, es general la opinión sobre su utilidad, especialmente en el bloqueo de contenidos «web» identificados en una «lista negra».

Un tipo particular de herramientas de filtrado lo constituyen los «software» de control parental, que pueden operar en distintos niveles, pero que tienen un alcance más amplio, pues no sólo filtran contenidos sino que controlan también el uso de ciertas aplicaciones (por ejemplo, «webcam», mensajería instantánea), informan detalladamente del uso «online» de los menores y posibilitan restringir el tiempo de dicho uso, por lo

que permiten afrontar un abanico de riesgos más amplio, no limitado a los de contenidos. Es ésta una de las ventajas principales de este tipo de herramientas, junto con la de confiar a las familias la decisión, en función de sus valores, sobre el tipo de contenidos y actividades admisibles, el momento y la frecuencia de uso de Internet para sus hijos.

La «Estrategia europea en favor de una Internet más adecuada para los niños» considera el control parental como «una medida complementaria que contribuye a proteger a los niños más pequeños de los contenidos en línea perjudiciales ya que permite filtrar contenidos y vigilar las actividades en línea».[45]

Sofía Fernández de Mesa informó a la Ponencia de un ejemplo de herramienta de filtrado en el nivel de la infraestructura, que habría desarrollado la compañía a la que representaba, aunque todavía no disponible en España, que, en sus palabras, ofrecería «una protección «online» integral (…) desde el acceso».

Joan Taulé se refirió a la obligación de la industria de desarrollar las tecnologías necesarias de protección de los menores y abogó por su implantación y utilización «tanto en el ámbito del hogar y el dispositivo individual como en el nivel de la infraestructura (proveedor de servicios de Internet o red de telefonía móvil)».

El Gobierno británico ha desplegado desde el mes de julio de 2013 un esfuerzo notorio, que incluyó una cumbre auspiciada por el propio Primer Ministro el día 18 de noviembre de 2013[46], con los principales proveedores de servicios de Internet, para promover tanto el bloqueo del acceso a contenidos de pornografía infantil y su retirada, como el bloqueo a contenidos nocivos.

Como resultado de tal esfuerzo, Google y Microsoft han introducido cambios en sus motores de búsqueda (de los que informaron a la Ponencia. Héctor Sánchez y Francisco Ruiz), para impedir, a escala mundial, que el uso de determinados términos (hasta 100.000 combinaciones) pueda conducir a imágenes de pornografía infantil. En el momento en que se conoció esto, el pasado mes de noviembre, Google anunció que los cambios se irían introduciendo en 159 lenguas en un período de seis

[45] COM(2012) 196 final, p. 13.

[46] Noticia disponible en https://www.gov.uk/government/news/internet-safety-summit-at-downing-street-communique.

meses. La iniciativa de Google y Microsoft comprende también la introducción de mensajes de advertencia claves que aparecerán siempre que alguien utilice uno de los términos de búsqueda incluidos en la «lista negra», informando al usuario de las consecuencias de sus acciones y remitiéndole a organizaciones de ayuda, así como cambios en la función de predicción de textos («autocompletion») para evitar sugerencias que conduzcan a búsquedas relacionadas con la pornografía infantil.

Héctor Sánchez informó también a la Ponencia de la tecnología PhotoDNA que ha desarrollado Microsoft para crear identificadores que permitan retirar las imágenes de abuso de menores y cualquier copia de las mismas en todo Internet, tecnología que han aceptado compartir otras compañías.

La acción desde la posición de las empresas proveedoras de servicios de Internet con el objeto de evitar la circulación de pornografía infantil en Internet, deberá encaminarse tanto en la dirección de profundizar en las líneas de actuación técnicas trazadas por los motores de búsqueda, para el bloqueo del acceso y la retirada de este tipo de imágenes, como en la más general de una colaboración activa y decidida de dichas empresas en la detección, información rápida a las fuerzas policiales y retirada de tales contenidos.

El Gobierno británico ha apostado también, con determinación, por poner freno al acceso a contenidos nocivos para los menores, mediante herramientas de filtrado en la infraestructura, al promover que todos los nuevos clientes de banda ancha dispongan de una herramienta familiar de filtrado (salvo que el titular de la cuenta deseche tal solución), de carácter integral, esto es, para cubrir cualquier dispositivo conectado a la cuenta de Internet del cliente, y que sólo el titular de la cuenta pueda cambiar. A su vez los proveedores de servicios de Internet tendrán de plazo hasta finales de 2014 para contactar con los clientes existentes y proponerles una decisión «inevitable» sobre si quieren o no instalar esta herramienta[47].

La «Estrategia europea en favor de una Internet más adecuada para los niños» invita a los Estados miembros a:

— promover la disponibilidad y uso de herramientas de control parental;

[47] «Online Safety», op. cit., p. 28.

— apoyar a la industria en sus esfuerzos al respecto;

— realizar ensayos y ciclos de certificación de este tipo de herramientas.[48]

En relación con los contenidos «web» para adultos se ha planteado también la posible implantación de métodos de verificación de la edad, cuya exigencia teórica por parte del poder público alcanzaría al menos a los radicados en el territorio bajo su jurisdicción. Se ha destacado en este sentido la diferencia legal existente entre la industria del juego «online» y la de aquellos contenidos, rigiendo para la primera la exigencia de verificar la edad. Diferencia que en parte se explica por ser la verificación de edad más complicada cuando el acceso a un servicio no implica una transacción financiera directa, en la que la posesión de una tarjeta de crédito válida aporta tanto la garantía financiera como la verificación implícita de la edad y del consiguiente derecho de la persona a apostar.

Como ejemplos de métodos adecuados para verificar la edad se han sugerido los siguientes[49]:

— Confirmación de ser propietario de una tarjeta de crédito u otra forma de pago cuya expedición requiera ser mayor de edad.

— Un servicio profesional de gestión de la identidad digital personal cuyas comprobaciones se funden en una base de datos independiente y fiable, como el censo electoral.

— Otras pruebas comparables de ser propietario de una cuenta que verifique la edad de forma efectiva.

En todo caso, ya se trate de la implantación de sistemas de verificación de la edad o de otros procedimientos, es general la opinión que considera que los proveedores de contenidos para adultos tienen una especial responsabilidad en evitar el acceso de menores, que debe poder serles exigida hasta donde alcance la jurisdicción nacional. En este sentido, el Informe «Online Safety» defiende una novedosa propuesta relacionada con la autoridad nacional que asigna los dominios de Internet: «ningún sitio .uk debería ofrecer pornografía para adultos sin obstáculos que eviten visitas de menores.» [50]

---

[48] COM(2012) 196 final, p. 13

[49] «Online Safety», op. cit., p. 22.

[50] Ibídem, p. 22.

Relacionadas con las herramientas de filtrado, se encuentran las medidas de clasificación por edades y etiquetado de contenidos.

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico establece que las Administraciones Públicas «estimularán, en particular, el establecimiento de criterios comunes, acordados por la industria, para la clasificación y etiquetado de contenidos» (artículo 18).

El reto en esta materia es el de la interoperabilidad, al menos a escala europea, o por decirlo en palabras de la «Estrategia europea en favor de una Internet más adecuada para los niños», contar a dicha escala «con un enfoque generalmente aplicable, transparente y coherente con respecto a la clasificación por edades (…) para diversos contenidos y servicios (incluidos los juegos en línea, las aplicaciones y los contenidos educativos y culturales en general) y explorar soluciones innovadoras (por ejemplo, calificación por los usuarios o automática)»[51].

Los poderes públicos españoles deben en este sentido intensificar sus esfuerzos en la línea marcada por la Ley de servicios de la sociedad de la información y comercio electrónico y la Ley general de comunicación audiovisual, situándolos en el marco de los sistemas de clasificación y etiquetado promovidos a escala de la Unión Europea.

En relación con los riesgos que afectan a la privacidad o protección de los datos de carácter personal y otros riesgos de contacto se ha discutido sobre la implantación de mecanismos de verificación de la edad y la configuración de los parámetros de privacidad en las redes sociales.

Varios comparecientes como Víctor Calvo-Sotelo, Borja Adsuara o Manuel Escalante, llamaron la atención sobre el riesgo que una mayor exigencia de la legislación española en aspectos como el de la verificación de la edad, puede tener en cuanto a penalizar a las empresas españolas. En este mismo sentido se pronunció Sebastián Muriel que, además de este efecto, puso de manifiesto la paradoja que suponen planteamientos restrictivos del marco regulador nacional en un contexto social que favorece el creciente uso por los menores de las nuevas tecnologías, produciéndose situaciones contrarias a las que se pretenden evitar (denuncias de usuarios por motivos de edad, como forma de acoso, con la intención de provocar vacío y exclusión social; quejas de padres por cerrar cuentas

[51] COM(2012) 196 final, p. 14.

de sus hijos; oposición de los padres a facilitar su DNI y libro de familia para autorizar el registro en Tuenti de sus hijos menores de catorce años), y paradoja también en un contexto de acelerada evolución tecnológica, con la irrupción de nuevas redes (Whatsapp, Line, WeChat, etc.) que no se rigen por los patrones de comportamiento y control comunes en las redes principales. La conclusión de S. Muriel fue: «cada vez tiene menos sentido poner el foco en el registro y la verificación de su edad, especialmente en entornos de movilidad, sino en la propia utilización segura y responsable de las TIC por los menores».

En este capítulo, la autorregulación continúa siendo la herramienta de acción principal, correspondiendo al poder público una acción de fomento de la misma, al tiempo que su acción normativa, en un país como España, miembro de la Unión Europea, debe situarse en el marco que en este nivel se establezca. Una de las regulaciones de este marco, de especial trascendencia, es la de protección de los datos de carácter personal, contenida actualmente en la Directiva 95/46/CE, pero que se encuentra en proceso de revisión, estando planteada, en sustitución de la misma, una propuesta de Reglamento (que como tal sería de aplicación directa en los Estados miembros), que aborda importantes aspectos, a algunos de los cuales ya nos hemos referido, como el de su ámbito territorial de aplicación, el «derecho al olvido» (considerando 53 y artículo 17), la recepción por vez primera de los menores como grupo con especiales necesidades de protección (considerando 25 y, entre otros, artículo 13), el principio de protección de los datos desde el diseño y por defecto (artículo 23) o el principio de «ventanilla única» («one-stop-shop») sobre los que una posición definida y clara de los Gobiernos de los Estados miembros cobra singular relevancia.

Finalmente, en relación tanto con los riesgos de contenido, como con los riesgos de contacto (en particular el ciberacoso y el «cibergrooming») un tipo de medida técnica considerada imprescindible lo constituyen las herramientas de denuncia habilitadas por redes sociales y otros proveedores de servicios de Internet.

Se trata de una medida que, aun confiada al campo de la autorregulación, debe recabar una mayor atención y seguimiento por parte de los poderes públicos, para promover no sólo su implantación general, sino también para que reúna las condiciones de visibilidad, accesibilidad, claridad y soporte humano adecuados, así como de conexión ágil cuando

proceda con las líneas de ayuda a cargo de las organizaciones de protección de menores o con las autoridades policiales y judiciales. Además, estas herramientas, como señala la «Estrategia europea en favor de una Internet más adecuada para los niños», servirán también al objetivo de facilitar a los ciudadanos la denuncia de los ciberdelitos[52].

Complementarias de estas herramientas de denuncia son los recursos paralelos disponibles en las organizaciones de protección de menores y en las páginas web de los cuerpos policiales, sobre los que en alguna comparecencia se mencionó su falta de visibilidad (Manuel Escalante) o incluso se apuntó la necesidad de implantar un «ciber112» (José Miguel Rosell).

Además de las medidas de carácter técnico señaladas, un nivel aceptable de seguridad en la Red tiene que ver también con la protección de los menores en relación al juego «online» y a la publicidad «online». En el primero de dichos ámbitos la acción de los poderes públicos debe poder asegurar la aplicación por las empresas responsables, de mecanismos eficaces de verificación de la edad, además de profundizar por vía normativa en la protección de los menores, especialmente desde el punto de vista de la publicidad. Frente a los riesgos asociados a la publicidad en línea, la autorregulación y la supervisión de los poderes públicos, y, si fuera necesario, la acción normativa de éstos, deben dirigirse, según la «Estrategia europea en favor de una Internet más adecuada para los niños», a asegurar «que las normas sobre publicidad en sitios web para niños permitan un nivel de protección comparable al de la publicidad en los servicios audiovisuales y que, en cuanto a la publicidad orientada a comportamientos no se creen segmentos para niños»[53].

Otro escalón de las acciones encaminadas a la protección de los menores proveniente de un nivel aceptable de seguridad de la Red, al que se refirieron algunos comparecientes (Eugenio Oñate, Jorge Flores), lo constituiría la medición por un tercero independiente de los parámetros de calidad que deben ser exigibles de las empresas proveedoras de servicios de Internet, con el fin de que los usuarios de Internet (también los menores y sus padres o tutores) puedan contar con una información fácilmente accesible, completa, comparable y fiable sobre tales parámetros.

---

[52] COM(2012) 196 final, p. 11.

[53] Ibídem, p. 15.

4.4. Protección a través de un sistema normativo y de aplicación de la Ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red

Una de las ideas también repetidas a lo largo de las comparecencias ante la Ponencia fue la de que el advenimiento de la sociedad de la información se ha producido con tal rapidez que no se ha visto acompañado de una cultura de seguridad que prevenga frente a los nuevos riesgos que presenta el uso de la Red (Manuel Escalante: «la revolución es de tal magnitud que hemos decidido vivir de espaldas al riesgo») ni de un marco institucional y normativo de protección adecuado, es decir, adaptado a la realidad de tales riesgos.

Además de la revisión y adaptación que proceda del Código Penal, especialmente en el marco de las obligaciones que para España se derivan tanto de los Convenios del Consejo de Europa de Budapest y Lanzarote, sobre ciberdelincuencia y sobre protección de los niños contra la explotación y el abuso sexual, respectivamente, como de la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil (Directiva 2011/92/UE) y de las recomendaciones indicadas por la comunidad científica o por las autoridades responsables de la aplicación de la Ley, fue general entre los comparecientes ante la Ponencia, sobre todo desde el ámbito de las fuerzas y cuerpos de seguridad del Estado y del Ministerio Fiscal y de las organizaciones de protección de los menores, la opinión favorable a una revisión en el campo del Derecho procesal que posibilite una mayor eficacia en las labores de investigación garantizando al propio tiempo los derechos de los ciudadanos y la integridad y autenticidad de las evidencias que se obtengan, revisión de particular interés en relación con la pornografía infantil, pero con una justificación que puede extenderse a otros tipos delictivos (por ejemplo, el «child grooming»), cuya comisión a través de Internet plantea un particular desafío en la lucha contra los mismos.

Con carácter general la «Estrategia europea en favor de una Internet más adecuada para los niños» alienta a los Estados miembros a la puesta en práctica de «instrumentos de investigación eficaces que potencien la capacidad de los investigadores para identificar a las víctimas de abusos sexuales, acompañados de salvaguardas eficaces para garantizar la responsabilidad democrática en el empleo de los mismos»[54].

[54] Ibídem, p. 17.

En este sentido un buen número de comparecientes abogaron por la figura del agente encubierto, actualmente regulada en el artículo 282 bis de la Ley de Enjuiciamiento Criminal en relación con la investigación de determinados delitos en la medida de su vinculación con la delincuencia organizada, pero que podría ser muy efectiva en el campo de la investigación tecnológica.

Óscar de la Cruz se refirió a esta figura como una técnica necesaria para hacer frente a la asimetría de la ciberdelincuencia, para poder ascender, por ejemplo, en la pirámide que representan los intercambios de archivos de pornografía infantil, más allá de las redes «peer-to-peer» y acceder a los ámbitos ocultos donde tienen lugar los intercambios de contenidos más violentos y graves. La preocupación por la persecución de la delincuencia oculta ha llevado a la creación por los Gobiernos del Reino Unido y de Estados Unidos de un grupo de trabajo para la búsqueda de soluciones al efecto.

En la misma línea Elvira Tejada defendió la ampliación de las posibilidades de aplicación de esta figura, que, en el campo de los delitos que se cometen a través de las TIC, requeriría, además de mantener las líneas básicas y esenciales de la figura (exigencia de autorización judicial o del Ministerio Fiscal, en atención a criterios de necesidad y proporcionalidad valorables en cada caso, y control pleno de la actuación del agente encubierto por parte del juez), de un régimen específico, en aspectos tales como la delimitación del ámbito de delitos a los que sería ampliable la aplicación de esta figura (ámbito que podría ser, a juicio de E. Tejada, el de la generalidad de los delitos que se cometen a través de las TIC, y teniendo en cuenta que con frecuencia las actividades ilícitas no están vinculadas a la delincuencia organizada, como ocurre por ejemplo con el acoso a menores), la delimitación entre el supuesto de navegación libre amparada en identidades supuestas a través de «nicknames», usual en Internet, y el de agente encubierto propiamente tal, que requiere autorización judicial, o el alcance de la exención de responsabilidad criminal por las actuaciones del agente encubierto en el desarrollo de la investigación.

También en relación con el ámbito de lo procesal, E. Tejada señaló que la retirada de contenidos de pornografía infantil o el bloqueo del acceso a los mismos que en la actualidad solicitan los jueces sobre la base del artículo 13 de la Ley de Enjuiciamiento Criminal y los artículos 8 y 11 de la Ley 34/2002 de servicios de la sociedad de la información y del comercio electrónico, encuentra un mayor respaldo en el proyecto

de Ley Orgánica de reforma del código Penal en curso de tramitación, al incluir entre sus novedades el reconocimiento expreso de la facultad de Jueces y Tribunales en tal sentido.

Finalmente, E. Tejada abogó también por una modificación de la Ley 25/2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, para, por un lado, que su aplicación para la investigación de los delitos que se cometan a través de las TIC no se vea limitada al ámbito delictivo acotado por la ley, nominalmente referido a los delitos graves y, por otro lado, para que obligue no sólo a «los operadores de servicios de comunicaciones» (para ser exactos «los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones» —artículo 2 de esta Ley—), sino en general a los prestadores de servicios de Internet.

Una sentencia del Tribunal de Justicia de la Unión Europea, de 8 de abril de 2014, declaró inválida la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, cuya transposición al Derecho español constituía el objetivo principal de la Ley 25/2007, y aunque tal declaración no afecta a la vigencia de la Ley española, cuya regulación, por otro lado, contiene algunos de los elementos (por ejemplo, la necesidad de previa autorización judicial para la cesión de los datos conservados) cuya ausencia en la Directiva fundamenta en buena parte el reproche de invalidez de la sentencia, ésta constituye indudablemente una referencia obligada en una futura revisión de aquella Ley.

Descendiendo del plano normativo al operacional, la «Estrategia europea en favor de una Internet más adecuada para los niños» enfatiza el objetivo de la lucha contra los abusos sexuales y la explotación sexual de los niños, en el que el nivel de la cooperación internacional resulta crucial, aunque a nivel nacional, las acciones pueden intensificarse en varias direcciones:

— Reforzar los recursos policiales destinados a la lucha contra la pornografía infantil en Internet, entre ellos, la I+D en soluciones técnicas para las investigaciones policiales, que permitan la identifica-

ción de los materiales de pornografía infantil, con vistas a su rápida retirada, a la identificación y rescate de las víctimas y a la puesta a disposición de la justicia de los autores, basada en procedimientos que garanticen la obtención e integridad de las pruebas.

— Reforzar la coordinación entre las unidades especializadas de las diferentes Fuerzas y Cuerpos de Seguridad del Estado y autonómicas.

— Reforzar la cooperación entre las empresas proveedoras de servicios, líneas de denuncia de organizaciones privadas y cuerpos policiales, para actuar con rapidez en la retirada del material ilícito.

V. *Conclusiones*

1. Dentro del escenario global de acelerada evolución tecnológica que las redes de alta velocidad, los nuevos dispositivos móviles, la web 2.0 y la convergencia de medios suponen para la conectividad e interactividad en Internet, los niños, adolescentes y jóvenes aparecen como «nativos digitales», al menos en el doble sentido de que para ellos Internet es una realidad natural, no contrapuesta a la del mundo físico, formando ambas parte de la misma realidad, y en el de ser usuarios intensivos, con algunas tendencias bien reflejadas en la evolución estadística: acceso a Internet a edades cada vez más tempranas, uso creciente a mayor edad, pluralidad de actividades «online» con presencia destacada de las comunicativas y participación en las redes sociales, y transformación del lugar y medios de conectividad como consecuencia de la irrupción de los dispositivos móviles.

La condición de «nativos digitales» no supone sin embargo «per se» un alto grado de posesión de competencias digitales. Antes bien, hablar de tal condición y de la existencia de una «brecha digital» entre los menores y sus padres, que, aunque con base real se ha exagerado también con frecuencia, oscurece la necesidad de emprender las acciones oportunas para garantizar la capacitación efectiva en aquellas competencias.

2. Internet ofrece enormes oportunidades pero al propio tiempo presenta una serie de riesgos, constituyendo precisamente un reto para

las políticas públicas encontrar el equilibrio adecuado entre unas y otras, sin que un énfasis excesivo en las oportunidades, sin medidas de protección, incremente las posibilidades de riesgo, ni un énfasis excesivo en estas medidas ahogue aquéllas.

En este contexto los menores presentan necesidades específicas, tanto desde la perspectiva de las oportunidades como desde la perspectiva de los riesgos.

3. La tipología de riesgos que pueden afectar a los menores como consecuencia del uso de Internet es muy variada, emergiendo de la nutrida información aportada por los comparecientes una división primaria que permitiría distinguir entre riesgos de Internet y riesgos en Internet. Los riesgos *de* Internet serían riesgos intrínsecos a Internet, no en el sentido de que sean inevitables sino en el de que su existencia es inseparable de la de Internet, mientras que los riesgos *en* Internet serían aquéllos asociados a situaciones que encuentran en este medio un soporte idóneo para producirse, aunque existían y existen también fuera del mismo.

4. Entre los riesgos de Internet, o intrínsecos a este medio, la Ponencia comparte la preocupación expresada por algunos comparecientes en relación con la descontextualización que caracteriza el proceso de comunicación a través de Internet, por las mayores repercusiones que puede tener para los menores, tanto desde el punto de vista de los contactos «online» con nuevas personas, al dificultar la obtención de una imagen cabal de éstas, dado que la mediación de la pantalla no permite contar con los signos de advertencia de lugar, tiempo y contexto que en el mundo físico previenen de ciertos riesgos, como desde el punto de vista de los problemas que a largo plazo puede tener la imagen proyectada por el menor a través de Internet, desconectada de las circunstancias concretas en que la información de aquél se vertió en cada momento.

De igual modo debe prestarse atención al problema del uso excesivo, que puede llegar a provocar un trastorno adictivo. Aunque las tasas de prevalencia de este riesgo no son elevadas, no debe minusvalorarse este problema, por las consecuencias negativas que puede tener en el desarrollo de los menores.

5. Especial preocupación suscitan determinados riesgos que, aun no siendo propios de Internet, encuentran en esta plataforma un soporte idóneo para producirse, pudiendo distinguirse entre los riesgos derivados de la circulación de contenidos en Internet (riesgos de contenidos) asociados a comportamientos de particular gravedad (pornografía infantil y otros contenidos ilícitos) o a comportamientos que, aun siendo lícitos, resultan nocivos para los menores, en cuanto pueden causarles un perjuicio físico, psíquico o moral (exposición a pornografía para adultos y otros contenidos inapropiados), y riesgos derivados de determinadas conductas en las que el menor tiene una u otra participación, voluntaria o involuntaria (riesgos de contacto), que pueden afectar a bienes jurídicos diversos, como la integridad física o psíquica del menor («ciberbullying», «cibergrooming», violencia de género digital, juego «online»), la intimidad y la protección de los datos de carácter personal («sexting», problemas a largo plazo para la propia imagen, cosificación de la identidad digital, uso malicioso de la información personal) y la propiedad intelectual (piratería digital).

Algunos de los anteriores riesgos pueden estar asociados a conductas delictivas y como tales forman parte del fenómeno de la «ciberdelincuencia», por lo que la prevención y la respuesta eficaz frente a los mismos constituyen un objetivo irrenunciable, derivado de la importancia que el ordenamiento jurídico concede a la protección de determinados bienes jurídicos, pero ello no resta relevancia a los demás riesgos, entre ellos, la exposición a contenidos nocivos, la violencia de género digital, el juego «online», determinados riesgos que afectan a la intimidad y a la protección de datos de carácter personal (los problemas a largo plazo que puede ocasionar la información personal vertida en Internet y la cosificación de la identidad digital derivada de prácticas invasivas de publicidad conductual) y el hábito de consumo de contenidos digitales a través de páginas web de descargas ilícitas, de todos los cuales la Ponencia ha hecho un análisis individualizado en epígrafes anteriores.

6. Los valores que encarnan los derechos fundamentales de la persona, reconocidos en la Constitución española y en los tratados internacionales, deben regir tanto en el mundo físico como en el mundo digital, y, en el caso de los menores, garantizan el «interés superior» de los

mismos como «consideración primordial» para autoridades públicas e instituciones privadas en todos los actos que les conciernan.

7. La existencia de diferentes actores con intereses relevantes en la materia objeto de estudio (poderes públicos, niños y padres, escuela y educadores, organizaciones privadas del sector de acción social y empresas de distinta índole relacionadas con la sociedad de la información), plantea la cuestión básica del papel respectivo que corresponde a los dos círculos principales en los que aquellos actores se encuadran, Estado y sociedad, que se corresponden con dos enfoques normativos diferentes (regulación y autorregulación), apuntando la respuesta a dicha cuestión a un sistema de responsabilidad compartida.

La trayectoria de la Unión Europea, en la que se han ido entrelazando, en atención a las diferentes categorías de riesgos, la autorregulación y la co-regulación con marcos normativos que identifican la protección de los menores en Internet entre sus principios básicos (Directiva de 2010 de servicios de comunicación audiovisual, Directiva de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, o, aún en fase de examen, la propuesta de Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos) constituye un modelo plausible a nivel nacional, en el que, desde el punto de vista de la autorregulación, deben fomentarse las alianzas público-privadas, entendiendo inherente a esta figura la participación activa del Gobierno en la negociación de los compromisos propuestos para su voluntaria adopción por las empresas privadas participantes.

8. La existencia de actores diferentes y enfoques normativos diversos (regulación y autorregulación) pone de relieve la necesidad, en paralelo a la planteada a nivel europeo («Estrategia europea en favor de una Internet más adecuada para los niños»), de una estrategia a nivel nacional, como palanca imprescindible de las políticas públicas referidas a las necesidades de los menores en Internet, en el entendimiento de que sus claves conceptuales son la coordinación y la coherencia.

La coordinación y coherencia deben además promoverse a través de concretas fórmulas organizativas que traduzcan un paso decidido desde la mera agregación de múltiples iniciativas públicas y privadas a una visión estratégica con alto liderazgo y compromisos a largo plazo, idea que puede considerarse uno de los hilos conductores de prácticamente todos los comparecientes ante la Ponencia.

9. Una palanca para la acción también imprescindible en todo lo relacionado con Internet, y por tanto también en lo que se refiere a las necesidades de los menores, es la cooperación internacional, tanto en el nivel de decisión político-normativa o de influencia en el mismo (nivel que para los países miembros de la Unión Europea tiene en las instituciones de ésta la plataforma natural de acción, sin olvidar otras, bien regionales como el Consejo de Europa, o de ámbito más amplio —OCDE, UIT, o el mismo Foro para la Gobernanza de Internet) como en el nivel operacional, nivel este último en el que la importancia de la cooperación se proyecta en varias vertientes: la armonización de los marcos estadísticos nacionales, para medir de forma consistente los aspectos de acceso, uso y prevalencia de riesgos de Internet en los menores; la cooperación transfronteriza de las autoridades policiales en la persecución y lucha contra el delito; la actividad de las redes de líneas de ayuda y centros de seguridad en Internet, respectivamente, INHOPE e INSAFE, originariamente europeas, pero hoy convertidas en modelos de cooperación internacional; las actividades de concienciación y sensibilización, de las que constituye un notable ejemplo el «Día para una Internet más segura» («Safer Internet Day»), organizada por INSAFE, cuya convocatoria cobra cada año mayor importancia; o las iniciativas que promueven estándares internacionales para la interoperabilidad de muchas técnicas, como los controles parentales en plataformas o dispositivos.

10. La Ponencia enuncia cuatro objetivos para una estrategia de oportunidades y uso seguro y responsable de Internet para los menores:

1) Capacitación en competencias digitales y sensibilización general.
2) Fomento de contenidos en línea de calidad para niños y jóvenes.
3) Protección a través de un nivel de seguridad aceptable de Internet.

4) Protección a través de un sistema normativo y de aplicación de la Ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red.

11. El epicentro de las acciones dirigidas a la capacitación de los menores en competencias digitales, y así lo expusieron recurrentemente los comparecientes en la Ponencia, lo constituye el aprendizaje escolar de las mismas, con un contenido que incluye pero no se limita a la seguridad digital. Buscar, jerarquizar, almacenar, utilizar, producir e intercambiar información, comunicarse y participar en redes de colaboración, gestionar la identidad digital y conocer los riesgos existentes en la Red y ser capaz de afrontar los mismos, son componentes básicos de aquel contenido, que apunta al concepto de «ciudadanía digital», que enfatiza las oportunidades creativas y de participación de Internet para los menores.

Constituyendo las competencias digitales, «competencias clave», en el sentido acuñado por la Recomendación del Parlamento Europeo y del Consejo de 18 de diciembre de 2006, sobre «competencias clave para el aprendizaje permanente», el enfoque primario en cuanto a su vertebración en el currículo educativo debe basarse en la transversalidad, sin perjuicio de su tratamiento a través de asignaturas específicas en las diferentes etapas del itinerario educativo.

12. Presupuesto y complemento necesarios de la vertebración en el currículo educativo de las competencias digitales lo constituyen, respectivamente, la formación de maestros y profesores, que debe comenzar en las propias escuelas universitarias, cuyos planes de estudio deben revisarse, sobre todo desde la perspectiva de la capacitación para adaptarse a la evolución tecnológica, y la formación de los padres que, como en otras actividades que comportan riesgos, deben acompañar a sus hijos en su aprendizaje.

13. Las acciones de capacitación en competencias digitales basadas en el aprendizaje reglado, que remiten a medidas normativas, deben complementarse con acciones de sensibilización general, sobre el uso seguro y crítico de las tecnologías de la sociedad de la información, basadas en el aprendizaje informal, dirigidas tanto a los

niños y adolescentes, como a padres y profesores y demás agentes implicados.

El reto en este apartado lo constituye el enmarcar la diversidad de iniciativas existentes y las que se planteen en el futuro en una estrategia que las coordine y alinee, valiéndose de alianzas público-privadas, que involucren también a los medios de comunicación. Además los contenidos deben ser de calidad y atractivos, tener en cuenta las diferencias de desarrollo según la edad entre los menores y fomentar la participación misma de los jóvenes como protagonistas de dichas acciones.

Debe promoverse asimismo la existencia de protocolos de actuación en las escuelas, en relación con las situaciones en las que los niños aparecen como agresores, como ocurre con el «ciberbullying».

14. Estrechamente relacionado con el objetivo de la capacitación en competencias digitales, se encuentra el de fomento de contenidos en Internet de alta calidad para niños y jóvenes, lo que entraña el fomento de la innovación y los desarrollos destinados a la creación de este tipo de contenidos y de las iniciativas de los propios niños y adolescentes, alentando en ellos una actitud no limitada al consumo sino al uso positivo de Internet y a la creatividad.

15. Aun cuando la alfabetización digital y mediática de los menores, con la escuela como piedra angular de la misma, constituye el núcleo de una estrategia sobre las necesidades de los menores en Internet, la Ponencia comparte la opinión de que la protección de los mismos debe provenir también de un nivel de seguridad aceptable de la Red.

Las acciones encaminadas a este objetivo son fundamentalmente de orden técnico y habitualmente confiadas a la autorregulación, aunque el poder público puede hacer mucho en este campo, incluso desde la sola acción de fomento, sin descartar una acción normativa que obligue a las empresas afectadas a establecer determinadas medidas, si la autorregulación no consiguiese los objetivos propuestos.

Así, los esfuerzos desplegados por el Gobierno británico desde el mes de julio de 2013 para obtener de los principales motores de bús-

queda un compromiso firme en relación con el bloqueo del acceso a imágenes de pornografía infantil y la retirada de dichas imágenes, que ha supuesto el desarrollo por dichas empresas de tecnologías de filtrado e identificación de imágenes, demuestran que el impulso gubernamental puede suponer avances significativos en la colaboración de las empresas prestadoras de servicios en Internet en la elevación del nivel de seguridad en la Red para la protección de los menores.

16. La acción del poder público en este sentido no se limita a la lucha contra la lacra del abuso sexual infantil, de la que la pornografía infantil es una de sus manifestaciones, sino que debe incluir también la promoción de medidas técnicas que preserven a los menores frente al riesgo de exposición a contenidos nocivos. Entre tales medidas hay que considerar:

— Las herramientas de control parental, cuya utilidad sobre todo para proteger a los niños más pequeños, no sólo de los riesgos de contenidos, es generalmente reconocida, y cuya disponibilidad y uso debe promoverse, fomentando el compromiso de la industria en tal sentido, sin descartar su aplicación desde la infraestructura para proporcionar soluciones integrales familiares, aplicables a todos los dispositivos dependientes de una misma cuenta de acceso a Internet.

— La clasificación por edades y etiquetado de contenidos, que debe avanzar con el objetivo de la interoperabilidad y, por tanto, en el marco de sistemas promovidos a escala de la Unión Europea e internacional.

— Los mecanismos de verificación de la edad u otros procedimientos eficaces en la restricción del acceso de los menores a sitios web que ofrezcan contenidos para adultos, que deben poder ser exigidos a los responsables de tales sitios, al menos hasta donde alcance la jurisdicción nacional.

17. Enderezadas también al objetivo de la protección de los menores proveniente de un nivel de seguridad aceptable en la Red, se sitúan las medidas que desde las redes sociales pueden adoptarse en relación con la verificación de la edad y la configuración de los paráme-

tros de privacidad, ámbito en el que el poder público debe promover el mayor nivel de avance posible a través de la autorregulación, al tiempo que su acción normativa, en un país como España, miembro de la Unión Europea, debe situarse en el marco que en este nivel se establezca. A este respecto, cobra singular relevancia una posición definida y clara de los Gobiernos de los Estados miembros en relación con el proceso de revisión del marco regulador de la protección de datos de carácter personal, proceso plasmado en una propuesta de Reglamento que sustituiría la vigente Directiva 95/46/CE, y que aborda importantes aspectos como el de su ámbito de aplicación territorial, el «derecho al olvido» (con una plausible explícita mención a su relevancia para los menores —artículo 17 y considerando 53, que afirma: «Este derecho es particularmente pertinente si los interesados hubieran dado su consentimiento siendo niños, cuando no se es plenamente consciente de los riesgos que implica el tratamiento y más tarde quisiera suprimir tales datos personales especialmente en Internet»—), la recepción de los menores como grupo con especiales necesidades de protección (considerando 25 —«los niños necesitan una protección específica de sus datos personales»— y, entre otros, artículo 8 que fija en trece años el umbral por debajo del cual padres o tutores deben prestar su consentimiento para el tratamiento de datos de carácter personal del niño, estableciéndose para el responsable del tratamiento la obligación de hacer «esfuerzos razonables para obtener un consentimiento verificable, teniendo en cuenta la tecnología disponible»), la adopción del principio de protección de datos desde el diseño y por defecto (artículo 23) o el principio de «ventanilla única» («one-stop-shop») en la relación con las autoridades nacionales de protección de datos.

18. Las herramientas de denuncia habilitadas por redes sociales y otros proveedores de servicios de Internet son imprescindibles en relación tanto con los riesgos de contenidos (contenidos ilícitos y contenidos nocivos), como con los riesgos de contacto (en particular el ciberacoso y el «cibergrooming») y por ello, aun confiadas al campo de la autorregulación, deben recabar una mayor atención y seguimiento por parte de los poderes públicos, para promover no sólo su implantación general, sino también para que reúnan las condiciones de visibilidad, accesibilidad, claridad y soporte humano adecuados,

así como de conexión ágil cuando proceda con las líneas de ayuda a cargo de las organizaciones de protección de menores o con las autoridades policiales y judiciales.

19. Un nivel aceptable de seguridad de la Red tiene que ver también con la protección de los menores en relación con el juego «online» y con la publicidad «online». En el primero de dichos ámbitos, la acción de los poderes públicos debe poder asegurar la aplicación por las empresas responsables, de mecanismos eficaces de verificación de la edad, además de profundizar por vía normativa en la protección de los menores, desde el punto de vista de la incidencia de los distintos tipos de juego y la publicidad.

Frente a los riesgos asociados a la publicidad «online», la autorregulación y la supervisión de los poderes públicos y, si fuera necesario, su acción normativa, deben dirigirse a asegurar que las normas sobre publicidad en sitios web para niños permitan un nivel de protección comparable al de la publicidad en los servicios audiovisuales y, que, en cuanto a la publicidad conductual no crea segmentos para niños.

20. La protección de los menores en Internet no puede prescindir de un sistema normativo y de aplicación de la Ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red.

A este respecto, además de la revisión y adaptación que proceda del Código Penal, especialmente en el marco de las obligaciones que para España se derivan tanto de los Convenios del Consejo de Europa de Budapest y Lanzarote, sobre ciberdelincuencia y sobre protección de los niños contra la explotación y el abuso sexual, respectivamente, como de la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil (Directiva 2011/92/UE), y de las recomendaciones indicadas por la comunidad científica y las autoridades responsables de la aplicación de la Ley, fue general entre los comparecientes ante la Ponencia, sobre todo desde el ámbito de las fuerzas y cuerpos de seguridad del Estado y del Ministerio Fiscal y de las organizaciones de protección de los menores, la opinión favorable a una revisión en el campo del Derecho procesal que posibilite una mayor eficacia en

las labores de investigación de la ciberdelincuencia, garantizando al propio tiempo los derechos de los ciudadanos y la integridad y autenticidad de las evidencias que se obtengan, revisión de particular interés en relación con la pornografía infantil, pero con una justificación que puede extenderse a otros tipos delictivos (por ejemplo, el «grooming»), cuya comisión a través de Internet plantea un particular desafío en la lucha contra los mismos.

21. Para el objetivo de la lucha contra el abuso sexual infantil resulta crucial la cooperación internacional, aunque también a nivel nacional las acciones pueden intensificarse en varias direcciones:

— Reforzar los recursos policiales destinados a la lucha contra la pornografía infantil en Internet, entre ellos, la I+D en soluciones técnicas para las investigaciones policiales, que permitan la identificación de los materiales de pornografía infantil, con vistas a su rápida retirada, a la identificación y rescate de las víctimas y a la puesta a disposición de la justicia de los autores, basada en procedimientos que garanticen la obtención e integridad de las pruebas.

— Reforzar la coordinación entre las unidades especializadas de las diferentes Fuerzas y Cuerpos de Seguridad del Estado y autonómicas.

— Reforzar la cooperación entre las empresas proveedoras de servicios, líneas de denuncia de organizaciones privadas y cuerpos policiales, para actuar con rapidez en la retirada del material ilícito.

VI. *Recomendaciones*

1. Alianzas público-privadas

La Ponencia considera que la autorregulación constituye un enfoque imprescindible en relación con la protección de los menores en Internet, en atención a su capacidad de adaptación al desarrollo tecnológico y a las tendencias sociales, y que el Gobierno debe profundizar en dicho enfoque, asumido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (artículo 18) y la Ley General de la Comu-

nicación Audiovisual (artículo 12), que incluye el fomento de alianzas público-privadas, entendiendo inherente a este concepto la participación activa del Gobierno en la negociación de los compromisos propuestos para su voluntaria adopción por las empresas privadas participantes.

La contribución de las empresas en cualquiera de las facetas que tienen que ver con la protección de los menores en Internet debe fomentarse mediante la creación de premios o «sellos» de responsabilidad social específicos.

El enfoque de la autorregulación debe entrelazarse, cuando sea necesario en función de la naturaleza y gravedad de los riesgos a los que se enfrentan los menores en Internet, con la iniciativa o acción normativa del Estado, desde la óptica del «interés superior» de los menores como «consideración primordial» para autoridades públicas e instituciones privadas en todos los actos que les conciernan, de conformidad con la Convención de las Naciones Unidas sobre los Derechos del Niño (artículo 3) y la Carta de los Derechos fundamentales de la Unión Europea (artículo 24).

2. Cooperación internacional

La naturaleza dinámica y global de Internet hace que objetivos y acciones a nivel nacional deban enmarcarse en los que se planteen a nivel internacional, adquiriendo así la cooperación internacional un relieve fundamental como palanca de acción de los Gobiernos.

En el nivel de decisión político-normativa o de influencia en el mismo, las instituciones de la Unión Europea constituyen para un país miembro de ésta como España la plataforma primaria de acción, siendo particularmente relevante en el momento actual una posición definida y clara del Gobierno en relación con el proceso de revisión del marco regulador de la protección de datos de carácter personal, proceso plasmado en una propuesta de Reglamento que sustituiría a la vigente Directiva 95/46/CE, y que, entre otros importantes aspectos, aborda la recepción de los menores como grupo con especiales necesidades de protección, el «derecho al olvido», o la adopción del principio de protección de datos desde el diseño y por defecto.

La cooperación internacional debe comprender otras plataformas relevantes, bien regionales, como el Consejo de Europa, o de ámbito más amplio (entre ellas, OCDE, UIT, o el Foro para la Gobernanza de Internet).

La cooperación internacional tiene también un relevante cometido en el plano operacional, con distintas vertientes en las que deben desplegarse los esfuerzos del Gobierno: la armonización de los marcos estadísticos nacionales, para medir de forma consistente los aspectos de acceso, uso y prevalencia de riesgos de Internet en los menores; la cooperación transfronteriza de las autoridades policiales en la persecución y lucha contra el delito; la actividad de las redes de líneas de ayuda y centros de seguridad en Internet, respectivamente, INHOPE e INSAFE, originariamente europeas, pero hoy convertidas en modelos de cooperación internacional; las actividades de concienciación y sensibilización, de las que constituye un notable ejemplo el «Día para una Internet más segura» («Safer Internet Day»), organizada por INSAFE, cuya convocatoria cobra cada año mayor importancia; o las iniciativas que promueven estándares internacionales para la interoperabilidad de muchas técnicas, como los controles parentales en plataformas o dispositivos.

3. Estrategia, coordinación y coherencia

La Ponencia reconoce la contribución de los instrumentos estratégicos aprobados por el Gobierno con incidencia en la materia de las necesidades de los menores en Internet, entre ellos la Agenda Digital para España y el «II Plan Estratégico nacional para la infancia y la adolescencia 2013-2016 (II PENIA)», si bien del conjunto de las comparecencias habidas ante la Ponencia se desprende la necesidad de realzar el valor de la estrategia como palanca para la acción en relación con los retos que plantean aquellas necesidades.

En este sentido una estrategia gubernamental renovada en este ámbito debe tener carácter global, esto es, contemplar las oportunidades y los riesgos de y en Internet para los menores y comprender las acciones de toda la Administración General del Estado, e incorporar los siguientes objetivos fundamentales:

A) Fines de la acción:

1) Capacitación de los menores en competencias digitales y sensibilización general
2) Fomento de contenidos en línea de calidad para niños y jóvenes.

3) Protección de los menores a través de un nivel de seguridad aceptable de Internet.

4) Protección de los menores a través de un sistema normativo y de aplicación de la Ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red.

B) Palancas para la acción:

1) Incrementar la coordinación de todas las acciones que está realizando el Gobierno con particular atención a los Ministerios de Interior, de Industria, Energía y Turismo, de Sanidad, Servicios Sociales e Igualdad, de Justicia y de Educación, Cultura y Deporte.

2) Dotar a todas las acciones del Gobierno de coordinación y coherencia aprovechando sinergias.

3) Promover un modelo organizativo ad hoc, concebido al efecto.

4) Promover las acciones de la Administración General del Estado en las Comunidades Autónomas dentro de sus competencias.

En este sentido, aun reconociendo el interés de figuras como la de un «Alto Comisionado Digital», en la estela del «Chief Digital Officer» (CDO) existente en algunas Administraciones del mundo anglosajón, la Ponencia considera que, sin separarse de las fórmulas organizativas típicas de la Administración pública española, es posible avanzar, en las políticas públicas relacionadas con la sociedad de la información en general y con la protección y necesidades de los menores en Internet en particular, en la dirección que permita una visión estratégica con alto liderazgo y compromisos a largo plazo.

Si en el modelo actual las competencias públicas relacionadas con Internet se sitúan en diferentes centros ministeriales, en concreto a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, incardinada en el Ministerio de Industria, Energía y Turismo, con el apoyo de una relevante entidad, RED.ES, a cuyas acciones se unen las de la Secretaría de Estado de Educación, la Secretaría de Estado de Asuntos Sociales, la Secretaría de Estado de Seguridad, a través de los Cuerpos y Fuerzas de Seguridad del Estado, y del Ministerio de Justicia complementándose con las que corresponden, desde distintos ángulos, a la Comisión Nacional de los Mercados y la Competencia (creada por Ley

3/2013 de 4 de junio, que agrupó las funciones de distintos organismos reguladores, entre ellos la Comisión del Mercado de las Telecomunicaciones y el Consejo Estatal de Medios Audiovisuales) y a la Agencia Española de Protección de Datos (regulada en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal), la Ponencia considera que el Gobierno debe revisar, en la línea de los modelos existentes en la Unión Europea y en sus países miembros, incluida la reflexión sobre una figura del tipo de la de un Alto Comisionado Digital, el engarce de todas estas piezas para que en su estructura y funciones incorporen como área prioritaria los riesgos y oportunidades de los menores en relación con Internet, y se cumplan en esta área las exigencias derivadas de las ideas de estrategia, coordinación y coherencia.

Al propio tiempo, la Ponencia considera que, si bien la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, contempla que uno de los Adjuntos del Defensor del Pueblo se haga cargo de modo permanente de los asuntos relacionados con los menores, podría darse un paso más, a través de la creación en el Defensor del Pueblo, como Alto Comisionado de las Cortes Generales para la defensa de los derechos comprendidos en el Título I de la Constitución (entre ellos los reconocidos a los niños en el artículo 39), de un Adjunto Tercero, con funciones específicas de «Defensor del menor», que incorporasen explícitamente el área de la protección de los menores en Internet, lo que requeriría modificar la Ley Orgánica 3/1981, de 6 de abril, del Defensor del Pueblo.

4. Alfabetización digital y sensibilización general

Desde la perspectiva, compartida por la Ponencia, que considera la alfabetización digital de los menores, esto es, la capacitación de éstos en competencias digitales, el núcleo de una estrategia sobre las necesidades de los menores en Internet, con la escuela como piedra angular de dicha capacitación, que no se limita a la seguridad digital, sino que apunta a un concepto más amplio (que entraña el uso seguro y crítico de las tecnologías de la sociedad de la información para el trabajo, el ocio y la comunicación, y que comprende tanto el conocimiento de los riesgos de y en Internet y los medios para afrontarlos como las oportunidades creativas y de participación de Internet), la Ponencia entiende que el Gobierno,

sin perjuicio de las competencias de las Comunidades Autónomas, debe garantizar en la vertebración del currículo educativo desde las primeras etapas el aprendizaje efectivo de las mencionadas competencias, basado en la transversalidad, en cuanto competencias clave, en línea con la Recomendación del Parlamento Europeo y del Consejo de 18 de diciembre de 2006, sobre «competencias clave para el aprendizaje permanente», sin perjuicio de su tratamiento a través de asignaturas específicas en las diferentes etapas del itinerario educativo.

Asimismo, toda vez que la formación de maestros y profesores constituye presupuesto necesario del aprendizaje escolar de las competencias digitales, el Gobierno debe promover dicha formación, para que las universidades, en ejercicio de su autonomía, planteen la revisión de los planes de estudio de los grados y másters de las escuelas universitarias donde se forman los futuros maestros, y de modo más general, puesto que la «seguridad desde el diseño» es un concepto que puede aplicarse no sólo a los productos o la prestación de servicios, sino también a la formación, de los planes de carreras y estudios de postgrado técnicos, para contemplar la capacitación profesional en ciberseguridad.

De forma complementaria a las anteriores acciones, tendentes a una formación de carácter reglado, la Ponencia considera, tras escuchar a todos los comparecientes ante la misma, que debe impulsarse la concienciación sobre el uso seguro y crítico de las tecnologías de la sociedad de la información, puesto que el problema de la protección de los menores en el uso de la Red es un problema de la sociedad en su conjunto y que es un aspecto clave para conseguir una internet más segura, dado que las acciones de prevención son las más efectivas.

Dicho objetivo debe dirigirse a sensibilizar a todos los agentes y basarse en las siguientes coordenadas:

— Universalidad de sus destinatarios: los menores, padres, abuelos, educadores, fuerzas y cuerpos de seguridad del Estado, fiscales y jueces y profesionales de los medios de comunicación.

— Colaboración público-privada, que involucre a los medios de comunicación, en particular la televisión.

— Contenidos amplios, no sólo referidos a la seguridad digital, sino también a recursos psicológicos (por ejemplo, la desconexión, la resiliencia, el respeto y la empatía), al derecho a la privacidad y a la

protección de los datos de carácter personal, a los valores cívicos, y a la propia legislación vigente y sus consecuencias, tanto sobre los menores como sobre sus progenitores.

— Contenidos diversificados, esto es, que tengan en cuenta los diferentes niveles de desarrollo de los menores, incluidos los que presentan discapacidades intelectivas o de aprendizaje.

— Contenidos atractivos en su forma de difusión: educación por iguales, responsabilizando a los jóvenes en este ámbito; talleres prácticos, basados en el uso de la tecnología; información basada en casos reales, anonimizados; campañas de difusión que alerten sobre peligros específicos, por ejemplo el ciberacoso, al modo de las que se han utilizado de forma eficaz por la Dirección General de Tráfico, o las más recientes en relación con el consumo de alcohol o drogas.

En esta dirección, el Gobierno impulsará campañas de información, concienciación y formación en colaboración con las comunidades autónomas.

En todas las campañas informativas y formativas en los centros educativos se fomentará la participación de expertos en la materia como son los agentes del Cuerpo Nacional de Policía, de la Guardia Civil y de las policías autonómicas en sus respectivas comunidades.

El Gobierno debe promover asimismo la existencia de protocolos de actuación en las escuelas, en relación con las situaciones en las que los niños aparecen como agresores, como ocurre con el «ciberbullying».

El Gobierno debe asimismo fomentar la puesta a disposición y difundir las innovaciones y los desarrollos destinados a la creación de contenidos en Internet de alta calidad para niños y jóvenes, y las iniciativas de éstos, alentando en ellos una actitud no limitada al consumo sino al uso positivo de Internet y a la creatividad.

5. Seguridad de Internet

Los esfuerzos del Gobierno deben alinearse con los de otros países avanzados en relación con la lucha contra la lacra del abuso sexual infantil, de la que la pornografía infantil es una de sus manifestaciones, cons-

tituyendo el compromiso de las empresas proveedoras de servicios uno de los baluartes de dicha lucha, tanto en la dirección ya emprendida del desarrollo de tecnologías de filtrado y de identificación de imágenes para el bloqueo del acceso y la retirada de este tipo de imágenes, como en la más general de una colaboración activa y decidida de dichas empresas en la detección, comunicación eficaz con las fuerzas policiales y retirada rápida de tales imágenes.

Asimismo la acción del Gobierno debe incluir la promoción de medidas técnicas que preserven a los menores frente a determinados riesgos en Internet, como la exposición a contenidos nocivos, el «ciberbullying» o el «cibergrooming», entre las cuales hay que considerar:

— Las herramientas de control parental, que constituyen una medida útil para proteger, sobre todo a los más pequeños, de los contenidos nocivos en Internet y de otros riesgos, confiando a las familias la decisión, en función de sus valores, sobre el tipo de contenidos y actividades admisibles, el momento y la frecuencia de uso de Internet para sus hijos. El Gobierno debe fomentar decididamente la disponibilidad y uso de estas herramientas, impulsando el compromiso de la industria en el desarrollo y oferta de las mismas, que deben incluir su aplicación desde la infraestructura, para proporcionar soluciones integrales familiares, comprensivas de todos los dispositivos dependientes de una misma cuenta de acceso a Internet, en la dirección promovida por el Gobierno británico.

— La clasificación por edades y etiquetado de contenidos, que debe continuar promoviendo el Gobierno, sin perjuicio de las competencias de supervisión y control de la Comisión Nacional de los Mercados y la Competencia, en la línea marcada por el artículo 18 de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico y el artículo 7 de la Ley General de la Comunicación audiovisual, impulsando el establecimiento por la industria de criterios basados en la interoperabilidad, en el marco de sistemas promovidos a escala de la Unión Europea e internacional.

— Los mecanismos de verificación de la edad u otros procedimientos eficaces en la restricción del acceso de los menores a sitios web que ofrezcan contenidos para adultos, que deben poder ser exigidos a los responsables de tales sitios, al menos hasta donde alcance la jurisdicción nacional.

— La respuesta permanente, a cualquier hora de cualquier día, a cualquier problema que pueda afectar a la integridad física, psíquica o moral o a la privacidad de los menores derivado del uso de Internet, y que puedan plantear los propios menores, sus padres o tutores o sus educadores, a través de las herramientas de denuncia puestas a disposición por las organizaciones de protección de menores y los cuerpos policiales, herramientas que el Gobierno debe analizar para promover su visibilidad y complementariedad.

6. Parámetros de edad y privacidad y herramientas de denuncia en las redes sociales

La posible implantación de mecanismos de verificación de la edad, bien en el momento de la creación de un perfil, bien «a posteriori», así como la elección por defecto, de la opción más exigente en cuanto a la privacidad en las redes sociales constituyen, en el parecer de la Ponencia, un ámbito insoslayable de discusión en el que la autorregulación, con la participación activa del Gobierno, continua siendo una herramienta de acción principal, sin renunciar a una acción normativa que, por sus consecuencias sobre el mercado digital, debe moverse, en un país integrante de la Unión Europea como España, en el marco normativo que en este nivel se establezca.

Por otro lado, las herramientas de denuncia habilitadas por redes sociales y otros proveedores de servicios de Internet son imprescindibles en relación tanto con los riesgos de contenidos (contenidos ilícitos y contenidos nocivos), como con los riesgos de contacto (en particular el ciberacoso y el «cibergrooming») y por ello, aun confiadas al campo de la autorregulación, deben recabar una mayor atención y seguimiento por parte del Gobierno, para promover no sólo su implantación general, sino también para que reúnan las condiciones de visibilidad, accesibilidad, claridad y soporte humano adecuados, así como de conexión ágil cuando proceda con las líneas de ayuda a cargo de las organizaciones de protección de menores o con las autoridades policiales y judiciales.

En este sentido, la Ponencia propone que sea el Gobierno quien promueva una acción política que desde la Unión Europea consiga que las empresas proveedoras de servicios de Internet cumplan con sus obligaciones para garantizar la seguridad en los accesos a las redes sociales a través de la implantación de mecanismos de verificación de edad y en la facilitación de datos a los cuerpos policiales y a la justicia.

Por otra parte, la Ponencia, desde la perspectiva de atender la imperiosa necesidad de una protección específica de los datos personales de los menores, como elemento fundamental de su seguridad en Internet, valora positivamente el criterio de «ventanilla única» en la relación con las autoridades nacionales de protección de datos, tanto desde el punto de vista de las empresas que operan en más de un Estado miembro de la Unión Europea, como desde el punto de vista de los ciudadanos en cuanto titulares del derecho a la protección de sus datos de carácter personal, en la dirección marcada por el Parlamento Europeo en su resolución de 12 de marzo de 2014 en el procedimiento sobre la propuesta de Reglamento sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

7. Seguridad de la Red en relación al juego «online» y a la publicidad «online»

El Gobierno debe asegurar la efectividad de la prohibición de la participación de los menores de edad en los juegos objeto de la Ley 13/2011, de 27 de mayo, de regulación del juego, entre ellos el juego «online», a través de mecanismos eficaces de verificación de la edad. Además debe desarrollar las previsiones de la citada Ley con la finalidad de garantizar una cabal protección de los menores, especialmente desde el punto de vista de la publicidad de dicha modalidad de juego.

Por otro lado, la autorregulación y la acción normativa, enmarcada ésta en la producida a nivel europeo, deben entrelazarse para asegurar un nivel de protección adecuado de los menores frente a la publicidad en Internet, en particular para asegurar que las normas sobre publicidad en sitios web para niños permita un nivel de protección comparable al de la publicidad en los servicios audiovisuales y para evitar la creación de publicidad conductual dirigida a niños.

8. Sistema normativo y de aplicación de la Ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red

España cuenta con un marco normativo de protección de los menores, en el que hay que situar la protección de los mismos frente a los riesgos de y en Internet, en cuyo vértice se encuentra la propia Constitución, a

través del mandato genérico contenido en el artículo 39.4, que remite a los acuerdos internacionales que velan por los derechos de los niños, entre ellos la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989, el Protocolo facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño de 2000 relativo a la venta de menores, la prostitución infantil y la utilización de los menores en la pornografía, el Convenio del Consejo de Europa sobre la Ciberdelincuencia de 2001 (Convenio de Budapest) y el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual de 2007 (Convenio de Lanzarote), todos ellos ratificados por España. En línea con tales instrumentos la Unión Europea aprobó en 2011 la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil (Directiva 2011/92/UE), que constituye un notable impulso para la adaptación del Derecho penal y procesal de los Estados miembros de forma que contemplen la incidencia de las TIC en la comisión de los delitos relativos al abuso y explotación sexual de menores, y se articulen instrumentos eficaces y consistentes en la lucha contra los mismos. Asimismo determinadas leyes incorporan la protección de los menores entre sus principios básicos como es el caso de la Ley Orgánica de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (artículo 3), de la Ley Orgánica de Protección Jurídica del Menor (artículo 5) o de la Ley General de la Comunicación Audiovisual (artículo 7), cuya revisión, en el contexto de la actual sociedad de la información, debe plantearse, a juicio de la Ponencia.

En particular, con ocasión de la tramitación en curso en las Cortes Generales del Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, será posible examinar la adaptación de este texto normativo desde el punto de vista de la protección de los menores en Internet frente a contenidos y conductas que por su gravedad merecen una respuesta del ordenamiento punitivo del Estado, especialmente en el marco de las obligaciones que para España se derivan tanto de los Convenios del Consejo de Europa de Budapest y Lanzarote, sobre ciberdelincuencia y sobre protección de los niños contra la explotación y el abuso sexual, respectivamente, como de la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil (Directiva 2011/92/UE), y de las recomendaciones de la comunidad científica y las autoridades responsables de la aplicación de la Ley.

Por otro lado, en línea con la «Estrategia europea en favor de una Internet más adecuada para los niños», que alienta a los Estados miembros a la puesta en práctica de «instrumentos de investigación eficaces que potencien la capacidad de los investigadores para identificar a las víctimas de abusos sexuales, acompañados de salvaguardas eficaces para garantizar la responsabilidad democrática en el empleo de los mismos», así como con el parecer general entre los comparecientes ante la Ponencia, ésta expresa su opinión favorable a una revisión en el campo del Derecho procesal que posibilite una mayor eficacia en las labores de investigación de la ciberdelincuencia, garantizando al propio tiempo los derechos de los ciudadanos y la integridad y autenticidad de las evidencias que se obtengan, revisión de particular interés en relación con la pornografía infantil, pero con una justificación que puede extenderse a otros tipos delictivos (por ejemplo, el «child grooming»), cuya comisión a través de Internet plantea un desafío en la lucha contra los mismos.

En particular, la Ponencia aboga por una ampliación al ámbito de la ciberdelincuencia o al menos a aquella parte de la misma relacionada con el abuso sexual infantil y el «child grooming» de la figura del agente encubierto, actualmente regulada en el art. 282 bis de la Ley de Enjuiciamiento Criminal en relación con la investigación de determinados delitos en la medida de su vinculación con la delincuencia organizada. Esta ampliación requeriría, además de mantener las líneas básicas y esenciales de la figura (exigencia de autorización del Juez o del Ministerio Fiscal, en atención a criterios de necesidad de la investigación y proporcionalidad y control de la actuación del agente encubierto por parte del Juez), de un régimen específico en aspectos tales como la delimitación de los delitos cometidos a través de Internet a los que sería ampliable la aplicación de esta figura (teniendo en cuenta que con frecuencia no están vinculados a una delincuencia organizada, como ocurre por ejemplo con el «child grooming»), la delimitación entre el supuesto de navegación libre amparada en identidades supuestas a través de «nicknames», usual en Internet, y el de agente encubierto propiamente tal, que requeriría autorización judicial, y el alcance de la exención de responsabilidad criminal por las actuaciones del agente encubierto en el desarrollo de la investigación.

Asimismo la Ponencia considera que deben estudiarse las posibilidades de modificación de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, para aumentar las capacidades de investi-

gación de aquellos delitos cometidos a través de las TIC que afectan a los menores, modificación que, en todo caso, tendría como referencia obligada la sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, que declaró inválida la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, cuya transposición al Derecho español constituía el objetivo principal de la Ley 25/2007.

Por lo demás, una respuesta eficaz del sistema de aplicación de la Ley frente a los contenidos y conductas ilícitas en la Red que acechan a los menores debe incluir, y a tal efecto promoverse por el Gobierno, una apuesta decidida por la formación continua en las tecnologías de la sociedad de la información, tanto en las Fuerzas y Cuerpos de Seguridad del Estado y autonómicas, como en el Ministerio Fiscal y el Poder Judicial.

La Ponencia propone que el Gobierno de España impulse en el seno de la Unión Europea la elaboración, en un proceso participativo, de una «Carta de Derechos de los Ciudadanos en Internet» que incida especialmente en proteger los derechos de los menores. Con especial énfasis en la regulación de la seguridad en la red y el derecho a la privacidad de los usuarios.

9. Capacidades operativas en la lucha contra el abuso sexual y la pornografía infantil

Además de la imprescindible cooperación internacional, la Ponencia considera que, en la lucha contra el abuso sexual infantil deben intensificarse las acciones a nivel nacional, en una triple dirección:

— Reforzar los recursos policiales destinados a la lucha contra la pornografía infantil en Internet, entre ellos, la I+D en soluciones técnicas para las investigaciones policiales, que permitan la identificación de los materiales de pornografía infantil, con vistas a su rápida retirada, a la identificación y rescate de las víctimas y a la puesta a disposición de la justicia de los autores, basada en procedimientos que garanticen la obtención e integridad de las pruebas.

— Reforzar la coordinación entre las unidades especializadas de las diferentes Fuerzas y Cuerpos de Seguridad del Estado y autonómicas.

— Reforzar la cooperación entre las empresas proveedoras de servicios, líneas de denuncia de organizaciones privadas y cuerpos policiales, para actuar con rapidez en la retirada del material ilícito.

ANEXO 1

Orden alfabético de comparecientes ante la Ponencia conjunta de estudio de los riesgos derivados del uso de la Red por parte de los menores, con indicación del cargo o condición que figura en el orden del día de la sesión correspondiente en la que intervinieron.

ADROHER BIOSCA, María Salomé. Directora General de Servicios para la Familia y la Infancia.

ADSUARA VARELA, Francisco de Borja. Director General de Red.es.

BAYARRI I NOGUERAS, Joaquim. Jefe de la División Técnica de Planificación de la Seguridad Ciudadana de los Mossos d'Esquadra.

BASTERRECHEA OÑATE, Natalia. Directora de Asuntos Públicos de Facebook en España.

BREZO FERNÁNDEZ, Félix. Ingeniero Informático e Ingeniero en Organización Industrial.

CALVO-SOTELO IBÁÑEZ-MARTÍN, Víctor. Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

CÁNOVAS GAILLEMIN, Guillermo. Presidente de la Asociación Protégeles.

CARBONEL PINTANEL, Luis. Presidente de la Confederación Católica Nacional de Padres de Familia y Padres de Alumnos (CONCAPA).

CARTES, Patricia. Directora de Seguridad de Twitter.

CASAL CASTRO, José Luis. Cofundador y Director de Marketing de Talk2Us Comunicación.

COMÍN HERNÁNDEZ, Miguel. Director de la Fundación Alia2.

Cosidó Gutiérrez, Ignacio. Director General de la Policía.

Cruz Yagüe, Óscar de la. Comandante Jefe del Grupo de Delitos Telemáticos de la Unidad Central Operativa (UCO) de la Guardia Civil.

Chóliz Montañés, Mariano. Profesor Titular de la Facultad de Psicología de la Universidad de Valencia.

Errasti Argal, Miguel. Presidente de la Asociación Nacional de Empresas de Internet (ANEI).

Escalante García, Manuel. Director General del Instituto Nacional de Tecnologías de la Comunicación (INTECO).

Fernández de Mesa Díaz del Río, Arsenio. Director General de la Guardia Civil.

Fernández de Mesa Echeverría, Sofía. Directora de Responsabilidad e Innovación Social Corporativas de Telefónica.

Flores Fernández, Jorge. Director y fundador de la Iniciativa PantallasAmigas.

Fontán Oñate, Eugenio. Decano Presidente del Colegio Oficial de Ingenieros de Telecomunicación (COIT).

Gallego Morales, María José. Responsable de consumidores y usuarios e interceptación legal de las comunicaciones de Jazztel.

González García, Carolina. Inspectora Jefa de Sección de Prensa y Redes Sociales de la Oficina de Prensa y Relaciones Informativas de la Dirección General de la Policía.

González Hermoso de Mendoza, Alfonso. Director General de Evaluación y Cooperación Territorial.

Guijarro Valladolid, Jesús. Mánager de Responsabilidad Social Corporativa de Orange España.

Gutiérrez Rubí, Antoni. Asesor de comunicación y analista de las redes sociales.

Igual Garrido, Carlos. Capitán del Grupo de Menores y Explotación Sexual Infantil de la Unidad Técnica de Policía Judicial (UTPJ) de la Guardia Civil.

Madrigal Martínez-Pereda, Consuelo. Fiscal de Sala Coordinadora de Menores.

Manzanas Manzanas, Juan Miguel. Comisario Jefe de la Brigada de Investigación Tecnológica de la Comisaría General de la Policía Judicial de la Dirección General de la Policía.

Martínez Monreal, Salud. Experta en innovación para la seguridad de la información.

Martínez Otero, Juan María. Vocal del Consejo Asesor de la Federación de Asociaciones de Consumidores y Usuarios de los Medios (iCmedia).

Martos Mota, Francisco Javier. Director Ejecutivo de UNICEF Comité Español.

McSweeney, Sinéad. Directora de Políticas Públicas, EMEA, de Twitter.

Muriel Herrero, Sebastián. Director General de Operaciones de Tuenti.

Navarrete Barreiro, Carlota. Directora General de la Coalición de creadores e industrias de contenidos digitales.

Orjuela López, Liliana. Coordinadora de los derechos de la infancia de Save the Children.

Pérez Subías, Miguel. Presidente de la Asociación de Usuarios de Internet (AUI).

Polo González, Íñigo. Director de Relaciones Institucionales de ONO.

Prats Moreno, Josep Manuel. Presidente de la Federació d'Associacions de Pares i Mares d'Escoles Lliures de Catalunya (FAPEL).

Reig Hernández, Dolors. Psicóloga Social experta en Sociedad-red y responsable del espacio El Caparazón.

Represa Estrada, Carlos. Director del Centro de Seguridad TIC Escolar (CNTiC).

Rodríguez Álvarez, José Luis. Director de la Agencia Española de Protección de Datos (AEPD).

Román Riechman, Ana María. Directora del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF).

Rosell Tejada, José Miguel. Socio-Director de S2 Grupo.

Ruiz Antón, Francisco. Mánager de Políticas Públicas y Asuntos Institucionales de Google España y Portugal.

Salido Navarro, Jesús. Vicepresidente de la Confederación Española de Asociaciones de Padres y Madres de Alumnos (CEAPA).

Sánchez Montenegro, Héctor. Director de Tecnología de Microsoft Ibérica.

Santos Ortega, Francisco Javier. Gerente de Seguridad Corporativa de ONO.

Sedes García, José Manuel. Mánager de Sostenibilidad y Calidad de Vodafone España.

Taulé Valdeperas, Joan. Director General de Symantec España.

Tejada de la Fuente, Elvira. Fiscal de Sala Coordinadora contra la Criminalidad Informática.

Tourné Alegre, José Manuel. Director General de la Federación para la Protección de la Propiedad Intelectual (FAP).

Urra Portillo, Javier. Primer Defensor del Menor de la Comunidad de Madrid.

Viota Maestre, Manuel. Jefe de la Sección Central de Delitos en Tecnologías de la Información de la Unidad de Investigación Criminal y Policía Judicial de la Ertzaintza.

ANEXO 2

Declaración, con motivo del «Día para una internet más segura» (11 de febrero de 2014), de los senadores miembros de la ponencia, constituida en el Senado de España, para el estudio de los riesgos derivados del uso de la red por parte de los menores

Los Senadores miembros de la **Ponencia, constituida en el Senado de España, para el estudio de los riesgos derivados del uso de la Red por parte de los menores** manifiestan su adhesión a la celebración del «Día para una Internet más segura» (*Safer Internet Day —SID—*), promovido en el marco de la Comisión Europea, y cuya edición de 2014 se desarrolla el 11 de Febrero.

En particular, saludan la celebración del «III Congreso Nacional Joven y en Red», organizado por el Centro de Seguridad en Internet para menores en España (Protégeles /Cesicat), como acto central de aquel Día.

Los Senadores miembros de la Ponencia hacen completamente suyo el lema de la jornada, «Hagamos juntos una internet mejor» (*Let's create a better Internet together*), reflejado en el programa y participantes del Congreso mencionado.

La Ponencia fue creada precisamente desde la clara conciencia de que las oportunidades y riesgos que plantea Internet tienen una proyección específica en los menores, y que deben ser afrontados entre todos. Los propios menores, junto con sus familias y educadores, constituyen protagonistas clave desde la perspectiva que sitúa en la prevención el enfoque básico para hacer frente a las amenazas o riesgos procedentes de la Red, y, por tanto, de las acciones de sensibilización y capacitación tendentes a promover una actitud responsable frente a la Red.

Una eficaz coordinación en el ámbito de los poderes públicos, una decidida alianza entre éstos y el sector privado, tanto el de acción social como el empresarial, con la participación de todos los actores, incluidos los jóvenes, y una estrategia con perspectiva europea e internacional, son herramientas imprescindibles en la construcción de una internet mejor y más segura, de la que iniciativas como las señaladas son un valioso ejemplo.

Palacio del Senado, 30 de septiembre de 2014. Emilio Álvarez Villazán, Iñaki Mirena Anasagasti Olabeaga, José María Ángel Batalla, Carmen Azuara Navarro, Francisco Boya Alós, Tomás Pedro Burgos Beteta, José María Chiquillo Barber, Andrés Gil García, Amalur Mendizabal Azurmendi, Jordi Miquel Sendra Vellvè.

4. DEBATE Y APROBACIÓN DEL INFORME DE LA PONENCIA POR EL PLENO DEL SENADO EN SU SESIÓN DE 15 DE OCTUBRE DE 2014*

* Diario de Sesiones, Senado, X Legislatura, número 127, de 15 de octubre de 2014 (sesión del Pleno núm. 60).

8. *Ponencias de estudio*

8.1. Informes

8.1.1. Ponencia conjunta de estudio sobre los riesgos derivados del uso de la red por parte de los menores.
Comisión: conjunta de las comisiones de interior, de educación y deporte, y de industria, energía y turismo.

(Núm.exp.543/000005)

El señor PRESIDENTE: Para la presentación del informe, tiene la palabra el coordinador de la ponencia, el senador Burgos, por tiempo de cinco minutos.

El señor BURGOS BETETA: Señor presidente, señorías, me cabe el honor de presentar ante esta Cámara el informe de la ponencia conjunta de estudio sobre los riesgos derivados del uso de la red por parte de los menores.

La ponencia inició sus trabajos en los primeros meses de 2013, y lo hizo a partir de una premisa fundamental: la consideración de los menores como grupo, con unas necesidades específicas en internet que debían ser objeto de estudio de manera integral. Han sido 53 comparecientes, que han aportado a la ponencia una abundante y valiosa información, procedentes de muy distintos ámbitos, departamentos ministeriales, Policía Nacional, Guardia Civil, Ertzaintza, Mossos d'esquadra, ministerio fiscal, Agencia Española de Protección de Datos y organizaciones privadas con una específica vocación en la protección de menores, asociaciones educativas y de usuarios de internet, de la industria, del ámbito de la creación de contenidos digitales y, finalmente, expertos de distintas disciplinas, como las nuevas tecnologías y la ciberseguridad, la psicolo-

gía o la comunicación digital. Se trata de un amplio elenco de personas, asociaciones e instituciones, públicas y privadas, con el que intentamos garantizar la participación de la mayoría de los sectores interesados. A todos ellos, nuestro reconocimiento y sincero agradecimiento, así como también a cuantas personas que, fuera del marco formal de estas comparecencias, han manifestado su interés por los trabajos de la ponencia y han remitido valiosos estudios y todo tipo de documentación.

Asimismo, y como no podía ser de otra manera, la ponencia adoptó en su metodología de trabajo la práctica de incorporar a la página web del Senado el texto de los informes o recomendaciones de los comparecientes, previo su consentimiento, para uso y consulta de todas las personas interesadas.

El informe tiene un capítulo introductorio y 5 títulos principales. Parte de la idea de niños, adolescentes y jóvenes como nativos digitales, en un escenario global, de rápida evolución tecnológica, marcada por la conectividad, la interactividad y la convergencia del mundo audiovisual. Es un escenario lleno de oportunidades, pero también de riesgos. En él, los menores presentan necesidades específicas desde una u otra perspectiva. Es un reto para las políticas públicas encontrar precisamente el adecuado equilibrio entre unos y otros.

El informe dedica uno de sus títulos al análisis de los riesgos, para más tarde abordar las claves para la acción política en este ámbito, partiendo de 2 ideas fundamentales: primera, que tanto en el mundo físico como en el digital deben regir los valores que encarnan los derechos fundamentales de las personas reconocidos en la Constitución y en los tratados internacionales y que, en el caso concreto de los menores, garantizan además su interés superior como consideración primordial; y segunda, que la existencia de actores muy diferentes con intereses relevantes en la materia reclama una responsabilidad compartida en la que las alianzas público- privadas son palancas fundamentales para la acción, junto con la cooperación internacional derivada precisamente de la naturaleza dinámica y global de internet.

El desarrollo de estas claves desemboca en la enumeración de 21 conclusiones y 9 recomendaciones, y aunque todas ellas son importantes y se hallan relacionadas entre sí, quisiera destacar algunas: la propuesta de creación de un adjunto tercero, con funciones específicas de defensor del menor en el seno de la institución del Defensor del Pueblo, que in-

cluya explícitamente el área de protección de los menores en internet; la alfabetización digital y mediática de los menores, con la escuela como piedra angular, que ha de incluir necesariamente —y se ha hecho mucho hincapié en ello— la formación de padres, maestros y profesores, y acciones de sensibilización en general; la exigencia de la seguridad en el propio entorno en línea con un sistema normativo de aplicación de la ley con respuesta eficaz, frente a contenidos y conductas ilícitos en la red. En este sentido, debemos mantener una posición decidida en relación con el proceso de revisión que se está produciendo del marco regulador europeo de protección de datos de carácter personal, para garantizar un nivel de seguridad aceptable en la red que contemple las necesidades específicas de los menores a través, por ejemplo y entre otras medidas, de la implantación de mecanismos de verificación de la edad, o la elección, por defecto, de la opción más exigente en cuanto a privacidad.

Quiero resaltar, y es muy importante, la propuesta de la ponencia a favor de una ampliación al ámbito de la ciberdelincuencia o, al menos, a lo relacionado con el abuso sexual infantil y el *cibergrooming*, de la figura del agente encubierto, regulado actualmente en relación con la investigación de otros delitos. Creemos que es un instrumento eficaz que, sin duda, debe regularse con todas las garantías exigidas en el Estado de derecho.

Señorías, estas son algunas recomendaciones reseñables, cuyo sentido unitario, en cualquier caso, solo puede desvelar la lectura completa del informe.

Para finalizar quiero subrayar que la unanimidad, reflejada por la firma de todos los grupos parlamentarios en la moción, que originó la constitución de esta ponencia y la colaboración fluida de todos sus miembros en sus trabajos, tuvo su conclusión en el voto unánime de la ponencia de acordar, en su pasada sesión del 30 de septiembre, aprobar y elevar al Pleno de la Cámara el informe presentado. Mi reconocimiento a los ponentes, don Emilio Álvarez, don Iñaki Anasagasti, don José María Ángel, doña Carmen Azuara, don Francisco Boya, don José María Chiquillo, don Andrés Gil, doña Amalur Mendizabal y don Jordi Sendra.

Señorías, sinceramente creo que aquí, en el Senado, hemos hecho un buen trabajo, y en él ha sido muy importante la implicación entusiasta del letrado de esta ponencia, don Eugenio de Santos, más allá del compromiso profesional que, por supuesto, nunca ha abandonado, y también,

cómo no, el apoyo expreso del presidente de la comisión conjunta, y del Senado, don Pío García-Escudero, siempre sensible y receptivo a las solicitudes de la ponencia.

Acabo ya. Nuestro objetivo ha sido aportar ideas, propuestas y soluciones ante una realidad compleja e imparable, en la que conviven los más detestables comportamientos que debemos prevenir, corregir, perseguir y erradicar, con las mayores oportunidades, que, sin duda, debemos y es necesario aprovechar.

Muchas gracias. *(Aplausos).*

El señor PRESIDENTE: Muchas gracias, senador Burgos. Pasamos al turno de portavoces.

Por el Grupo Parlamentario Mixto, tiene la palabra la senadora Mendizabal.

La señora MENDIZABAL AZURMENDI: Muchas gracias, señor presidente.

Solamente dos palabras para manifestar mi agradecimiento. Considero que la experiencia de esta ponencia ha sido muy interesante. Han venido más de 50 comparecientes. El saber no ocupa lugar y todo lo que han dicho ha sido ciertamente muy interesante.

Respecto al trabajo, me gustaría resaltar que entre todos hemos conseguido recoger todos los aspectos en los que ha incidido cada compareciente. Es verdad que algunos resaltaban un aspecto más que otro; por ejemplo, unos resaltaban el área de la educación, y otros iban por otro camino, pero considero que la labor de todos ellos ha sido la de caminar para encontrar una solución al problema de las redes sociales y sus riesgos en lo que respecta a los menores.

Para terminar, quiero resaltar la gran labor realizada por el señor letrado, porque no ha sido fácil reflejar todo lo que quería decir cada ponente, y creo que se ha conseguido en el texto final reflejar el pensamiento de cada uno de ellos, razón por la que se ha podido aprobar el informe en comisión por unanimidad.

Gracias.

El señor PRESIDENTE: Muchas gracias, senadora Mendizabal.

Por el Grupo Parlamentario Vasco en el Senado, tiene la palabra el senador Anasagasti.

El señor ANASAGASTI OLABEAGA: Muchas gracias, señor presidente.

Señorías, estamos ante un buen trabajo parlamentario que casi justifica la existencia del Senado. Este tipo de iniciativas exhaustivas, bien llevadas, poliédricas, que analizan un problema desde todos sus ángulos, solo se puede hacer desde una institución que reflexiona con pausa, que aúna esfuerzos, que capta los problemas de una sociedad cambiante y, sobre todo, que propone soluciones.

Sabemos que la realidad política se mueve por impulsos y por el estallido de fuegos artificiales y que uno de los problemas más importantes que detecta el ciudadano, además del paro, es la impunidad ante la corrupción. Pues bien, esta metástasis de la sociedad ya fue analizada en su día por este Senado sin que sus conclusiones jamás se tomaran en cuenta. Otro gallo habría cantado si los medios de comunicación social y los partidos políticos hubiéramos llevado esta iniciativa al Código Penal, y a otros proyectos, las conclusiones de este magnífico trabajo en el que se han dado cita muchos elementos: grupos y senadores que han trabajado sin mayores discrepancias; un presidente conservador que ha tenido mano izquierda y que ha llevado bien la comisión, salvo en una cuestión, no haber permitido que el CNI nos aportara su visión del problema; un letrado a quien conozco desde el Congreso de los Diputados, don Eugenio de Santos y, por tanto, sé de su profesionalidad y entrega, que se ha volcado en hacernos fácil el trabajo y que ha llevado asimismo el peso de toda la investigación, con sus derivaciones y bibliografía, porque, entre otras cuestiones, el tema le ha apasionado. Una iniciativa que tocaba el nervio de un problema no suficientemente abordado. Solo queda que los medios de comunicación se hagan eco de este trabajo y los directamente implicados lean sus conclusiones, que valen la pena.

Queremos agradecer a don Manuel Viota Maestre que aceptara nuestra invitación para darnos el punto de vista de la Ertzaintza, que, a pesar de ser un cuerpo policial joven, trabaja con profesionalidad en este

asunto, y, lo más importante, lo lleva a la escuela. Su ejemplo de que una charla explicativa sirvió para que los propios chavales denunciaran un delito nos alumbró sobre la importancia de este renglón en la lucha contra los diversos ciberacosos. Estas fueron las recomendaciones de Manuel Viota, jefe de la sección central de delitos en tecnologías de la información de la Unidad de Investigación Criminal y Policía Judicial de la Ertzaintza. Pero hay 22 conclusiones, que invito a sus señorías y a los interesados a leer, porque vale la pena este trabajo.

Internet no es todo lo que vemos los que no somos nativos digitales y nos enteramos de que existía esta palabra; no somos nativos digitales, ¡menudo disgusto nos llevamos! Hay quien lo compara con un iceberg pequeño en la superficie pero gigante en las profundidades y en sus posibilidades para el bien y para el mal. El territorio sumergido está compuesto por páginas que no están indexadas en buscadores convencionales, por su antigüedad —los buscadores las ignoran— o porque han sido diseñadas con un código que las oculta, y son el paraíso del cibercrimen, del ciberacoso, del espionaje político y comercial, incluso del sabotaje y de la fabricación de armas. Además existen otras categorías, como el *hacktivismo* y el robo de la propiedad intelectual.

Por todo esto, los senadores que hemos formado parte de esta ponencia tan interesante y tan constructiva hicimos nuestro el lema: Hagamos juntos un internet mejor, y firmamos la declaración de febrero de 2014, y es que la ponencia fue creada precisamente desde la clara conciencia de que las oportunidades y riesgos que plantea internet tienen una proyección específica en los menores, y deben ser afrontados entre todos. Los propios menores, junto a sus familias y educadores, se constituyen en protagonistas claves, desde una perspectiva que sitúa en la prevención el enfoque básico para hacer frente a las amenazas y a los riesgos procedente de la red y, por tanto, de las acciones de sensibilización y capacitación tendentes a promover una actitud responsable frente a la red. Una eficaz coordinación en el ámbito de los poderes públicos, una decidida alianza entre estos y el sector privado, tanto en el aspecto social como en el empresarial, con la participación de todos los actores, incluidos los jóvenes, y una estrategia con perspectiva europea e internacional son herramientas imprescindibles en la construcción de una internet mejor y más segura, e iniciativas como las señaladas son un valioso ejemplo de ello.

Confiamos en que este trabajo se publique y, sobre todo, que ustedes lo lean y que los medios de comunicación se hagan eco de ella.

Muchas gracias, señor presidente. *(Aplausos).*

El señor PRESIDENTE: Muchas gracias, senador Anasagasti.

Por el Grupo Parlamentario Entesa pel Progrés de Catalunya, tiene la palabra el senador Boya.

El señor BOYA ALÓS: Gracias, señor presidente.

Quisiera, en primer lugar, aprovechando la oportunidad de estos breves minutos, trasladar a los miembros de la ponencia y a la Cámara una reflexión sobre el informe de esta ponencia que acaba de finalizar.

Vaya por delante mi agradecimiento a todos ellos, presidente, y muy especialmente al letrado, Eugenio de Santos, que con su buena disponibilidad y su buen hacer nos ha hecho muy fácil el trabajo. Quiero también agradecer a todos los comparecientes, a los 53, que han aportado sus conocimientos y reflexiones a esta ponencia, que ha sido extensa, amplia e intensa y que ha llevado a cabo un trabajo importante sobre un asunto que en el momento de abordarlo, como saben muy bien, en los primeros debates no era fácil, poliédrico exactamente; hemos tenido que abordarlo desde 3 comisiones diferentes, pero, sin duda, es un asunto de amplia trascendencia para nuestra sociedad.

Tenemos que condensar en estos breves minutos muchas horas de trabajo, y el presidente ha hecho un relato muy exacto de lo que ha sucedido en la ponencia y de las conclusiones del informe.

En este esfuerzo colectivo, un esfuerzo transversal que hemos hecho esta Cámara y tantos responsables de las instituciones y expertos que nos han asistido en la reflexión, yo personalmente he encontrado sentido a mi cometido como representante de la sociedad que nos ha elegido para servir en un ámbito como es esta Cámara.

Esta ponencia nos ha permitido establecer un debate relativo a una cuestión sobre la que nuestra sociedad tiene hoy muchas ambigüedades, muchas incógnitas, que ha sido sereno, pausado, como ha dicho el senador Anasagasti, que permite unas conclusiones dignas de ser leídas y difundidas entre la totalidad de la sociedad.

Ya saben aquello que se dice: que mientras más avance la tecnología, más complicada será nuestra existencia. Efectivamente, lo hemos podido palpar en estos meses de debate. Y nos ha llevado a una reflexión —que también se ha apuntado aquí— que considero una de las más trascedentes del informe: la necesidad de habilitar en nuestras escuelas formatos para que nuestros alumnos, nuestros hijos se doten de capacidades, de competencias y de habilidades para ser alfabetizados en este mundo digital y, por tanto, en este trabajo colaborativo que implican las nuevas tecnologías.

Ha sido muy importante también el debate sobre el papel de las empresas, de los cuerpos de seguridad —como se ha explicado— frente a la criminalidad y las conductas abusivas y delictivas, que encuentran en internet un nuevo campo de acción. Nos ha parecido que podría ser una apuesta interesante incorporar el concepto de ventanilla única para las empresas o, en este caso, un comisionado digital para coordinar la acción del Gobierno.

Ciertamente, hemos aprendido mucho y espero que hayamos sido útiles a los propósitos que nos llevaron a crear esta ponencia. Si es que me quedaba aún alguna duda, he comprendido que la sociedad eminentemente tecnológica en la que nos vamos sumergiendo día tras día tiene enormes posibilidades pero también muchos riesgos, y estas oportunidades y estos riesgos van conformando una nueva cultura y nuevas formas de relación. Las viejas normas ya no nos sirven en el mundo digital, lo cual no quiere decir que obviemos la necesidad de sustituirlas o acomodarlas a estos nuevos formatos.

Por ello, el debate no ha hecho más que empezar. Autorregulación, coordinación institucional, supervisión, denuncia, derecho a la intimidad son términos que señalan de alguna forma un camino difuso por el que circula la nueva ciudadanía digital y por el cual han de establecerse patrones de comportamiento ante los riesgos de los nuevos paradigmas. Pero también es muy cierto que estas prevenciones, señorías, no pueden condicionarnos para sacar el máximo provecho a las inmensas oportunidades que sin duda nos ofrecen —y también en el futuro— los avances tecnológicos en el ámbito de la comunicación.

Acabo, señor presidente, diciendo que personalmente he aprendido mucho. Quiero agradecer a los ponentes su cordialidad en los debates, y muy especialmente como padre —permítanme que lo diga—, como creo

que harán también muchos otros padres que puedan leer este informe, porque es muy loable que esta Cámara se haya ocupado de aquellos que tienen más riesgos en unos tiempos en que todo es susceptible de cambios: hablo de los adolescentes que precisamente viven una etapa de su vida que los hace especialmente vulnerables.

Por tanto, hoy puedo concluir esta intervención diciendo que el propósito fue bueno, pero el resultado ha sido mucho mejor.

Muchas gracias. *(Aplausos)*.

El señor PRESIDENTE: Gracias, senador Boya.

Por el Grupo Parlamentario Catalán en el Senado Convergència i Unió, tiene la palabra el senador Sendra.

El señor SENDRA VELLVÈ: Gracias, señor presidente.

Señorías, hoy aprobamos un documento elaborado en la ponencia conjunta de estudio sobre los riesgos derivados del uso de la red por parte de los menores, que durante año y medio ha trabajado arduamente para conocer, a través de diversas comparecencias de destacados representantes de entidades públicas y privadas y reconocidos expertos en la materia, de esta grave problemática que afecta a nuestros menores y adolescentes en su trato diario con el mundo de internet; un escenario, el de internet y el mundo digital, de consecuencias revolucionarias en las relaciones humanas y sociales pero con muchas maldades también en las redes sociales, entorno que se ha convertido en un escenario habitual de nuestra juventud.

Por aquel entonces, cuando iniciamos los trabajos, todos teníamos en mente lo sucedido en Estados Unidos con Amanda Todd, joven de 15 años que se suicidó tras ser linchada socialmente a raíz de la publicación de una foto en *topless* que se hizo frente a la webcam para un extraño. En el vídeo que la adolescente colgó en YouTube antes de morir relataba la presión que venía soportando desde hacía tres años por parte de sus compañeros de escuela, tanto en el patio como en las redes sociales. Todos vimos en Amanda Todd a nuestros hijos como hipotéticas presas de los delincuentes de la red.

Además, entre los jóvenes —que son nativos digitales como usuarios intensivos de las nuevas tecnologías— y los adultos —nosotros, los pa-

dres— existe la denominada brecha digital, pues en la mayoría de los casos desconocemos la complejidad de las nuevas tecnologías y, por tanto, no podemos aconsejar a nuestros hijos como debiéramos —y nos gustaría— en relación con el buen uso de esas tecnologías.

Las extraordinarias y valiosísimas aportaciones hechas por parte de los expertos en el tema han llevado a focalizar los esfuerzos que los poderes públicos deberán realizar en varios aspectos —todos fundamentales— para el uso seguro de internet por los menores. Hemos debatido y acordado recomendaciones en relación con: alianzas público-privadas; cooperación internacional; estrategia y coordinación y coherencia; alfabetización digital y sensibilización general —importantísimo—; seguridad de internet, parámetros de edad y privacidad y herramientas de denuncia en las redes sociales; seguridad de la red en relación con el juego *online* y con la publicidad *online;* sistema normativo de aplicación de la ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la red; capacidades operativas en la lucha contra el abuso sexual y la pornografía infantil.

No voy a entrar en el contenido de los nueve puntos, porque están debidamente explicados en el documento que hoy aprobamos. Seguramente nos hubiera gustado incidir más en determinados temas, pero hemos entendido que era necesario un documento unánime de todos los ponentes para así asegurar el apoyo de todos los grupos parlamentarios a las recomendaciones al Gobierno que hoy aprobamos —el esfuerzo en la lucha contra la ciberdelincuencia en las redes sociales que afecta a nuestros jóvenes bien lo merece—.

Quiero mostrar mi agradecimiento a todos y cada uno de los comparecientes en este largo año y medio y a los poderes públicos con ámbito competencial. Y quiero hacer mención expresa al extraordinario trabajo que realizan en este campo todos los cuerpos policiales —desde el Cuerpo Nacional de Policía hasta los Mossos d'Esquadra en Cataluña—; a las organizaciones privadas representativas de asociaciones educativas y usuarios de internet; a los expertos de distintas disciplinas como las nuevas tecnologías y la ciberseguridad, la psicología o la comunicación digital; y también a la industria creadora de contenidos digitales. A todos ellos, muchas gracias por su colaboración y —reitero— sus valiosas aportaciones.

Mi agradecimiento personal a los miembros de la ponencia, que han trabajado con espíritu positivo y constructivo, lo que ha permitido un

trabajo cómodo y agradable. Y lo personalizo en el presidente de la ponencia, el senador Tomás Burgos, que ha sabido dirigir con diligencia los trabajos a lo largo de este año y medio. A él le pido la misma diligencia para que este documento sea recibido como merece por el Gobierno y sus recomendaciones sean atendidas y llevadas a cabo con prontitud.

Acabo. Felicito al letrado de la ponencia, Eugenio de Santos, por su trabajo ingente a lo largo de este año. Su capacidad de sintetizar dieciocho meses de comparecencias en un documento excelente merece mi más sincero reconocimiento. Gracias, señor letrado. Gracias, Eugenio.

Señorías, nuestros adolescentes, nuestros jóvenes y su seguridad en el uso de las redes sociales merecen que el esfuerzo realizado por la ponencia dé sus frutos y, por eso, pido al Gobierno que atienda nuestras recomendaciones. Velaremos por que así sea.

Muchas gracias. *(Aplausos).*

El señor PRESIDENTE: Muchas gracias, senador Sendra.

Por el Grupo Parlamentario Socialista, tiene la palabra el senador Gil García.

El señor GIL GARCÍA: Muchas gracias, señor presidente.

Señorías, en nombre de mi grupo me gustaría comenzar esta intervención poniendo en valor el trabajo desarrollado durante todo este largo año en este marco de la ponencia conjunta que ha estudiado los riesgos derivados del uso de la red por nuestros hijos e hijas en nuestro país, trabajo cuyo objetivo no ha sido solo hacer un compendio, un análisis de estadísticas sobre la problemática del uso de las redes o el uso de internet por nuestros menores, sino, ante todo, poner encima de la mesa un conjunto de propuestas y de estrategias claras para hacer frente a problemas como son el acoso, el abuso sexual, la pederastia y, no menor, los comportamientos sexistas o de violencia de género que se dan entre nuestros adolescentes en el marco digital.

El Grupo Socialista está satisfecho con el trabajo que se ha desarrollado a lo largo de estas veintisiete sesiones, en diecinueve de las cuales han comparecido esos cincuenta y tres expertos, venidos de ámbitos muy diversos —del ecosistema de internet, de los cuerpos y fuerzas de seguri-

dad del Estado, de asociaciones y de distintas empresas—. A todos ellos queremos agradecerles las aportaciones y las ideas que nos han puesto encima de la mesa, que se han podido hacer públicas a través de la página web del Senado. También, cómo no, quiero agradecer al letrado don Eugenio Santos su asistencia y su brillante trabajo, pues nos ha ayudado, y mucho, en esta ponencia.

Sinceramente, lo digo en serio, creo que hemos hecho un buen trabajo, probablemente uno de los más actualizados y concretos que sobre esta materia tan compleja haya hecho ningún estamento oficial o Cámara parlamentaria en el marco de la Unión Europea. Sí exceptuamos el trabajo que está desarrollando el propio Parlamento británico, con el cual esta ponencia ha mantenido contacto y con el que hemos intercambiado información para no duplicar materias y poder aprovecharnos unos de otros respecto a lo que se estaba realizando.

Me gustaría remarcar una idea, y dejarla clara, que ha sobrevolado todos los trabajos de la ponencia: Internet no es el enemigo, internet es solo una herramienta. Los ponentes nos han avisado de que poner el foco en prohibir no es el camino correcto. Como destacó el representante de la Policía Autónoma Vasca, no debemos proteger a los menores de internet, debemos protegerles de las personas que hacen un mal uso de la red, incluso de ellos mismos. Pues bien, partiendo de esta premisa, nuestro grupo considera que, para lograr conjugar las grandes oportunidades que internet ofrece, con los riesgos que su uso conlleva en ocasiones, debemos realizar el trabajo principal siempre desde el ámbito educativo. Es en la escuela —aunque no solo desde ella— donde debemos implementar estrategias de capacitación de los menores en competencias digitales, como así nos han indicado la mayoría de los ponentes. En definitiva, señorías, se trata de constituir una estrategia que involucre a toda la sociedad y que tenga como eje la educación como principal política preventiva; y no me refiero solo a la escuela, que también. Quisiera destacar algunas de nuestras principales aportaciones a este documento. La primera: que este es un asunto que nos concierne a todos y no solo afecta a Policía y Guardia Civil investigar a los pederastas que operan en la red, por tanto, es una materia transversal. En segundo lugar, quisiera destacar y valorar hoy aquí una aportación pionera que se recoge en el informe de la ponencia: consideramos que es necesario abordar la creación de un marco legislativo específico que proteja los derechos de los ciudadanos

en internet. Es decir, se trataría de iniciar un proceso participativo con la ciudadanía para elaborar una carta europea de los derechos ciudadanos en internet, de la cual nos gustaría que España fuera su principal promotor en el marco de la Unión Europea. Esta carta debe garantizar sobre todo los derechos de los menores en cuanto a su privacidad y a la preservación de su identidad digital. Ejemplos de ello tenemos en el reciente marco civil de internet aprobado por el Senado Federal del Brasil, que creo puede ser una muy buena referencia.

Concluyo. Ya solo queda que el Gobierno esté a la altura y asuma la importancia del reto que tenemos por delante. Esperamos y confiamos que las acciones del documento que vamos a aprobar no caigan en saco roto y sean tenidas en cuenta por el Gobierno, y no solo sobre el papel, sino que cuenten con el correspondiente respaldo de recursos económicos. Me temo, señorías, que en esta, como en tantas otras cuestiones, no se puede hacer más con menos. Porque si algo nos ha quedado claro es que en la red los malos hacen más con más recursos cada segundo, y no podemos permitirnos el lujo en esta materia que afecta a la seguridad de nuestros hijos e hijas ir por detrás como estamos yendo. Si esto no fuera así, señorías, habremos hecho un trabajo fantástico y un documento precioso que terminará seguramente en una estantería o sirviendo para debates y foros sobre la materia.

Dado el buen trabajo y buen diálogo mantenido entre todos los grupos en el seno de la ponencia, consideramos buena la recepción del respaldo económico de las medidas concretas que proponemos en este informe.

Muchas gracias. *(Aplausos)*.

El señor PRESIDENTE: Gracias, senador Gil García.

Por el Grupo Parlamentario Popular, tiene la palabra la senadora Azuara.

La señora AZUARA NAVARRO: Señor presidente, señorías, como bien han apuntado los senadores que me han precedido en el uso de la palabra, cada vez más el mundo digital y las nuevas tecnologías ocupan más espacio en nuestras vidas. Y es que la era digital e internet se han instalado fuertemente en nuestra sociedad con la intención de quedarse

y ser parte de nosotros. Por ello tenemos que aprender a potenciar las grandes oportunidades que nos ofrecen y sus capacidades de desarrollo.

Dentro de los usuarios de internet, de la sociedad de la información y de las nuevas tecnologías se encuentran nuestros hijos, nuestros menores, nuestros adolescentes, que son los más vulnerables en el ecosistema digital. Y es que internet y las tecnologías no son el problema en sí, como bien se ha dicho anteriormente, sino la forma en la que algunas personas pueden llegar a utilizarlas. Porque no tenemos que tener miedo, no debemos de poner freno a su desarrollo, sino todo lo contrario, aprovechar todos sus potenciales.

Internet, las redes sociales y la tecnología son una realidad, ya son una realidad, una realidad que está en constante cambio, y eso nos obliga a fijar nuestra atención para ser conscientes de los riesgos derivados de su uso y, en especial, de los riesgos a los que se enfrentan los menores de nuestro entorno, porque estamos viviendo una auténtica revolución, y creo que todos coincidimos en que se trata de un problema global que afecta a todas las sociedades.

Señorías, durante las sesiones de trabajo de esta ponencia hemos tenido el privilegio de contar con numerosos testimonios, que han aportado gran riqueza al trabajo que hoy estamos presentando en esta Cámara. Nos han acompañado desde el secretario de Estado de Telecomunicaciones con parte de su equipo, así como los máximos estamentos y representantes de los cuerpos y fuerzas de seguridad del Estado; los cuerpos de policía autonómicos; los fiscales de la Audiencia Nacional en criminalidad informática; instituciones; asociaciones que trabajan en la protección y defensa del menor como Unicef o Protégeles; representantes de asociaciones de padres; asociaciones de usuarios; empresas gestoras de redes sociales como twitter; operadores y un gran número de expertos en la materia. Por ello, señoría, les invito a que comprueben en la introducción del dictamen el gran número de personalidades que nos han aportado sus experiencias, sus visiones y recomendaciones a la hora de abordar los problemas derivados del uso de internet y de las redes sociales por nuestros menores. A ellos debemos agradecer su disposición a compartir sus inquietudes y sus esfuerzos para hacer que internet sea un mundo más seguro.

Señorías, en el dictamen que hoy presentamos a esta Cámara se reflejan los problemas a los que se enfrentan nuestros niños y adolescentes en

las redes sociales y en la red, y al mismo tiempo se incorporan los pilares fundamentales para enfrentarnos como sociedad a su minimización o erradicación.

Como bien han comentado mis compañeros, queda patente la labor educativa como herramienta fundamental en el uso de las nuevas tecnologías, pero no solo para los menores, sino también para todos los actores del mundo digital. La formación de nuestros niños, padres, profesores y usuarios en general es imprescindible para reconocer los riesgos y así reforzar la confianza digital. La escuela es un elemento esencial de socialización de nuestros niños, y es en ella en la que debemos poner todos nuestros esfuerzos para que desde edades cada vez más tempranas aprendan a convivir con las TIC y sean capaces de reconocer los riesgos inherentes en ellas. Tenemos la obligación de educar a nuestros menores para que sean conscientes de las consecuencias de sus actos y de sus conductas en la red, concienciarles de que no solo les puede afectar a ellos directamente, sino también a todo su entorno. Y para ello, como he apuntado antes, tenemos que implicarnos tanto padres como educadores y profesores, tanto empresas como Administración y, en general, toda la sociedad. Y como herramienta deberemos emprender acciones de sensibilización o alfabetización digital. Esto lo conseguiremos con campañas de divulgación, donde la colaboración de las administraciones, comunidades autónomas, asociaciones y las empresas que trabajan en el sector es fundamental.

Un objetivo que recoge el informe es la necesidad de abordar la regulación y el cambio legislativo, con la revisión y reforma de leyes existentes en el marco normativo de nuestro Código Penal para adaptarlo a la sociedad de la información y el uso de las nuevas tecnologías. Entre todos se destaca, como bien se ha comentado ya, la posibilidad de establecer la figura del agente encubierto. Desde el seno de esta ponencia, esperamos que pueda ser contemplado en la nueva reforma del Código Penal.

Es muy importante el refuerzo de la colaboración público-privada en la detección, prevención y respuesta a comportamientos lesivos para los usuarios, y muy especialmente para nuestros hijos. Al mismo tiempo hay que estimular la ciudadanía digital aprovechando las infinitas oportunidades que nos brinda internet.

Queda claro en este informe que estamos hablando de un problema global, donde la coordinación y la colaboración internacional en esta

materia son fundamentales. Y no me quiero extender más porque creo que se han comentado ya muchas cosas.

Les invito a leer el documento que hoy vamos a aprobar y, para finalizar, permítanme sumarme a los agradecimientos a don Eugenio de Santos, letrado de esta ponencia, cuyo trabajo de coordinación ha sido fundamental para el desarrollo de este año de trabajo y cuyo informe ha conseguido la unanimidad de todos los miembros de esta ponencia. Y, cómo no, mis más sinceros agradecimientos y reconocimientos por el trabajo realizado a los senadores que hemos trabajado en esta ponencia, y muy especialmente a nuestro compañero don Tomás Burgos, que ha coordinado perfectamente a todos sus miembros, logrando cumplir ampliamente nuestros objetivos.

Muchas gracias. *(Aplausos).*

El señor PRESIDENTE: Muchas gracias, senadora Azuara.

Señorías, del contenido de las intervenciones de los portavoces creo que podríamos proponer la aprobación del informe de la ponencia por asentimiento. (*Asentimiento*).

Queda aprobado por asentimiento el informe de la ponencia conjunta de estudio sobre los riesgos derivados del uso de la red por parte de los menores.

Enhorabuena a todos los miembros de la ponencia por el trabajo que han realizado. *(Aplausos).*

5. INTERVENCIONES DE LOS COMPARECIENTES PUBLICADAS EN LA WEB DEL SENADO*

* Se insertan, por el orden cronológico de las sesiones en que intervinieron, aquellas disertaciones de los comparecientes que, contando con su conformidad, fueron publicadas en la web del Senado.

COMPARECENCIA DEL SECRETARIO DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN, D. VÍCTOR CALVO-SOTELO IBÁÑEZ-MARTÍN, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 9 DE MAYO DE 2013.

El señor **SECRETARIO DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN** (D. Víctor Calvo-Sotelo Ibáñez-Martín): Muchas gracias y muy buenos días a todos. Quería empezar pidiendo perdón por el retraso.— Estaba en una conferencia del secretario de Estado de Seguridad que abordaba el tema de la seguridad en el siglo XXI y que, como no podía ser de otra manera, en parte se hablaba de las cosas que yo creo que preocupan a esta ponencia y sobre las que habrá que hablar.

Antes de pasar a la intervención, a modo de resumen general, creo que esta es una iniciativa oportuna y en un momento adecuado para que el Senado estudie en profundidad estos asuntos. Por lo tanto, quiero agradecer la invitación a venir hoy aquí y felicitarles por esta iniciativa. Porque los asuntos de los que se tiene que ocupar esta ponencia son, como ya he dicho, oportunos por dos aspectos, en primer lugar porque es un tema que preocupa mucho a la sociedad debido a su importancia. Y en segundo lugar porque estamos en unos momentos de cambio, tanto tecnológico como normativo y de aproximación a este tipo de problemas en la escala global, y que las reflexiones que se produzcan aquí pueden ser muy útiles.

Por enmarcar la presentación querría decir que, en general, desde la Secretaría de Estado de Telecomunicaciones, y como no puede ser de otra manera, vemos los asuntos de las nuevas tecnologías con optimismo, frente quizás a algunos otros sectores que ven las nuevas tecnologías más bien con temores por su propia fuerza. Yo creo que nosotros las vemos con optimismo porque esa fuerza se puede utilizar y se está utilizando para una transformación social y económica muy importante y muy provechosa, pero no hay que desconocer los riesgos que entraña. Es un fenómeno social de gran intensidad, esta es hoy una realidad fluida y cambiante.

Las nuevas redes de gran capacidad que están entrando ahora en España con más fuerza, van a cambiar de manera notable el uso y los servicios con los que nos vamos a encontrar, los nuevos dispositivos, los nuevos servicios que va a haber. Es un mundo tecnológicamente complejo, es un mundo que no tiene soluciones fáciles ni desde el punto de vista normativo ni desde el punto de vista de la tecnología.

Este es un mundo en el que la dicotomía entre libertad y seguridad o privacidad y seguridad se manifiesta, y en el que creo que una aproximación importante es saber que en la parte legislativa, en las partes normativas es muy importante buscar el espacio de la Unión Europea como actor fundamental, es decir, en la globalización, y más en el mundo virtual, donde la imposición de barreras locales no ayuda a los ciudadanos ni a los consumidores de los países. Estas barreras penalizan a las empresas que hacen negociaos en esos países porque simplemente se van a otros sitios a hacerlos. Por tanto hay que tener muy en cuenta ese nivel internacional de la cuestión. Actualmente, la propia Unión Europea ahora está en un proceso también de aceleración, de intentar conseguir que en Europa, y ese es uno de los objetivos que la vicepresidenta de la Comisión, Neelie Kroes, se ha planteado en estos quince meses que quedan de mandato en la actual Comisión, que es dar un impulso muy importante al mercado digital único en Europa. En la conciencia de que ese mercado digital único en Europa ayudará a que las empresas de este mundo digital en Europa sean capaces de competir con las de otros sitios, fundamentalmente con Estados Unidos, donde sí tienen ese mercado único digital.

Y eso tiene que llevar a una homogeneización de las condiciones en las que se mueve el mundo de las nuevas tecnologías en Europa que nos permita también tener un diálogo con Estados Unidos y con otros países para fijar unas bases mínimas de funcionamiento. Por eso digo que ahora mismo hay un impulso muy importante en la Unión Europea, la vicepresidenta Neelie Kroes se ha comprometido a presentar en la próxima cumbre de octubre un ambicioso plan de mercado digital único. Sabemos que es ambiciosa, que quiere ser ambiciosa en esta última parte de su mandato, pero no sabemos todavía los detalles.

Y también en el tiempo coincide con la nueva iniciativa de un pacto transatlántico con Estados Unidos. De las cuestiones quizá más complejas en ese pacto transatlántico de comercio con Estados Unidos, aparte de las

clásicas, como puede ser la agricultura, el mundo de las nuevas tecnologías y la sociedad de la información también tiene ahora un papel importante.

Hay actitudes y normativas distintas en Estados Unidos y Europa frente a los problemas de las nuevas tecnologías. Quizás sería, y yo creo que puede ser oportuno que a la vez que Europa avanza hacia un mercado digital único, avance en unas conversaciones con Estados Unidos para intentar crear ese marco común de las economías desarrolladas en este campo. Por eso insistía en la importancia de mirar mucho hacia el exterior, de plantear los trabajos que podamos hacer aquí como apoyo para lo que podamos defender en Europa, y lo que podamos impulsar en Europa en este campo.

Dicho esto, paso a la presentación propiamente dicha.

Empezaba diciendo que este es un fenómeno social de gran intensidad. En un momento de crisis económica, como es en el que vivimos, hacía pocos meses, prácticamente en la misma semana, venía un artículo en *Expansión* y otro en el *Wall Street Journal* contando cómo la gente se estaba quitando de otro tipo de gastos para comprarse los últimos artilugios, ya sean tabletas, ya sean teléfonos inteligentes, mejorar su plan de datos porque es una demanda social y cada vez hay mayor consumo.

Empezamos a centrar el problema hablando de diversos estudios ,muy interesantes, elaborados por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, del ONTSI, en los que se mencionan a los jóvenes. A este respecto, en el último se concluye que de los 2.600.000 niños que hay entre 10 y 15 años en España, el 91% ha usado Internet en el año 2012. Es decir, este número de jóvenes internautas supera la población de Barcelona y Valencia juntas.

Los niños y jóvenes acceden a Internet y a las nuevas tecnologías a edades cada vez más tempranas. La edad media de inicio en el uso de Internet es de 10 años, 11 en el teléfono móvil, y 13 en los *smartphones*.

Como decía, recomiendo la lectura de los informes que hay en el observatorio nacional sobre el uso de redes sociales también en Internet. En ese estudio se señala que el 61% de los usuarios declara que consultan las redes sociales diariamente, y el 84% de manera muy habitual. Los datos demuestran que las redes sociales son una parte muy importante de la vida diaria de nuestros jóvenes.

Los llamados nativos digitales, que han nacido ya en un entorno tecnológico, tienen una aproximación muy diferente a la de los adultos, ya sean padres, madres o educadores. Los adultos utilizamos Internet buscando una utilidad concreta, mientras que los niños y jóvenes viven en Internet y hacen parte de su día a día como elemento inseparable de sus días. Como usuarios avanzados aprovechan al máximo las ventajas de las tecnologías, pero al mismo tiempo son un colectivo especialmente vulnerable y en ocasiones proclive a asumir riesgos que pueden derivar en situaciones no deseadas, tales como el ciberacoso.

El ciberacoso es una de las problemáticas que está ganando más peso y conciencia en la sociedad actual. Las nuevas tecnologías hacen posible el contacto con otras personas, conocidas o desconocidas, menores o adultos, y en esta interrelación, donde es fácil ocultar la verdadera personalidad, existe el riesgo de que los menores sean acechados o acosados por otras personas.

El inicio del contacto puede proceder tanto de la víctima como del acosador. En cualquier caso, hay menores que amenazan y son amenazados a través de Internet, del teléfono móvil y las plataformas de juego *on-line*.

El acecho reviste una singular gravedad ya que puede invadir en cualquier momento los espacios del menor, provocando situaciones angustiosas para las que este puede carecer de mecanismos y criterios para reaccionar.

Mención especial merece el *ciberbullying* o el ciberacoso entre iguales, fenómeno que supone el hostigamiento de un niño hacia otro niño. Esta situación incluye acciones de chantaje, vejaciones, insultos, utilizando medios electrónicos.

Es importante también mencionar otros riesgos relacionados como el *grooming*, que es la palabra que tipifica el acoso ejercido por un adulto con el fin de establecer una relación y un control emocional sobre un menor, generalmente como fase previa a un posible intento de abuso sexual.

Este tipo de conductas de acecho es preexistente a las nuevas tecnologías, como es obvio, si bien es cierto que Internet puede ampliar su incidencia, dadas las características de anonimato, generalidad e inmediatez inherentes a la red.

Todos, mayores y menores, construimos la sociedad de la información como un espacio de convivencia, por lo que es importante que los

adultos transmitamos a las nuevas generaciones que en Internet, como en la vida real, tan importante es respetar como ser respetado.

El fenómeno del ciberacoso es un fenómeno global, y como tal supone una preocupación para los gobiernos nacionales y los organismos internacionales. En los últimos años se han desarrollado diferentes iniciativas y marcos estratégicos que tratan de combatir el ciberacoso, dentro de la actuación para la protección de los menores en Internet, e incluso como parte de los delitos asociados a la ciberseguridad.

El compromiso en la lucha contra el ciberacoso se refleja por ejemplo en las actuaciones desplegadas por organismos internacionales de protección de la infancia y en el entorno digital. Así la ITU (Unión Internacional de Telecomunicaciones), promueve la iniciativa «*Child On-line Protection*», en cuyo programa de actuaciones se contemplan diferentes actores y perspectivas y se incluyen proyectos de colaboración y cooperación, así como recursos *on-line*. También Unicef lleva a cabo estudios sobre la infancia, W-Safety como referentes en el plano internacional.

En el ámbito de otros países, Estados Unidos, que es un país en el que confluye un conjunto de iniciativas públicas y privadas que actúan en la protección del menor en el ciberespacio desde un enfoque integral, desde el plano cuenta con la *Children's On-line Privacy Protection Act* como legislación específica para la protección del menor en Internet y con programas de concienciación, operaciones de investigación y persecución de delitos contra la infancia en Internet. Asimismo Estados Unidos es referencia en cuanto a la incorporación de contenidos de seguridad en los itinerarios educativos en parte de sus diferentes estados.

En la Unión Europea, que creo —insisto— que tiene que ser el marco de referencia en el que nos tenemos que mover, la salvaguarda del menor se recoge en dos acciones estratégicas: la Agenda Digital para Europa y también la reciente Estrategia Europea de Ciberseguridad, que establecen el marco para el desarrollo de acciones concretas de lucha contra contenidos ilegales y ciberdelitos, como pueda ser la pornografía infantil, iniciativas de concienciación y alerta temprana, y campañas para la protección on-line del menor.

En este marco de la Unión Europea me gustaría destacar tres programas: el *Safer Internet Programme*, la estrategia europea en favor de una Internet más adecuada para los niños, estrategia de mayo de 2012; y por

último el Libro Verde sobre el sector audiovisual, recientemente publicado el mes pasado.

El *Safer Internet Programme* pretende luchar contra los contenidos y conductas ilícitas que existen en Internet. Se han diseñado tres programas: el primero de ellos en 1999 hasta 2004; el segundo, 2005-2008; y el vigente, que comenzó en 2009 y finaliza este año 2013.

Las actuaciones de estos programas se han llevado a cabo en cuatro grupos: proyectos financiados en el marco del programa, que han cubierto la sensibilización, la lucha contra los contenidos ilícitos, el filtrado y etiquetado de contenidos, la participación de la sociedad civil en cuestiones de seguridad en línea y la creación de una base de datos sólida de información relacionada con el uso de las nuevas tecnologías por parte de los jóvenes.

Algunos ejemplos de proyectos financiados en este ámbito son el estudio *EU Kids On-line* o los centros para un Internet más seguro, que en el caso de España están gestionados por Protégeles, que entiendo que la organización Protégeles está ya invitada como ponente por esta comisión, y que les podrán explicar más el contenido de sus actuaciones; cooperación internacional con otros países, por la lucha contra las conductas inapropiadas en la red que puedan perjudicar a los menores; foros como *Safer Internet Forum*; autorregulación, como ejemplo mediante la aprobación en febrero de 2007 del marco europeo para la seguridad en la utilización del móvil en adolescentes y niños, en el que los principales operadores móviles y los proveedores de contenidos firmaron un acuerdo para promover un uso más seguro del móvil por los adolescentes y por los niños.

Posteriormente, en el año 2009 se firmaron los principios de redes sociales más seguras en la Unión Europea, que es un acuerdo entre las principales redes sociales que operan en Europa para evaluar la seguridad de sus propias páginas o de sus propios servicios.

La estrategia europea en favor de una Internet más adecuada para los niños, que se aprueba en una comunicación, en mayo de 2012, de la Comisión al Parlamento Europeo, está enmarcada dentro de las actuaciones que se están llevando a cabo en el marco de la Agenda Digital para Europa, en concreto a través de la DG CONNECT, que es la dirección general dependiente de la vicepresidenta Neelie Kroes, y que impulsa la autorregulación

y la corregulación para proteger a los menores en la red, involucrando a todas las empresas de la red y de tecnología para crear un Internet más seguro, para evitar regular mediante directiva, dado que la regulación podría quedar obsoleta en poco plazo. Esta es una iniciativa llamada Coalición.

El énfasis —creo que es importante este concepto que adopta la propia Unión Europea— es que ante estos problemas complejos sociales el marco legislativo no es suficiente para resolver el problema, tiene que verse acompañado de una participación muy directa de la sociedad entera, de las empresas, de todos los sectores involucrados. Ante una realidad tan cambiante, los marcos de corregulación y de autorregulación son esenciales. En mi opinión ese el camino adecuado, y es el camino que ha elegido Europa. Es decir, este no es un problema que se pueda resolver simplemente a través del Boletín Oficial del Estado, exige la flexibilidad, la capacidad de adaptación de técnicas y de modelos, como es el de la autorregulación y la corregulación.

La estrategia europea se articula en torno a cuatro pilares que se refuerzan mutuamente: primero, estimular los contenidos en línea de calidad para los jóvenes; segundo, intensificar la sensibilización y la capacitación; tercero, crear un entorno en línea seguro para los niños; y cuarto, luchar contra los abusos sexuales y la explotación sexual de los niños.

En esta estrategia europea se proponen una serie de acciones que serán llevadas a cargo por la Comisión, otras por los Estados miembros y por el resto de agentes del sector.

Las actuaciones propuestas serán una combinación de instrumentos basados en legislación, autorregulación y apoyo financiero. Por otro lado, algunos países europeos están poniendo en marcha medidas nacionales, generalmente basadas en la autorregulación. En el Reino Unido, por ejemplo, los proveedores de servicios de Internet han adoptado un código de prácticas que promueve la elección activa y cuya implantación decide cada uno de los proveedores: han implantado un sistema de clasificación de los vídeos musicales por edades, han puesto en marcha mecanismos de denuncia de contenidos y comportamientos nocivos e ilícitos. En Francia los proveedores de servicios de Internet están obligados también a facilitar programas informáticos de control parental. En Alemania se puede utilizar un programa informático de protección de los jóvenes para evitar también acceder a contenidos nocivos, y algunos proveedores califican distintos tipos de contenidos en línea como

vídeos, páginas o juegos. En Finlandia también hay consenso sobre códigos de conducta; en Bélgica del mismo modo; en Italia, Republica Checa y en España hay mecanismos de denuncia de contenidos y de comportamientos nocivos e ilícitos.

En España por ejemplo, por señalar alguna otra, la semana pasada la Agencia Española de Protección de Datos, que es un ámbito que tiene su importancia en las cuestiones que aquí tratamos, ha firmado un acuerdo con Autocontrol de unas normas básicas de la utilización de *cookies* en Internet, de acuerdo con la última directiva y el último marco legislativo.

Por otro lado, el Ministerio de Educación en la ley que planteará próximamente, la Ley de educación, tiene un capítulo dedicado a las nuevas tecnologías, su importancia y su presencia en el mundo educativo. Como es normal, el Ministerio de Sanidad, que tiene las competencias de menores, tiene también distintas políticas en este campo. Es decir, este es un asunto que toca desde el punto de vista de la administración a muchos ministerios. Nosotros, desde la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información damos, por así decirlo, un soporte técnico a todos ellos.

El último punto que quería comentar sobre las actuaciones de la Unión Europea es también muy reciente, el Libro Verde sobre la convergencia entre los radiodifusores de contenidos tradicionales y el mundo de Internet. Efectivamente esa convergencia, que no va a hacer más que incrementarse con las nuevas redes de alta velocidad, es decir, con los contenidos audiovisuales a los que se va a poder acceder ahora en Internet, con las nuevas redes de fibra, incluso con las nuevas redes de telefonía móvil LTE, 4G, que tienen una grandísima capacidad de transmisión de datos, hace que podamos acceder a contenidos audiovisuales a los que antes solo podíamos por radio, o sobre todo por televisión, con una oferta muchísimo mayor, mucho más desarrollada, en la que habrá un momento en el que ya no se distinguirá muy bien qué es lo que está viendo en la tableta o en la pantalla de la tele o en la pantalla del ordenador.

Y esa convergencia obliga a replantearse cómo están regulados esos distintos sectores, porque los sectores tradicionales, precisamente por su larga historia y por su influencia importante social, tienen una regulación completa, mientras que este nuevo mundo que se está incorporando a dar prácticamente el mismo servicio no lo tiene. La Unión Europea, que —repito— creo que es el ámbito esencial donde tenemos que actuar

como país para influir en sus decisiones y para conseguir que esa posición de Europa, refleje también lo que en España consideramos adecuado, ha publicado este Libro Verde donde hace un primer análisis de cómo está esa convergencia y plantea una serie de preguntas a los países. Tenemos unos pocos meses ahora para contestarlas y para dar nuestra opinión sobre las alternativas que se ofrecen y que hay que actuar sobre ellas por la convergencia a la que hacía mención.

En el marco de la OCDE, por seguir con un último organismo internacional, se publicó en 2012 un informe sobre los posibles riesgos sufridos por los niños en la red y políticas para protegerles; un libro en el que también se recomienda la autorregulación y la corregulación, antes que una regulación *ad hoc* específica que podría no tener la flexibilidad suficiente para afrontar estos problemas. El informe de la OCDE habla de tres principios generales que deben ser cumplidos por las políticas que se vayan a tomar: fortalecimiento, proporcionalidad y valores fundamentales, flexibilidad.

Actualmente la OCDE está trabajando en un reenfoque y nuevas recomendaciones sobre seguridad y las nuevas tecnologías, donde quizá plantea que una excesiva obsesión por la seguridad puede convertirse en un inhibidor tanto del desarrollo social como del desarrollo económico. Plantea que hay que buscar ese equilibrio que incentive a la vez el desarrollo y la innovación.

Por otro lado, desde la Secretaría de Estado de Telecomunicaciones, la estrategia de la Secretaría de Estado se recoge en la Agenda Digital para España, que aprobó el Consejo de Ministros después de un proceso largo de un año de consulta con todo el sector, con la sociedad, con una página abierta a sugerencias, con contactos también con los grupos políticos, con su paso por la Comisión de Industria. Es una hoja de ruta y yo he señalado más de una vez que tan importante como el documento final era el propio proceso de desarrollo de esa agenda con un nivel de comunicación y de intercambio de información con todos los sectores concernidos muy intenso.

En términos de competencias propias de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en esta materia incluyen la protección del menor en los medios audiovisuales tradicionales, de ámbito nacional, además de Internet. En el plano audiovisual, en las televisiones nacionales la Secretaría de Estado actúa; en diciembre

de 2003 se firma un convenio para la autorregulación en publicidad, que fue un convenio también con Autocontrol, que es el mismo organismo que lo ha firmado ahora con la Agencia de Protección de Datos, con los operadores de televisiones, que ha sido calificada por todos los agentes como un éxito y que consiste en la calificación previa de los anuncios antes de emitirse. Y hay una detección preventiva y retirada de los contenidos publicitarios que pudieran infringir lo dispuesto en la Ley General de Comunicación Audiovisual.

Dentro de este convenio de corregulación merece especial atención la protección de los menores en televisión. Se han realizado en este tiempo 2.958 solicitudes de consulta previa sobre publicidad dirigida a niños en televisión durante el año 2012. De estos 2.958 casos, en 2.500 no se han apreciado inconvenientes al contenido del anuncio, en 408 casos —por lo tanto es un porcentaje significativo— esta comisión ha recomendado modificaciones, y en 50 casos directamente se ha desaconsejado la emisión del anuncio.

Yo creo que las cifras demuestran que este es un sistema que funciona, que a la vez va, por así decirlo, educando al sector en qué tipo de cosas se pueden presentar y cuáles no, pero esa acción es permanente en el tiempo, es decir, que se siguen presentando anuncios que no son idóneos, la mayoría con pequeñas modificaciones acaban siendo aceptados. Y yo creo que esta es una historia de éxito de Autocontrol que es importante señalar.

En este ámbito, en diciembre de 2004 se firmó el acuerdo para el fomento de la autorregulación sobre contenidos televisivos e infancia, entre el Ministerio de la Presidencia, el Ministerio de Industria y las televisiones. En marzo de 2010 se aprueba la Ley General de Comunicación Audiovisual, donde la competencia en materia de protección del menor sobre contenidos y protección del horario infantil recae en la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

También hay que tener en cuenta ahora que, con la creación de la Comisión Nacional de los Mercados y de la Competencia, parte de las competencias que hoy están asignadas a la Secretaría de Estado relativas a la vigilancia y seguimiento de algunos de los temas en materia audiovisual van a pasar a esta Comisión Nacional del Mercado de la Competencia, de control del mundo audiovisual de algunas cuestiones, a un órgano que es independiente en el que hay una representación más diversa, y que creo que son cuestiones que están bien llevadas hacia la comisión.

En el plano de Internet, las acciones para protección del menor desde la SETSI se enmarcan dentro del Plan Estratégico Nacional de la Infancia y de la Adolescencia, recientemente aprobado. El objetivo 3 de este plan es Medios y tecnologías de la comunicación, impulsar los derechos y la protección de la infancia con relación a los medios de comunicación y a las tecnologías de información en general. Este plan consta de nueve medidas en las que la Secretaría de Estado colabora a través de Red.es y de Inteco en educación en valores, formación y sensibilización para el acceso a Internet de los menores, seguridad en la red, estudios de opinión de los niños sobre la red, fomentar una visión crítica de la televisión, reforzar los mecanismos de control en televisión. Actualmente se está trabajando ya sobre estas medidas.

En la Agenda Digital para España, que comentaba, el objetivo 4.2 de esta agenda es reforzar las capacidades para la confianza digital, e incluye dentro de este apartado la protección de los menores en la red.

La SETSI, en colaboración con el Ministerio del Interior, ha firmado un convenio por el que se proporciona asistencia a las Fuerzas y Cuerpos de Seguridad del Estado en sus funciones de protección del menor. Las actuaciones concretas para la consecución del objetivo se desarrollan en el plan de confianza en el ámbito digital, donde se propone consolidar a Inteco —cuyo director general está hoy aquí y comparecerá más adelante ante esta comisión— como centro de excelencia en confianza digital. Y creo que ha desarrollado ya unas labores muy importantes en este mundo, siendo de especial importancia su participación.

La actividad actual de Inteco en esta materia incluye un rango bastante amplio de actuaciones. A través del portal «Menores» proporcionando servicios de información, prevención, campañas y recursos de concienciación y formación, entre otros. Inteco trabaja en elevar el nivel de ciberseguridad en Internet y en la búsqueda de soluciones tecnológicas que apoyen la investigación de ciberdelitos. Todas las actuaciones que realiza son en colaboración con diversos agentes del ámbito tanto público como privado. A través de esta experiencia y capacidades se desarrollan programas de sensibilización, de concienciación, de educación y formación, abordando de forma integral los diversos ámbitos de la confianza para todos los colectivos. Estos programas buscarán el apoyo del resto de sectores de la sociedad a través de modelos de cooperación

público-privada y potenciarán la creación de talento para lograr un foco de excelencia en España en el ámbito de la ciberseguridad.

También se impulsa la incorporación de contenidos en los itinerarios del sistema educativo, en materias de seguridad, protección de la privacidad y uso responsable de las nuevas tecnologías.

Se va a realizar un seguimiento y diagnóstico permanente de la confianza digital mediante un conjunto de indicadores e información integrada. Para ello se está actuando reforzando y racionalizando las estructuras de observatorio ya existentes y armonizando los sistemas de seguimiento con los indicadores de referencia europeos e internacionales. Insisto mucho en que todas las medidas que hacemos de observatorio y de estadísticas sean medidas que sean comparables con el resto de los países, es decir, no tener indicadores más o menos originales que se nos puedan ocurrir, pero luego no nos permitan comparar cómo lo estamos haciendo con respecto a otros países.

Desde la Secretaría de Estado se actúa también a través de la entidad pública Red.es, cuyo director general hablará después también. Red.es ha tenido una especial sensibilidad hacia todo lo relacionado con los menores en Internet, especialmente en el impulso de actuaciones encaminadas a potenciar el uso de las TIC por parte de los menores, en su desarrollo, tanto desde la perspectiva pedagógica como desde una óptica vinculada al equipamiento TIC en las aulas. Y está desde el origen de la propia institución.

Red.es tiene como vocación y misión la promoción de las nuevas tecnologías y de la sociedad de la información. Destacan, en cuestiones que ha desarrollado la empresa, el proyecto Agrega y el portal de sensibilización Chaval.es. Además apoya webs dedicadas a la protección de menores en la red, como es el caso de la que mencionábamos antes, Protégeles, u otras como pueden ser «Pantallas amigas», «Fundación aliados», «Fundación Dédalo», la Asociación de Internautas y otras.

Con esto termino la exposición y quedo a disposición de preguntas. Y volviendo al principio, creo que es un momento oportuno, creo que el propio calendario de trabajos que se han planteado es adecuado, es darle suficiente tiempo a analizar estas cuestiones. Coincide en el tiempo con el desarrollo de la Agenda Digital para España, el desarrollo de una política europea más unificada en todas las cuestiones que tienen que ver con

el mundo de las nuevas tecnologías y de la sociedad de la información. Y que dentro de ese ámbito, como he dicho al principio, este es un fenómeno social muy intenso, con muchas derivadas. Y yo creo que es importante la reflexión que desde un órgano como el Senado se puede hacer, convocando a todas las partes afectadas, y que con las conclusiones que se puedan derivar de estos trabajos podamos reforzar también la acción del propio Gobierno y de las iniciativas legislativas, tanto nacionales como internacionales, que se ocupan de este problema.

Muchas gracias.

COMPARECENCIA DEL DIRECTOR GENERAL DE RED.ES, D. FRANCISCO DE BORJA ADSUARA VARELA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 9 DE MAYO DE 2013.

El señor **DIRECTOR GENERAL DE RED.ES** (D. Francisco de Borja Adsuara Varela): Muchas gracias, señor presidente y señores senadores.

Es un honor para mí comparecer en la ponencia y venir de nuevo a esta casa, al Senado, porque, aparte de venir hoy como director general de Red.es, he sido asesor parlamentario durante muchos años, del Congreso y también del Senado. Por lo cual, la siento un poco también como mi casa. E, incluso, cuando dejé de ser asesor y pasé al Ministerio, en mi primera época, me acuerdo de que me invitaron a participar en otra Ponencia de estudio. En aquella ocasión era sobre los concursos en televisión, porque en la Dirección General para el Desarrollo de la Sociedad de la Información llevábamos también los temas de televisión, aparte de los de Internet. Y he venido más veces, y lo volveré a hacer la próxima semana, a celebrar el día de Internet en el Senado. Una cámara que desde los inicios de Internet ha estado muy sensibilizada con los temas de la red. De hecho, hubo aquí una comisión muy activa, la Comisión de Sociedad de la Información, en los comienzos de ésta. Por todo lo cual para mí es un placer y un honor volver a esta casa para hablar de Internet.

Quería antes de nada, porque creo que es de buena educación, presentarme, porque comparezco por mi actual cargo de director general de Red.es, pero ya he dicho que también estuve como director general para el desarrollo de la sociedad de la información, cuando se creó la primera dirección general y las primeras políticas de la sociedad de la información hace ya doce años. Y ha cambiado mucho la cosa desde entonces: no había redes sociales, porque la Sociedad de la Información estaba empezando. Me gusta decir que ahora estamos en la adolescencia de la Sociedad de la Información. Ya ha dejado de ser una niña, todavía no es una sociedad de la información consolidada y madura. La adolescencia, los que tenemos hijos adolescentes lo sabemos, es una edad muy importante, porque todavía no son personas maduras y es en esta época cuando se fija la personalidad que va a tener cuando sea un adulto. Y yo creo que

es el momento que nos toca vivir ahora en estos temas, donde es verdad que ya se han hecho cosas y se ha avanzado, pero todavía, en fenómenos muy recientes como el de las redes sociales, estamos dando los primeros pasos y tenemos que orientar bien hacia dónde se tienen que dirigir.

Por otra parte, cuando no he estado en los ministerios, lo que realmente soy es profesor de derecho, especializado en temas de derecho de la sociedad de la información; y muy especialmente, en temas de derecho de la información, derecho de los contenidos y derecho al honor, la intimidad y la propia imagen, con una especial atención a temas de protección de la infancia, información al consumidor, etc., que creo que también tienen mucho que ver con el que hoy nos ocupa.

Como Director General de Red.es explicaré las iniciativas que desde Red.es se han realizado, no solo en este último mandato, sino en toda su existencia, porque hay que agradecer que en todas las políticas de telecomunicaciones y sociedad de la información ha habido una continuidad desde el origen de las mismas y, de hecho, las instituciones que se crearon al principio (Red.es tiene más de diez años) han continuado y se han reforzado.

Inteco mismo, cuyo director general hablará después de mí, nació del seno de Red.es y, por la importancia que fue adquiriendo, se independizó y especializó en temas de ciberseguridad. Es un buen ejemplo de que ha habido siempre una política de continuidad y mejora en estos años. Y creo que eso es muy de agradecer.

También quiero añadir una cuestión personal, por lo que yo pueda aportar y resulte de interés. Y es que, además de Director General de Red.es y Profesor de Derecho especializado en temas de internet, soy un usuario intensivo de las redes sociales, y es bueno hablar de estos temas «desde dentro», porque seguramente vendrán muchos expertos para hablar desde fuera, pero estos fenómenos conviene vivirlos en primera persona. Sé que muchos de los senadores también están en la red y hacen como yo; cada vez que hay un tema polémico, preguntan en la red qué se opina sobre ello y esa actitud nos acerca a la realidad.

Es bueno tener esa sensibilidad, porque —y anticipo una de las conclusiones— en Internet y en la red hay una cierta reticencia a todo lo que suponga un intento de control excesivo, de encorsetamiento, porque tiene sus propias normas y no va mal la autorregulación y el

autocontrol que se va estableciendo en ámbitos de libertad y al mismo tiempo de seguridad. Porque hablaremos de eso en la ponencia, igual que lo ha hecho el Secretario de Estado: no todo se consigue con la regulación externa y con medidas coercitivas, sino fomentando la autorregulación y el autocontrol y, sobre todo, la educación, incluso la «netiqueta» de los internautas. Yo creo que es básico. Por eso, una de mis conclusiones, ya la anticipo, como usuario y tuitero intensivo y como padre también de adolescentes con uso muy intensivo de las redes sociales, es que las prohibiciones no sirven de nada, porque se les puede quitar el móvil, pero lo van a hacer a través del teléfono de amigos. Por eso hay que intentar educarles, en el mismo sentido de la comparación que ya se ha puesto aquí, porque una cosa es conducir el coche y otra cosa es saber circular. No sólo hay que aplicar el código de circulación, sino que también debe haber educación vial. Son los dos aspectos que vamos a tratar.

En cuanto a la moción y el objeto de estudio de la ponencia, me la he leído con mucho detenimiento, quizá por deformación profesional de cuando era asesor parlamentario. Y me gustaría hacer —y en esto va a consistir la primera parte de mi presentación— **cinco consideraciones** genéricas, o de concepto, sobre el objeto de estudio, para ver si pueden ayudar a dar alguna idea para la delimitación del mismo, porque, si no, puede resultar demasiado amplio.

Luego comentaré **cinco medidas** o iniciativas que se han puesto en marcha desde Red.es. Algunas ya las ha dicho el secretario de Estado, y otras las explicará el Director General de Inteco, que es la entidad que, de una forma más intensa, ha trabajado el tema de los menores (a través de la Oficina de Seguridad del Internauta, en menores.osi.es). Yo me limitaré a contar lo que se ha hecho en estos diez años desde Red.es, centrándome en cinco medidas.

Y terminaré mi intervención con **cinco conclusiones** (como actual director general de Red.es y también personales, aunque solo sea por la experiencia propia de estar en las redes) de por dónde creo yo que se podría orientar este tema de la presencia y el uso de las redes sociales por los menores.

Mis **cinco observaciones** en cuanto al objeto de estudio de la ponencia tienen que ver con estos temas (he cogido frases entrecomilladas de la moción, porque a lo mejor se puede hacer algún comentario):

Primero: el nombre y la materia de la ponencia es «riesgos derivados del uso de la red por parte de los menores». Y se me ocurren una primera consideración, una pregunta que a lo mejor nos tenemos que hacer. En el título se habla de «la red», en singular, y más adelante, en el cuerpo de la moción, se habla de «las **redes sociales**», en plural. ¿Son cosas distintas? Lo digo porque, aunque es verdad que ahora se han configurado las redes sociales como un hecho novedoso en Internet, ¿qué es Internet sino una red social desde el comienzo? «La red» es una red social, es una red de personas, no es una red de ordenadores, es una red de personas que están detrás de los ordenadores. Y, antes de que existiera Facebook o Tuenti o Twitter, existía —yo me acuerdo— en los orígenes de internet, por ejemplo, el ICQ, que era el antecedente del Messenger y del WhatsApp. Y tampoco está muy claro si Twitter es una red social o un medio de comunicación, si WhatsApp, con sus grupos, es una red social. No se sabe. Entonces, al final, aunque hablemos de las «redes sociales» —en plural— como un fenómeno novedoso, yo creo que la red —en singular— es una red social o no es nada. Porque, de hecho, sirve para unir personas. Las distintas aplicaciones que se hagan son las que pueden variar, la forma de conectarse las personas, pero los que ahora estamos en Twitter, antes usábamos el correo electrónico, los grupos de correo, las listas de distribución, los foros, etc.

RedIRIS, por ejemplo, que es otra de las competencias que tiene Red. es, fue el origen de Internet en España y desde el comienzo tenía grupos de discusión, que es lo más parecido a las redes sociales actuales. Con lo cual, creo que nos deberíamos preguntar qué es una red social y qué tipos de redes sociales hay, porque hay muchos tipos de redes sociales. Y eso sí tiene consecuencias, jurídicas incluso, porque no es lo mismo Facebook que Tuenti. Hay redes sociales que son abiertas y que te puede ver todo el mundo y se publica y se indexa en Google el contenido —como es Facebook— y hay otras —como Tuenti— que son clubes privados, donde solo puedes entrar por invitación, y no se publica ni se indexa el contenido en Google, y en donde la cuestión de la privacidad, precisamente por ser española y estar sujeta a las leyes españolas, es mucho más estricta.

Por eso, quizá no es justo meter a todas las redes sociales en el mismo saco, porque se asimilan unas, que son más laxas, con otras que lo están haciendo muy bien y son más estrictas, entre otras cosas porque están en España. Y eso, más que verlo como un inconveniente, puede tenerse

como una ventaja competitiva, porque los padres pueden estar mucho más seguros si sus hijos están en Tuenti que si están en Facebook, porque saben que la primera cumple y se atiene a la normativa española, a la jurisdicción española y a la Agencia de Protección de Datos, que es especialmente activa en estos temas.

El **segundo** concepto —que parecerá de Perogrullo, pero luego no lo es tanto y también tiene consecuencias jurídicas— es qué es un menor. Porque cuando decimos «**menores**», claro, nos referimos a un menor de edad; menor de 18 años. Pero ¿es lo mismo un menor de 13 años que un menor de 18 años, sobre todo en las redes sociales? ¿O un menor de 14? Además, ¿dónde ponemos los tramos? Porque, a efectos del Código Penal, sí hay diferencia en determinados delitos si es un menor de 13 años o es de 13 a 16 o de 16 a 18. Luego, estamos hablando de si para entrar en una red social tienes que tener 14 (no sé por qué 14 y no 13). Yo creo que hay que hacer un esfuerzo para reflejar en las leyes lo que ocurre en la realidad. Y es que, aunque es una ficción jurídica que a los 18 años alcanzamos la mayoría de edad plena, la mayoría de edad es progresiva, como la madurez, y en la educación no es lo mismo un niño de primaria que un niño de secundaria o de bachillerato. Al niño se le va educando según puede entender las cosas.

Como éste es un tema, sobre todo, de educación, hay que ir progresivamente educando a los menores de edad en el uso de las nuevas tecnologías, según la etapa de la minoría de edad en la que están. Porque no es lo mismo los jóvenes de 14 a 16 años, que los de 16 a 18, que los menores de 14 o los menores de 13 años.

Creo que sería bueno el tener eso presente porque luego, si lo ponemos en conexión con determinados delitos, llegamos a casos que a la gente les choca. Por ejemplo, ¿cómo puede haber una edad a partir de la cual los jóvenes pueden tener relaciones sexuales consentidas —y no es ningún delito, porque se considera que son maduros para tenerlas—, y sin embargo, si se fotografían o graban ellos mismos están cometiendo un delito de producción de pornografía infantil? Porque el delito de «pornografía infantil», aunque se dice «infantil», se refiere a un menor de edad, un menor de 18 años. Por lo cual, aunque tenga 17 años, 11 meses y 29 días, sigue siendo un menor de edad. Entonces, habrá que tener alguna consideración a los tramos de edad, para que coincidan las cosas que se pueden hacer en el mundo físico con determinadas edades

(aunque se sea todavía menor de edad) con las cosas que se pueden hacer en el mundo virtual, en la red, y no tratarles como delincuentes (sobre todo, aplicándoles un tipo penal que está pensado para mayores de edad que abusan de menores). Y no me decanto en un sentido o en otro, digo que haya coherencia. Y para eso está el Legislativo, para ver cuáles son los tramos de edad que hay que tener en cuenta en relación con los menores, y no tratar igual a todos los menores de edad, sino determinar las consecuencias jurídicas que deben desprenderse de cada tramo de edad.

En tercer lugar, se habla en la ponencia de los ámbitos relacionados con la prevención y la lucha contra los nuevos delitos cibernéticos. Y eso me plantea una reflexión, y es: la prevención y la lucha tienen que ver con medidas de educación, formativas, divulgativas, y policiales. Pero creo que hay otras que, quizá por obvias, por implícitas, no se citan, que son las **legislativas**. Y ésta —también es una de mis conclusiones— es una de las cosas más importantes que tendrían que salir de esta Ponencia, que puede ser un mandato al Gobierno o un automandato al Parlamento, y es revisar las leyes que existen en el marco normativo para adaptarlo a la sociedad de la información.

Se ha hecho en algunas leyes, en otras no. Pondré un ejemplo. Cuando se habla de «los nuevos delitos cibernéticos», digo: ¿son tan nuevos?, ¿realmente hay nuevos delitos cibernéticos o hay nuevas formas de comisión de los delitos de siempre? Porque los «ciberdelitos» que salen en las noticias son o delitos contra el honor (de injurias y calumnias), o delitos contra la intimidad (de descubrimiento de secretos o revelación de secretos), o delitos de coacciones y amenazas, o delitos de corrupción de menores (de pornografía infantil o exhibición de pornografía a un menor). Son más o menos los cinco delitos que pueden darse. Esos ya están en el Código Penal. Lo que ocurre ahora es que han aparecido nuevas formas de comisión de esos delitos, que antes se hacían con medios físicos y ahora se pueden hacer con medios electrónicos. Por la especificidad del medio electrónico, a lo mejor requieren alguna especificidad legislativa, o por lo menos, como dicen los italianos, un *aggiornamento* de las leyes que ya existían, para adaptarlas a la sociedad de la información y al nuevo entorno digital.

En la Constitución de 1978, la piedra angular de nuestro ordenamiento, se regulan estos temas en el artículo 20 y en artículo 18: la libertad

de expresión y, en general, el derecho de contenidos, en el artículo 20; y el derecho al honor, la intimidad y la propia imagen, en el artículo 18.

Y en 1982 se aprobó la Ley Orgánica de Protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen. Pero en 1982 apenas se conocía la microinformática e Internet no existía. Luego hemos visto —iba a decir «padecido»— la evolución que han tenido, no ya en Internet, sino incluso en la televisión todos los temas relacionados con la intimidad. No parece que fuera muy adecuada la ley de 1982, pero no se revisó. Hemos tenido que esperar a que haya jurisprudencia del Supremo, que siempre es lenta. Por eso, a lo mejor ha llegado el momento de hacer el *aggiornamento* de la ley de 1982 para adaptarla a la sociedad de la información.

Sí ha ocurrido, por ejemplo, en materia de Protección de Datos, que desde la LORTAD hasta la LOPD se ha ido actualizando en estos temas. Pero, aun así, debe seguir adaptándose ante fenómenos nuevos, que están ahora explotando, como las redes sociales o la mensajería por móvil.

También ocurre con la Ley General de Comunicación Audiovisual, que está pensada para televisión, para los contenidos en televisión, y también sucede con el convenio de autorregulación de contenidos para la protección de la infancia, que estaba pensado para televisión. Pero los contenidos de Internet y, sobre todo ahora, los contenidos en los móviles, ¿con qué ley los vamos a tratar?, ¿con la ley pensada para televisión, basada en horarios de protección; cuando los horarios en Internet son un poco absurdos?, ¿tiene sentido hacer franjas de protección horaria para menores en internet? Con lo cual, tendremos que ver qué regulación se hace para proteger a los menores en Internet, en relación con determinados contenidos que pueden ser nocivos para ellos.

Son necesarias adaptaciones a la nuevas tecnologías, de leyes que existían muy vinculadas a tecnologías antiguas.

Ya he dicho que los nuevos delitos yo creo que no son tan nuevos, son los viejos delitos de siempre con nuevas formas de comisión. Pero es verdad que hay una especificidad que hay que tener en cuenta. Igual que la especificidad del comercio electrónico hizo que se aprobara una ley en 2002 de comercio electrónico, o la especificidad de la administración electrónica hizo que se aprobara también una ley de administración electrónica en 2007. Pero, al final: ¿hay dos administraciones distintas,

la electrónica y la que no es electrónica? No, la administración es única. Lo que pasa es que hay que regular los nuevos canales electrónicos. Pero no hay un procedimiento administrativo distinto, es el mismo procedimiento administrativo. Pues también los delitos serán los mismos delitos, pero con formas de comisión distintas: unas seguirán siendo físicas y otras serán electrónicas.

Aparte de esas medidas legislativas de regulación, hay que fomentar, como decía antes, la autorregulación. Porque no todo se resuelve con el Código Penal; ni siquiera con las leyes civiles o las leyes administrativas con un régimen sancionador. Hay que fomentar la autorregulación porque Internet ha dado buenas muestras de que la gente se autoorganiza bien, y que hay cosas que se consienten y cosas que no se consienten. Todas las instituciones y empresas que están en Internet tienen la posibilidad de poner condiciones o términos de uso de sus servicios y contenidos; e, incluso, existe la posibilidad de acordar convenios sectoriales de autorregulación, códigos de autorregulación. Hay que fomentarlo, porque se resuelve mucho más por esta vía, que —a lo mejor— con sistemas sancionadores, administrativos o penales, que además son mucho más lentos, e Internet va muy rápido. Por eso, quizás es mejor poner de acuerdo a los agentes de Internet sobre qué cosas se pueden y no se pueden consentir, para que ellos mismos se autorregulen. Por esta vía, además, pueden las redes sociales, aparte de cumplir con la ley, ir incluso un poco más allá de la ley y decir: «esto será legal, pero yo no lo quiero en mi red social».

Podemos abrir otro debate, que es el de si los términos de uso pueden más que la libertad de expresión. Pero, en todo caso, ahí hay un amplio margen para la autorregulación.

Cuarta observación. Se fija la ponencia en los temas de «acceso» de los menores a las redes sociales, y en la utilización de la información personal y privada, es decir, la privacidad. Yo decía antes que también encontramos los temas de honor, que esa es la denominación más tradicional, o los temas de la propia imagen, que es por donde van ahora las nuevas tendencias, y creo que son muy importantes. Incluso me atrevería a decir que ya no la imagen sino la identidad digital y los temas de la usurpación de la identidad digital, etc., son temas que hay que regular, y me consta que ya hay alguna iniciativa legislativa en ese sentido.

Pero también es importante —insisto— el tema de los contenidos; no solo la persecución de contenidos directamente delictivos, como es la

pornografía infantil, sino la regulación de contenidos que, siendo legales, son contenidos para adultos y pueden ser nocivos para los menores, para el desarrollo psicológico de un menor.

Pero incluso iría más allá: podemos ser mayores de edad y sin embargo no querer ver determinados contenidos. Por lo que, aparte de la protección de menores, que es lo que nos trae hoy aquí, ese sistema de regulación de los contenidos también tiene que ir orientado a la información al consumidor. Para que cada uno, igual que cuando vas a comprar un alimento viene el etiquetado y sabes, si eres celiaco, que si tiene gluten no lo puedes tomar, porque te va a hacer daño, que cada uno, aunque sea mayor de edad, sepa por un sistema de información cuáles son los contenidos y pueda elegir si quiere verlo o si no quiere verlo; o como padre, si quiere que lo vean sus hijos o no. Creo que en los temas de los contenidos también hay un margen para la regulación y la autorregulación.

No me meto en temas de propiedad intelectual, porque entonces haríamos otra ponencia, así que lo dejaremos en el «control de contenidos», no solo para la protección de los menores, sino como información para los consumidores y usuarios, Al ser ya todos los contenidos digitales y tener la posibilidad de llevar, no ya una señalética visual como hasta ahora en los programas de televisión o en las películas, sino un conjunto de metadatos para poder identificar los contenidos, igual que los motores de búsqueda sirven para encontrar esos contenidos, la misma tecnología utilizada inversamente sirve para bloquear contenidos, los que no queramos ver nosotros o los que no queramos que vean nuestros hijos menores. Es otro campo que yo creo que está empezando y que tiene un largo recorrido, y hay países que ya están trabajando en ese sentido.

Por último, y es la **quinta observación**, se hace referencia en la ponencia a centros escolares, profesores y educadores, empresas gestoras de redes sociales y Fuerzas y Cuerpos de Seguridad del Estado. Y me ha parece que hay un olvido, aunque ha sido subsanado en las intervenciones de los miembros de la ponencia: ¿y los **padres**, qué? ¿Dónde están los padres? Porque en el texto de la moción no aparecen los padres por ningún lado. Yo creo que los educadores y los profesores y los centros escolares tienen una responsabilidad, pero la primera responsabilidad la tienen los padres, que son los responsables de la educación de sus hijos. Porque, además, si el menor está en el colegio, en clase (y atendiendo), tiene poco tiempo para estar en las redes sociales. Realmente es fuera del

colegio cuando pueden ser más activos. Con lo cual sí es muy importante implicar a los padres, y me consta que luego habrá comparecencias en representación de los padres y educadores fuera del ámbito escolar.

Simplemente quería dejar constancia de esta omisión el texto de la moción, que me ha sorprendido. Sé que ha sido subsanada, por lo que, simplemente, ha sido un lapsus y no le doy mayor importancia.

Después de las cinco observaciones genéricas o de concepto, voy a hablar de lo que ha hecho Red.es en estos años. Me centraré en las **cinco medidas** que son las que más se conocen de Red.es, pero aparte hay una multiplicidad de pequeñas intervenciones que a lo mejor se conocen menos (se proyecta una presentación).

Primero, unos gráficos del Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información. Son datos que ya ha dado el secretario de Estado.

En usuarios de Internet, ya estamos en los 30 millones. Hogares con acceso a banda ancha, estamos en el 66,7%, que es un poco mayor, porque esto son hogares con acceso a banda ancha fija, pero nos hemos dado cuenta de que ya hay muchas personas, especialmente jóvenes, que no contratan la línea fija en casa, se conectan directamente con su móvil. Porque por Internet móvil también hay banda ancha, que, además cada vez va a ser más rápida, cuando funcionen los servicios 4G. Por lo que cada vez más gente optará por conectarse a internet por banda ancha móvil.

Estos son los niños que usan Internet (para ser usuario se ven los accesos en los últimos tres meses) y estamos en un 91,2%, según fuentes del Instituto Nacional de Estadística. Estas estadísticas sobre niños varían por lo que decía antes: según el tramo de edad que se coja. Hay algunas fuentes que solo cuentan a partir de los 14 años; otros desde menos. ¿Qué es un usuario de Internet? El que se conecta a Internet. Incluso ahora, no está claro que esa definición valga, porque los jóvenes no se conectan a Internet, viven en Internet. Es la era del *allways on*, permanentemente conectados, incluso demasiado conectados, porque algunos adolescentes duermen con el móvil debajo de la almohada, por si les mandan un mensaje en mitad de la noche.

Red.es, para quien no la conozca, nació en el año 2002 y depende de la Secretaría de Estado de Telecomunicaciones y Sociedad de la Infor-

mación. Inteco es una «hija» de Red.es, que cobró independencia por la importancia que justamente ha adquirido, y va a adquirir cada vez más, la seguridad y la confianza en Internet. Y CENATIC es una fundación que se dedica a la promoción del software libre o de fuentes abiertas.

Aparte tenemos otras fundaciones en las que participamos como Patronos: la EOI, que es la Escuela de Organización Industrial, a través de la cual estamos orientando y canalizando toda la formación en nuevas tecnologías, tanto de máster como de formación profesional y de formación certificada de soluciones de empresas; CENTAC, es una fundación en la que participamos para los temas de accesibilidad; y FUNDETEC, que es una fundación privada de empresas del sector TIC en la que estamos también desde el principio apoyando, no solo cuestiones de alfabetización y de educación (hay un programa para menores, para educar en el buen uso de internet), como también en temas de pymes, que es uno de los temas —aunque no sea el objeto de la ponencia, lo digo— en los que España está un poco por debajo de la media europea, especialmente en el número de micropymes que están en Internet. Y últimamente está desarrollando funciones también en *smart cities*, manteniendo la secretaría de la Red Española de Ciudades Inteligentes, y apoyando todo el desarrollo que están impulsando los ayuntamientos.

Las **principales iniciativas**, he escogido cinco para no alargarnos, son éstas:

1º) La iniciativa más antigua es la de Internet en la educación. Empezamos por el equipamiento y la conectividad y luego fuimos a los contenidos educativos. Tenemos el **proyecto Agrega**, que es un agregador de contenidos educativos. Es importante que en las redes sociales y en la red, en general, haya contenidos educativos de calidad y de formación en valores, para poder educar a nuestros niños en el uso de nuevas tecnologías.

2º) Uno de los primeros proyectos que hicimos desde Red.es, en el año 2002, es **Chaval.es**. Que nació, incluso, creo que un poco antes que Protégeles. Porque ya en los inicios de Internet se vio que hacía falta educar tanto a los chicos como a los padres y educadores en el uso de Internet. Es un proyecto del que nos sentimos muy orgullosos y que ha recibido muchos premios. Luego explicaré la evolución que ha tenido, porque ahora lo orientamos más directamente a los padres, porque los chicos ya no entran en chaval.es como antes; ahora entran directamente

en las redes sociales. Y chaval.es ha quedado como un repositorio de información y de recursos para padres y tutores.

3º) Estamos trabajando junto con la Secretaría de Estado, y en la línea que se sigue en otros países, en el tema del **etiquetado de contenidos**.

Hay una primera fase que consiste en ponernos de acuerdo en usar la misma señalética para contenidos con independencia de las ventanas en las que éstos se ven; porque las películas de cine tienen una señalética, los programas de televisión tienen otra, los videojuegos tienen otra,… y uno se pregunta: ¿por qué la película, si se proyecta en pantalla grande, va a estar calificada de una forma, si va a la pantalla pequeña de la televisión, que ya no es tan pequeña, va con otra señalética, y cuando esté en el PC o en el móvil, qué señalética va a tener? ¿Vamos a crear una nueva señalética? ¿No tiene más sentido que la señalética la lleve el contenido, con independencia de la pantalla? Si la prescripción por edades (que realizan psicopedagogos que conocen lo que pueda afectar a un chico en su evolución, por tramos de edad) va unida al tipo de contenido, a la naturaleza del contenido, lógicamente tendrá que ser la misma lo veas en una pantalla o en otra. Ése creo que es el primer paso que hay que dar, el de la homogeneización de la señalética de los contenidos.

¿Cuál es el segundo paso? El del etiquetado con metadatos; el etiquetado que no conlleva un símbolo en la pantalla, pegado encima del contenido, sino que se basa en una red semántica de etiquetas que permiten realizar tanto la búsqueda como el filtrado. Pero ése es el paso en el que todavía no están claras las cosas. Aunque ya hay grupos de trabajo, que están avanzando en esa línea, en los países que quieren ofrecer herramientas a los consumidores y usuarios y a los padres para que ellos sean libres de decidir lo que quieren ver y lo que no quieren ver, o lo que quieren que vean sus hijos o no quieren que vean sus hijos.

4º) La **cuarta iniciativa** que tiene Red.es en el tema de Internet y menores es una iniciativa que hemos recuperado y que ya pusimos en marcha en los albores de Internet y en los inicios de Red.es, donde que existió desde el comienzo un **grupo de trabajo** público-privado de «Internet y menores». Lo hemos recuperado en esta nueva etapa. Funcionó muy bien.

Realmente son varios grupos, porque hay un grupo de coordinación de la Administración General del Estado, otro con las Comunidades Autónomas y otro con las Entidades privadas (Asociaciones y Fundaciones) que trabajan en estos temas de «menores e internet».

En el grupo de coordinación de la Administración General del Estado, están presentes el Ministerio de Industria (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, INTECO y Red.es), el Ministerio del Interior (Secretaría de Estado de Seguridad, Policía y Guardia Civil), el Ministerio de Justicia, el Ministerio de Educación, y (aunque no sé si comparecerá en esta Ponencia) el Ministerio de Sanidad, Servicios Sociales e Igualdad (Dirección General de Familia e Infancia y el Instituto de la Juventud). Y también se ha propuesto y aceptado que participe la Fiscalía del Menor.

Creemos que era importante recuperarlo porque no había una voz «oficial» en estos temas. Sí había asociaciones privadas que realizan un trabajo muy meritorio, pero faltaba un organismo oficial de coordinación en esta materia de los distintos ministerios afectados.

5º) Por último, me referiré muy brevemente, es el **estudio del Observatorio** Nacional de Telecomunicaciones y Sociedad de la Información sobre las redes sociales, donde daré algunos datos del uso de las redes sociales.

Voy a ir muy rápido, porque casi he resumido las diapositivas que vamos a ver a continuación, y además quiero pasar lo antes posible a las preguntas, que creo que van a ser lo más interesante de la comparecencia.

El **proyecto Agrega** se puede encontrar en la página de Red.es. Insisto, está hecho con el Ministerio de Educación. También con el Ministerio de Educación estamos participando en el Plan Estratégico de Educación, en el que va a haber un eje sobre la seguridad de los menores y lo vamos a desarrollar de acuerdo con ellos, con el Instituto Nacional de Tecnologías de la Educación y de la Formación (INTEF). Agrega, sobre todo, se refiere a contenidos educativos que van a estar disponibles para que los puedan usar en cualquier centro. Es una plataforma tecnológica y está hecha en colaboración del Ministerio de Educación y con todas las consejerías de Educación de las comunidades autónomas. Estamos ahora en una fase de evolución de esa plataforma a una plataforma semántica para poder manejar mejor y gestionar mejor esos contenidos educativos.

Chaval.es nació para promover prácticas seguras del uso de TIC entre los niños. En aquellos momentos en que Internet se abría como la mar océana y los padres nos quedábamos intranquilos si los niños se metían en Internet, la idea era funcionar como cuando uno baja en verano a la piscina, y si tiene niños pequeños y se quedan en la piscina para niños,

uno está muy tranquilo, y si se quieren meter en la piscina grande, pues ya le tiene que poner los manguitos y estar más atento. Pues chaval.es era la piscina para niños: un conjunto de webs seguras, con contenidos especialmente orientados a niños. Mientras estuvieran en ese entorno, porque no era una página web, sino una galaxia de páginas web, podías estar tranquilo de que no iba a ver cosas que no debía ver o hacer cosas que no debía hacer.

También desde el principio, no solo se trataba de orientar y recomendar contenidos para niños, sino de formar a los adultos, tanto a los padres como a los educadores, para saber cómo tenían que comportarse con los niños en Internet.

Nos hemos dado cuenta de que la situación en 2013 no es la misma del 2002, cuando nació, y que ya no entran tantos chavales en chaval.es; van directamente a las redes sociales. Y, por eso, la hemos reorientado justamente al *target* de padres y tutores, para que encuentren ahí recursos en todo lo que quieren saber sobre la red o las redes sociales, para poder saber lo que están haciendo sus hijos y educarles convenientemente de cómo deben circular por la red y por las redes sociales.

Recientemente hemos recibido un premio, con lo cual parece que también está siendo útil. De hecho, tenemos estadísticas tanto de visitantes de la web como de seguidores en Twitter o en Facebook, que demuestran que es un recurso útil para padres y tutores en todo lo que se refiere a información sobre el uso por los menores de Internet en general y de las redes sociales en particular.

Éstas son distintas acciones que se han hecho dentro de la marca Chaval.es: jornadas de Internet dirigidas a la infancia, una semana en 2008 de entrega del decálogo de buen uso de Internet, el congreso «Internet en el aula», jornada de buenas prácticas en la infancia y adolescencia, la estación Chaval.es en la quinta edición del día de Internet, una campaña de Navidad, unos premios que dimos Chaval.es.

Y éste es el posicionamiento de Chaval.es dentro de todas las acciones que hay sobre menores e Internet; Chaval.es está en contenidos, servicios, juegos de calidad, oportunidades, en el área de responsabilidad social corporativa. Y no nos metemos tanto, como por ejemplo está Protégeles, en las líneas de denuncia. No es la función de Chaval.es. Es más de recomendaciones en positivo que de denunciar contenidos negativos.

Éstas son todas las relaciones con colaboradores; porque alrededor de Chaval.es hemos colaborado, como decía el secretario de Estado, con instituciones públicas y asociaciones privadas, que son las mismas que se van a integrar también en el grupo de trabajo de menores e Internet.

El proyecto de **etiquetado de contenidos digitales**, como ya he explicado, va a partir, primero, como un intento de homogeneizar el etiquetado de todos los contenidos con independencia del formato o de la ventana en que se vean, y luego queremos avanzar en el estudio del etiquetado de metadatos junto con los países de nuestro entorno, porque eso sí que no lo puede hacer España en solitario. Si hay una solución en este sentido, tendrá que ser europea como mínimo, y, seguramente, tendrá que ser mundial. Porque no conseguiremos nada si España etiqueta los contenidos de una forma, pero solo lo hacen los españoles. Por lo cual, este asunto tiene que pasar por acuerdos y estándares internacionales. Al igual que ha habido protocolos de internet para poder ver las páginas web o para poder recibir los correos electrónicos, puede haber también protocolos de Internet para el etiquetado de contenidos. Insisto, esto está naciendo; yo creo que todavía tiene recorrido, pero es un tema que puede ser muy importante.

En el **grupo de trabajo**, al que también me he referido, está la secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, a través de la Subdirección General de Contenidos de la Sociedad de la Información, en la parte regulatoria; está Red.es, en la parte de fomento de la sociedad de la información; está Inteco, como un referente en toda la actuación que está haciendo en el tema de seguridad y confianza; también está Secretaría de Estado de Seguridad, la Policía y la Guardia Civil, por parte del Ministerio de Interior; está el Ministerio de Justicia, la Dirección General de Evaluación de la Educación por parte del Ministerio de Educación; la Dirección General de Familia e Infancia y el Instituto de la Juventud, por parte del Ministerio de Sanidad, Servicios Sociales e Igualdad; y la Fiscalía del Menor, que también se acaba de incorporar.

Creo que es un buen grupo de trabajo, que se reunirá con las asociaciones privadas que trabajan en estos temas para coordinar esfuerzos. Y que también hará de pegamento (desde Red.es lo hemos hecho siempre, en todos los proyectos) con las Comunidades Autónomas.

El **estudio del observatorio** sobre redes sociales es de 2011. Está enfocado no tanto al uso que los menores hacen de ellas, sino, en general,

en la definición, tipologías, frecuencias, motivaciones en la utilización en la empresa de las redes sociales. O sea, que es genérico. Pero sí hay algunos datos que podemos extraer referidos a menores. Sobre todo, el principal es que el uso mayoritario de las redes sociales se realiza por menores de 20 años. Es más, yo diría que entre 15 y 20, que coincide con la afirmación que hacía antes de que estamos en la adolescencia de la sociedad de información y el uso intensivo es el de los adolescentes, sobre todo de las nuevas modalidades de sociedad de la información, que son las redes sociales.

Hasta aquí era la presentación que quería hacer de las cinco iniciativas. Y quería terminar, a modo de propuesta y por si pudiera tenerse en cuenta alguna en las **conclusiones** de la ponencia, dando las mías personales. Y son estas:

Primera conclusión (esto lo he preguntado en las redes sociales y es lo primero que me han dicho): no hagamos una aproximación, ya no exclusivamente, sino ni siquiera prioritariamente policial al tema de los menores en las redes sociales. En las redes sociales dicen que no criminalicemos las redes sociales.

¿Por qué? Porque es verdad que muchas veces el impacto de determinadas noticias que aparecen en los medios de comunicación impulsan a regular un tema desde el punto de vista penal. Pero, una vez pasado el primer impacto de esas noticias, que son terribles, debemos pensar que precisamente son noticias porque son excepcionales, y estadísticamente, comparándolas con el gráfico que hemos visto del uso intensivísimo que se hace por los adolescentes o por los menores de edad de las redes sociales, rara vez se dan esos casos, y son muy, muy marginales. Por lo cual, no podemos pensar, por esos casos, que eso es lo normal en las redes sociales.

De hecho, los que estamos en las redes sociales y los que vemos a nuestros hijos cómo se manejan, comprobamos que los menores tienen mucho más sentido común de lo que pueda pensarse. En Red.es hemos hecho varias campañas por los colegios, la última patrocinada por una operadora, yendo por los colegios con un autobús, en el que había un monitor que les intentaba enseñar a los chicos cómo había que manejarse por las redes sociales. Y los que le daban clase eran los chicos de 10 y 12 años al monitor. Tienen muchísimo más sentido común del que creemos. Es verdad que, desgraciadamente, se producen algunos casos que no de-

berían producirse, pero estadísticamente son casos excepcionales, igual que con cualquier delito. No creemos que sea ni la norma ni un estado preocupante de generalización de ciertas conductas.

Mi **segunda conclusión**, que tiene que ver con la primera, es que lo más importante es educar en el uso de las nuevas tecnologías. Porque al final a los niños hay que educarlos para el mundo que les va a tocar vivir. Y desde luego, las redes sociales ya forman parte de su mundo y formarán parte de su mundo profesional.

Yo doy clases en la universidad, y mis alumnos de último curso pasan, sin solución de continuidad, de Facebook, que es una red de ocio, a LinkedIn, que es una red profesional. Es verdad que les tengo que enseñar que en LinkedIn no hay que portarse como en Facebook, porque se siguen portando como en Facebook. Y luego, pasan a redes sociales corporativas, porque en muchas empresas no se usa el correo electrónico interno sino que se trabaja de forma colaborativa en una red social interna. Con lo cual, cuanto antes se habitúen a manejarse en las redes sociales y sepan distinguir lo que se puede hacer y lo que no se debe hacer, mejor. Por eso, insisto, no a una aproximación criminal o policial a las redes sociales, sí a la educación en las nuevas tecnologías.

Tercera conclusión, y resumo lo que ya he dicho antes: son muy importantes las medidas legislativas, y la adaptación al nuevo entorno digital de leyes antiguas, que no estaban pensadas para el entorno digital. He puesto algunos ejemplos, tanto de Código Penal como la Ley de Protección Civil del derecho al honor, la intimidad y la propia imagen y alguna más que hay por ahí, especialmente la Ley General de Comunicación Audiovisual, que está pensada para la televisión y no está pensada para los contenidos en Internet.

Cuarta conclusión, que puede parecer contradictoria pero no lo es: no hay que ir a una hiperregulación. ¿Por qué? Porque las leyes son territoriales, y puede ocurrir que, con la buena intención de regular y dar mucha seguridad jurídica en España, creemos «corsets» jurídicos que solo se aplican en España. Por ejemplo, la única red social española es Tuenti. Si le ponemos muchos corsés a Tuenti, pueden pasar dos cosas: que los usuarios se vayan directamente a otra red social a la que no lleguemos, ni el regulador, ni la Agencia de Protección de Datos ni los tribunales, o que Tuenti se vaya a Palo Alto y dé sus servicios desde allí. Hay un principio en filosofía del derecho que se aplica aquí, y es que «cualquier

idea, por buena que sea, llevada a sus últimas consecuencias se contradice a sí misma». Esto quiere decir que, con la buena intención de regular y dar muchísima seguridad a los menores, al final podemos desproteger a los menores, porque se irán a otra red social donde no llega la regulación española, porque las leyes son territoriales. Y lo mismo está ocurriendo también en comercio electrónico. Si no hay un estándar internacional, y no todo el mundo juega con las mismas reglas, los sistemas legislativos también compiten y las empresas van al sistema legislativo que le viene mejor. Y entonces, si ponemos muchas trabas las empresas en España en comercio electrónico, no podrán realizar determinadas ofertas ¿qué ocurrirá?: que el consumidor español recibirá las ofertas de empresas que no están sujetas a la legislación española, con lo cual, pese a la buena intención de protegerles, acabarán más desprotegidos frente a empresas extranjeras.

Por todo ello —y ésa es la **quinta conclusión**— hay que trabajar porque exista una coordinación y una colaboración internacional en esta materia. Porque solos no podemos ir a ningún lado. Crearemos una ficción de seguridad que no se cumplirá. La única forma de avanzar en el tema de menores e internet, igual que en el comercio electrónico, es ir a estándares internacionales de protección, aunque sean estándares mínimos de protección, pero que las reglas sean las mismas para todos. Mientras no trabajemos, que es por donde ha empezado el secretario de Estado, teniendo muy en cuenta el ámbito internacional y lo que hacen otros países en nuestro entorno, todo lo que hagamos será perfectamente inútil, porque Internet es global, no es territorial.

Desde su casa un menor se puede conectar a una red social o a otra sin salir de España. O un consumidor puede contratar con una empresa u otra sin salir de España, y se te aplica una legislación distinta. Por eso, aparte de la labor que se haga en las leyes nacionales, en paralelo hay que ir trabajando en la colaboración y la cooperación internacional. Incluso, en la persecución de los delitos. Porque, por ejemplo, hay determinados delitos que se cometen en las redes sociales, que si son en de una empresa que no es española y no colabora el administrador de esa red, es muy difícil perseguir al culpable, al delincuente. Sin embargo, si es española, colaboran y es más fácil. Hay que intentar ver las ventajas para la seguridad que tiene colaborar con las empresas que están sujetas a la legislación española. Porque imponiéndoles muchas barreras, lo único que vamos a conseguir es que los usuarios no entren

en esas redes y se vayan a otras, extranjeras. O que estas empresas digan «aquí no hay forma de hacer nada, porque estoy compitiendo con otras redes en desigualdad de condiciones, así que me voy fuera de España para dar el servicio».

Éstas son algunas de las conclusiones a las que hemos llegado después de todos estos años trabajando en esta materia. Y con esto yo me callo, porque seguro que lo más interesante estará en sus preguntas. Muchas gracias.

COMPARECENCIA DEL DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (INTECO), D. MANUEL ESCALANTE GARCÍA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 9 DE MAYO DE 2013.

El señor **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (INTECO)** (D. Manuel Escalante García): Muchísimas gracias, presidentes, senadores. Para mí es un auténtico honor estar aquí con todos ustedes, es mi primera experiencia en este ámbito, y la verdad es que estoy encantado de tenerla.

Tengo una doble dificultad: una es que las exposiciones han sido muy buenas y muy prolijas y que las preguntas también han sido muy buenas, con lo cual el tema se me ha ido acotando bastante. En cualquier caso, todavía hay cosas sobre las que se puede profundizar y voy a intentar ir precisamente a esos temas en los que yo creo que merece la pena que profundicemos.

Antes de empezar con mi presentación, querría comentar algunas notas que he tomado y que creo que nos pueden ayudar a enfocar bastante el problema. Así, deberíamos hacer un zoom mayor de la problemática; es decir, estamos hablando de los menores, pero a mí me gustaría reflexionar sobre qué está pasando con la sociedad en su conjunto, porque nos puede ayudar mucho a entender qué es lo que está pasando con los menores, qué es lo que se puede hacer en el ámbito de los menores y qué es lo que no se puede hacer en el ámbito de los menores, porque es probablemente imposible.

Haciendo ese *zoom-out*, nos damos cuenta de que es un problema global que afecta a toda la sociedad. En Inteco nos dedicamos a la ciberseguridad y eso nos hace tener una visión y una perspectiva de conjunto muy amplia de lo que sucede. Estamos viviendo una auténtica revolución, lo sabemos todos. Lo que no sé si tenemos muy claro es cuál es la dimensión de esa revolución que estamos viviendo, que probablemente explique muchas cosas de las que están sucediendo y que veremos a continuación.

El aumento del uso de la sociedad de la información y de las tecnologías de la información es constante y exponencial: hace diez años no

estábamos hablando de lo que estamos hablando hoy aquí, ni dentro de diez años estaremos hablando de lo que estamos hablando aquí hoy. Es decir, es una verdadera revolución. Cuanto más valor añadido hay en la Red, hablando por ejemplo en el ámbito empresarial, en el ámbito bancario, en las administraciones, mayor valor añadido, mayor posibilidad de hacer un negocio para el ciberdelicuente y, por tanto, aumenta el riesgo. Esto es así.

Y luego sucede otra cosa muy importante y es que hemos decidido vivir de espaldas al riesgo. Las sociedades han decidido vivir de espaldas al riesgo. Y probablemente eso hila con lo que he dicho antes, porque la revolución es de tal dimensión que hemos decidido vivir de espaldas al riesgo: a mí esto me aporta tantísimo que sé que pueden suceder cosas, pero no pueden ser tan graves. Y no será porque no hay noticias todos los días en los medios de comunicación, todos los días, sistemáticamente, cosas gravísimas que están sucediendo. Bueno, pero es que esto me aporta demasiado. Esa revolución es demasiado grande, es mi percepción.

Incluso, lo estamos viendo, en empresas de carácter estratégico. Incluso el nivel de preparación en materia de seguridad no es el que uno esperaría en empresas o en instituciones de ese nivel. Por hacer un símil, ¿qué sucedió cuando entró el ferrocarril en España? Era una revolución. Sin embargo, inmediatamente, en una revolución no tan socializada ni probablemente tan grande, se percibió el riesgo: cuidado, esto es una vía de entrada para una invasión. ¿Qué hicimos? Pues se crearon las brigadas de ferrocarriles, no recuerdo exactamente cómo se llamaban, y se puso un ancho de vía distinto a España (por aquí no entran porque descarrilan los trenes); drástica pero totalmente real. ¿Por qué? Porque había una percepción muy clara del riesgo, estaba muy claro, por ahí podían entrar. Ahora no, y está clarísimo también, porque lo estamos viendo todos los días. Hace diez años podíamos decir «no está claro que esto puede suceder». Hoy está clarísimo que esto está sucediendo.

Pero está sucediendo a empresas no de pequeño tamaño, puesto que todos los días estamos resolviendo problemas de empresas de 100, 200, 500 empleados; está sucediendo a empresas estratégicas, cuya información, cuya propiedad intelectual es la base de su negocio, y le ha sucedido a Northern Networks, que ha estado a punto de desaparecer con una bajada en bolsa de sus acciones terrible, por un problema de robo de propiedad intelectual procedente de algún país. Le ha pasado a Sony, le

ha pasado a Google, le ha pasado a SpamHouse, que es una empresa de seguridad; le ha pasado hace muy poquito a una empresa que se llama Kinetics Systems, que es una empresa de altísima tecnología que trabaja para el ejército de Estados Unidos, que todos entendemos que deberá de tener unos niveles de seguridad terribles; pues le ha pasado también, llevan un año robándole propiedad intelectual a Kinetics Systems. Quiero decir, esta es la situación.

Les está pasando a las instituciones. Ahora mismo hay un tema con el ciberespionaje, y está pasando a ámbitos diplomáticos, a ámbitos de alto nivel de decisión de las administraciones. Todos hemos oído hablar del famoso «Octubre Rojo». «Octubre Rojo» no es más que un virus que se dirige hacia una determinada persona que maneja unos determinados niveles de información, que infecta las organizaciones, que es dificilísimo —por no decir imposible, en algunos casos— de detectar, y que es dificilísimo —por no decir imposible también— en muchos casos de limpiar. Es decir, estamos hablando ya de otra historia. Esto no tiene nada que ver con lo que vivíamos hace unos años: el 2010 marcó el antes y el después en el ámbito de la ciberseguridad.

Y también ocurre con las infraestructuras críticas. En Estados Unidos, por poner un ejemplo, son conscientes de que tienen muchos aviones, muchos barcos y muchos portaaviones, pero que a través de las redes de comunicaciones pueden «apagar» el país. Y cada vez más lo van a poder «apagar» en la medida en que las redes de distribución eléctrica estén informatizadas a través del *smart grid*. Por tanto, la vulnerabilidad está en casa: alguien con escasos medios, al que ni siquiera voy a ver la cara, va a poder causar un daño terrible en mi territorio.

Y les pasa también a los adultos. Lo sabemos porque conocemos lo que está pasando en los hogares, ya que tenemos 3.500 hogares panelizados y estudiamos sus hábitos de navegación y analizamos el nivel de seguridad y de infección de sus equipos. Los adultos, los usuarios habituales del ordenador, no es que tengan infectado el ordenador una vez, es que lo tienen infectado cien veces y no son conscientes. Esos adultos, ¿qué les van a contar a los menores? Es difícil ayudar cuando no se cuenta con el conocimiento completo.

¿Cómo se resuelven estos problemas en el ámbito empresarial? No pretendo dar miedo, pretendo hacer una radiografía del problema, de lo que está sucediendo, porque es importante. ¿Cómo se resuelve esto en

el ámbito empresarial, en las infraestructuras críticas, en las instituciones públicas? Pues se resuelve con un doble factor, que son los medios tecnológicos y el capital humano formado en materia de seguridad de la información, ambos imprescindibles. También es imprescindible la formación de los usuarios, puesto que pueden tener mucha tecnología a su alrededor, pueden estar rodeados de medidas de seguridad, pero siempre hay alguna forma de sortear una medida de seguridad. Entonces, o el usuario está formado y es consciente del riesgo primero y del daño que puede infligir a su organización, o da igual las medidas de seguridad que despleguemos. Y esto lo estamos viendo todos los días. Las cosas entran porque alguien abre un correo que no debe abrir, enchufa un *pendrive* que nunca debería haber enchufado —esto pasó en una central nuclear de Irán, todos lo sabemos, alguien enchufó un *pendrive* en un sistema SCADA de control de las centrifugadoras de uranio con un virus sofisticadísimo—. Bueno, pues esto es porque los usuarios no están preparados. En el ámbito empresarial, en estos ámbitos profesionalizados, una parte muy importante del problema se puede resolver con las medidas tecnológicas y un porcentaje un poco menor con las medidas de carácter humano.

¿Y qué pasa en el ámbito de los menores? Pues muy parecido al de los adultos: necesitamos medidas tecnológicas y necesitamos —ahí voy a repetirme, pero es que es la clave— que estén muy formados para el mundo en el que van a vivir. Ya no solo para cuando tengan 13 años u 11 años y entren en las redes sociales, es que van a vivir en un mundo completamente distinto y, o son capaces de utilizar las nuevas tecnologías y que eso no sea un agujero para ellos, para su seguridad, para sus finanzas, para su privacidad, o no van a poder desenvolverse adecuadamente en el mundo.

En este caso además, por fortuna, las medidas formativas, lo que son los controles humanos —como lo llamamos habitualmente— que puede desplegar un menor, resuelven un porcentaje muy alto de los problemas graves, al contrario de lo que sucede en las organizaciones. El sentido común que seamos capaces de desarrollar y la formación que seamos capaces de desarrollar en los menores resuelven los problemas graves. El problema de los menores es que su personalidad no está desarrollada, y el daño que le pueden infligir no es un daño económico o un daño a su imagen, es un daño psicológico o es un daño incluso a su integridad física. Ese es el gran problema. Y eso en general no se resuelve con tec-

nología eso se resuelve con formación. Porque que el ordenador va a estar infectado, esa es la realidad que vivimos hoy. Y puede estar infectado para capturar su webcam.

Otro problema que nos encontramos y que también es importante enmarcarlo es que no existen fronteras. No existen fronteras en ningún sentido. No existen fronteras legislativas: en un porcentaje muy alto de los casos de ciberataques o de los incidentes en los que nosotros trabajamos no se producen desde España, prácticamente nunca, o alguna vez hay algún servidor o un reducido número de usuarios involucrado. Igual sucede en Estados Unidos o en Alemania: el ataque tampoco se produce en esos países, sino que a lo mejor se produce desde España, o desde Rusia o China, que suelen estar entre los países de origen. Pero no suele suceder dentro. Con lo cual tenemos una dificultad añadida muy grande con el tema legislativo.

Prueba de que hay un problema jurisdiccional muy grande es que la figura de los CERT —los CERT son los *Computer Emergency Response Team*, los equipos de ciberseguridad— han proliferado en el ámbito internacional y han ganado muchísimo protagonismo. ¿Por qué? Porque estos problemas en general son problemas que duran horas, días o semanas. Y el ámbito judicial no actúa en esos tiempos, es imposible literalmente. Cuando pedimos una orden judicial el problema original ha desaparecido y ha derivado en otros problemas. Con lo cual, esto no funciona. ¿Qué tienen los equipos de respuesta? Que trabajan bajo el radar, trabajan, por decirlo de alguna manera, en base a redes de confianza, que no tienen nada que ver con el ámbito judicial. Hay un ISP donde hay un servidor que está infectado y que está inyectando malware en equipos españoles. Pues nosotros contactamos con el CERT y le avisamos de que hay un equipo que está infectado en dicho ISP y de la actividad que está desplegando. Y ellos, con sus relaciones de confianza internas dentro de su país, se encargan de solucionar el problema.

Eso solo funciona en ese ámbito. En el ámbito judicial, cuando llegamos a ese servidor ha hecho todo el daño que tenía que hacer, ha robado todo lo que tenía que robar y el virus en cuestión ha desaparecido. Esto es lo que hace que los CERT cada vez tengan mayor importancia y que la coordinación sea no necesaria, sino crucial en este ámbito.

Ahondando en el tema de las fronteras, ¿qué tipo de fronteras podemos establecer? ¿Podemos marcar aquello que nos parece mal y filtrarlo?

Lo digo porque es un debate también muy interesante y que en algunos países ya se han planteado. La pregunta es qué es malo y qué es bueno. Y qué es malo y qué es bueno, no digo en cuanto al contenido, sino que muchas veces los servidores desde los que se ataca no son servidores malos, son servidores buenos infectados. Es decir, el bueno que tiene un negocio en ese servidor no sabe que hay un malo que le ha infectado y que está haciendo cosas malas desde su equipo.

Entonces, ¿qué es malo y qué es bueno? ¿Podemos filtrar, podemos establecer fronteras? Pues difícilmente. Estaremos filtrando un negocio legal cuya seguridad ha sido vulnerada. Por eso tenemos también muchas dificultades cuando hay un servidor que está haciendo algo malo y decimos «ese servidor, habría que bloquearlo». Y seguimos escalando y vemos que realmente hay un servicio de comercio electrónico totalmente lícito, además hay en el mismo servidor una red social totalmente lícita, pero alguien ha conseguido infectar ese servidor y está distribuyendo *malware* a nivel global. ¿Cómo se soluciona ese problema? Pues no es evidente. No puedes ir y capar la IP, digamos, para que no se acceda desde un determinado país, sino que habrá que resolver el problema de forma individual. Es un problema técnico y tendrá que resolverse en ese plano.

Un tema importante que también tenemos que tener en cuenta —esto es introducción pero es importante— se refiere a los medios con los que cuentan «los malos». Este es el entorno, quiero decir que esto es lo que vivimos y, si no somos conscientes de esto, difícilmente vamos a ser conscientes de cómo tenemos que abordar el problema con los menores. Sobre todo para no pensar que podemos hacer cosas que no podemos hacer. Y que la respuesta puede estar en otro sitio. Y hay ejemplos ya; Internet tiene ya un tiempo de vida suficiente como para que tengamos ejemplos en la mano de que «poner puertas al campo» en Internet es prácticamente imposible.

Los medios con los que cuentan los delincuentes son tremendamente sofisticados. En ámbitos como el de la pornografía infantil hay un modelo de negocio y los medios tecnológicos que utilizan para la ocultación y para el intercambio de contenidos son tremendamente sofisticados. Aquello que se colgaba en un servidor, en una red social... No, eso no está ahí, no nos equivoquemos. Los contenidos de verdad perjudiciales están en redes anónimas, en particular existe la llamada red Tor, que

además se da la paradoja de que es una red que inventó Navy y la puso a disposición del mundo y que ahora está siendo utilizada por los terroristas para intercambiar información y los pederastas para también intercambiar contenidos. Ahí hay un modelo de negocio. El nivel de sofisticación es terrible y las herramientas que ellos tienen son tan potentes o más que las de «los buenos». Y eso es un grave problema y nos mete en una carrera tecnológica muy compleja.

Y eso es una de las conclusiones también: hay una carrera tecnológica y una carrera por la persecución del delito que no podemos olvidar, por lo que debemos tener capacidades técnicas para abordar este problema. Hace pocos días salió una noticia de que se ha construido ya y están circulando por la Red planos de una pistola que se puede imprimir en una impresora 3D y que es perfectamente funcional. Hoy en día la tecnología está a disposición de todo el mundo y en el caso de Internet, ni siquiera tengo que disponer de una impresora 3D, puedo pagar 50 dólares y tengo a mi disposición una red de equipos infectados para hacer lo que me dé la gana. Esos negocios están en la Red, hay una profesionalización, hay un modelo de negocio, en el que unos desarrollan tecnología y la ponen a disposición de los demás y otros la utilizan para cometer delitos con ella. Por ejemplo, uno comete el delito robando, por ejemplo tarjetas bancarias, y lo pone a disposición de otro, que es el que se atreve a establecer una red de muleros para que al final el dinero salga. En el momento en que hay un modelo de negocio y hay unos ingresos, hay sofisticación y hay inversión en tecnología. Y a eso es a lo que nos enfrentamos.

Decía que la ocultación de la identidad es muy sofisticada. Estoy hablando de los temas de pederastia, pornografía infantil, ciberterrorismo y otros temas, pero utilizan los mismos medios, que son básicamente estas redes anónimas, donde la estrategia tecnológica es muy compleja. Es más, estamos en ello, quiero decir que es un tema que nadie ha resuelto. Porque de hecho esto son unas redes que diseñó la Navy estadounidense para poder intercambiar información confidencial a través de Internet sin más medios que Internet, con la garantía de que esa información no podía ser vista por nadie. Pues esto, que socializó Navy igual que se socializó en su día Internet, se puso a disposición del mundo y ahora lo utilizan los malos, como suele suceder con esas cosas.

El tema de la identidad digital es complejísimo. Si no existen fronteras y no existe interoperabilidad en los modelos de identidad digital

en los diferentes países, o hacemos negocios locales —cosa que creo que está muy claro que no es viable—, o el tema de la identidad digital es muy complicado. El DNI funciona en España, y es verdad, lo decía Borja, tenemos un Ferrari en el bolsillo, sin lugar a dudas. Pero de ahí a la obligación hay un paso muy grande. Si obligamos, por ejemplo —una cosa que se me ocurre—, a que todos los usuarios de Tuenti tengan que entrar con el DNI electrónico, Tuenti no puede tener un negocio internacional. Entonces hemos dejado a Tuenti frente a Facebook, por ejemplo, no en inferioridad de condiciones, sino es que lo hemos matado, entre otras cosas porque los niños se irán a Facebook. Y Facebook tratará diseñará su modelo de negocio con los menores.

Y es más, incluso aunque fuéramos capaces de imponer la identidad digital en todas las redes sociales, sospecho que los chavales se irían a otros medios, igual que antiguamente utilizábamos el IRC Chat. Con la propiedad intelectual ha pasado un caso muy parecido: empezamos con Napster para el intercambio de música. En Napster había un servidor centralizado, encontrábamos la música, nos la bajábamos gratuitamente. Y alguien dijo «ese repositorio es ilegal» y *¡pumba!*, Napster desapareció. Y tardó muy poco tiempo en aparecer esa distribución de contenidos a través de páginas web: cifrado, recortado con una aplicación que se llamaba Hacha, comprimido, etcétera. El modelo de negocio duró una temporada; aquello era incómodo, pero, bueno, uno se bajaba las canciones; como era, digamos, identificable, las sociedades de gestión principalmente fueron a por ello; y de nuevo desapareció. Y entonces apareció el Napster sin servidor centralizado. Entonces, esto ya era más difícil, puesto que ya no había un servidor que tuviera la lista, sino que estaba distribuido. Este modelo ya era más complicado de eliminar. Pero de nuevo han ido apareciendo otros modelos de negocio diferentes, como el negocio de las descargas y luego el *peer-to-peer*. Y si el negocio de las descargas lo cortamos por aquí, el *peer-to-peer* ganará presencia. Por último, aparecen los *cyberlockers*; y ahora los *cyberlockers* están cifrados. Por ejemplo, el servicio Mega de king.com ahora está cifrado, ya nadie le puede pedir responsabilidades a Mega de los contenidos que alberga en sus servidores. Es decir, que la tecnología es tan flexible, tan versátil y avanza tan deprisa que va a haber una respuesta alternativa a cualquier cosa. Eso ya lo estamos viviendo, eso ya es una lección que tenemos aprendida.

Todo esto, y por hacer un poco el *conclusions first*, me lleva a la actividad a la que nos dedicamos y, por la experiencia que nos da esa acti-

vidad, a una aproximación muy realista. Y la aproximación es que probablemente se puedan hacer bastantes cosas, pero la aproximación tiene que estar centrada en el individuo. El individuo tiene que estar preparado para esto que va a vivir, donde las puertas al campo van a ser muy difíciles de poner. Entonces, tenemos que formar al individuo.

Formar al individuo se puede hacer de diferentes maneras. Por ejemplo, que el propio individuo acuda a formarse, cosa que por experiencia ya sabemos en Inteco que no suele suceder. El menor cuando entra en Internet, y más los pequeños, ni lo entienden; pero cuando entran van a ver los dibujos, van a jugar, los que son un poquito más mayores ya van a chatear,... Con lo cual, por ahí lo tenemos todo perdido.

La siguiente es: vamos a intentar que los padres naveguen con ellos y que tengan contenidos divertidos para poder formar a los menores. Tenemos un problema y es que los padres no perciben el riesgo. Todavía no han entendido que esto es un grave riesgo para sus hijos. Es más, en una encuesta, en un trabajo de campo que realizamos hace un par de años obtuvimos un dato escalofriante y es que de todos los menores entrevistados, que fueron 1.250 en todo el país, solo el 1% decía que ante un caso de ciberacoso o de un problema en una red social, por ejemplo, acudiría a sus padres. El problema es terrible, ya no es una cuestión solo de tecnología ni de formación: es que los menores no confían en los padres para eso, entre otras cosas porque se avergüenzan, porque las tácticas utilizadas por los acosadores están muy orientadas a que el menor en un momento dado tenga algo de lo que avergonzarse, que puede ser una tontería, pero desde el punto de vista del menor ya tiene algo que ocultar. Y cuando el menor tiene algo que ocultar, el que está al otro lado se aprovecha.

Y luego, otro tema que yo considero que es básico es que el colegio como institución tiene que tener un protagonismo en todo esto, no solo en la formación, sino también el despliegue de protocolos de actuación frente a casos de ciberacoso. Estoy hablando un poco del «patio del colegio», esto es, que alguien está acosando al compañero de allí y está diciendo que es feo o le ha suplantado o lo que sea; entonces, esto es el patio del colegio, pero el patio del colegio digital. El centro educativo tiene que tener un papel en todo esto.

Y decía, teniendo claro que el menor no se va a aproximar a la formación, teniendo claro que los padres no están preparados, y que intenta-

remos llegar a ellos y lo hemos intentado en el pasado, tenemos la experiencia pero es muy difícil llegar a ellos, lo que sí que seguro no nos va a fallar es la escolarización. Y puesto que todos pasamos por el sistema educativo, ese es el filtro y el tamiz por el que tenemos que formar a los ciudadanos del futuro.

Por otro lado —y es un tema muy interesante también, y lo decía Borja—, el equipamiento en prácticamente todos los colegios y los contenidos digitales, son limitados y no siempre suficientes. ¿Qué le pasa al profesor que tiene que llevar a los niños al aula de informática? Este colectivo necesita contenidos de calidad en materia de seguridad de la información —que se pueden hacer muy atractivos, luego veremos un par de ejemplos— para dar una clase amena y que fuera del interés de los alumnos.

Empiezo con mi presentación, que voy a ir muy rápido, insisto, porque creo que es importante que ustedes conozcan las capacidades y los organismos que trabajamos en este ámbito. Inteco es una sociedad estatal, adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones. Inteco lo preside el secretario de Estado, don Víctor Calvo-Sotelo. El accionista único es Red.es, como ha mencionado antes Borja Adsuara. Somos, dentro de la estrategia de la secretaría de Estado, entidad de referencia en confianza digital y en ciberseguridad, de lo que hablaremos luego en el ámbito de la Agenda Digital para España.

Y los tipos de actividades que desarrollamos son por un lado la prestación de servicios ¿Qué tipo de servicios? Pues servicios claramente preventivos para intentar evitar que las cosas sucedan, para desplegar servicios de alerta temprana monitorizando lo que está sucediendo en Internet. Así, los incidentes que están teniendo otros los utilizamos para analizar cuál es el problema e intentar desplegar soluciones antes de que se materialice la amenaza, como decimos nosotros. También servicios reactivos, cuando se produce un incidente. Puesto que cuando esto ocurre, las empresas están absolutamente perdidas, es el caos; ese día descubren hasta qué punto sus sistemas de información son críticos para su negocio. Ahora mismo estamos trabajando con un caso en el que hay un virus, un *ramsonware*, que infecta a los servidores corporativos, cifra los archivos que hay ahí (de recursos humanos, financiero, control logístico o lo que sea) y entonces pide un rescate de, por ejemplo, 5.000 dólares

por descifrar aquellos ficheros. La mayor parte de las empresas lo que nos preguntan es «¿cómo les pago?» No preguntan «¿cómo desinfecto?» Están tan desesperados, necesitan tanto sus sistemas de información que lo que quieren saber es cómo pagar. Evidentemente, nosotros les decimos: «quieto, tenemos respuesta. Mándanos información y nosotros acudimos en tu rescate». Ahí hay un problema muy grave que vemos todos los días.

Y luego, por supuesto, prestamos servicios de concienciación y de sensibilización, que son tan importantes en todos los ámbitos, incluidos los empresariales.

También realizamos investigación, por dos motivos. El primero, porque necesitamos tecnología para poder prestar esos servicios; esa tecnología en general no está en el mercado porque el concepto CERT es relativamente reciente, por lo tanto tenemos que desarrollar tecnología y tenemos que tener capacidades para desarrollar tecnología. Y luego, por otro lado, porque necesitamos saber cuáles son las nuevas tendencias en amenazas. Alguien lo ha preguntado, no recuerdo quién ha sido: ¿estamos viendo qué es lo que va a suceder en el futuro? Pues sí, claro que lo estamos viendo, lo estamos viendo constantemente; necesitamos estar investigando cuáles son las nuevas tendencias porque tenemos que tener soluciones preparadas para el día en que las cosas sucedan. Y ojo, no siempre lo conseguimos, lo conseguimos en un porcentaje «equis» de las ocasiones.

Y como decía, trabajamos en coordinación, porque la ciberseguridad es un tema en el que, si no es con la colaboración con otros, es imposible ser efectivo. No solo colaboración en el ámbito nacional, que también es importante, sino muy especialmente en el ámbito internacional, cuando estamos de alguna forma atravesando fronteras de carácter jurisdiccional.

¿Cómo hacemos esto? Pues ya decía, Inteco es confianza y ciberseguridad. Ponemos mucho énfasis en generar inteligencia, recibimos volúmenes ingentes de datos, de dato crudo a través de nuestra sensorización; nosotros tenemos sensorizada una parte importante de lo que sucede en Internet, ojo, sin saber quién es la persona y sin saber cuáles son los contenidos que circulan por allí, eso ni lo sabemos ni lo queremos saber; simplemente obtenemos información de posibles amenazas, de focos de amenaza, de generadores de *spam*, de quién está inyectando *malware*,

quién está haciendo ataques de denegación de servicio... Generamos esa inteligencia que nos permite dar alerta temprana a las instituciones.

Damos soporte, como decía, imprescindible cuando se produce un incidente y tratamos de dinamizar, por qué no, la industria española de ciberseguridad, que es pequeña pero potente.

Y tenemos nuestros valores de excelencia, cooperación, servicio, sostenibilidad, etc.

¿A quién prestamos servicio desde Inteco? Pues prestamos servicio a todos esos sectores de la sociedad: a los ciudadanos, con especial atención a los sectores más vulnerables, que son los menores (objeto de este debate); a las empresas, y en particular a los ISP y prestadores de servicio en la Sociedad de la Información —que son una gran parte de la solución, no del problema—, así como a los sectores estratégicos. Los sectores estratégicos ahora mismo tienen un problema, y es que el ciberespionaje industrial está a la orden del día. Grandes empresas de defensa, bancos, empresas de telecomunicaciones están sufriendo espionaje industrial, están siendo infectados con *malware* destinado a robar su propiedad intelectual, con lo cual estamos perdiendo competitividad internacional, sin lugar a dudas.

Damos servicio también al dominio.es, al ESNIC que gestiona Red.es y también estamos trabajando en dar soporte en materia de respuesta a incidentes y de alerta temprana a RedIRIS (que también gestiona Red.es), la red académica y de investigación que une a los centros universitarios y organismos de investigación.

Eso es de alguna forma lo que está enmarcado dentro de la Agenda Digital para España, y que forma parte de nuestro contexto de referencia como instrumento político estratégico. Y junto con la Agenda, está el convenio que ha mencionado el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información con la Secretaría de Estado de Seguridad, el cual nos permite trabajar en dos ámbitos más: uno, que es la lucha contra el ciberdelito y la ciberdelincuencia con Fuerzas y Cuerpos de Seguridad del Estado, y otro, en la protección de las infraestructuras críticas en aquello que afecta a los sistemas de información que dan soporte a esas infraestructuras, ya sea energía, transporte o banca, entre otras.

Ese es nuestro marco de actuación, que no es pequeño.

No me voy a parar en las iniciativas de referencia porque las ha contado muy bien el secretario de Estado. Simplemente, llamo la atención sobre un tema, y es que en Estados Unidos, que van un poquito por delante de nosotros en este tema, han decidido que deben tener contenidos de seguridad en los itinerarios educativos como algo imprescindible para la competitividad de su sociedad del futuro. Eso es algo en lo que nos tenemos que fijar.

Y luego, por supuesto, las iniciativas de la Unión Europea, en particular la Estrategia europea en favor de una Internet más adecuada para los niños, que es lo que digamos que viene más al caso en el día de hoy.

En cuanto a las iniciativas de referencia en el ámbito nacional, hay muchas: se puede destacar el Observatorio de la Infancia, el Inteco, Red.es... Ahí se incardinan las iniciativas de la SETSI. Son muchas. En algunos casos podría haber algún solapamiento, y también podría suceder que haya alguna cosa interesante que se nos esté escapando, es algo que en ese grupo de trabajo que ha mencionado Borja, que yo creo que va a ser un gran éxito, identificaremos y trataremos, tanto para que aquello que no se está haciendo se haga, como para que aquello que se está haciendo dos veces procuremos hacerlo solo una vez y mejor.

Esta es la actividad de Inteco; esta es la estrategia de Inteco con respecto a los menores. Estamos participando en el diseño estratégico; gracias a que tenemos experiencia y tenemos conocimiento, parece razonable que de alguna manera influyamos en aquello que se va a hacer. Prestamos servicios de ciberseguridad intentando encontrar un entorno más adecuado para los niños. Trabajamos en el desarrollo de soluciones tecnológicas para ayudar a las Fuerzas y Cuerpos de Seguridad del Estado a perseguir este tipo de ciberdelito, insisto, tan sofisticado en muchos casos. Y luego, por supuesto, trabajamos en la concienciación y sensibilización para elevar la cultura de seguridad de los menores, de los padres y de los educadores, incidiendo en la importancia de trabajar todos los colectivos, no exclusivamente el de los menores.

Y luego, por último, tenemos una capa transversal de colaboración sin la cual sería imposible nuestro trabajo. Es importante que veamos la correspondencia que hay entre esa estrategia y la mencionada Estrategia europea en favor de una Internet más adecuada para los niños, porque se cubren todos los ámbitos que se desarrollan en esa estrategia, y esto no es fortuito, esto es que lo hemos trabajado en paralelo y hemos visto que

la estrategia europea tiene muchísimo sentido y ¿por qué no empezar ya a dar respuesta a algo que en cualquier caso va a ser preceptivo?

En cuanto a la participación en el diseño estratégico, pasaré directamente a la Agenda Digital para España y al convenio con la Secretaría de Estado de Seguridad, por ir acortando un poco. La Agenda Digital para España ya la ha comentado el secretario de Estado: hay un objetivo, que es el objetivo IV, que pretende reforzar la confianza en el ámbito digital, y en él está desarrollada en seis puntos la estrategia de Inteco, que cubre muchos de los aspectos de los que hemos hablado hoy.

Uno, extender la participación de Inteco a todos los ámbitos de la confianza. En este sentido, había ámbitos en los que de alguna manera no trabajábamos (el ámbito de la privacidad no es un ámbito en el que estuviéramos trabajando directamente). Y se reconoce también de alguna manera el trabajo de Inteco, la implicación de Inteco en el ámbito de los menores.

Otro, situar a Inteco como una entidad de referencia en ciberseguridad para sectores estratégicos. Insisto, esto es nuevo, entre nuestros clientes no estaban antes estos sectores, que ahora sí lo están junto a empresas y ciudadanos.

En tercer lugar, esto es muy importante, establecer las capacidades necesarias para estudiar los riesgos emergentes, que era lo que comentaba antes, estar preparados para lo que va a venir. Saber que Facebook, por ejemplo, ha anunciado que su aplicación Graph permite en un momento dado encontrar restaurantes en función de los restaurantes que han visitado mis conocidos o permite saber qué cosas debo visitar en una ciudad porque sé automáticamente que esa ciudad la han visitado mis conocidos (las implicaciones desde el punto de vista de la privacidad son terribles). Tenemos que estar viendo todas estas cosas para ver dónde están los agujeros en la privacidad, por ejemplo, como sucedió en su día con el Timeline, con la biografía que se introdujo también en Facebook. Hay que alertar a los usuarios y decirles: «Oye, esto es fantástico, pero mira, esta pestañita de aquí si la pones de esta manera sucede esto y las implicaciones son estas; esta pestañita de aquí si la pones así, sucede de esta otra manera,… Entonces, te recomiendo por defecto esta configuración». Eso, que parece algo muy simple, es importantísimo, porque el usuario cuando se enfrenta a unas opciones que cada vez son más difíciles de entender y cada vez son más numerosas, necesita que alguien le diga «mira, si vas por aquí vas bien, si vas por aquí te puede pasar todo esto».

En cuarto lugar, se encuentra el desarrollo de programas de sensibilización, concienciación, educación y formación, que comentaba antes.

Tras estos programas, hay un planteamiento en el que ya estamos avanzando, relativo al desarrollo de contenidos de seguridad para su inclusión en los itinerarios del sistema educativo. Estamos avanzando, intentando lanzar una experiencia piloto, para lo cual hemos tenido reuniones con una dirección provincial y con una consejería de Educación. Desde luego, la receptividad es muy grande y hay interés por parte de numerosas comunidades autónomas, porque esto tiene sentido sin lugar a dudas.

Y por último, y muy importante, hay que hacer un seguimiento y un diagnóstico de lo que está sucediendo. Y aquí también tenemos algunas barreras que superar.

Inteco dispone también de otro instrumento estratégico, el convenio entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, que básicamente consiste en unir esfuerzos y capacidades para intentar entre todos «parar el tsunami», por decirlo de alguna manera. ¿En qué ámbitos? Pues en la lucha contra los ciberdelitos y contra el ciberterrorismo, con las Fuerzas y Cuerpos de Seguridad del Estado, y ahí en particular hay una línea que es la protección de los menores; el alcance es mucho mayor, pero por centrarme es la línea de protección de los menores, y la protección de los menores yendo al delito más grave, que es el delito de la pederastia y la explotación infantil; ayudar a las Fuerzas y Cuerpos de Seguridad del Estado a disponer de tecnología para poder captar evidencias en los registros. Ahora los registros ya no son como antes, el agente de las FCSE no se lleva un libro de cuentas o un cuadro, no; tiene que recoger evidencias electrónicas y que además lo vea un juez. O incluso llega a un registro y se encuentra con ordenadores, discos duros, discos duros externos, USB, DVD, etcétera y un registro no puede durar un mes, no va a estar el secretario judicial con el agente un mes, eso es imposible. Por ello, necesitamos facilitarles herramientas para que en un registro haya tecnología que ayude al profesional a buscar aquellas evidencias que hacen más probable que allí se esté cometiendo un delito.

Y luego un trabajo muy importante es la lucha contra las *botnets*, las redes de ordenadores zombi, u ordenadores cuyos usuarios no saben que están infectados y controlados y que constituyen una infraestructura muy

potente para cometer cualquier otro tipo de delitos. Esto da para muchas horas. Por citar un ejemplo, una *botnet* que desarticuló el FBI el año pasado, y que contó con la colaboración de Inteco en la parte de España, había afectado a 5 millones de máquinas en el mundo, una sola *botnet*, y en España había 500.000 equipos infectados. Y *botnets* hay todos los días, cada mes. Por supuesto, la gente no lo sabe. El individuo puede, en un momento dato, detectar que su conexión a Internet va un poco más lenta y a lo mejor está participando en un ataque de denegación de servicio al Senado y no lo sabe. Lamentablemente, esto funciona así. Una *botnet* es una infraestructura latente y se utiliza para determinadas cosas.

Junto con la lucha contra los ciberdelitos y contra el ciberterrorismo, trabajamos en la protección de las infraestructuras críticas también con el Ministerio de Interior, con el Centro Nacional para la Protección de Infraestructuras Críticas, en lo que creo que es un modelo de racionalización. El Centro Nacional para la Protección de Infraestructuras Críticas del Ministerio de Interior necesitaba tener capacidades de respuesta a incidentes en seguridad de la información, y decidieron que en vez de reinventar la rueda se iban a apoyar en las capacidades, en el conocimiento del CERT de Inteco, y de esa manera hemos ampliado de alguna forma la clientela de nuestro CERT, y junto con el Ministerio de Interior estamos ya dando respuesta a los incidentes que afectan a las infraestructuras críticas; incidentes que todavía no son muy numerosos (exceptuando el caso de la banca), pero que lo serán sin lugar a dudas. En el momento en que nuestra red eléctrica sea una red con cierta capacidad de inteligencia, sin lugar a dudas va a ser un foco de atención para los ciberdelincuentes y para los ciberterroristas.

Y además, trabajamos con ellos en difusión, concienciación, formación y capacitación, que esto es transversal pero en muchos casos es lo más importante.

De un vistazo, esa es la actividad que desarrolla Inteco: servicios de prevención y asistencia, útiles gratuitos y enseñamos a los usuarios a manejar esos útiles gratuitos (gestores de correo para niños, filtros para niños, herramientas, por supuesto, antivirus, control de horas de uso del ordenador, etc.), contenidos para la concienciación para diferentes rangos de edades —luego voy a enseñar muy rápidamente la web para que veamos cuál es el modelo—, y luego, muy importante, una línea de formación a padres y educadores (insisto, esa es la línea en la que más expectativas tenemos, por experiencia, de que funcione).

Y luego, junto con todo eso, pues desarrollamos tecnología e investigamos para poder dotar de herramientas a las Fuerzas y Cuerpos de Seguridad del Estado, colaboramos con todos los agentes que tienen algo que decir en esta materia, hemos impartido también charlas presenciales, que nos da un *feedback* muy interesante también de los padres o de los tutores, incluso también de los niños, y nos permite redefinir nuestros servicios; y ahora estamos trabajando en esa propuesta de contenidos educativos.

En el ámbito de los servicios de ciberseguridad, en cuanto al contexto simplemente he tratado de poner ahí un poco las iniciativas que hay, para que veamos que en general no solemos estar solos, hay muchos haciendo cosas. En cuanto a esos servicios de ciberseguridad, los prestamos a partir del portal Menores OSI y también a través de los perfiles de las redes sociales, que son muy interesantes porque están muy a mano y, si alguien se apunta a nuestros perfiles estará recibiendo consejos muy interesantes y alertas muy interesantes. Es decir, todos los días aparecen aplicaciones maliciosas en las redes sociales y la gente no lo sabe. Entonces, un perfil como este nos sirve para alertar de situaciones del tipo «esta aplicación es muy bonita, pero lo que va a hacer es infectar tu equipo». Esta es una labor constante a través de los perfiles de redes sociales, que es la forma de estar «embebido» dentro de la propia red social y ser un individuo más de esa red social.

Hemos dado más de 500 alertas y destacados sobre riesgos para los menores. Y luego, mantenemos una relación de herramientas gratuitas de control parental, protección en todas las líneas. Y colaboramos, insisto, con otros CERT del ámbito internacional; en particular nosotros colaboramos con 273 CERT en el ámbito internacional, que es con los que nos relacionamos día a día.

Y en cuanto a las actividades que tenemos previstas para el futuro, recogidas en la Agenda Digital para España, está el refuerzo de la colaboración público-privada en detección, prevención y respuesta. ¿Por dónde hemos empezado? para que esto no parezca una frase vacía, os diré que por Tuenti, como no puede ser de otra manera. Nosotros ya tenemos presencia en Tuenti, pero vamos a intentar hacer que nuestra presencia en Tuenti sea todavía más efectiva mediante un esquema de colaboración. Y estamos a punto de firmar un convenio con este objetivo.

Desarrollamos soluciones tecnológicas para el ciberdelito, como decía. Ahí los protagonistas son las Fuerzas y Cuerpos de Seguridad del Estado, que son los que tienen que perseguir el delito, sin lugar a dudas.

Estamos desarrollando herramientas para que sean capaces de automatizar la actividad que hacen los policías. Necesitamos desarrollar sistemas de visión artificial para que un policía no tenga que ver millones de imágenes y millones de vídeos, sino que haya un sistema que sea capaz de decirle «esto tiene pinta de ser, esto tiene pinta de no ser; aquí hay un cuadro que tiene pinta de parecerse mucho a ese cuadro que está en la base de datos y que está asociado a otro caso; los metadatos de esta cámara se parecen a los metadatos de aquella otra cámara; las evidencias que había en el sistema operativo donde se capturó esto se parecen a estas y a estas, etcétera». Conseguir que la labor policial de establecer relaciones, buscar evidencias y tirar del hilo sea más sencilla, porque estamos hablando de un volumen tan grande que la actividad policial se complica muchísimo. Y lo que sucede hoy es que el número de casos que se pueden perseguir, a pesar de la abnegación y de la capacidad de trabajo y de sacrificio que tiene la Brigada de Investigación Tecnológica de la Policía y el Grupo de Delitos Telemáticos de la Guardia Civil, es la que es porque no se puede llegar a más.

Estamos desarrollando también una herramienta para la detección de evidencias en registros.

Y luego, estamos empezando a realizar ya algunos experimentos de monitorización de fuentes abiertas, redes sociales, de redes de intercambio (*peer-to-peer*) y de esas redes anónimas que comentaba anteriormente. Hemos hecho una primera aproximación de monitorización de Tuenti y hemos encontrado que hay no uno, sino muchos perfiles de Tuenti que están ofreciendo contenidos y solicitando abiertamente contenidos de pornografía infantil. Todo esto hay que perseguirlo y sabemos que es muy complicado. Después de identificar estas situaciones de riesgo hay que acudir a Tuenti para que nos dé evidencias de cuáles son las IP desde las que se han conectado y se han subido esos contenidos. Todo esto es muy complejo: identificas un perfil —evidentemente nadie se da de alta con su nombre y apellidos— y entonces empieza una investigación hacia atrás que choca con Tuenti y con la legislación de Tuenti. En fin, todo esto es muy complicado, pero en ese camino hay que avanzar, sin lugar a dudas.

Se pueden hacer muchas cosas, hay que formar al individuo, pero a la vez hay que perseguir a «los malos». Eso siempre, seguro. Si no, el problema cada vez es mayor.

En este caso estamos finalizando los desarrollos. Algunas de estas herramientas serán utilizadas por Fuerzas y Cuerpos de Seguridad del Estado de ámbito europeo porque así nos lo pide la Comisión Europea.

Llegamos a la parte de concienciación y sensibilización y formación, que es tan importante. En este campo, ¿qué necesidades detectamos? Que los educadores necesitan orientación y formación, si no, difícilmente van a ser capaces de trasladar esa información. A día de hoy no se está haciendo de un modo oficial, no hay —que sepamos— nadie que tenga un programa oficial de formación a formadores para que luego puedan dar clase a los alumnos, y sí existen actividades o iniciativas más o menos dispersas. Se requieren contenidos de seguridad de la información, no basta con que estos profesionales estén formados, sino que tenemos que darles contenidos de seguridad atractivos para que eduquen a los chavales sin aburrirles. Esta es una premisa básica: hay que contar las cosas de un modo ameno —y ahora veremos cómo lo intentamos nosotros— e introducir esos contenidos en el itinerario educativo.

Y hay diagnóstico, pero no somos muchos los que estamos haciendo el diagnóstico: el 50% o el 60% estamos sentados aquí ahora mismo. Y, por otro lado, en general no existe homogeneidad en ese diagnóstico, con lo cual se dificulta la comparación. Y por otro lado, no tenemos datos consolidados de todas las denuncias o de todos los incidentes que se están reportando en los diferentes sitios, no existe una ventanilla única, y por tanto no tenemos ese dato para decir qué es lo que está pasando de verdad. Yo sé lo que está pasando en cuanto a lo que me está llegando a mí, pero no sé lo que le está llegando al de al lado, ni sé lo que le está quedando al de al lado ni lo voy a saber razonablemente nunca, salvo que nos pongamos entre todos de acuerdo. Ahí hay un punto débil y una oportunidad.

Por seguir con la concienciación y sensibilización, el portal Menores OSI se ha inventado para públicos de edad, de 5 a 8 años, de 9 a 12, de 13 a 17, y luego ya están los padres y los educadores. Desde que se lanzó el portal hemos tenido más de 585.000 páginas vistas que, si bien no parece mucho, lo es teniendo en cuenta que son contenidos de seguridad; no es mucho teniendo en cuenta que es un portal de Internet, pero va aumentando el interés. Un reto es hacer que esto se conozca más y que se utilice más.

Además, se han desarrollado guías y materiales de concienciación. En particular hay publicadas seis guías en materia de protección del me-

nor en Internet que son interesantes y que han tenido 48.000 descargas. También hemos tenido 63.000 reproducciones de nuestro canal Menores OSI en YouTube; hemos desarrollado juegos educativos; tenemos 40 recursos pedagógicos recopilados; ponemos a disposición del público una plataforma de formación on-line en la que actualmente se ofrece un curso para padres y educadores, con más de 1.700 inscritos a pesar de la reciente publicación de esta formación y del que sabemos que va a tener muchísima demanda.

Siguiendo con las actividades de concienciación, hemos dado más de 90 charlas, en las que hemos tenido a más de 7.000 asistentes. Como hemos visto que el impacto de nuestras charlas no es suficientemente grande estamos haciendo ya experiencias piloto on-line para llegar a muchísima más gente con nuestras charlas. E insisto, esta actividad, que es intensiva para nosotros en recursos humanos, nos obliga a desplazarnos, nos obliga además a llevar a una persona con un perfil experto y que, mientras que está haciendo esto, no está haciendo otra cosa, pero el *feedback* que recibimos de los oyentes es muy importante para nosotros.

También quiero mencionar el desarrollo de contenidos que hemos realizado para el canal Clan TV de Televisión Española, que es probablemente lo más visto por los niños, y tenemos ahí un personaje que se llama Mosi que es un marcianito que empieza a contarles cosas a los niños de cómo se utilizan las tecnologías.

En redes sociales tenemos los perfiles que nosotros llamamos «pienso, luego clico» y que tienen ya más de 3.000 seguidores en Tuenti y en Facebook, que me va a decir Borja que es muy poco, pero ahí estamos, intentando subirlo.

Y, por último, hemos mantenido durante los últimos años más de 50 indicadores sobre menores, de los que muestro algunos ejemplos en la presentación.

Y como Borja, me gustaría extraer algunas conclusiones, también, por supuesto, de carácter personal de todo esto que hemos hablado.

La primera conclusión, y como transversal y de igual manera que he empezado mi intervención, es mejorar en general el nivel de ciberseguridad de la Red, lo que afecta a todos los sectores de la sociedad, porque si no, difícilmente vamos a poder proteger a nuestros menores. Ahora mismo existe un elevadísimo número de iniciativas que pueden provocar

efectos perversos, como son la gran dispersión de las actuaciones, lo cual genera confusión por parte del usuario, de quien va a consumir esos servicios. No hablo solo de contenidos, sino también de canales de soporte o de denuncia. La ciudadanía tiene que tener muy claro una marca a la que va a acudir cuando tenga un tema de menores. Ahí va a ser muy interesante este grupo de trabajo que nos permitirá a todos aunar esfuerzos, evitar duplicidades, y que no se quede por cubrir ningún ámbito que debería estar cubierto.

A día de hoy hay un ámbito que no está cubierto, que son los protocolos de actuación en los colegios. Por tanto, la actuación que se requiere pasaría por desarrollar esos protocolos —para lo cual ya existen ideas e iniciativas importantes en la materia— y por que los colegios asuman que tienen una responsabilidad como institución en todo esto. Eso tampoco es un detalle menor.

Es necesario elaborar la cultura de seguridad entre los más pequeños, para lo cual necesitamos contenidos específicos en el itinerario educativo, esto también consideramos que es clave.

Debe dotarse a los padres y educadores, que son los que tienen que utilizar estos contenidos, de los conocimientos necesarios (ahí hablaba también de los protocolos de actuación).

Y volviendo otra vez a lo mismo, es imprescindible habilitar fórmulas de colaboración que permitan aunar esfuerzos, evitar duplicidades, tener indicadores saneados y todo este tipo de cuestiones.

Y yo creo que he ido muy rápido, pero espero haber sido claro. Y muchísimas gracias por mantener la atención después de tantas horas.

Sin más, por mi parte quedo abierto a las preguntas que consideren formularme.

COMPARECENCIA DEL DIRECTOR GENERAL DE LA POLICÍA, D. IGNACIO COSIDÓ GUTIÉRREZ, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 16 DE MAYO DE 2013.

El señor **DIRECTOR GENERAL DE LA POLICÍA** (D. Ignacio Cosidó Gutiérrez): Muchas gracias, presidente. Antes que nada, quiero agradecer a todos los miembros de la ponencia la oportunidad que dan al Cuerpo Nacional de Policía para explicar cuáles son nuestros proyectos, cuáles son nuestras actuaciones, también cuáles son nuestras propuestas en una materia que creo que es importante, y además constituye una de las prioridades, como verán, en nuestra política de seguridad.

Quisiera expresarles además la felicitación, tanto a la Comisión de Interior como a la de Educación y Deporte y a la de Industria, Energía y Turismo, por haber puesto en marcha esta iniciativa, que a mí me parece tan oportuna y tan necesaria.

Por último, también quería decirles que no solo ya como director de la Policía, sino como exsenador, pues es para mí una especial satisfacción volver a esta casa y poner de manifiesto que con iniciativas como esta yo creo que el Senado tiene una importante capacidad para contribuir a hacer una sociedad mejor, que en el fondo creo que es lo que nos anima a todos desde nuestras diferentes perspectivas o ideologías.

Querría pedirles disculpas porque ha surgido un compromiso ineludible con posterioridad a haber acordado ya la fecha y la hora de mi intervención, y yo necesariamente tendré que ausentarme a las once y media, pero también les digo que dado que tanto el comisario jefe de la Brigada de Investigación Tecnológica como la responsable de Redes Sociales dentro del Cuerpo Nacional de Policía van a intervenir a continuación, pues creo que va a haber oportunidades para que cualquier cuestión que pueda surgir también pueda ser resuelta por ellos.

Es un hecho que las redes sociales se han convertido en parte de nuestra vida, y yo diría que con especial intensidad en la vida de nuestros adolescentes, que a través de esta forma de comunicación los jóvenes se relacionan entre sí, intercambian experiencias, sus gustos, motivaciones y que, en definitiva, las redes sociales son un espacio en el que los jóvenes vuelcan ya gran parte de sus vidas.

Y todo esto en mi opinión tiene efectos muy positivos. Yo creo que toda idea de criminalizar o de tener una visión negativa de todo este fenómeno no es acertada.

Las redes sociales abren formas de comunicación hasta ahora desconocidas, eliminan barreras temporales y geográficas y suponen nuevas oportunidades de comunicación humana. Pero simplemente tenemos que ser conscientes de que también tienen riesgos, como lo tiene conducir un vehículo. Cuando ofrecemos información personal, estamos atentando a veces, y lo que es más peligroso, de forma inconsciente, a nuestra propia intimidad. Porque cada vez estamos más dispuestos a que los demás accedan a determinados aspectos de nuestra vida privada en un afán por mantenernos permanentemente comunicados.

Debemos reconocer que la privacidad en Internet y cómo gestionarla correctamente sigue siendo una asignatura pendiente en nuestra sociedad, y por eso creo en el acierto de esta ponencia.

Los ciudadanos tienen el derecho a decidir quién puede o no utilizar nuestra información, porque lo contrario nos lleva a perder este derecho, de forma que todo lo que colguemos en Internet queda ahí para siempre y al alcance de cualquiera que pueda acceder a ello sin nuestra autorización.

Por desgracia, esta información personal puede ser utilizada por terceros como una forma de acoso, cuando no como un medio para el chantaje o un instrumento para cometer delitos. Estamos hablando en definitiva del cibercrimen como manifestación de los nuevos delitos cometidos mediante la utilización de las tecnologías de la información, contra el cual lucha el Cuerpo Nacional de Policía.

Para comprender la relación que existe entre el cibercrimen y las redes sociales resulta imprescindible contar con una visión panorámica que sitúe cuál es el escenario de nuestra sociedad y cuál es el impacto de estas tecnologías en nuestra sociedad. Yo estoy seguro de que voy a repetir datos y de que probablemente ustedes conozcan mejor que yo esta realidad, pero permítanme recordar de manera muy breve que actualmente uno de cada tres habitantes del mundo es usuario de Internet, es decir, más de 2.400 millones de personas interconectadas cada día entre sí, desde un extremo a otro del planeta, esperando que en el año 2015 sean 2 de cada 3 los ciudadanos del mundo conectados a Internet; que el número de usuarios de telefonía móvil en el mundo alcanza ya el 85,7 %

de la población, con 5.200 millones de terminales en uso. Y que dadas las cifras de crecimiento constante de la telefonía móvil, se estima que a lo largo del presente año se alcance el momento en el que por primera vez en la historia una tecnología de consumo igualará en tamaño a la población humana. El número de usuarios de las redes sociales supera además los 3.000 millones de usuarios; tengan presente que una persona en muchas ocasiones tiene más de una vinculación a una red social, pero son 3.000 millones de usuarios.

Nuestro país se incorporó hace ya años al tren de las tecnologías de la información, y creo que es importante cuando hablamos de estas cuestiones, no hablar de futuro, sino decir que esta es una realidad que está presente y que está plenamente consolidada. En 2012 existían en España más de 24 millones de internautas, lo que significa casi un 70% de la población española, y el 73% de esos internautas accede a Internet diariamente. Y el porcentaje llega al 85% si nos referimos a los jóvenes, entre 16 y 24 años.

¿Cuál ha sido el gran motor de crecimiento? La telefonía móvil, que es utilizada casi ya por la mitad de los internautas para acceder a Internet. De hecho, el 63% de los usuarios de móvil en España utiliza un *smartphone*, lo que representa el porcentaje más alto entre las cinco mayores economías de la Unión Europea.

De acuerdo con el primer estudio sobre redes sociales en España del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, que no sé si habrá ya comparecido, España ocupa el tercer puesto en el ranquin mundial de usuarios activos en las redes sociales, con un 77% de los usuarios de Internet. Y uno de cada tres de estos usuarios de las redes sociales se conecta todos o casi todos los días. Y el 41% de ellos de 19 a 25 años utiliza dos redes sociales de media.

Yo insisto, creo que todo esto es sumamente positivo, es decir, creo que esto es bueno. Sin embargo, y como muy acertadamente señala la propia constitución de esta comisión por el Pleno del Senado, en la creación de la presente ponencia, existen otros datos que sí resultan preocupantes: el 75% del total de los entrevistados por el Observatorio se muestra poco o nada preocupado acerca de lo que otras personas vean o piensen de ellos a través de las redes sociales. Y yo les diría que aquí el reto fundamental son los menores. Los menores acceden a páginas de temáticas y contenidos inadecuados, ya estemos hablando de pornogra-

fía, de violencia, sexismo, racismo, apología de la drogadicción, a veces apología del suicidio o de enfermedades como la anorexia. Pueden sufrir un potencial encuentro físico con sujetos que enmascaran su identidad en la red para invitar a los niños a diferentes chats o luego tratar de citarse personalmente con ellos. Pueden sufrir fraudes en ventas de artículos, incluso pueden ser objeto de espionaje, en el sentido de tratar de captar información personal o de su entorno familiar, ya que los menores son especialmente proclives a facilitar ese tipo de información.

Los profesionales de la seguridad saben que tienen un reto formidable para garantizar la seguridad de todos los usuarios en la red, pero yo diría que de manera muy particular en el caso de los menores.

Este problema ha crecido además de forma paulatina hasta alcanzar unas cotas que ciertamente resultan preocupantes. De tal suerte que actualmente el delito más lucrativo a nivel mundial después de la prostitución y el tráfico de drogas es el cibercrimen. Internet se ha convertido en una infraestructura de información tan esencial para las personas que es imprescindible que nuestras redes y sistemas informáticos sean resistentes, confiables y seguros ante todo tipo de amenazas. Y en este sentido la seguridad se configura como un presupuesto necesario para el efectivo desarrollo de la sociedad de la información.

En Internet el clásico debate entre libertad y seguridad se concilia cuando se trata del ejercicio de derechos y libertades en Internet: una red abierta y libre, necesariamente tiene que ser una red segura. En la Agenda Digital para Europa que ha elaborado la Comisión Europea se reconoce que los ciudadanos no emprenderán actividades en línea cada vez más sofisticadas si no están convencidos de que tanto ellos como sus hijos pueden fiarse plenamente de las tecnologías de la información. Por tanto, la Comisión insta a los Estados miembros a combatir el auge de las nuevas formas de delincuencia, la ciberdelincuencia, que abarca una amplia tipología de delitos, como ya les he señalado, desde la pornografía infantil al robo de identidades o los ciberataques.

La propia Comisión Europea aprobó en 2012 su primera estrategia en favor de un Internet más adecuado para los niños. En esa estrategia señala que los menores en Internet merecen un tratamiento específico para conseguir que la red se convierta en un lugar seguro en el que los niños puedan acceder al conocimiento, comunicarse, desarrollar sus aptitudes y mejorar sus perspectivas, incluso laborales, de futuro. Pero que los

riesgos experimentados por los jóvenes en Internet son bastante evidentes, y similares además en toda Europa.

En 2010, cuatro de cada diez menores en Europa dijeron haber encontrado uno de los siguientes riesgos: comunicación en línea con alguien que no conocían personalmente; exposición a contenidos inapropiados para su edad generados por usuarios en los que se promovía la anorexia, la automutilación, el consumo de drogas o el suicidio; exposición a imágenes sexuales en línea y uso indebido de los datos personales; encuentros en el mundo real con personas conocidas en línea; o ser víctimas de ciberacoso. Es decir, esto, cuatro de cada diez menores entrevistados.

Surgen además nuevas pautas de comportamiento, como la distribución de imágenes de agresiones físicas a otros niños tomadas con la cámara de un móvil, o el envío a compañeros de imágenes o mensajes con contenido sexual.

Además se está expandiendo el uso de Internet para la captación de víctimas, para la trata de personas y la publicidad de sus servicios, incluyendo en ocasiones a los menores.

Conocen además que Internet constituye un vehículo para la fácil difusión de la pornografía infantil. Lamentablemente hoy daremos cuenta de una nueva operación en relación con esta cuestión. Son numerosos los retos que debemos encarar los responsables públicos para luchar contra el cibercrimen, y en espacial contra el que afecta a jóvenes y menores.

Permítanme comentarles muy brevemente tres características de Internet que hacen especialmente difícil el trabajo de persecución del delito en la red, que llevan a cabo profesionales como el comisario que a continuación les va a hablar.

En primer lugar, Internet es muy complejo, es un sistema, yo diría casi un ecosistema tecnológico en el que intervienen entidades públicas y privadas con intereses muy diversos y que en ocasiones resultan contradictorios. Para garantizar la seguridad de nuestros jóvenes en Internet entran en juego desde la responsabilidad primera de los padres, los centros educativos, la industria de los contenidos digitales, los operadores de telecomunicaciones, los proveedores de acceso a Internet, los fabricantes de equipos y de software, las asociaciones en defensa de los derechos de los menores, y lógicamente los poderes públicos; el poder legislativo, muy en primera instancia, pero los organismos reguladores, los jueces y

tribunales y, por supuesto, las Fuerzas y Cuerpos de Seguridad del Estado. Son muchos actores.

En segundo lugar, en Internet, como bien conocen, no hay fronteras ni físicas ni geográficas. En el cibercrimen es muy habitual que la víctima y el autor del delito estén separados por miles de kilómetros en países diferentes. El carácter de amenaza global del crimen organizado se ve potenciado por el empleo y el aprovechamiento de estas nuevas tecnologías que permiten a las redes criminales actuar desde lugares donde pueden sentirse seguros frente a la acción penal y procesal, canalizando sus beneficios ilícitos mediante un sistema financiero global. Esto supone un importante reto de cooperación policial internacional, al tener que coordinar actuaciones policiales de varios países, y además a mucha velocidad para poder ser eficaces en la lucha en este delito.

Y en este campo, quiero decirles que estamos avanzando de manera muy notable. Un ejemplo es la reciente detención en Dubái en febrero de este año de un ciudadano ruso autor del conocido «virus de la policía», quien utilizaba una célula financiera radicada en la Costa del Sol en una operación que fue protagonizada por la Brigada de Investigación Tecnológica. Y otro éxito muy reciente es la detención en Barcelona el pasado mes de abril de un activista holandés responsable del mayor ataque de denegación de servicio distribuido de la historia, quien en marzo de 2007 colapsó el funcionamiento de Internet en todo el mundo. Por tanto, segunda característica: el carácter global que tiene este fenómeno.

La tercera característica que hace especialmente difícil la lucha contra el cibercrimen es la especialización y organización del mismo. Dejando aparte los casos de acosos entre menores que se producen en entornos escolares, puede decirse que lamentablemente el cibercrimen en general se ha convertido en un negocio que mueve un elevadísimo volumen de dinero. De acuerdo con el *Internet Crime Complaint Center*, que es un centro respaldado por el FBI, las pérdidas totales en el año 2009 debidas a cibercrimen ascendieron a 500.000 millones de dólares en el mundo. Un informe de 2011 de la empresa Norton señaló que el coste del cibercrimen se acerca al valor del tráfico de drogas, es decir, al valor global del tráfico de droga, y si lo quieren tomar como referencia, el cibercrimen supera en más de cien veces los gastos anuales de Unicef.

Por su parte, Europol ha puesto en evidencia que el modelo de negocio cibercriminal difiere significativamente de la tradicional delincuencia

organizada, porque el ciberespacio y la infraestructura de Internet contribuyen a hacer del cibercrimen un modelo orientado al servicio, donde no hay jerarquía, sino proveedores de servicios cibercriminales unificados por la propia infraestructura del ciberespacio. Es lo que podemos denominar como «el crimen como servicio».

La consecuencia es que las plataformas tecnológicas que utilizan los cibercriminales son multicrimen. Pongo un ejemplo: una red de miles de ordenadores infectados, lo que se denomina una *botnet*, puede ser ofertada por una organización criminal para distribuir correos electrónicos fraudulentos (la práctica conocida como *phishing*) o para la realización de un ataque de denegación de servicio a otras organizaciones criminales. Las redes Tor permiten intercambiar de forma anónima todo tipo de contenido delictivo, desde material de pornografía infantil hasta mensajes entre terroristas. Otro ejemplo: Internet ofrece medios cada vez más perfeccionados para poder blanquear los beneficios financieros obtenidos del cibercrimen de forma ilícita por las empresas de cibercriminales.

Por lo tanto, si bien el Código Penal tipifica de forma separada los distintos tipos de delito, desde la Policía Nacional creemos que es imprescindible una estrategia transversal de lucha contra el cibercrimen, precisamente por esta naturaleza que tiene de criminalidad como servicio. No se puede resolver un problema concreto de abuso sexual de menores sin tener una estrategia integral para la lucha general contra el cibercrimen.

Los delitos cibernéticos a los que nos enfrentamos son de muy variado tipo. En el Convenio sobre la Ciberdelincuencia del Consejo de Europa, firmado en Budapest en el año 2001, se utiliza el criterio de diferenciar dos tipos básicos: el que tiene como objetivo el sistema de información, o bien el que utiliza estas tecnologías como forma para cometer otros delitos que tradicionalmente ya se cometían.

Así, siguiendo esta clasificación, se encuentran los delitos en los que el ordenador, la red informática o un dispositivo electrónico es el objetivo propio de la actividad criminal. Los delitos contra los que lucha la Policía Nacional en este primer campo son, entre otros, los accesos no autorizados a sistemas de información, como por ejemplo la piratería o *hacking*, para copiar, modificar, borrar o destruir datos y programas; la difusión de códigos maliciosos, el *malware*, tales como los virus, los gusanos, los troyanos o las bombas software; la interrupción o denegación de los servicios, por ejemplo, los ataques de denegación de servicios

DoS, el robo o mal uso de los servicios, como puede ser el robo de una cuenta en Internet o de un nombre de dominio, para después enviar con identidad falsa mensajes; o finalmente, los ataques contra infraestructuras críticas fundamentales, con consecuencias potencialmente desastrosas para el conjunto de la sociedad, lo que podríamos denominar como ciberterrorismo.

Para clarificar este tipo de delitos, les citaré brevemente dos casos de éxito de operaciones importantes de la Policía Nacional. El primero de los casos fue la reciente detención de un pedófilo *hacker* que grababa imágenes de la vida íntima y sexual de sus vecinos a través de las cámaras web de los ordenadores personales de estos. El sujeto asaltaba las conexiones WiFi de sus vecinos, les infectaba los ordenadores con un *malware* tipo troyano que le permitía controlarlos a distancia y grabar a los propietarios con las cámaras de sus propios ordenadores infectados.

El segundo caso consiste en la detención el pasado mes de 35 personas de una red internacional especializada en la clonación de tarjetas bancarias. La red criminal operaba a nivel mundial e instalaba dispositivos para clonar las tarjetas (lo que conocemos como *skimming*) en cajeros automáticos y datáfonos. Copiaban los datos de las tarjetas y se los enviaban a otros integrantes de la banda para su falsificación y uso. Y finalmente enviaban el dinero fuera de España para blanquearlo.

Igualmente la Policía Nacional lucha de forma eficaz contra las redes de pederastia y pornografía infantil. Los éxitos más recientes de operaciones policiales son la detención en Barcelona en noviembre de 2012 del pederasta que acosó a 50 menores a través de videoconsolas, la detención en Gandía en abril de este año del acosador sexual de 300 niñas a través de Internet, y también este mismo mes la detención de 25 personas y la imputación de otras 16 por pornografía infantil dentro de la denominada operación «Ciudadano». Esta operación, la operación «Ciudadano», es un buen ejemplo de colaboración ciudadana, ya que se realizó gracias a las informaciones aportadas por los ciudadanos a través de denuncias realizadas en las comisarías de policía y también las remitidas al correo electrónico de la policía, correo que había sido difundido a través de los canales de redes sociales de la Policía Nacional.

Yo destacaría —luego lo haré— que aquí es básico y fundamental la colaboración ciudadana. Sin eso es muy difícil que nosotros podamos ser eficaces.

Los tres principales problemas a los que se enfrentan nuestros jóvenes y menores son: en primer lugar, el acceso a contenidos inapropiados, como les mencionaba y les enumeraba antes.

En segundo lugar, cada vez más casos de acoso en línea (lo que se denomina como el ciberacoso o el *ciberbullying*). Este tipo de ciberdelincuencia implica el uso del ordenador para causar un daño personal al menor, por ejemplo ansiedad, angustia o daño psicológico. Y lamentablemente hemos llegado a tener casos de suicidios como consecuencia de este tipo de acoso. Se considera como tal el envío de *e-mails* abusivos, amenazantes o de odio, la publicación de información lesiva para una persona en páginas web, foros o redes sociales, bien a través del ordenador, de las tabletas, de los teléfonos móviles, con la intención de intimidar, amenazar o acosar a la víctima, normalmente con intención de dañar su imagen.

Y el tercer gran problema que se encuentran los menores es el abuso sexual infantil (también denominado el *child grooming*). Este ciberdelito abarca una serie de conductas que tienen un elemento objetivo de daño sexual al menor, como son las acciones deliberadas por parte de un adulto de cara a establecer lazos de amistad con el objetivo de obtener imágenes eróticas o pornográficas del mismo para satisfacción sexual o incluso como preparación o chantaje para un posterior encuentro.

Según las normas internacionales, esta conducta incluye la producción, la posesión y el acceso a imágenes que registren el abuso sexual de niños por parte de adultos, así como de imágenes de niños involucrados en una conducta sexualmente explícita o de los órganos sexuales. Este tipo de imágenes son producidas y utilizadas principalmente para fines sexuales con o sin el conocimiento del niño.

Desde una perspectiva práctica, este tipo de ciberdelincuencia se puede clasificar en tres componentes: la producción, que es la creación del material; la distribución, la carga y difusión del material; y el consumo, la descarga del material.

Desgraciadamente la capacidad para obtener y almacenar imágenes y contenidos se ha facilitado por la ubicación de las redes de comunicación y por los avances relacionados con la tecnología digital, es decir, cualquiera puede grabar con un teléfono móvil o con cualquier dispositivo a muy bajo coste, y además almacenarlo en dispositivos con una enorme capacidad.

El *child grooming* es un proceso que comúnmente puede durar semanas o incluso meses. Comienza cuando el adulto procede a entablar lazos de amistad con el menor, normalmente simulando ser otro menor. De esta forma, el adulto va obteniendo datos personales y de contacto. En un segundo momento, y utilizando tácticas como la seducción o la provocación, por ejemplo mediante el envío de imágenes en bañador o ropa interior, el delincuente consigue finalmente que el menor se desnude frente a la *webcam* o le envíe fotografías de naturaleza sexual. A partir de ese momento el menor está perdido, ya que el pederasta inicia un ciberacoso de chantaje a la víctima para obtener cada vez más material pornográfico en una espiral creciente de mentiras y miedos dirigidos a tener un encuentro físico con el menor para abusar sexualmente de él.

Puedo asegurarles que la Policía Nacional tiene la más firme determinación para luchar contra todas las formas que pueda adoptar el cibercrimen en general, pero yo les diría que de forma especial contra estas formas de cibercriminalidad a las que nos estamos refiriendo. Como muestra de este compromiso hemos decidido potenciar la unidad responsable de la lucha contra este tipo de delitos mediante la creación de una nueva unidad de investigación tecnológica encuadrada dentro de la Comisaría General de Policía Judicial. La idea es transformar la actual brigada en una unidad de la que dependan dos brigadas: una Brigada Central de Investigación Tecnológica, a la que corresponde la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial, y los fraudes en las telecomunicaciones; y una segunda brigada, que sería la Brigada Central de Seguridad Informática, a la que corresponde la investigación de las actividades delictivas que afecten a la seguridad lógica, es decir, a la seguridad de los sistemas, y a los fraudes.

El responsable de esta unidad intervendrá posteriormente para exponer a sus señorías cómo se realiza el trabajo de investigación y de persecución de estas actividades delictivas. Pero la creación de esta unidad, yo querría destacar que pretende duplicar el número de efectivos dedicados a la lucha contra el cibercrimen y dotarles además de los medios tecnológicamente más punteros y especializados para que cumplan eficazmente su función de dar confianza a nuestros ciudadanos en el ciberespacio.

Yo les diría que ninguna tipología delictiva está creciendo al ritmo al que lo está haciendo la ciberdelincuencia, y que, por tanto, es imprescin-

dible que aumentemos nuestras capacidades para poder investigar este tipo de delitos.

Pero no se trata solo de crear una nueva unidad para luchar contra el cibercrimen, porque yo creo que lo más importante es conseguir que la totalidad de las unidades de la Policía Nacional, por supuesto las unidades territoriales de Policía Judicial, pero de manera especial las unidades centrales especializadas asuman una parte de la responsabilidad en la lucha contra esta ciberdelincuencia.

Así, la Comisaría General de Información debe realizar una especial vigilancia digital de la red en su lucha contra el terrorismo y el «hacktivismo». La Comisaría General de Seguridad Ciudadana realiza el seguimiento en redes sociales y foros de aquellos perfiles de grupos violentos que puedan derivar en violencia en nuestras calles. La Comisaría General de Policía Científica está trabajando en informática forense y en la captura y preservación de evidencias digitales. La Unidad de Informática es responsable de dotar de las herramientas y el apoyo tecnológico a todas estas unidades. La Unidad de Cooperación Internacional debe establecer mecanismos de interrelación más eficaces para luchar contra este tipo de delincuencia.

Pero si tuviera que destacar, más allá de la propia unidad de investigación, unas unidades que resultan fundamental en esta estrategia son aquellas que se dedican a la colaboración ciudadana. Porque todas las actuaciones de difusión y prevención que realizamos en este ámbito, creo que son trascendentes si realmente queremos tener eficacia en la lucha contra este fenómeno. Y en ese sentido la inspectora que es responsable de redes sociales dentro del Cuerpo Nacional de Policía les informará con más detalle de cuáles son esas iniciativas.

Con esta visión integral del cibercrimen, la Policía ha aprobado un Plan estratégico que abarca los años 2013 a 2016. En este plan se recogen los objetivos prioritarios para la Policía Nacional en los próximos años, y pone en marcha un plan de transformación de la Policía que está basado en muy buena medida en la innovación tecnológica y en un uso más eficiente de los recursos para lograr que España sea un país más seguro. El plan pretende la transformación del Cuerpo Nacional de Policía en una verdadera «Policía Inteligente» a través de un objetivo que hemos denominado «Policía 3.0».

¿Cuáles son las prioridades de este plan?

Claramente hemos situado el ciberdelito como una de las prioridades máximas, como uno de los objetivos estratégicos del Cuerpo Nacional de Policía. La estrategia a seguir en los próximos cuatro años y sus objetivos han sido establecidos con especial compromiso en la transparencia y en la participación ciudadana. Se va a potenciar la colaboración ciudadana a través de las redes sociales y el contacto constante con sus unidades de participación ciudadana.

Como medidas concretas que se recogen en este plan se encuentran la de impulsar las investigaciones relacionadas con los fenómenos delictivos emergentes derivados del uso de las tecnologías de la información; realizar la respuesta ante la proliferación de los delitos contra las personas cometidos a través de la red, especialmente en el ámbito de la protección al menor y la explotación sexual infantil; potenciar las investigaciones relacionadas con amenazas y vulnerabilidades a los sistemas informáticos, así como la actividad delictiva derivada de las mismas, con especial incidencia en la protección de las infraestructuras críticas; promover y participar en las investigaciones de investigación y desarrollo y colaborar con otras instituciones públicas y privadas, e impulsar el desarrollo y actualización de herramientas técnicas legales para una mejor eficacia contra este tipo de delincuencia; así como participar en instituciones internacionales (yo destacaría en este campo Interpol y Europol, y de manera muy particular un centro de nueva creación, el *European Cybercrime Center*, creado en el seno de Europol), así como incrementar la cooperación bilateral que mantenemos con otras policías en este tipo de delincuencia. Les puedo decir que la Policía Nacional está formando policías de otros países del norte de África o de Iberoamérica en relación con las técnicas de investigación de este tipo de delincuencia.

Una medida de gran relevancia para luchar contra este ciberdelito es la creación en el seno del Cuerpo Nacional de Policía de un equipo de respuesta a emergencias informáticas. Una tarea fundamental de este CERT de la Policía Nacional será la coordinación centralizada para las cuestiones relacionadas con seguridad de las tecnologías de la información dentro del Cuerpo Nacional de Policía. Desde una perspectiva externa, el CERT debe mantener una relación fluida y constante con otras fuerzas y cuerpos de seguridad del Estado, con otros CERT públicos y privados y con entidades europeas, no solamente Europol, sino también ENISA.

Junto a todas estas medidas, reviste especial importancia la consideración que da el plan estratégico a la formación del personal del Cuerpo Nacional de Policía en materia de ciberseguridad. Y en este campo pretendemos aumentar la formación en ciberseguridad en los planes de estudio del personal de nuevo ingreso, para dar ya una información básica en nuestras escuelas de policía, y diseñar e impartir una formación especializada, específica, para las unidades del Cuerpo Nacional de Policía que trabajan en este campo. Y esa formación, necesariamente tiene que ser una formación en colaboración con entidades externas, con otros CERT, con la universidad, con entidades privadas, incluso con empresas, porque este es un mundo que evoluciona a tal velocidad que uno no puede nunca aspirar a ser autosuficiente.

Otra medida importante incluida en el Plan Estratégico es la revisión —y esto les afecta de manera muy directa— del actual marco normativo y de colaboración en materia de ciberseguridad. En este sentido, considero que es necesaria una reflexión sobre la legislación existente para eliminar posibles barreras a una actuación policial eficaz, teniendo presente siempre la salvaguarda de los derechos fundamentales, del derecho a la intimidad de todos los ciudadanos. Y por eso es importante no solamente hacer esta reflexión sobre la legislación, sino establecer protocolos muy precisos para el intercambio de información con los operadores de telecomunicaciones y los proveedores de acceso a Internet, siempre con un escrupuloso respeto al marco legal de protección de datos de carácter personal, que les puedo asegurar que en España es particularmente exigente. Esta ponencia, estoy seguro de que va a hacer alguna aportación importante en ese terreno.

Para mejorar los niveles de seguridad ciudadana, el plan estratégico diseña un nuevo sistema —si me permiten— de patrullaje inteligente, e implementa una nueva herramienta informática para la gestión de los servicios de protección a nivel nacional.

Por otra parte, la preocupación de los grupos vulnerables se convierte en otro objetivo prioritario de la Policía, por lo que impulsaremos una actuación policial integral que consiga un aumento de la prevención, la efectiva protección de las víctimas y una mayor eficacia en la investigación de los hechos delictivos.

Con el objetivo de promover la seguridad de los menores, muy particularmente en el entorno escolar y las redes sociales, se va a intensificar

la participación en los programas de concienciación para un uso seguro y responsable de las redes sociales; se fomentará la colaboración entre las administraciones y con los administradores de estas redes en la protección del menor; y se intensificarán y mejorarán las campañas de educación en seguridad en el entorno escolar, con especial atención al acoso escolar y al *sexting*, y se promoverán campañas que prevengan su integración en actividades delictivas, así como su captación por bandas juveniles.

Y finalmente —y termino ya— el Plan Estratégico realiza también una apuesta decidida por la participación ciudadana, no como una necesidad impuesta desde el exterior, sino como un valor que debe formar parte cada vez más de nuestra propia cultura policial. El nuevo marco de seguridad pública exige abrirse a la colaboración ciudadana facilitando su participación e integración, habilitando nuevos canales de comunicación a través de las redes sociales. No voy a hacer publicidad porque ya lo conocen todos ustedes, pero creo que la Policía Nacional es en estos momentos una clara referencia internacional para otros cuerpos de seguridad de cómo utilizar las redes sociales para mantener una comunicación y para mantener una colaboración con los ciudadanos.

Señorías, como resumen de mi intervención, puedo decirles que el Cuerpo Nacional de Policía se encuentra comprometido en la lucha contra el cibercrimen, y en especial en la lucha contra todas las manifestaciones de delitos que afectan a nuestros menores en su relación con las tecnologías de la información, que creo que en este campo es el principal reto que tenemos común.

Un marco adecuado de seguridad es el presupuesto necesario para construir una sociedad de la información libre. En este empeño —como ven— estamos trabajando con mucho entusiasmo, y quiero reiterarles toda nuestra colaboración para el éxito de esta ponencia, que estoy seguro de que va a contribuir también de manera decisiva a este reto común que tenemos por delante.

Muchísimas gracias, y siento haberme extendido más de lo que inicialmente el presidente me había sugerido, aunque en este trámite parlamentario entiendo que no había esta limitación temporal. Escucho con toda atención sus intervenciones, y si queda alguna cuestión más por contestar, seguro que los otros representantes del Cuerpo Nacional de Policía pueden también participar en el mismo.

COMPARECENCIA DEL COMISARIO JEFE DE LA BRIGADA DE INVESTIGACIÓN TECNOLÓGICA DE LA COMISARÍA GENERAL DE LA POLICÍA JUDICIAL DE LA DIRECCIÓN GENERAL DE LA POLICÍA, D. JUAN MIGUEL MANZANAS MANZANAS, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 16 DE MAYO DE 2013.

El señor **JEFE DE LA BRIGADA DE INVESTIGACIÓN TECNOLÓGICA DE LA COMISARÍA GENERAL DE LA POLICÍA JUDICIAL DE LA DIRECCIÓN GENERAL DE LA POLICÍA** (D. Juan Miguel Manzanas Manzanas): (...) en primer lugar que mi intervención es la representación de un equipo de gente, como digo yo, de gente echada para adelante, profesionales comprometidos, con espíritu positivo y abierto, y que tengo la suerte y el lujo de dirigir.

Todos ustedes conocen personal o profesionalmente motivos de la importancia de las redes sociales como elemento de esta nueva revolución social y de su incidencia positiva, y a veces negativa, en la sociedad en general y los jóvenes en particular. La visión panorámica que les voy a relatar un poco, a exponer, está ubicada en ese tanto por ciento de utilización perversa de las nuevas tecnologías, vinculada con el delito, y por tanto menos agradable, pero en la que el Cuerpo Nacional de Policía tiene entre sus competencias la de identificar, localizar y detener a los autores de estos hechos delictivos.

La comúnmente conocida como BIT es la unidad que está encuadrada, como ha dicho el director general, dentro de la Comisaría General de Policía Judicial, en ese organigrama dentro de la Dirección General. Y su misión primordial, como el resto de unidades de Policía Judicial, es eminentemente operativa, operativa y de investigación. Y está dirigida a la localización y detención de los autores de los hechos delictivos, es decir, una vez que se han cometido esos hechos, para ponerlos a disposición de la Fiscalía o de la autoridad judicial, proporcionando los medios de prueba necesarios para demostrar su culpabilidad o inocencia en los hechos.

De alguna forma, el origen de la BIT, de la comúnmente denominada BIT, se sitúa en torno al año 1995; lo hemos fijado en esa fecha porque es cuando se creó de alguna forma, por parte de un pequeño grupo de

tres, cuatro personas, investigadores, que dentro de una entonces llamada Brigada de Delincuencia Económica y Fiscal, a esos pequeños delitos que tenían que ver de alguna forma con la parte informática o con más dificultades informáticas, dar una respuesta a los ataques y vulneraciones —en aquel momento— contra la piratería de software y determinadas estafas bancarias que se estaban produciendo en ese momento. Les hablo de unas fechas en las que, como ustedes recordarán, los sistemas operativos era el MS-DOS, los dispositivos de almacenamiento masivo eran los disquetes de 3½» y de 5¼», en fin, el acceso a las redes era impensable, lo que tenemos hoy en día. Esto, hablamos de 1995; a lo largo de ese tiempo se ha ido incrementando la actividad en ese área, paulatinamente, a la vez que se ha ido produciendo la nueva tecnología. Y en 2002 se conforma, se amplía, por decir así, el campo de actuación de ese pequeño grupo que se inició y se crea la Brigada de Investigación Tecnológica, la conocida BIT, hasta ahora. Ahí ya se incrementan una serie de actividades, entre las que ya tienen de una forma más consolidada la lucha contra la pornografía infantil y los abusos sexuales contra los menores, es decir, la protección contra el menor. Y el añadido, que es el motivo por el que inicialmente comenzó, algunas de las pequeñas estafas que se estaban produciendo por estos medios.

Es a partir de enero de este año precisamente, con la entrada en vigor de la orden ministerial a que ha hecho referencia el director cuando se pretende dar un impulso, un reforzamiento de esta forma por parte del Cuerpo Nacional de Policía a la investigación en estos medios e incentivar de alguna forma, e incrementar la potencialidad de capacidades en este campo, creándose la Unidad de Investigación Tecnológica, que es sobre la que vamos a estar poniendo los pilares —esperamos— del futuro de esta línea de investigación.

El auge de las tecnologías de la información y la comunicación y la orientación de las nuevas formas delictivas en estos medios suponen un nuevo escenario que precisa una mayor respuesta en la investigación. Y para ello, en esta Unidad de Investigación Tecnológica, como antes ha mencionado el director también dentro de esta unidad, dentro de esta estructura, se creaban dos brigadas, con la finalidad de incrementar su actividad. Y además orientadas de una forma muy clara, precisamente para diferenciar las diferentes formas de actuación en la investigación, que implican, por un lado, los delitos que están relacionados con las personas, de lo que es la investigación de los delitos relacionados con

los sistemas informáticos y con la red. La problemática es distinta; las formas de investigar son distintas; las formas de recibir las denuncias y los hechos también son muy distintos. Y esto nos obliga a actuar también de forma diferente.

En el ámbito de la investigación de los delitos contra las personas, lógicamente estaría integrada la protección al menor, la pornografía infantil, los delitos contra la libertad sexual, delitos contra el honor y la intimidad, las calumnias, injurias, redes sociales.

En esa otra brigada que está orientada a la investigación de los delitos contra los sistemas informáticos y la red es donde vamos a encuadrar toda esa actividad delictiva en el campo del cibercrimen que está vinculada con los delitos contra el patrimonio, en el que el objetivo principal es el ánimo de lucro inicialmente, aunque luego existen robos de información de datos, existen otra serie de delitos con carácter ideológico, de carácter de terrorismo, de espionaje industrial, entre Estados, etc. Es una actividad que en una gran parte está orientada al campo de la actividad fraudulenta, a la obtención de un patrimonio, que es la más propiamente delictiva, hasta ir avanzando a una delincuencia de alta tecnología, por decir así. De hecho, esto es un poco lo que otros colegas a nivel europeo, por ejemplo los holandeses, que en un informe que han hecho de forma trianual, se puede ver que tienen la misma problemática; o sea, tenemos una situación de identidad en los problemas que tenemos, a pesar de que sean «holandeses», y que llevan más tiempo trabajando estos temas. Existe una identidad en sus conclusiones con la mayor parte de las problemáticas que tenemos. Esto no es un consuelo, pero es una forma de partida de que también estamos trabajando en ello. Y esta es la orientación que ellos han generalizado.

Dentro de esta investigación de lo que es la delincuencia de alta tecnología es donde tendremos un punto de colaboración con ese centro de respuesta y alerta temprana que se pretende crear dentro del Cuerpo Nacional de Policía, como se ha mencionado antes, y en el que intentaremos recoger todas las novedades y noticias que estén llegando de todos los países a nivel del cibercrimen, y colaboraciones directas con otras policías, no solamente del ámbito europeo sino del ámbito internacional americano, etc.

Esta organización de la unidad central potenciará igualmente nuestra labor de lo que comúnmente se conoce como BIT, que no es estricta-

mente este grupo de personas, sino que consta además de una estructura a nivel policial, como ustedes conocerán, a través de la Jefatura Superior de Policía, en cada comisaría provincial, en donde existe un pequeño grupo de personas que reciben las pequeñas denuncias, las pequeñas investigaciones más directas a lo mejor con el ciudadano, que unas son de pequeña actuación y otras tienen que ver en el contexto de un gran volumen de hechos o de daños que, generalizados, hay que coordinar desde la unidad central.

Y esa es la labor de la unidad, la de coordinación de toda esa actividad, a través también de esas pequeñas unidades que se creen a nivel periférico en cada comisaría provincial. Que además tienen que ser el soporte, y lo son de hecho, en el campo de las estafas, pero también, y lo están haciendo así, en el campo sobre todo de la pornografía infantil. Nuestra labor no es exclusivamente con los efectivos que tenemos, porque si no, sería imposible físicamente poder llevarlo a cabo, el nivel de detenidos que se hace al año en estos temas, y el nivel de operaciones que se están realizando, porque tenemos que contar con que se hacen operaciones simultáneamente en ocasiones de 10, 15 provincias, si no en el mismo día en días muy aproximados, y lógicamente, esto exige un nivel de respuesta coordinado con el resto de compañeros.

Hecho un poco este esbozo de lo que es la presentación de lo que va a ser la unidad, voy a intentar relatarles lo que son los campos de actuación, las áreas de intervención que hasta ahora estamos hablando, de lo que era esa Brigada de Investigación Tecnológica, con una infraestructura, con una estructura determinada. Hablaba antes de que inicialmente se creó con un grupo en el que los medios que se estaban utilizando eran los sistemas de almacenamiento de 3½»; en la etapa de 2002 hasta ahora estamos hablando de una etapa en la que la Brigada de Investigación Tecnológica estaba orientada fundamentalmente a la actividad de los delitos relacionados con la informática y en las redes, y esto suponía el estar orientada esa investigación a tener un terminal de un ordenador en casa, en el trabajo, en donde sea, en el que puedes estar conectado a la red. Es decir, tenías una identificación mediante una dirección IP que era la que te geolocalizaba, te identificaba, te situaba y te ubicaba en una zona.

Parece que esto se corresponde con esa nueva tendencia que se está produciendo en este campo, y es que hoy en día escasamente ya quedan ordenadores en casa, quiero decir ordenadores de sobremesa conecta-

dos a un punto fijo, y que todo se traslada a través de redes, redes WiFi, tabletas, *smartphones*, telefonía móvil... Es decir, el punto de conexión con la red lo tiene cada individuo en su bolsillo en cualquier momento en cualquier zona del territorio nacional o extranjero. Esto cambia la dimensión de los parámetros que suponen para nosotros esos niveles de investigación y supone un reto añadido a esas dificultades que se van implementando. Es decir, es verdad que las nuevas tecnologías de la información y la comunicación van más deprisa que nosotros, afortunadamente también es un hecho interesante y bueno socialmente, y nosotros tenemos que ir con esos nuevos retos.

Para el Cuerpo Nacional de Policía constituye una de las prioridades todo lo relacionado con la protección del menor en el ámbito de las nuevas tecnologías e incidiendo especialmente en la lucha contra la explotación sexual infantil, participando en todo tipo de proyectos con las diferentes instituciones públicas y privadas, nacionales e internacionales, tanto universidades como ministerios, proveedores de servicios, etc. En la actualidad esta unidad está dimensionada con tres grupos operativos de protección al menor en los que se planifican operaciones encaminadas a la identificación y posterior detención de los usuarios de los programas de intercambio de ficheros a través de Internet, ya que constituyen la mayor fuente de victimización secundaria de los menores, circulando entre los pederastas las imágenes de los abusos de forma indefinida en el tiempo por Internet. Este es uno de los problemas que intentamos atajar.

Por eso la lucha contra la pornografía infantil abarca fundamentalmente dos aspectos: por un lado, trata de reducir en la medida de lo posible la cantidad de pornografía infantil disponible en la red. Así, intentamos luchar contra la red para intentar sacar toda la posibilidad de existencia de este tipo de imágenes. Y por otro, identificar a los agresores sexuales y sus víctimas.

No solamente hay que tener en cuenta esas imágenes y además las víctimas, sino que detrás de ellos existen unas etapas evolutivas de determinadas personas que no solo se benefician del comercio o lúdicamente de esas imágenes, sino que además llegan a unos estadios en ese desarrollo, en esa evolución, en la que llegan a llegar al abuso, a la agresión sexual de esos menores. Y además con unas connotaciones francamente aberrantes. Hablábamos esta mañana de una de las operaciones que se han dado a conocer —Carolina seguramente... lo hemos estado hablan-

do—, y resultan francamente difíciles, con menores de dos años con determinadas agresiones. Resulta francamente difícil.

Traía una serie de operaciones especificas para relatarles pero no les quiero cansar con estas cosas, voy a hablarles de cuestiones más generales.

Una de las implicaciones más importantes de esta área de protección al menor, necesariamente es la formación. Los especialistas no solo están especializados en investigación de policía judicial, sino que además tienen que reunir una serie de conocimientos específicos necesarios, de tipo informático, a veces un poco más friqui, como solemos decir nosotros, pero es verdad que tienen que estar ahí; hay que estar despiertos, hay que estar abiertos, son gente lista.

Entonces, ¿por qué? Porque cuando se interviene en cualquier tipo de operación tenemos que pensar en la otra parte de lo que es nuestro fin, no solamente detener a esa persona, sino buscar esas evidencias electrónicas que tenemos que proporcionar a la autoridad judicial. Y eso es un problema que tiene la policía en general, y en este caso nosotros en particular, porque la verdad es que proporcionar o conseguir ese tipo de evidencias cuesta; cuesta y hay que conocer los entresijos de verdaderos especialistas y técnicos que hay en estos temas a nivel de usuario, a veces elemental; cualquier chaval hoy en día, son superavezados y llegan a conseguir auténticas maravillas.

Esto implica una serie de actividad de mejora permanente en el propio policía a través de formación no solamente nacional, sino con empresas privadas, a nivel internacional. Estamos acudiendo a cualquier grupo de trabajo o país que está incorporando cualquier novedad sobre estos temas, e incluso, es verdad, nos procuramos arrimar mucho a algunas empresas privadas, por ejemplo de antivirus, etc., porque en ese contacto con ellos también existen, se generan unos círculos de confianza que nos proporcionan, por un lado, esos conocimientos que ellos tienen sobre las maldades que se pueden llegar a detectar, y nosotros la forma en que se están produciendo para poder intervenir. Es una especie de mutua colaboración.

Quiero significar una cosa muy importante en esta área de protección al menor: y es que las personas que están aquí dedicadas tienen —cómo les diría—, se encuentran sometidas a una presión especial. Quiero decir,

que estar viendo y buscando determinadas imágenes de este tipo tan aberrantes supone a veces, depende de cada persona y su situación, personal, familiar y demás, puede suponer una carga importante.

En otros países, como aquí también, hemos tenido ocasiones en que alguna vez que buenos profesionales, buenos policías hemos tenido que sacarlos porque podían llegar a tener problemas incluso psicológicos. De hecho, en algunas unidades policiales del centro de Europa existe más o menos una... se van haciendo unos exámenes, incluso test psicológicos, y a lo mejor a los dos años o tres años, cuando se ve necesario, se les traslada a otras unidades, a otros grupos para que cambien, porque realmente el permanecer mucho tiempo viendo esto puede perjudicar, «por muy buena pasta que se tenga». Esto quería que quedara claro, porque aparentemente pasa desapercibido, nadie lo ve, pero cuando se ven determinadas imágenes, si se ven permanentemente y tan diferentes, llega a suponer una carga importante.

Quiero hablarles un poco del ámbito de colaboración precisamente que se produce en este campo de la pornografía, de protección del menor. El ámbito de colaboración en diferentes frentes: en el ámbito internacional, yo creo que el volumen de actividad o de colaboración en el ámbito internacional es el mayor, es decir, el estar permanentemente en los grupos de trabajo de Interpol y de Europol y en permanente contacto con las policías de todos esos países, y las bases de datos que se generan sobre pornografía infantil, son los que mantienen el volumen de operatividad y a veces y, seguramente también, el nivel de eficacia que se tiene, en general creo que va correlacionado.

Este nivel de colaboración es tan puntual que se mantiene permanentemente a lo largo del día en contacto con cualquier policía: de Finlandia, de Suecia, de Alemania, etc. de modo que en cualquier momento nos comunican determinada imagen que han visto, nos lo trasladan porque creen que ese tipo de imagen puede estar orientada en una zona, una región de España; lo vemos, y entonces empiezan a sacarse conclusiones sobre determinados objetos o determinadas situaciones, y se empieza a intentar geolocalizar esa imagen, etc. Esa relación con todas esas policías es la que genera una actividad mayor potencialmente, y es la que, digamos, nos está llevando un poco en volandas en este campo. El entendimiento es increíble. Además la colaboración en este campo es muy buena. Independientemente de que por nuestra parte también estamos rastreando cualquier imagen en lo que es el entorno a nivel nacional. Y

las denuncias, lógicamente, que se producen a través de los propios ciudadanos en las comisarías, y también en gran medida de las denuncias a través de las redes sociales que tenemos en la dirección y de la página web. Es una fuente importante que nos permite estar muy en contacto con la realidad puntualmente, y a cada víctima la podemos ir tratando según la situación en la que psicológicamente puede llegar a encontrarse, que esto también es importante en este caso.

El nivel de colaboración, ya digo, en el campo de las nuevas tecnologías, tanto en Interpol como en Europol, he señalado aquí algunos de los grupos en los que se interviene: el Grupo Europeo de Nuevas Tecnologías de Interpol, en el Grupo Latinoamericano también de Interpol, en la lista 24/7 de Interpol, proyecto CES(?), proyecto CIRCAMP, en fin, la *Virtual Global Task Force*, una serie de grupos, en los que además cada uno de los jefes de grupo está asignado, acuden permanentemente de forma regular. Cuando aparece una operación se convoca y asiste cada uno de los jefes de grupo en Bruselas, en Lyon, etc., y se generan unas pautas de trabajo que en cada unidad policial a nivel nacional luego se va aportando lo que en definitiva se va trasladando en cada país. Hay algunas operaciones en este sentido, no solamente en el campo de Europol e Interpol, por ejemplo la operación «Espada», que procedía de una información que nos vino a través de Toronto en Canadá, supuso del orden de 56 detenidos aproximadamente, que se llevó a cabo y que fuimos el país que más actividad desarrollamos en la identificación incluso de las víctimas, y en ese caso la verdad es que tuvimos la suerte de que la propia policía canadiense nos felicitó y quieren que asistamos cuando el resto de países haya finalizado cada una de sus operaciones a nivel internacional, para que compartamos esa rueda de prensa o puesta de largo de finalización de esa operación, en la que también Estados Unidos tuvo una parte importante.

Preguntaron ustedes cuando estaba el director sobre el tema de la prevención: nosotros somos una unidad eminentemente operativa, de investigación. Pero el campo de la prevención tampoco lo hemos desechado, es decir, aunque la tarea policial de lo que es la prevención la lleva Seguridad Ciudadana, y también la tarea de la prevención en el campo de las redes sociales fundamentalmente lo lleva Carolina, que ya les indicará algunas cuestiones más nosotros, no obstante, siempre que hemos realizado cualquier operación, en base a la experiencia que hemos ido teniendo hemos introducido algunas pautas, comentarios, sugerencias que

luego en prensa se han ido recogiendo al finalizar cada operación, para que los usuarios y cualquier persona lo tengan en cuenta.

Pero no solamente hemos dado esas líneas de prevención, sino que además colaboramos precisamente con esta unidad provincial que digo que es de seguridad ciudadana, a través de la Unidad Central de Participación y Programas. Esa una unidad dedicada especialmente, dentro del campo de la seguridad ciudadana a nivel nacional, en todas las capitales de provincia, donde existe un delegado provincial de participación ciudadana, que es el interlocutor con todos los grupos sociales locales, a nivel provincial, etc., que son los que intervienen y dan charlas, tanto programas del tipo «Policía-escuela», «Mayores», «Violencia de género», etc.. Precisamente a ellos es a los que les proporcionamos la formación y la información para que luego puedan trasladarlo a nivel nacional. Y ellos son los que luego a nivel nacional participan regularmente, unas veces a petición y otras veces de forma oficial, por nuestra parte en los colegios, en las escuelas, en los institutos, haciendo algunas indicaciones sobre todo esto.

Además en muchas ocasiones, por otras circunstancias también hemos sido requeridos expresamente para participar y lo hemos hecho así, sobre todo y principalmente, como es lógico, a este sector de clientes que son los menores y en temas de redes sociales.

Otro de los ámbitos de colaboración que se planteaba, y que ha sido también objeto de una pregunta, es la colaboración con el sector público y el sector privado. Hay una importante colaboración, sobre todo aquí, con las ONG (Protégeles, Save the Children, etc.); son, digamos, una parte importante para nosotros, y ellos también lo entienden así con nosotros. Es decir, hay una comunicación muy buena, muy cordial, muy fluida, el entendimiento es permanente; proporcionamos y nos proporcionan un *feedback* muy importante de lo que sucede, de lo que está sucediendo, e incluso nos trasladan gran parte de las denuncias. Y esa parte previa a la denuncia que representa ese choque para el que está sufriendo ese ataque, ese acoso o esa situación, el canalizarla muchas veces a través de esas ONG facilita esa preparación previa para que luego podamos intervenir. Y la verdad es que en este campo, en este sentido la colaboración es estupenda y creo que muchas veces es bastante patente y muy satisfactorio para ambas partes. La verdad es que es una de las cuestiones más agradables dentro de todo esto por la buena sintonía que hay y por la afinidad en ese entendimiento.

Otras cuestiones motivo de colaboración: en proyectos de investigación, de I+D. Precisamente desde la brigada, desde hace año y medio, va a hacer casi dos años, se está llevando a cabo un proyecto a través de subvención de la Comisión Europea en el que estamos participando, poniendo, por decir así, en valor la experiencia y el conocimiento que tenemos para conseguir unas herramientas que nos faciliten y mejoren el trabajo a la hora de intervenir el material informático que recogemos en las intervenciones, en las entradas y registros, y que todo ello además nos sirva de filtro y que nos genere procesos automáticos que nos facilite la recogida de evidencias electrónicas para luego aportarlas con las mejores garantías a la Fiscalía y a la autoridad judicial. Y cuando digo «con las mejores garantías», hablo de intentar introducir cada vez más y de la mejor manera posible esa cadena de custodia que muchas veces no sabemos cómo hilvanar en este campo de la actividad de la red, de los delitos informáticos. Porque no sabemos muchas veces cómo tratar, o nuestros interlocutores, a veces los jueces, los fiscales y demás, no saben percibir en ese mundo físico y virtual en el que nos encontramos cómo detectar. Una evidencia física en un asesinato de una persona mediante un cuchillo la evidencia es palpable: el cuchillo. Aquí (en internet) una evidencia es algo abstracto que no aparece en ningún sitio, que yo digo a veces que implica un efecto de acto de fe por los jueces, aunque nuestros atestados y nuestra cercanía permanente con ellos para intentar aclararles cómo es, cómo se produce, dónde está, por qué es así, la verdad es que ellos también ponen una parte importante en ese esfuerzo para poder conseguirlo.

Como decía, este proyecto de colaboración se está llevando a cabo con el Instituto de Telecomunicaciones de la Secretaría de Estado de Telecomunicaciones está bastante avanzado el proyecto. El otro día estuvimos precisamente en León, en su sede, y ya está hecha la maqueta, estamos en un momento en el que se va a intentar introducir la prueba piloto para ver cómo se empieza a desarrollar, y creo que puede ser una de las herramientas que no solamente a nivel nacional, sin que incluso —y esto puede ser muy bueno a nivel nacional— puede ser vendible, es decir, no de la imagen de la propia policía, sino de España, en otras policías a nivel europeo e internacional.

Por la experiencia, porque ha sido realizado íntegramente por gente que está trabajando permanentemente en esto, en razón a sus necesidades y con la buena predisposición de los mejores técnicos e informáticos y desarrolladores de estas aplicaciones. Espero que esa herramienta nos

dure mucho tiempo, que no se nos quede desfasada en poco tiempo, que es el problema a veces de estas situaciones. Pero creemos que vamos a conseguir un producto que por lo menos nos va a dar unas bases muy consistentes en la investigación, facilitarnos mucho las tareas y sobre todo a nivel judicial, porque vamos a poder integrar en ese sistema de gestión de evidencias, que además le va a proporcionar una mayor garantía, seguridad y tranquilidad a la Fiscalía y a la autoridad judicial, con la que precisamente, si conocen en nuestro ámbito, la Fiscalía especial contra la criminalidad informática, con Elvira Tejada, con la que por supuesto estamos en permanente contacto y comunicación en este sentido.

Cómo no, la colaboración con las empresas prestadoras de servicios, especialmente de redes sociales: también ha sido objeto de una de las preguntas. Creo que puedo contestarles con ello también a una parte, y otra parte seguramente se lo va a contestar en su discurso Carolina. Nuestra función primordial es la de investigación, el contacto con los operadores y con las empresas prestadoras de servicios de redes sociales. Nuestro caso es orientado a recabar la información, los datos sobre el momento en que se ha producido el hecho, el delito. Creo que la situación el director la ha perfilado perfectamente: es verdad que es difícil porque muchas de estas empresas (menos alguna que está en España, lógicamente), están todas situadas en países extranjeros, en los que no se percibe de idéntica forma esa situación en la que los datos, dependiendo de cuál sea el delito, la consideración que tiene ese delito, o la interpretación y las costumbres de ese país que puedan hacerse de ese delito puedan facilitar en mayor o menor medida la informacion y los datos. Esto realmente supone un problema importante para nosotros en la investigación, sobre todo en algunos delitos vinculados a calumnias, injurias, sobre todo en personas mayores de edad.

Sin embargo, tengo que decir también que en el campo de la pornografía infantil, en el de la protección del menor suelen ser bastante sensibles, suelen participar mucho, e incluso nos suelen proporcionar esa información con mucha más facilidad, con mucha más asiduidad, incluso sin recabar el correspondiente mandamiento judicial, porque parece que es un delito universal en todos los países y se entiende muy bien esa problemática y todo el mundo colabora. Es una forma, yo creo que es la forma más fácil y en la que todo el mundo lucha más desinteresadamente en todo el ámbito internacional.

No quiero hablarles ya de lo que es el acoso sexual a los menores, el *grooming*, les ha mencionado también el director, también el *cyberbullying*, el acoso escolar a través de medios como el YouTube y demás. Seguramente también tiene que ver un poco lo que vayan a percibir cuando Carolina les haga la mención sobre redes sociales.

Lo que sí quiero trasladarles es la idea de la mayor utilización de los *smartphones* hoy en día. Es nuevo reto que se nos está planteando, es una nueva dimensión de lo que implica esto en el campo del crimen dentro de las tecnologías de la información y la comunicación, es un elemento de una difusión muy rápida, muy eficaz, exponencialmente de forma geométrica, y que el pequeño detalle que pueda suponer una difusión a un amigo, a un tercero de una determinada imagen puede representar un daño brutal a nivel de la víctima.

Un poco derivado por la fluidez y la agilidad de lo que puede suponer en la red, y que además, como se suele decir, todo lo que entra en Internet se queda en la red. Eso es un problema que está ahí y con el que tenemos que luchar.

El campo de las injurias y calumnias y amenazas tiene su problemática, y además importante. El gran crecimiento que ha experimentado tanto el uso de los *smartphones* como de las redes sociales, gracias a la expansión de las conexiones móviles, está propiciando un notable auge de los delitos contra las personas en lo referente a las calumnias e injurias, así como contra la intimidad. Todo ello queda reflejado en el aumento de las querellas y denuncias por estos delitos, ya sea contra particulares, personajes públicos, políticos, empresas, etc. Parece que existe esa anonimización, ese anonimato que genera el estar dentro de la red, las posibilidades de anonimizarse por parte del que produce esas injurias y esas calumnias hacen desinhibir muchos principios, incluso sociales o fomentarlos y sacarlos fuera a través de la red, con el problema o el perjuicio que ello ocasiona a todas esas personas.

Es un problema realmente importante, vinculado también precisamente con las empresas que prestan esos servicios: el que exista esa dicotomía a la hora de trasladar o de facilitar esos datos para poder intervenir en nuestro caso. Hay que tener en cuenta que este tipo de delitos son delitos semipúblicos en los que interviene mucho la consideración de la posible injuria; hay ocasiones en las que son muy evidentes, muy claras, auténticas barbaridades atroces; otras en las que puede estar rayando la

interpretación o el pequeño... la intuición, un trasfondo detrás de ese mensaje que puede generar psicológicamente esa duda, esa inseguridad, ese problema a esa persona.

Este tipo de delitos, realmente tiene escasa penalidad, seguramente porque tiene que ser así, no lo sé, pero eso también motiva el que en muchas ocasiones nuestra intervención a la hora de judicializar cualquier intervención de este tipo, la propia autoridad judicial define si considerarlo como delito o sobreseerlo porque no ve realmente que en ese mensaje pueda llegar a interpretarse de esa forma (sin embargo, para la víctima sí); o incluso que pueda derivarlo a un enjuiciamiento por faltas. Esto es, que procedimiento se debe seguir.

Pero nuestra intervención para llegar a conseguir esos datos implica que para poder llegar a determinar —si es que se puede llegar a determinar— la identidad de esa persona, tendríamos que recavarlo a través de esas empresas de servicios, seguramente de servidores extranjeros, y además mediante una comisión rogatoria internacional. Claro, esto, pensando en la consideración del delito, etc., llega muchas veces a dificultar tanto que realmente resulta más que dificultoso el éxito de la investigación. Es realmente un problema añadido y una cierta inseguridad en la víctima, eso sí es verdad.

No obstante, intentamos alertar a los usuarios en este sentido, de alguna forma para evitar esos enlaces, llegar a cerrar, o para evitar ese ciberacoso que puede haber, y hacemos un seguimiento para que en cualquier atisbo de que pueda desviarse o de que pueda incurrir en algún fallo esa persona, ese delincuente, poder identificarlo.

Algunas de estas empresas de servicios proporcionan algunos mecanismos a la hora de investigar dichos delitos. El poder identificar, como he dicho, a la persona que realiza los hechos teniendo como único dato un correo electrónico o solamente un *nick* o seudónimo, como ocurre en la red social Twitter, ya que en la mayoría de las ocasiones estas empresas tienen ubicado el domicilio social en el extranjero y estando sujetas a las disposiciones legales de esos terceros países no ofrecen ningún tipo de dato para la identificación de sus clientes.

Quiero incluir en ese otra área de la Unidad que inicialmente he mencionado, que está orientada a la investigación de los sistemas informáticos y la red por la importancia que tiene en los delitos vinculados con las estafas, los fraudes, etc. Porque aparentemente son una serie de delitos

de pequeña cuantía, pero que potencialmente generan un daño social importante por su expansión, por su atomización.

La estafa, en cualquiera de las manifestaciones, constituye la actividad más lucrativa y menos punitiva individualmente, y hacia la que se encamina el resto de las actividades cibernéticas en general. Por lo que los sistemas de ocultación o navegación anónima y suplantación de identidad, para no ser identificados los autores y los grupos delictivos, son cada vez más sofisticados y complejos de investigar.

Cuando hablábamos de que inicialmente, cuando se creaba la Brigada, hubo un pequeño grupo que se encargaba de investigar estas pequeñas estafas estábamos hablando de estafas que eran trasladar aquellos timos antiguos del tocomocho, etc., que se producían en el nivel físico, trasladarlos a un entorno de la red; hoy en día están alcanzando un grado mucho más complejo, mucho más elevado, de tal forma que eso es lo que ha dado lugar a que creemos un área de investigación más potente que es el de seguridad lógica.

Porque precisamente existe un campo de estas estafas que está vinculado a una serie de actividad delictiva con determinados grupos que realizan estafas a través de transferencias electrónicas fraudulentas, el denominado *phishing* bancario, que ha sido tradicionalmente conocido por todo el mundo, el *pharming*, etc., o a través de ventas y subastas ilícitas en Internet o ventas y subastas también fraudulentas de artículos que luego revenden, etc.

Digamos que todo este campo más tradicional de las estafas, de los fraudes está llegando a tener un componente todavía mayor a la hora de que, para llegar a estafar, lo que se hace es lanzar en la red, así sin más, un cartucho: ese cartucho va por la red como Pedro por su casa porque se lo permiten determinados ordenadores llamados zombis, de los que podemos tener uno en casa y no lo sabemos, y que nos lo están utilizando, a través de determinados servidores que anonimizan la autoría, la entrada y salida de quien lo está realizando.

Realmente son auténticos cartuchos explosivos que, llegados a un usuario final, le proporcionan el virus que va a originar cualquier tipo de actividad fraudulenta, ya sea cualquier tipo de estafa, ya sea recoger datos o información de nuestros propios ordenadores, utilizar nuestro propio ordenador como un *botnet* más para utilizar sus medidas, etc.

Estoy hablando a nivel particular, esto es, sin tener en cuenta que a nivel empresarial, es decir, a nivel de la pequeña y mediana empresa, que también tienen sus pequeños servidores domésticos a veces, pequeñas empresas de 8 o 10 personas con sus dos o tres ordenadores para gestionar su pequeña contabilidad, su pequeño negocio, etc., pues lógicamente ahí el daño todavía adquiere una dimensión mayor.

No digamos si esto se hace a nivel de las grandes empresas, incluso empresas nacionales o multinacionales, tanto españolas como extranjeras, en las que esto puede suponer una auténtica bomba en sus sistemas de seguridad lógica y repercutir gravemente en la seguridad de su información, a nivel de usuarios, de sus clientes, seguridad en sus sistemas, seguridad de espionaje en su propia red, y que luego van a vender a otra empresa de su competencia. Es decir, entramos en un mundo un poco mucho más complejo.

E incluso, dentro ya de ese grado más, el que todos consideramos en llamar de las infraestructuras críticas, con lo que representa y puede perjudicar a nivel nacional en cualquier Estado cualquier fallo de seguridad en estos sistemas.

Hasta el día de hoy teníamos esa tendencia a considerar las infraestructuras críticas, y orientar la seguridad de éstas en la seguridad privada, de esas grandes centrales nucleares, de esa subestación eléctrica, etc.; realmente el esfuerzo en seguridad privada que han hecho esas empresas es grande, pero es verdad que los problemas realmente y potencialmente más graves y que pueden perjudicar no solamente a los usuarios sino al funcionamiento de los sistemas, en la vida normal en un país pasan por estas grandes empresas, por eso son de infraestructuras críticas, y cualquier daño que se les pueda producir puede repercutir muy gravemente en la sociedad.

No voy a extenderme mucho en el tema de los fraudes, no quiero cansarles. La gente que estaba conmigo, todo el mundo quería aportar sus cosas, sus ideas, (todo el mundo quiere meter sus cosas); no quiero cansarles con todo ello.

Sí que es verdad que al hilo de lo que les estaba diciendo en el tema de este tipo de fraudes y de estafas, hay sector que es en el que estamos trabajando, en esas estafas de *phishing* que todavía siguen llegando, ahora mucho más sofisticadas. Antes el *phishing* llegaba porque te plantaban

una página web que te pedían tus datos de códigos y contraseñas de determinada entidad bancaria en la que de modo *online* estabas trabajando; hoy en día, todo esto se traslada al uso de la tecnología móvil, en la que además de esas medidas de seguridad las entidades bancarias te permiten que si quieres hacer cualquier operación, o transferencia te van a enviar un mensaje a tu teléfono móvil para darte un código que puedes introducir, y así garantizar que tienes esa seguridad en la trasferencia; pues esto también ya lo han conseguido. Es decir, el que estén utilizando a su vez no solamente esa contraseña, perciben cuál es tu teléfono, te mandan un mensaje a tu teléfono y te indican que el banco con el que estás operando, supuestamente, te va a dar este archivo para que de forma encriptada puedas hacer estos mensajes con total garantía y con total seguridad.

Ese es justo el momento en el que se ejecuta un pequeño virus que te están mandando a tu teléfono móvil, fundamentalmente a los *smartphones*, seguramente porque es el tipo de telefonía más extendido en la mayor parte de la población hoy en día, sin descontar cualquier otro tipo; y a partir de ahí conocen tus datos, tus claves, tienen secuestrado tu teléfono, de tal forma que entran, ven tus cuentas, tus líneas, y si tienen que hacer cualquier transferencia lo van a estar derivando a través de ese teléfono móvil que ellos van a encontrar para hacer la transferencia, la operación, sin que tú te des cuenta. Esto es así.

Es verdad que operan con mucha rapidez, tienen mucha agilidad. Además, cuando lo hacen, lógicamente lo hacen mediante unas líneas de telefonía móvil, de mensajería, que acuden a unos servidores —nosotros tenemos detectado uno ahí en el norte de Europa— en los que a su vez redirige esos sistemas de mensajería, con lo cual resulta poco menos que difícil o imposible. Entramos ya en la dinámica de tener que acudir al exterior para poder lograr identificar a esa posible persona. Con la dificultad también añadida de que puede estar en un correo electrónico, en fin, no quiero...

Esta es una de las últimas, no sé si novedades o tendencias, en la que por supuesto tenemos una investigación pendiente que nos está llevando tiempo pero que está trasladando una parte importante de nuestra actividad. Y precisamente es una de las líneas que tenemos que empezar a orientar con más potencialidad y en la que necesitamos más ayudas, que tenemos que ir buscando, y formación que tendremos que ir proporcionando. Y es en el uso de la telefonía móvil, como elemento, ya digo, de

integración del acceso a la red de cualquier persona. Es uno de los problemas realmente importantes.

Bien, en el campo de las ventas y subastas fraudulentas, esto ya es un poco, si se quiere, más doméstico. Mediante correos *spams* te recibes un correo en el que te... o a través de alguna página web en la que se vende cualquier artículo, aquí hablamos de los estafadores de temporada; es decir, cuando la mayoría de la gente tiene que buscar un apartamento para ir a la playa en verano, pues se produce un movimiento de búsqueda de ese tipo de páginas en las que queremos buscar un apartamento en determinadas zonas para alquilar. Ese es el momento idóneo para poner ese tipo de anuncios de alquiler de apartamentos falso. Cuando pasa el verano, pues de apartamentos para los estudiantes para la universidad, cuando llegan las Navidades, de artículos de electrodomésticos, de bicicletas, de ordenadores, etc. Esta es un poco la secuencia.

No voy a extenderme mucho más, porque sí quería indicarles la tendencia o la orientación que vamos teniendo en el área de seguridad lógica, y en la que seguramente las investigaciones son más difíciles, son más costosas de tiempo y de esfuerzo, en la que tenemos gente preparada y muy espabilada, en la que tenemos una gran fuente y una gran conexión y apoyo con las policías internacionales porque si no, de otra forma tampoco sería posible, que es en el tema de seguridad lógica.

Ha mencionado el director algunas de las operaciones en las que hemos intervenido: una de ellas, la detención en Navidades precisamente de la persona responsable de lo que es la organización criminal más importante que estaba originando uno de los mayores problemas de seguridad y de estafa en la red, que es la operación «Ransomware»; una persona, un ruso que desde Rusia estaba lanzando una serie de mensajes mediante página web que en cada país se determinaba un anuncio en que conminaba al usuario en particular a pagar una multa por haber entrado, supuestamente, en algunas páginas de contenido no deseado, ya sea de pornografía infantil, de juego *online*, etc., y por las que debíamos pagar una multa.

Esto es falso, hemos dado recomendaciones sobre esto permanentemente, e incluso a través de Inteco se realizó un pequeño software para que todos los usuarios acudieran y desinfectaran su ordenador de este virus. Pero esta gente aprende. Y estos virus los reciclan, los cambian. Esto le llegó a pasar hasta a mi hijo, que me dice «me ha pasado el virus

este, pero es que además estoy saliendo en una ventanita por la pantalla». O sea, llega un momento en que no solamente te introducen el virus en el ordenador, sino que acceden a tu cámara web y desde ahí la activan y te encuentras con la sorpresa de que te estás viendo incluso allí mismo. Esto a cualquier usuario, no solo le sorprende, sino que le invade de inseguridad.

Esta línea es la que nos ha obligado a trabajar en que no solamente tenemos que trabajar en verificar quiénes son los que estaban introduciendo los códigos para introducir este virus a nivel internacional; hemos tratado con cerca de diez o doce países en el ámbito europeo a través de grupos de trabajo de Europol, en los que además se les ha participado cómo se trabajaba y en los que ellos también están trabajando cada uno en sus países.

Potencialmente el que más daños —creemos, o porque lo ha contabilizado así— ha sido Alemania, pero también una parte importante en Estados Unidos, en la que a través del FBI se les ha proporcionado una parte importante de lo que es la organización, que la están explotando a su manera, de otra forma, están sacando mucho más partido seguramente por la idiosincrasia, las formas procedimentales y judiciales que existen allí, etc.

La investigación no solamente era buscar, localizar e identificar a estas personas, sino además qué es lo que pasaba con ese daño patrimonial que se estaba causando a los usuarios. Es decir, por un lado existía la rama técnica, que era esta; por otro lado la rama patrimonial.

Es decir, una vez que se producía el daño y la persona pagaba, mediante unos medios de pago en *Ukash*, o *paysavecard*, que simplemente se pueden adquirir en una gasolinera, (pagas 100 euros y es un cheque al portador), metes esos códigos en Internet y ya has pagado.

Tenían sus propios paneles de pago e inmediatamente detectaban que ya habías pagado y te liberaban el ordenador: tal cual.

Ahora viene la segunda parte, cómo recoger el fruto del delito. Y ahí entraba toda esa secuencia de forma de blanqueo en el que actúan en cada uno de los países. En todos los países tenían alguna de las células que se dedicaban a blanquear, mediante diferentes sistemas, bien a través de mulas, lo pasaban en efectivo, lo metían a través de locutorios, lo reenviaban a través de Western Union o Money Gram: un auténtico labe-

rinto de ingeniería que nos ha supuesto mucho esfuerzo verificar, hasta llegar, por supuesto, que el dinero llegase a Rusia en este caso.

Por eso el trabajo que estamos dedicándole a la estafa se nos está identificando con toda esta problemática de estos sistemas.

Quiero decir que la colaboración internacional es tan grande en este sentido, que incluso estamos participando, como ha señalado también el director recientemente, en grandes operaciones. En Semana Santa se produjo uno de los mayores ataques de denegación de servicio, DDoS, en la red a través de Internet, a través de grandes empresas, una alemana, una holandesa y demás, que realmente no bloquearon la red a nivel internacional pero sí la saturaron de tal forma que hubo bastantes problemas, sobre todo en Estados Unidos, Inglaterra, Alemania y Holanda, incluso Suiza.

En esos dos o tres días, la comunicación, el contacto, el conocimiento entre profesionales de policía de diferentes países nos llevó a que se pusieron en contacto entre ellos. Nos comentaron cuál era la situación, nuestro equipo vio a través de un dato que le dieron (no sé si era una IP y demás), y consiguieron determinar dónde se encontraba el objetivo, conseguimos ver quién era, Lo hemos seguido durante quince o veinte días esperando a que llegara la comisión rogatoria internacional que Holanda hizo, y por medio de la cual, a través de los canales de Europol y de Eurojust y la Fiscalía, en este caso de Barcelona, se llevó a efecto la entrada y registro en el domicilio de esta persona y la intervención de los equipos, con la colaboración de dos policías holandeses que acudieron precisamente aquí para echarnos una mano.

Quiero significar esto, ¿por qué? Porque aquí en España no existía el delito, no teníamos ningún delito sobre este caso, pero teníamos al delincuente. Y en este caso, si no hubiese sido por la actuación nuestra, difícilmente podría haberse llegado a determinar quién era. Quizás en España no ha tenido esa repercusión o esa importancia, pero para esos otros países de la Unión Europea la tuvo, y mucho, por el problema tan importante que generó en la red.

Es un poco el sistema... no sé si es desinteresado, o no es desinteresado; al final Holanda, Alemania y el resto de países y de policías integrantes del contexto de Europol, no solo nos los han agradecido, sino que efectivamente es una forma de confianza de intervenir en muchas más

operaciones y en las que seguro que nos hemos ganado su confianza y su participación en otras.

No quiero seguir algunas de las operaciones que se hicieron ya un poco anteriores, sobre Anonymous, operación «Latina», operación «Escondido», en fin, no voy a comentar más.

Intervenimos también, por supuesto, en delitos contra la propiedad intelectual e industrial, dentro de las particularidades que tiene, en medicamentos y anabolizantes, en fin.

Esto sí quiero comentarlo al menos brevemente: hay un grupo de actividad que estamos intentando potenciar y es el de redes abiertas. No solamente nos dedicamos a recibir la denuncia o el delito, sino que exploramos en la red para conocer no solamente los delitos que se están produciendo sino determinados comportamientos que socialmente pueden llegar a ser constitutivos de delito. Hablo de cuestiones, por ejemplo, hace año y medio o dos años se tuvo una intervención en la que se producían carreras ilegales de vehículos en Palma de Mallorca con importantes problemas no solamente de seguridad del tráfico, sino también para las personas, y se consiguió localizar e identificar precisamente a través de Internet.

Cuestiones de identificar ventas de tráficos de armas, anabolizantes, medicamentos falsos, en fin, cuestiones de racismo, xenofobia... Se van tocando determinados problemas sensibles y determinados comportamientos que pueden alterar la vida social.

Y por último, y ya no les canso más, tengo que mencionarle que todo esto no se puede llevar a cabo sin un buen equipo de un área técnica de laboratorio: es imprescindible. A esta gente que tenemos allí yo la llamo «la gente de cacharreo»: son los que se encargan de recoger toda la información de los discos duros, los clonados, etc., y hacerlo con las mejores garantías para ponerlo a disposición de la autoridad judicial, y eso implica una labor muy importante de «cacharrear» en esos discos duros, en esos ordenadores, en esos móviles, recoger toda esa información.

Además son los que están más al tanto de cualquier innovación y por eso les tenemos encargado también que participen como profesores en la formación del resto de la gente, en cualquier novedad que aparece, para que de forma integral lo conozca toda la Brigada o toda la Unidad. Y participan tanto en el extranjero como a nivel nacional en cualquier ámbito.

No quiero seguir más. Hay seguramente alguna pregunta de la que han hecho ustedes anteriormente que puede que se haya quedado sin contestar. Si me la repiten, dentro de lo que pueda se la contesto.

Precisamente he visto la primera de ellas, sobre el tema del juego *online*: Precisamente es uno de los temas que estamos explorando en este último grupo que hemos visto de redes abiertas, y realmente resulta inquietante. ¿Por qué? Porque en esta secuencia que les he manifestado antes del desarrollo de la operación «Ransomware», esa parte de organización patrimonial estaba derivando la importante carga de actividad de blanqueo de dinero a través de diferentes medios, como he dicho antes, y no solamente a través de eso sino a través de juegos *online*. ¿Cómo? Pues lógicamente, a través de dinero virtual que introducen... De todo esto, lo van pasando y van perdiendo pequeños tantos por ciento de comisión, pero esto es algo que tienen de forma estudiada y preparada; saben que de aquí a aquí les va a suponer un 3%, pasa a un 4%, después cogen una «mula» para que lo pase a efectivo, lo meta en otro sitio, de ahí lo pasan... En fin, y ese recorrido lo pueden ir complicando cada vez más para tener cada vez más medidas de seguridad, o según el grado de confianza que tengan en ese grupo en que, como ha dicho el director, tiene externalizado ese servicio la criminalidad. Es verdad que es un tema preocupante el juego *online* y estamos trabajando, estamos explorándolo.

La percepción que tenemos es que a día de hoy estamos viendo todo desde el punto de vista a nivel físico y no sabemos trasladarnos a ese punto de vista virtual en el que los conceptos son distintos y las formas de trabajar son distintas. E intuimos que no solamente la actividad delictiva o el resultado del delito se blanquea por este medio, sino que otras formas de blanqueo de dinero puedan estar pasando por ahí y no lo sabemos.

COMPARECENCIA DE LA INSPECTORA JEFA DE SECCIÓN DE PRENSA Y REDES SOCIALES DE LA OFICINA DE PRENSA Y RELACIONES INFORMATIVAS DE LA DIRECCIÓN GENERAL DE LA POLICÍA, DÑA. CAROLINA GONZÁLEZ GARCÍA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 16 DE MAYO DE 2013.

La señora **INSPECTORA JEFA DE SECCIÓN DE PRENSA Y REDES SOCIALES DE LA OFICINA DE PRENSA Y RELACIONES INFORMATIVAS DE LA DIRECCIÓN GENERAL DE LA POLICÍA** (Dña. Carolina González García): El grupo de Redes Sociales está enmarcado dentro de lo que es la Oficina de Prensa y Relaciones Informativas de la Policía Nacional y gestiona los distintos perfiles de la Policía Nacional en Twitter, Facebook, Youtube y Tuenti.

Voy a informarles del trabajo que realizamos dentro de la Oficina de prensa, principalmente para concienciar a los ciudadanos de los riesgos que puede conllevar el uso de las redes sociales, y las campañas de prevención que hacemos dentro de nuestros perfiles. Como les he comentado, esta gestión se realiza dentro de la oficina de prensa. Nosotros, además, llevamos a cabo toda la labor de comunicación, planificación, preparación y coordinación de las comunicaciones y las relaciones de la Policía Nacional con los medios de comunicación social.

La Oficina de prensa mantiene además un contacto directo y permanente con los agentes especializados de la Brigada de Investigación Tecnológica, para intercambiar informaciones de interés que nosotros conozcamos gracias a nuestra actividad en estas Redes.

Les adelanto en mi presentación algunos datos de nuestro trabajo en 2012, como el número de tuits que hemos difundido, vídeos que damos con consejos en YouTube o requerimientos que tenemos de los medios de comunicación, muchos de ellos para hablar sobre este papel que tenemos importante en las redes sociales.

Pero para comenzar voy a hacerles un repaso de cuáles son las redes en las que estamos presentes y mantenemos actividad, ya que realmente ésas son en las que ahora mismo estamos, pero tenemos de cara al futuro inmediato, y a la espera de su evolución, perfiles creados en nuevas

plataformas en las que de momento no tenemos actividad, pero dada la rápida evolución de las redes sociales posible que es breve estemos ya con acciones de comunicación en otras plataformas.

Hace unos cinco años que la oficina de prensa de la Policía Nacional decidió dar un salto adelante, innovar en las estrategias de comunicación que teníamos y adentrarnos en lo que son las tecnologías de la información y las redes sociales como una herramienta más de lo que era el gabinete de prensa. Queríamos ofrecer confianza, credibilidad, más transparencia de la actuación de la Policía. Esa era nuestra primera intención.

Comenzamos a trabajar con la puesta en marcha de un canal de YouTube, youtube.com/policia; comenzamos en 2006, pero cuando se hizo visible al público fue en 2010. En él incluimos vídeos de operaciones policiales, pero también campañas específicas contra la violencia de género, consejos para una navegación segura en Internet, consejos para los mayores. Tenemos actualmente unos 145 vídeos subidos con más de 3.400.000 visionados. Esto nos sitúa en la primera institución pública en número de visionados y de impacto.

En marzo de 2009 iniciábamos también nuestra andadura en Twitter, la red social de *microblogging*. Éramos la primera institución pública en tener un perfil. Ser los primeros nos hizo trabajar con cierto desconocimiento de la utilidad real, pero nos hemos convertido en la primera institución pública en número de seguidores, sobrepasamos los 500.000; y somos el segundo cuerpo policial del mundo, tan solo detrás de FBI. Nosotros pusimos esta cuenta de @policia con la intención de que fuera una herramienta más de la oficina de prensa para difundir nuestras informaciones sobre operaciones policiales, sobre despliegues o unidades especializadas. Y ,de hecho, durante el primer año el 80% de nuestros seguidores eran medios de comunicación, periodistas, *bloggers* o personas vinculadas con los *mass media*. Pero nos dimos cuenta de las posibilidades que nos estaba ofreciendo esta red social y comenzamos a ampliar mucho más nuestra actividad.

Sólo para que se hagan una idea, nuestra evolución en Twitter es la siguiente: en 2010 teníamos 3.000 seguidores; en 2012, 217.000; y en 2013 ya estamos actualmente sobrepasando los 460.000 seguidores. Cuando llegamos a los 10.000 seguidores nos dimos cuenta de que nuestros mensajes no sólo iban dirigidos al que era nuestro interlocutor habi-

tual, es decir, periodistas, sino que detrás de @policia había ya un público mucho mayor, mucho más heterogéneo.

Entonces comenzamos a dar un giro a nuestro contenido y comenzamos a ofrecer consejos dirigidos a todos los ciudadanos, a los menores, a los más mayores y al público en general, sobre todo sobre el uso de las nuevas tecnologías; sobre los nuevos *gadgets,* como tabletas o *smartphones*; sobre los timos, estafas, fraudes que nos encontramos en la red; cómo actuar en caso de *grooming*, de *cyberbullying*, de *sexting*, de amenazas, de calumnias. También les informamos de qué es delito en la red, porque a lo mejor en muchas ocasiones estamos aconsejando para evitar ser víctima del *grooming*, del *cyberbullying*, pero en ocasiones también hay que asesorar a los menores para que no se conviertan en autores de delitos.

Hemos ampliado mucho más nuestro campo de actuación. Somos un referente a nivel internacional en materia de comunicación y de seguridad en esta red. De hecho, Twitter se ha convertido en una herramienta de comunicación con el ciudadano y en una pieza clave en la retroalimentación y la colaboración ciudadana.

Desde otro de los perfiles que tenemos abiertos desde el curso 2010-2011 del Cuerpo Nacional de la Policía, junto con la Guardia Civil, es el canal de Tuenti «Contigo». Esta red social, —que está dirigida a los jóvenes de 14 a 18 años, aunque actualmente podemos encontrar que hay menores de 11 o 12 años que están utilizando esta red—, se ha convertido en la favorita de los adolescentes, incluso por encima de Facebook. Gracias a www.tuenti.com/contigo hemos logrado acercar aún más el Plan director para la convivencia y mejora de la seguridad escolar, como han comentado tanto el director como el comisario. Este es un plan que tenemos activo por parte del Ministerio de Interior, y que ofrece a los jóvenes y a los adolescentes todo tipo de consejos e informaciones en las aulas, en el colegio. Nosotros lo que estamos haciendo es trasladarlo también a las redes sociales, informar de eso mismo que se lleva a los colegios desde la redes, y ofertándoles la posibilidad de que se pongan en contacto con los compañeros de Participación Ciudadana para acudan a sus colegios a ofrecerles charlas sobre todo tipo de cuestiones.

Más de 75.000 adolescentes se han unido a este canal en Tuenti, que está especialmente pensado para ellos y en el que además pueden informarse del acoso escolar, de las drogas, del alcohol, de las bandas juve-

niles, de los riesgos de Internet o incluso de la violencia de género, que también empieza a ser un problema entre estos adolescentes.

El plan «Contigo», que es como se denomina nuestro canal en Tuenti, ofrece también una dirección de correo para contactar con los agentes y resolver cualquier tipo de duda. Hemos atendido ya más de 4.000 dudas y preguntas planteadas tanto por los jóvenes a través de este canal como por sus padres, y en algunas ocasiones también profesores. ¿Qué es lo que hacemos nosotros desde este perfil? Pues contestar estas dudas, remitirles, si es conveniente, a las unidades especializadas o a una comisaría para que formalicen la denuncia, o ponerles en contacto con esos agentes de participación ciudadana.

Estamos ofreciendo consejos desde Tuenti para preservar la intimidad en la red, para navegar de forma segura. Hemos alertado del peligro de grabar imágenes de contenido sexual, y lo que conlleva su difusión; consejos para disfrutar de fiestas seguras (en Nochevieja, en carnaval, en fin de curso), los límites de una novatada al comienzo del año escolar. También les informamos sobre fraudes o timos, o hacemos test autoevaluadores, que están tan de moda, como «¿navegas seguro en la red?». De lo que se trata es de ofrecerles información útil sobre problemas y riesgos que les afectan más a ellos, a los adolescentes, y de motivarlos para adoptar esas conductas seguras. Les felicitamos una información que les sea útil para el uso de Internet y para uso también de la telefonía móvil o del ocio digital, que también es un área de riesgo.

Es decir, el tanto por ciento de jóvenes y menores que navegan por Internet y que usan las redes es muy elevado. Es decir, el número de adolescentes expuesto a esos riesgos es también muy elevado. Pero si educamos a los menores y los orientamos en esas pautas saludables en la red, conseguiremos que no lleguen a ser víctimas o autores del ciberdelito. Es decir, criminalizar a la red: no es malo que los menores utilicen Internet; de hecho en cierto modo España se sitúa entre uno de los primeros países en utilizar las redes sociales, en utilizar Internet. Todos los jóvenes conocen Facebook; un elevado tanto por ciento utiliza también otras redes sociales como Twitter o como Tuenti, y eso en cierto modo es positivo. Todo ello nos empuja a fomentar una formación constante y periódica por parte de distintos agentes implicados, entre ellos la Policía, como una asignatura más. Actualmente la Policía está en las aulas a petición de los padres o si los profesores nos lo solicitan, estamos a

requerimiento de ellos. A lo mejor, si ellos no detectan esa problemática o esa necesidad, estamos «perdiendo» la posibilidad de que unos agentes expliquen no sólo a los alumnos, sino también a los profesores y a los padres, —que a veces lo necesitan más que los propios alumnos—, de las pautas que tienen que seguir para que no ser víctima ni autor de determinados delitos.

La Policía Nacional también está en Facebook. Todos los jóvenes, como les he dicho, conocen Facebook; el 85% lo usa; el 34% lo califica como su red favorita, incluso por detrás de Tuenti. Es una red a la que dedican —el director y el comisario han dado muchas cifras— casi seis horas a la semana, y actualmente nosotros tenemos en Facebook 47.000 «amigos» que nos siguen y que conectan, interconectan, difunden nuestros mensajes a través de sus amigos.

Desde la oficina de prensa comenzamos a poner en marcha todos estos perfiles y nuestro primer objetivo, como les he dicho, era utilizarlo como una herramienta más de comunicación. Pero su desarrollo, nuestro importante poder de viralidad y de penetración nos ha conducido a convertirlo en un canal de comunicación con el ciudadano para estar más cerca de él y al servicio también en las redes sociales. En cierto modo, nuestros canales en las redes sociales se han convertido en una oficina de atención al ciudadano, en un punto de información al público abierto casi las 24 horas. En el gabinete de prensa trabajamos alrededor de 15 personas; concretamente en redes sociales estamos 7 u 8 personas que nutren de información y contestan a las preguntas o a la dudas que se nos plantean casi las 24 horas, desde primera hora de la mañana hasta la una o las dos de la madrugada.

Tengo que recordar que aunque nuestros perfiles se hayan convertido en un canal de comunicación con el ciudadano, al menos de momento no son un medio para efectuar una denuncia. Nosotros atendemos, recogemos, pero finalmente la denuncia oficial tiene que ser tramitada en una dependencia policial o judicial. Nosotros alertamos a los investigadores de determinados hechos que sean constitutivos de delitos y que sean perseguibles de oficio, pero a veces es necesaria una denuncia, y la víctima debe acudir a formalizarla en una dependencia policial o judicial.

Como ha mencionado el comisario, seguramente hoy informaremos de uno de esos casos en el que gracias a esa presencia nuestra constante en las redes sociales, @policia detecta un vídeo —en este caso es la se-

gunda ocasión que nos sucede con un corto margen de tiempo—, que se está convirtiendo en *trending topic*, en tendencia en las redes sociales, que se está compartiendo, que es constitutivo de delito. Rápidamente nos ponemos en contacto, —sea la hora que sea, en alguna de las ocasiones ya de madrugada—, con agentes especializados de la BIT para alertarles de que hay un vídeo con menores, con pornografía, con abusos a menores que se está difundiendo. Inmediatamente los agentes de la BIT, a las dos de la madrugada, se ponen manos a la obra, conectan con las compañías y despliegan los programas informáticos para, en menos de 24 horas, proceder a realizar los primeros interrogatorios y detenciones.

Las cifras confirman la importancia de nuestra presencia en las redes, y hechos como este que les comento nos impulsan a seguir en esta línea.

Los datos: más de 500.000 seguidores en Twitter, primera institución en España, la segunda fuerza en el mundo; YouTube, más de 3 millones de reproducciones; Tuenti, 70.000 jóvenes adolescentes que están siguiéndonos, o Facebook como ventana abierta, no ya a los adolescentes, sino a todo el público en general.

La importancia de nuestro trabajo en las redes sociales se refleja también en el interés mostrado por otras instituciones, como también ha mencionado el director. Es frecuente que otros cuerpos de seguridad o responsables de la Unión Europea nos visiten para informarse de nuestra actuación en las redes sociales e intentar plasmar en sus policías, en sus instituciones, el mismo modelo que estamos desarrollando nosotros.

Este desarrollo de una «Policía 3.0» se encuentra dentro de los objetivos estratégicos de la Dirección General de la Policía. Y para la oficina de prensa, ese liderazgo en las redes nos permite mejorar de forma directa la comunicación con los usuarios, aumentar la confianza de ellos en Internet y también en la labor de su Policía, y que estamos intentando ofrecer un servicio público eficaz.

Así pues, la colaboración ciudadana es una pieza clave para cualquier cuerpo de seguridad. Aunque la Policía investigue y tenga sus propias herramientas de investigación contra el delito, las informaciones de los ciudadanos nos son muy útiles para luchar contra la pornografía infantil, contra el maltrato, contra los abusos, contra el acoso, para luchar contra el narcotráfico o para hacer frente al terrorismo, como de hecho se ha puesto recientemente de manifiesto en los atentados de Boston.

La Dirección General de la Policía está impulsando el desarrollo de la cercanía con el ciudadano y la colaboración de estos en la seguridad de todos. La Policía hace una profunda labor de prevención y de investigación para evitar y, en su caso, perseguir los delitos. Pero los datos que nos pueden aportar los ciudadanos en estos casos concretos son esenciales para aflorar determinadas conductas punibles. Algunos de estos vídeos que les he mencionado, incluso los fraudes o los timos que hay en la red, nos llegan muchas veces por los propios internautas, que nos hacen pantallazos de esos timos. En el caso de los vídeos, siempre incidimos en que no hay que compartir, no tienen que poner el *link* del vídeo porque eso ya es constitutivo de delito, pero son ellos los que nos informan muchas veces de hechos que pueden ser constitutivos de delito para que lo investiguemos.

Desde las redes sociales hemos desarrollado muchas campañas y acciones de comunicación sobre temas concretos. Voy a centrarme en algunos de ellos, como por ejemplo la Twettredada contra el tráfico de estupefacientes. Desde nuestros perfiles en las redes sociales hemos solicitado a los internautas que se pongan en contacto con nosotros siempre que conozcan la venta de droga, traficantes o puntos negros en sus barrios. Tenemos una dirección de correo que es antidroga@policia.es, en la que de forma anónima y confidencial se pueden remitir datos que son posteriormente enviados a la Brigada Central de Estupefacientes. Hemos recibido más de 11.000 correos, una media de 600 al mes, dentro de esta acción de la lucha contra el tráfico de estupefacientes.

Y estas informaciones nos han posibilitado desmantelar muchos pequeños puntos negros, pero también hay grandes investigaciones en curso. La primera operación culminada gracias a los datos que hemos recibido en la twettredada nos permitió localizar 277 kilos de cocaína que estaban ocultos en un camión entre pieles de bovino y fue gracias a uno de esos correos que nos llegó de colaboración ciudadana.

También difundimos en las redes sociales otro correo para luchar contra esta lacra que es la pornografía infantil. Solicitamos a los ciudadanos que nos alerten de cualquier imagen o vídeo de contenido sexual que pueda contener imágenes de menores; el correo es denuncias.pornografia.infantil@policia.es. Además avisamos, como les he comentado, que compartir este tipo de enlaces es también delictivo y que en ningún momento reenvíen los *links*. Otro ejemplo es el de un lamentable vídeo

grabado por cuatro jóvenes en una playa realizando actos de contenido sexual. Esas imágenes fueron subidas posteriormente a la red, un vídeo en el que menores estaban realizando acciones de carácter sexual. Rápidamente los investigadores identificaron a los autores, se efectuaron las primeras detenciones, y aunque ya lo habíamos avisado en varias ocasiones, de nuevo recordábamos que en el Código Penal se califica como delictiva no solo la distribución sino la tenencia. Varias personas fueron detenidas posteriormente por compartir los *links* que daban acceso a este vídeo.

A través de las redes sociales, y gracias a esa retroalimentación existente con el ciudadano, nos llegan muchas versiones de nuevos timos, de estafas, de falsos premios de lotería, de supuestas novias que desean venir a España, de multas que se hacen usurpando nuestra identidad, como el «virus de la policía»; y nuestro objetivo desde la redes sociales es alertar a todos de estos fraudes y de las estafas en Internet aportando imágenes y ejemplos para evitar que sean víctimas de esos delitos.

En cuanto a los jóvenes y adolescentes nos encontramos lo que se denominan nativos digitales que hacen un constante uso de Internet, beneficiándose, como les he dicho, de sus innumerables ventajas, pero a los que hay que guiarles también para usar con prudencia y con conocimiento las redes sociales, los *smartphones*, las tabletas, cualquier dispositivo que a fin de cuentas se pueda convertir en una ventana a su privacidad, a la privacidad de ellos y a la privacidad, en muchas ocasiones, también de la familia. Nuestra misión es enseñar y guiar también a los padres y a los profesores y ofrecerles aspectos educativos y preventivos para que ni sus hijos ni ellos, los padres, sean víctimas de delitos vinculados a las nuevas tecnologías, como el *cyberbullying*, como el *grooming*, como el *sexting* o como las estafas, incluso en compras *online*.

Según un estudio de la Unión Europea, el 92% de los jóvenes son miembros de al menos una red social; casi el 40% pasa al menos dos horas al día de un día normal de colegio delante del ordenador utilizando las redes sociales; y las chicas son las que suelen utilizar más estas plataformas, más que los chicos.

Para intentar prevenir todo esto, que sean víctimas y que sean autores de delitos vinculados a Internet, desde la Policía, desde @policia y desde todos los canales y plataformas que tenemos, hemos puesto en marcha campañas sobre el uso seguro de *smartphones*, sobre cómo navegar o

proteger una tableta u otros dispositivos, como *smartphones*; pero quizá los que han contado mayor viralidad y los que han llegado a un mayor público, sobre todo al joven, han sido campañas que hemos desarrollado sobre cómo proteger la intimidad o cómo navegar seguro, con jugadores de la selección española y con cantantes españoles como Chenoa, Alejandro Sanz, Marta Sánchez, con Bisbal, que nos han ofrecido sus consejos para navegar seguros. He de decirle que la puesta en marcha de todo esto, desde los canales hasta las campañas que hacemos con la selección y con Chenoa, con Alejandro Sanz, con Marta Sánchez, es con un presupuesto cero. La Policía Nacional cuenta con la voluntariedad y el esfuerzo de todos los agentes que trabajamos en su Oficina de Prensa y que nos creemos en que estamos haciendo, y la colaboración de personajes públicos que desinteresadamente colabora con nosotros. A pesar de ese presupuesto cero nos hemos convertido en líderes en las redes sociales, y creemos que estamos haciendo una eficiente labor de concienciación.

De cara a los menores y a los jóvenes y adolescentes, la Dirección General de la Policía desarrolla lo que les he mencionado, el Plan director para la convivencia y la mejora de la seguridad escolar; y la oficina de prensa aprovecha esta ventanilla de atención al ciudadano, —las redes sociales—, para trasladar el contenido de este plan. Durante este curso que está a punto de finalizar, habremos estado presentes en más de 5.000 colegios de toda España. Aún no tenemos los datos concretos. El objetivo es garantizar la seguridad en los centros educativos, en su entorno, erradicar cualquier conducta violenta y fortalecer la cooperación policial con la comunidad escolar. Eso es lo que hacemos de forma física en los colegios. Nosotros nos lo llevamos al plano virtual, y desde las redes sociales ofrecemos unas direcciones de correo para que nos soliciten nuestra presencia en los centros para hablar desde el acoso al consumo de drogas o el alcohol, que es otro de los temas que quizá más les interesa, la presencia de bandas juveniles o conductas incívicas y vandálicas en las aulas, para evitar situaciones de racismo o de xenofobia, o consejos para el uso seguro de Internet y las nuevas tecnologías, que es uno de los que actualmente más nos demandan. Nosotros, cuando nos ponemos en contacto con los colegios, son ellos los que nos piden hablar de un tema o de otro, y últimamente lo que más prima es hablar de redes sociales y de la seguridad en Internet. El año pasado estuvimos en 4.900 colegios, casi 5.000 colegios de toda España; ofrecimos 8.500 charlas a alumnos sobre Internet, como les he dicho, que son las más demandadas; ofreci-

mos 3.700 a personal docente; y más de 700 con las AMPA, con las asociaciones de madres y padres de alumnos de estos colegios. Una labor de educación y de concienciación sobre seguridad realizada desde el mundo real, en las aulas, y también desde el virtual.

Desde la oficina de prensa trasladamos estos contenidos a nuestras plataformas siendo conscientes de cuál es el público que tenemos en cada momento y cuáles son las franjas del día más apropiadas para difundir una información u otra. Generalmente a primera hora de la mañana nuestros tuits son de carácter informativo, se hacen eco de la nota de prensa que en ese momento estamos dando, pero es por la tarde-noche cuando nuestros tuiteros son mucho más informales y cuando se está buscando otro tipo de información. Ahí nuestro lenguaje cambia, nuestro lenguaje se adapta al público y a la franja horaria, y abordamos el acoso escolar, las drogas, el alcohol, las bandas juveniles, la violencia de género, la pornografía infantil, pero en un tono más cercano, más con los giros que ellos suelen dar, aunque detrás de todo ello se esconde una moraleja.

También de forma periódica tuiteamos pautas para concienciar a los jóvenes de las conductas que deben tener tanto en su vida real como en la vida virtual. Son tuits que tienen un amplio retuit, generalmente en pocos minutos se viralizan. Decimos «no al acoso», en clase, por Internet; no humillar, no jugar con tu intimidad; para estar «on fire» no es necesario acosar en clase. Esos son los giros de palabras que utilizamos para intentar hablar como ellos, para llegar a ellos.

A través de Internet, de las redes sociales recibidos diariamente centenares de menciones o de peticiones que son siempre atendidas desde la oficina de prensa y derivadas, en su caso, a la unidad correspondiente. Estamos en torno a unas mil menciones al día. Eso quiere decir que nos citan; en algunos de ellos, evidentemente, nos alaban o nos agradecen nuestro trabajo; y en muchas ocasiones todo lo contrario, es un medio para focalizar esa rebeldía juvenil contra el sistema y contra la Policía. Una broma que suele haber generalmente es que la Policía no sigue a nadie, no seguimos a nadie, pero a todos los que nos mandan algún mensaje solicitándonos cualquier tipo de ayuda o duda o cuestión, a todos los contestamos por mensajes directos y los derivamos, en su caso, a la unidad que sea necesario.

Al otro lado de nuestros perfiles, por último, quería recordarles, como he dicho al principio, tenemos un equipo de agentes que está preparado

para atender estas dudas y derivarles, bien a la Brigada de Investigación Tecnológica, a la Brigada Central de Estupefacientes, al GRUME o a los compañeros de Seguridad Ciudadana o Judicial. Pero evidentemente, también recordamos que si te están robando, si eres víctima de un delito, a quien hay que llamar es al 091. Nosotros ofrecemos un consejo, somos lo más rápido que podemos, pero no somos una patrulla que pueda acudir en un minuto a solventar ese problema. Para hacer una denuncia hay que presentarse en una dependencia policial o, en caso de una emergencia, llamar al 091.

Nuestro objetivo es sensibilizar, informar, mediar en los casos que se nos planteen derivándolos a la unidad correspondiente.

Las cifras y nuestra implicación en casos concretos como los que les he mencionado nos hacen pensar que vamos por buen camino, pero el desarrollo de las redes sociales y de las nuevas tecnologías de la información es constante y están en permanente evolución y transformación. Por lo tanto, desde la oficina de prensa somos conscientes de que tenemos que seguir aprendiendo, que tenemos que seguir desarrollando campañas y estrategias de concienciación para prevenir el delito y para educar a los menores, y quizá sí sería conveniente que este tipo de concienciación que hacemos en la red también se hiciera, como he mencionado, en el colegio de forma reglada.

COMPARECENCIA DEL DIRECTOR GENERAL DE LA GUARDIA CIVIL, D. ARSENIO FERNÁNDEZ DE MESA DÍAZ DEL RÍO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 20 DE MAYO DE 2013.

El señor **DIRECTOR GENERAL DE LA GUARDIA CIVIL** (D. Arsenio Fernández de la Mesa): Muchas gracias, señor presidente. Señorías, quiero empezar expresando mi pésame por la muerte de la senadora María Jesús Burró, y les ruego que transmitan al grupo parlamentario en el que estaba integrada y al propio PAR mi sentir por el fallecimiento —de una manera trágica, además— de una senadora tan joven.

En segundo lugar, señor presidente, contestando a sus palabras sobre la inmediata respuesta, y agradeciéndola; habiendo sido parlamentario durante muchos años y muchas legislaturas, no puede ser de otra forma: la inmediata respuesta por respeto a esta cámara, por respeto al Senado, por respeto al trabajo de todos los senadores, y también de todos los diputados, de todos los parlamentarios, que efectivamente son injustamente tratados en muchas ocasiones, y que realmente yo conozco el trabajo que se realiza no solo en esta cámara durante los días que aquí se realizan los debates en comisión o en Pleno, sino en cada una de las circunscripciones cuando llegan los fines de semana. De manera que, por respeto al Senado, por respeto a sus señorías, y en segundo lugar por la importancia que tiene el tema que vamos a tratar, no cabía esperar otra respuesta de la Dirección General de la Guardia Civil. Agradezco sinceramente la invitación que se nos ha hecho, y reitero que para mí es un honor especial estar en esta cámara para poder aportar algo, si puede ser, en este lamentable aspecto que es los delitos en la red, los delitos cibernéticos, sobre todo cuando atañen a menores de edad.

Las tecnologías de la información y de las comunicaciones se han consagrado como un verdadero motor de cambio y han revolucionado todos los aspectos de nuestra vida cotidiana. Se han modificado positivamente los métodos de trabajo, las transacciones comerciales o las relaciones humanas, de modo que nos permiten ser más eficientes, teniendo un mayor acceso a la información e incrementando nuestras posibilidades de comunicación en todos los ámbitos. Además, presentan una

marcada potencialidad en cuanto a su uso futuro por parte de las Fuerzas y Cuerpos de Seguridad del Estado.

Estas ventajas y posibilidades tampoco han pasado desapercibidas para el mundo criminal, que las emplea alentado por el anonimato y por la facilidad de ocultamiento, que son algunas de sus principales fortalezas. Hoy en día se puede hacer uso del ciberespacio desde cualquier parte del mundo, no existiendo fronteras convencionales, lo que dificulta notablemente la persecución de este tipo de delitos y genera una gran sensación de impunidad.

Los ciberdelincuentes han encontrado en la red un negocio criminal de bajo riesgo y alta rentabilidad, y muchos son los ámbitos donde han fijado su objetivo, entre los que se encuentran, por ejemplo, las redes sociales. De este modo, las TIC generan cada vez una mayor dependencia por parte de la sociedad, que por otro lado exige a las Fuerzas y Cuerpos de Seguridad del Estado mantener una constante preparación profesional y técnica que les permita dar respuesta a las amenazas y riesgos que las tecnologías de la información y las comunicaciones entrañan.

En este escenario, la ciberseguridad como tratamiento global e integrado ante las amenazas cibernéticas forma parte del mapa estratégico y de las prioridades de todos los países e instituciones del mundo. En particular la Unión Europea cuenta con una Estrategia Europea de Ciberseguridad, un ciberespacio abierto, protegido y seguro. Del mismo modo, España, consciente de las posibilidades que la sociedad de la información ofrece al país, y sabedora del enorme desafío que supone mantener un ciberespacio accesible, seguro y confiable, cuenta con una Estrategia Española de Seguridad (llamado técnicamente EECS), sumándose de esta forma a las iniciativas de otros países de nuestro entorno, que han desarrollado sus estrategias nacionales como el mejor camino para implantar de forma coherente y estructurada todas las acciones de prevención, detección y respuesta que requieren las amenazas del ciberespacio. En esa misma línea de trabajo nos encontramos en el Ministerio de Interior, y por supuesto la Guardia Civil.

El propósito de la estrategia es desarrollar un modelo de ciberseguridad integrado que, dirigido por el Gobierno, garantice a España su seguridad y progreso a través de la adecuada coordinación de todas las administraciones públicas entre sí, con el sector privado y con los propios

ciudadanos, y canalizando las iniciativas y esfuerzos internacionales en defensa del ciberespacio.

En este marco, la lucha contra la ciberdelincuencia conforma una prioridad máxima de manera recurrente en el seno de la Unión Europea, y está siempre presente en el ciclo político de la Unión contra la delincuencia organizada y grave, en los documentos de evaluación de la amenaza (SOCTA), en los planes plurianuales (llamados MAP), y en los planes de acción operativos anuales (OAP) que se desarrollan en el seno de los proyectos del *European Multidisciplinary Platform Against Criminal Threats*. Fruto de la iniciativa europea ha entrado ya en funcionamiento el nuevo Centro Europeo de Ciberdelincuencia, que tiene su sede en la Oficina Europea de Policía de Europol en La Haya, concebido para contribuir a proteger a las empresas y a los ciudadanos europeos frente a esta amenaza.

Además de estas amenazas que pueden afectar a la estabilidad de los Estados, existe un cibercrimen que ataca directamente cada día a los ciudadanos. Son muy variadas las actividades criminales cometidas a través de las tecnologías de la información y de las comunicaciones, como la violación de la privacidad de los ordenadores o los robos de identidad; o lo que es más grave y nos trae a este foro, la distribución de contenidos relacionados con la pornografía infantil.

Merecen especial atención los delitos cometidos a través de las redes sociales, las cuales han modificado las pautas de relaciones humanas. Como en otros entornos, aquí también los grupos más vulnerables de nuestra sociedad se encuentran especialmente expuestos, y particularmente preocupante es el caso de los menores, potenciales víctimas de acosos a través de Internet.

Conscientes de la importancia y alarma social que provocan estos delitos, la Guardia Civil ha articulado una respuesta especializada y acorde a esta amenaza en varios niveles. Los equipos de investigación tecnológica (EDITE) y los equipos Mujer-Menor (EMUME) desplegados por toda nuestra geografía son el primer escalón que protege a nuestros ciudadanos, y en especial a los menores de edad implicados en este tipo de hechos.

Para investigar delitos de especial gravedad contamos con un Grupo de Delitos Telemáticos (GDT), de la Unidad Central Operativa, una sección de la Unidad Técnica de Policía Judicial dedicada a la elaboración de inteligencia relacionada con la delincuencia tecnológica, y un depar-

tamento del Servicio de Criminalística con las capacidades de elaboración de peritajes informáticos y digitales, así como de análisis forense de dispositivos electrónicos.

Todo ello sin olvidar que, en el ámbito de la lucha contra la amenaza terrorista, la Jefatura de Información del Cuerpo cuenta también con los recursos necesarios, humanos y materiales, para hacer frente a esta lacra a través del ciberespacio.

Durante el año 2012, en base a los datos de los que disponemos actualmente, la Guardia Civil ha explotado un total de 88 operaciones y ha abierto 227 en el campo de la ciberdelincuencia; además se ha detenido a 66 personas y se ha imputado a otras 61. Entre estas operaciones cabe destacar la operación «BOEL», desarrollada por la Policía Judicial de la Comandancia de Navarra, que consiguió desarticular un grupo de sicarios que ofrecía sus servicios a través de un foro alojado en un servidor mexicano y que se saldó con la detención de 15 personas y la imputación de otras dos. También la operación «UKUNGA», realizada por la guardia civil de Ciudad Real, en la que se desarticuló una red de delincuentes de nacionalidad nigeriana dedicada a la comisión de estafas bancarias a través de Internet, dando como resultado la detención de 8 personas.

Respecto a los delitos contra menores en Internet, especialmente pornografía infantil y acoso sexual a menores, conocido como *grooming*, las estadísticas reflejan el nuevo marco que se ha querido imprimir en la lucha contra este tipo de delitos, centrándose en los autores con mayor número de descargas en Internet, lo que implica que en cada operación explotada participa un número importante de unidades. Acabo de leer hace muy pocos minutos en un teletipo del Ministerio de Interior que se había producido, precisamente por parte del Cuerpo Nacional de Policía, una detención importante en este sentido.

La ubicación de los objetivos se encuentra dispersa por todo el territorio nacional. Sin querer hacer ningún tipo de comparación, sino simplemente de evaluar la importancia que tiene este fenómeno con la evolución de los años, podemos decir que estas operaciones en el año 2011 fueron 47 las que se realizaron, en este año pasado 2012 cerramos con 88. Y el número de imputados pasó de 6 a 61. Y esta es una labor que de cara al futuro se irá incrementando cada año, porque el trabajo que se está realizando de auténtica concienciación en los Cuerpos y Fuerzas

de Seguridad del Estado y el utilizar equipos cada vez más sofisticados, hace que cada vez se alcancen mejores resultados.

En el año 2012 la Guardia Civil ha realizado 62 operaciones con un resultado de 97 detenidos y 51 imputados contra este tipo de delitos. Entre estas destaco las operaciones «Tribu» y «Mecen», operaciones internacionales de la Unidad Central Operativa en colaboración con el FBI, Europol y los servicios de seguridad de Rusia, que actuaron contra redes pedófilas y de abusos de menores con un resultado de 18 personas detenidas en diferentes países. En este tipo de operaciones contra pornografía infantil y acoso sexual, entre los años 2011 y 2012 las operaciones de 2011 fueron 51, y en 2012, 62, y los detenidos han pasado de 80 a 97.

Pero hay que seguir trabajando y mejorando para luchar contra este tipo de amenazas. Y es necesario afrontarlas desde un enfoque integral que aglutine de forma coordinada los esfuerzos de todos los actores nacionales e internacionales. A nivel nacional la Guardia Civil colabora estrechamente con la Fiscalía de Criminalidad Informática, de forma que sus fiscales delegados coordinan las actuaciones de las unidades encargadas de la investigación de este tipo de delitos.

Participamos en múltiples foros nacionales, entre los que destacan las colaboraciones con la Escuela Judicial del Consejo General del Poder Judicial, el Consejo General de la Abogacía y diversas universidades, entre las que se encuentran la de Alcalá, la Politécnica de Madrid o la Universidad de Granada, sin dejar de tener en cuenta que este año, con el inicio de Bolonia, con la Universidad Carlos III se está avanzando en este terreno de manera muy importante.

En la misma medida es de vital importancia la colaboración a nivel internacional, porque no existen fronteras en relación con los delitos tecnológicos. La Guardia Civil materializa esta colaboración a través de organismos internacionales como Europol o Interpol, en diferentes foros de la Unión Europea, y directamente a través de relaciones bilaterales: este próximo viernes trataremos en el IV Comité de Planificación y Coordinación Estratégica de Seguridad Interior Hispanofrancés, que se celebrará aquí en Madrid, el protocolo relativo a la posible creación de una unidad conjunta de análisis entre la Gendarmería Nacional francesa y la Guardia Civil para intercambio de información de ciberdelincuencia, con especial atención a los delitos de pornografía infantil.

Quiero destacar la trascendencia de la cooperación con el sector privado, estableciendo canales de comunicación y entendimiento con los administradores de las redes sociales y de los proveedores de servicios, entre otros, y señalar que debe existir una intensa colaboración con la comunidad académica, esencial en el desarrollo de herramientas que faciliten la lucha contra la ciberdelincuencia y en la formación de investigadores policiales.

Las actividades preventivas en el ámbito de la seguridad de los menores en Internet es un punto fundamental, y creemos que está dando buenos resultados. Se incluyen en el marco del Plan director para la mejora de la convivencia y seguridad escolar, a través del cual se participa en la formación de padres, profesores y alumnos, de centros escolares y de educación secundaria, en temas como el uso seguro de Internet y la prevención del acoso sexual a los menores a través de Internet.

A su vez, por parte de la Guardia Civil la Unidad Técnica de Policía Judicial se han elaborado materiales específicos sobre seguridad de los menores en Internet al objeto de que sean utilizados en las charlas que los guardias civiles realizan dentro del citado plan director, y se ha formado a los responsables provinciales del plan en este tema. Dentro del marco del citado plan, y con el objetivo de contribuir a la prevención de los delitos contra menores en Internet, la Guardia Civil mantiene una estrecha y permanente colaboración con organizaciones que tienen como objetivo la protección de los menores. Por ejemplo, la fundación ANAR, que en virtud del convenio de colaboración entre el Ministerio de Interior y esta fundación para el fomento de la prevención e intervención en situaciones de riesgo para la seguridad del menor, de 22 de abril de 2008, comunican todo tipo de situaciones presuntamente delictivas que reciben tanto a través de su teléfono de atención al menor como a través de su línea de atención *online*, entre las cuales se encuentran las relativas a explotación sexual infantil. También se mantiene una estrecha colaboración con la fundación Protégeles, que está constituida como una *hot line* o línea de denuncia integrada en la Red Europea de Líneas de Ayuda Infantil. A Protégeles llega todo tipo de comunicaciones relativas a la seguridad de los menores, pero especialmente en lo relativo a pornografía infantil y explotación sexual de menores a través de Internet, que son oportunamente transmitidas a las Fuerzas y Cuerpos de Seguridad del Estado. Igualmente la fundación Alia2, en virtud del convenio de colaboración suscrito con el Ministerio de Interior para la erradicación de la porno-

grafía infantil en Internet y la lucha contra la pederastia, colabora con las Fuerzas y Cuerpos de Seguridad del Estado a través de su línea de denuncia.

De la misma forma, se mantienen contactos habituales con los administradores tanto de la red social Tuenti como de la red Habbo, por ser ambas de amplio uso entre los menores de edad en España. Por otro lado, se ha facilitado el acercamiento a los menores víctimas de delitos en la red y a otros actores aprovechando las tecnologías de la comunicación. En este sentido, se ha creado la dirección de correo proteccion-menor@guardiacivil.org que gestiona el EMUME central de la Unidad Técnica de Policía Judicial —EMUME, lo recuerdo, son los equipos Mujer-Menor—. También se dispone de la plataforma telemática «Colabora», que se gestiona conjuntamente con el Grupo de Delitos Telemáticos. La Unidad Central Operativa de la Policía Judicial recientemente ha puesto en funcionamiento una aplicación a través de la dirección electrónica segura https://www.gdtguardiacivil.es, para realizar este tipo de comunicaciones a través de teléfonos móviles de última generación. Igualmente se tienen conocimiento de estos hechos mediante las comunicaciones que los ciudadanos realizan a través de la página web del cuerpo en Internet.

¿Pero qué proyectos y líneas de actuación del cuerpo tenemos por delante? Analizando el fenómeno de la ciberdelincuencia en España, así como del resto de países de nuestro entorno, y previendo la evolución que probablemente tendrá en el futuro, es razonable concluir que va a ir en aumento en cualquiera de sus facetas, ya como medio para delinquir, ya como objeto material de ciberdelincuentes. Inevitablemente, con el incremento de usuarios de Internet y redes sociales, el número de potenciales víctimas que pueden sufrir un delito en la red aumenta en la misma proporción. En este marco, para hacer frente a esta evolución en materia de ciberdelincuencia se trabajan las siguientes líneas de actuación:

En reforzar las capacidades de especialistas en investigación de delitos tecnológicos; reforzamos en la medida de lo posible la capacidad de las unidades forenses de investigación y análisis criminal, tanto a nivel central como a nivel territorial, en cuanto al número de especialistas, los medios empleados y en cuanto a su formación específica.

Se está trabajando mediante un plan de formación específico dirigido a todas las unidades de policía judicial y mediante la introducción de nuevas funcionalidades y herramientas de análisis, en mejorar el empleo

del sistema de investigación SINVES como una verdadera herramienta de gestión y coordinación de investigaciones, buscando lograr una mayor calidad y eficiencia.

Estamos orientando a los especialistas hacia la realización de investigaciones tecnológicas autónomas, de manera que la investigación de delitos que emplean la red solo como herramienta básica de apoyo, como por ejemplo la difusión de pornografía infantil, puedan ser desarrolladas mediante una cualificación básica, por especialistas en otras áreas delictivas, por ejemplo en la investigación de delitos contra las personas. Ello permitirá aumentar la capacidad y agilidad investigativa en la institución, así como descargar a los EDITE (equipos de investigación tecnológica) de las investigaciones más sencillas, pudiendo dirigir todos sus esfuerzos a la resolución de aquellas investigaciones que requieran un más amplio nivel de conocimientos y técnicas.

También se apuesta por la búsqueda de protocolos de trabajo en los que se conjuguen conocimiento, esfuerzo técnico e imaginación. Con ello se garantiza que las pruebas que se obtengan en una investigación tecnológica puedan ser puestas a disposición judicial con las necesarias garantías procesales. En este sentido, en el Servicio de Criminalística se trabaja en el desarrollo de un sistema que permita una gestión adecuada de las necesidades de análisis forense estableciendo una plataforma integral de acceso remoto para el almacenamiento y análisis de las evidencias digitales.

Se trabaja también de manera conjunta con las universidades y otras instituciones públicas y privadas en desarrollar métodos de investigación basados en la utilización de software y buscadores específicos que permitan una detección rápida de conductas delictivas en la red.

Otra de las líneas de actuación es impulsar la formación especializada. En la era de la tecnología, es de interés que todos los investigadores tengan una formación básica en la materia. De este modo, en los cursos y jornadas de formación de investigadores impartidos en la Escuela de Especialización de la Guardia Civil o por la Jefatura de Policía Judicial se realizan sesiones de introducción a la investigación tecnológica.

Pero es esencial seguir apostando por la formación especializada superior. Con ella, aquellos de nuestros investigadores con mayores conocimientos o destinados en las unidades llamadas a asumir las actuaciones

investigativas de mayor complejidad podrán mantener sus capacidades a la altura de la evolución tecnológica que la delincuencia especializada está alcanzando. Y para esto se pretende, primero, continuar con futuras ediciones de cursos universitarios, como el desarrollado en colaboración de la Universidad de Alcalá, cuyas materias a desarrollar serán periódicamente actualizadas a requerimiento de las potenciales evoluciones delictivas.

Igualmente, continuar con los cursos básicos en investigación tecnológica, estudiar la implantación de nuevos cursos de teleformación con los que complementar los conocimientos de los profesionales actuales, permitiendo con ellos la capacitación en tipos delictivos concretos; impulsar el desarrollo de instrucciones y guías de procedimiento técnico.

Otro objetivo a desarrollar es el establecimiento de canales de comunicación directa e inmediata a través de la red a modo de foros. Con ello se facilitará un intercambio fluido de opiniones y experiencias que servirán como apoyo a los investigadores menos experimentados. Además, este sistema permitirá la existencia de un repositorio de buenas prácticas, legislación y artículos de interés con los que favorecer la autoformación de los investigadores.

Impulsar la colaboración internacional, tanto en el ámbito bilateral como en el multilateral, de manera que sobre la base de la reciente Instrucción 7/2012 de la secretaría de Estado, que instaura los contactos directos de la Guardia Civil, se pueda aumentar la colaboración con los distintos ficheros y *focal points* de Europol relacionados con la investigación tecnológica, así como proponer la presencia de la Guardia Civil en el Centro Europeo de Cibercrimen (EC3), de reciente creación.

Impulsar la asistencia y participación en los distintos foros y talleres de trabajo que se planteen por parte de organizaciones internacionales, y aumentar los niveles de colaboración policial con las unidades de investigación tecnológica de las policías de nuestro entorno, con el fin de garantizar un intercambio de información eficaz que nos permita dar una respuesta ágil a los delitos informáticos, caracterizados por su transnacionalidad.

Finalmente, nos proponemos incrementar la colaboración y coordinación con organismos públicos y privados, continuando la colaboración en la labor formativa con la Fiscalía General del Estado y con la Universidad de Alcalá en materia de investigación tecnológica, re-

forzando la colaboración con el Consejo General del Poder Judicial, y sobre todo con la Fiscalía de Criminalidad Informática, mediante el nombramiento de un oficial de enlace ante la misma, afianzando la relación con el Ministerio de Industria, recogida en el Convenio Marco de colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad del Ministerio de Interior y la Secretaría de Estado de Telecomunicaciones y de la Sociedad de la Información, del Ministerio de Industria, Energía y Turismo, que se materializará en diferentes reuniones de coordinación y la realización de proyectos conjuntos con el organismo público INTECO.

Incrementando los contactos y la colaboración con los distintos actores nacionales implicados en materia de seguridad informática y tecnológica, como pueden ser las propias Fuerzas Armadas; potenciando la relación con los medios de comunicación social generalistas o especializados, de manera que se pueda difundir a la sociedad la problemática derivada del empleo de las nuevas tecnologías, fortaleciendo los cauces de comunicación del ciudadano con nuestra institución a través de las vías de comunicación electrónica ya establecidas, así como mediante el uso de las redes sociales; favoreciendo una respuesta rápida a aquellos requerimientos que, enviados a través de correos electrónicos o las redes sociales, requieran una respuesta rápida; incrementando la colaboración con el sector privado para desarrollar nuevas herramientas tecnológicas que permitan mejorar las técnicas de investigación o para atender las denuncias sobre agresiones tecnológicas que las empresas o los ciudadanos puedan sufrir; continuando la colaboración con las instituciones sociales públicas y privadas para la difusión a los sectores más vulnerables de los riesgos en Internet.

Y por supuesto, hay otros aspectos que pueden ayudar a mejorar la lucha contra este tipo de actividad delictiva, además de las modificaciones normativas que proponen los expertos y que son responsabilidad de las Cámaras. Se trata de la prevención; y no hay mejor prevención que la educación. Cualquier aspecto que se implante para mejorar la educación en ciberseguridad, especialmente de los menores y de sus familias, disminuirá las posibilidades de que se cometan muchos de estos delitos. Así, esta formación debería extenderse a los entornos más cercanos que rodean al menor, especialmente padres y profesores, para que sean capaces de aconsejarles en las mismas condiciones que lo hacen sobre los peligros que les acechan en la vida real.

La Guardia Civil y las Fuerzas y Cuerpos de Seguridad del Estado hacemos un esfuerzo para explicar y acercarnos a los problemas que tienen los menores en el uso de la red. Sin embargo, debido a la extensión de contenidos que a día de hoy ya supone la ciberseguridad, habría que contemplar la posibilidad de incluir en los planes de estudio escolares una asignatura o módulo más extenso sobre navegación segura y ciudadanía digital.

Quiero transmitir mi expresa voluntad de dar continuidad en el futuro al esfuerzo del cuerpo en esta lucha, como no puede ser de otra forma, y continuando la labor empezada hace años ya. Las características tan singulares del entorno en el que se cometen los delitos tecnológicos, hacen necesario que todos los actores implicados en su lucha dispongan de una permanente actualización de conocimientos, buscando a la vez sinergias entre todos ellos para dar una respuesta eficaz a estos ilícitos.

Espero y deseo que podamos sacar las mejores conclusiones en este foro para conseguir una mejor protección de los derechos y libertades de nuestros menores. La dirección de correo electrónico proteccion-menor@guardiacivil.org y el portal «Colabora» están a disposición de los ciudadanos para ayudarles y aconsejarles ante estos delitos. Disponemos además de una aplicación para teléfonos móviles del Grupo de Delitos Telemáticos de la Guardia Civil que recoge los mismos aspectos que la página web, con consejos de seguridad y ayuda.

El pasado día 17 de mayo de 2013 se ha presentado el libro *Por una red más segura*, de un guardia civil que se llama Ángel Pablo Avilés, componente del Grupo de Delitos Telemáticos. Con este libro se pretende transmitir los conocimientos adquiridos y sus experiencias sobre menores, seguridad y estafas en la red. Y ya estamos viendo la forma de poder hacerlo llegar al mayor número de colegios posible.

Para finalizar, debemos recordar a los usuarios, y en especial a los padres y a los menores, que deben usar el sentido común, no proporcionando datos que no sean necesarios; tener presente que detrás de cada dirección electrónica hay una persona que no tiene por qué ser siempre quien dice ser. Y tener siempre actualizado el sistema operativo y antivirus.

En caso de duda, acudir a la Guardia Civil o a cualquier otro de los Cuerpos de Seguridad de Estado, a través del portal «Colabora» del Grupo de Delitos Telemáticos, Guardia Civil en las redes sociales a través de

YouTube, Tuenti o Facebook y correo de atención al ciudadano y todas las oficinas del cuerpo.

Yo creo, señorías, que estamos ante uno de los problemas más graves por ser los menores los más indefensos ante ataques de esta virulencia; y yo creo que todos los medios que ponga el Gobierno, o que ponga la sociedad a disposición de quienes en cada momento tienen la obligación de velar por la seguridad de los menores, serán pocos porque, sinceramente, creo que hasta que hayamos conseguido erradicar definitivamente —algo que es un sueño y una utopía probablemente— esta lacra social que ahora se avecina, y que sin duda, de acuerdo con la evolución que vaya teniendo Internet y que vayan teniendo las redes sociales, se irá agrandando.

De manera que yo creo que todos los esfuerzos que se puedan hacer serán pocos y por eso felicito a esta ponencia, al Senado por esta iniciativa, porque yo creo que del resultado de la misma saldrán cosas muy interesantes, y sobre todo cuestiones que habrá que tener en cuenta para que de cara al futuro esta lacra, lamentable y repugnante, seamos entre todos capaces de atajarla en la medida de lo posible.

Muchas gracias, señor presidente; gracias, señorías.

COMPARECENCIA DEL COMANDANTE JEFE DEL GRUPO DE DELITOS TELEMÁTICOS DE LA UNIDAD CENTRAL OPERATIVA (UCO) DE LA GUARDIA CIVIL, D. ÓSCAR DE LA CRUZ YAGÜE, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 20 DE MAYO DE 2013.

El señor **COMANDANTE JEFE DEL GRUPO DE DELITOS TELEMÁTICOS DE LA UNIDAD CENTRAL OPERATIVA (UCO) DE LA GUARDIA CIVIL** (D. Óscar de la Cruz Yagüe): Buenas tardes. En primer lugar, agradezco la oportunidad de estar aquí, creo que es un honor poder comparecer ante ustedes, y sobre todo en esta casa, una de las sedes en las que radica la democracia. Intentaré ser breve y conciso en varios puntos que quiero tratar, e intentar ser constructivo, es decir, aspectos que quiera poner de manifiesto de cosas que creo podemos mejorar entre todos.

En primer lugar, para ubicar dentro de la Guardia Civil cómo nos estructuramos en lo que respecta a investigaciones tecnológicas, yo represento al Grupo de Delitos Telemáticos, ya que muchas veces por tener mucha visibilidad, sobre todo en medios de comunicación, quiero decir que no somos ni mucho menos los únicos en la Guardia Civil que investigamos. Como bien decía el Director de la Guardia Civil, dentro de la estructura periférica que tiene en cada provincia, en cada Unidad nuestra que se llama Comandancia hay un grupo que se dedica a investigar todos los delitos relacionados con nuevas tecnologías en la red, que son los EDITE, y en los cuales tienen suficiente capacitación y formación como para hacer frente a todo este tipo de investigaciones.

¿Cuándo interviene el Grupo de Delitos Telemáticos? Nosotros somos una especie de segundo escalón. Cuando en estos equipos, hay investigaciones que por necesidades de recursos humanos o materiales no son capaces de dar continuidad, o incluso hay investigaciones que afectan a varias provincias a la vez, es cuando nosotros como Unidad con demarcación nacional entramos en escena, y bien asumimos la investigación. Obviamente, también de oficio nosotros iniciamos nuestras propias investigaciones y operaciones.

Aparte de esto, existe una Unidad Técnica de Policía Judicial, en la cual no voy a incidir porque es la que representa mi compañero el Capitán Carlos Igual, pero por resumir un poco y ubicar, son los que hacen la coordinación de estas unidades periféricas así como la elaboración de inteligencia, de toda esa información que se va recopilando de la explotación de operaciones e investigaciones, ellos son los que generan esa inteligencia en cuanto a nuevos modus operandi, nuevas formas de operar que tienen los delincuentes, para luego diseminarlo otra vez a las unidades operativas.

En cuanto a las funciones del Grupo de Delitos Telemáticos, nuestro ámbito de tipología penal que perseguimos es plena; si bien hay delitos que son los más puramente tecnológicos, por así decirlo, aquellos que atacan a los sistemas de información como son las intrusiones, denegaciones de servicio, etc., hay otros tipos de delitos tradicionales que ya existían antes, pero que hacen uso de las nuevas tecnologías para su comisión. Cuando este grado de implicación de nuevas tecnologías es importante como para que haya detrás una unidad especializada en investigación de estos delitos, nosotros también asumimos su investigación.

Por esquematizar un poco estas grandes áreas, tomamos como referencia el Convenio de Ciberdelincuencia de Budapest, que se firmó en 2001, y lo categorizamos en cuatro grandes áreas. Una sería relativa a la persecución de la pornografía infantil, así como aquellos delitos que tienen como objetivo los menores (*grooming*, *cyberbullying*, abusos, acoso sexual a menores), que creo que es el área en la que más se enmarca esta ponencia. También perseguimos todo tipo de fraudes y estafas en la red, tanto en su vertiente de comercio electrónico como bancario; perseguimos también los delitos de *hacking*, que son contra los sistemas de información, así como los delitos contra la propiedad intelectual e industrial.

También quiero hacer referencia dentro de la colaboración y cooperación, que es una de las grandes líneas que voy a tocar: en el ámbito europeo estamos en Europol y en el recientemente creado EC3, así como en grupos de trabajo de Interpol, tanto en el grupo latinoamericano como en el grupo europeo.

Y ya para entrar un poco en materia, las tres grandes líneas, por marcar primero el esquema, van a ser prevención, colaboración, y luego mejoras a nivel legislativo, que yo personalmente creo que es lo más importante y en lo que más puede mejorar nuestra calidad de trabajo y de operaciones.

En primer lugar, en cuanto a prevención, por hilar un poco actividades realizadas la semana pasada, para que vean el nivel de concienciación que tenemos nosotros con estas actividades. Aunque somos unidades operativas y nuestra función es la persecución y la investigación del delito, entendemos que gran parte del éxito es la prevención y así lo hacemos. Y aunque no sea nuestra función principal, como conocedores de esos riesgos y esas amenazas, porque es lo que estamos persiguiendo diariamente, pensamos que podemos hacer muy buena labor en este aspecto. De hecho, como comentaba, la semana pasada con ocasión del día de Internet, que fue el viernes día 17, hicimos una serie de actividades en torno a este día y a este acto. Se celebraron unas jornadas de concienciación dirigidas sobre todo a los colectivos que entendemos que tienen que tener una protección especial, como son menores, menores e incapaces (porque muchas veces aludimos solo a los menores, pero creemos que los incapaces deberían entrar bajo el mismo paraguas de protección); mayores también, de hecho uno de los talleres de formación que hicimos, de forma cariñosa se denominaba «para ciberabuelos», porque entendemos que es gente que está entrando en el uso y el contacto de las nuevas tecnologías y no tienen la suficiente formación como para poder detectar todas estas triquiñuelas que utilizan los delincuentes para engañarlos, lo que conocemos como ingeniería social; así como el navegante medio, ya que muchas veces no tiene los conocimientos básicos como para poder defenderse de todas estas actividades delictivas que pueden sufrir.

Otro de los actos centrales de la semana pasada fue la presentación de un libro, como ha hecho alusión el Director, escrito por un guardia civil del Grupo, que hace un año, de forma totalmente particular —aunque sabíamos de su actividad— en un blog de seguridad empezó a publicar consejos de navegación pero escritos de una forma muy sencilla, ya que al final estamos habituados a tratar en un ambiente muy técnico y hay veces que utilizamos terminología y no conseguimos llegar a quien tenemos que llegar. Él, sin embargo, utiliza un lenguaje muy básico, sin términos técnicos, para conseguir llegar a quien queríamos, al ciudadano medio, y sobre todo también a los padres, a los padres que se tienen que encargar de educar y concienciar a sus hijos. Yo me he permitido traer un ejemplar, sólo uno, porque de momento ha sido una primea edición muy limitada, y como el ejemplar se está regalando, pues no teníamos suficientes recursos como para poder traer un ejemplar para todos. De

momento lo dejo aquí, pero si tienen interés en recibir algún ejemplar más, se lo haríamos llegar a posteriori.

La intención de todo esto es romper con esa brecha, esa brecha digital que es la que está haciendo que muchas veces los padres no se sientan capacitados de aconsejar a sus hijos en el uso de nuevas tecnologías. A todos nosotros de pequeños nuestros padres nos decían «no abras la puerta a extraños, no cojas caramelos de extraños en el colegio»; sin embargo, hoy en día la mayoría de los padres no saben cómo funcionan las redes sociales o las nuevas tecnologías y no tienen ese conocimiento para poder aconsejar y educar a sus hijos. En estos talleres se ponía como ejemplo muchos padres que se encargan de llevar al niño al colegio, que no le pase nada, recogerlo, que venga acompañado y no vaya solo, y sin embargo llegan a casa y le dejan en la habitación solo con un ordenador. Entonces, es completamente ilógico. Aquí es donde sí esperamos que se pueda incidir, y sobre todo con el tema de la educación reglada en colegios.

Aunque la eficacia del plan director para la mejora de la convivencia y seguridad escolar es mucha, creemos que a día de hoy con una visita que puedan hacer una mañana, tanto Policía como Guardia Civil, en un colegio no es suficiente como para poder aleccionar a los chavales de todos los riesgos. Entendemos que ya sería momento de que en los planes de estudio se incluyera o bien una asignatura, o bien un módulo con un contenido estudiado por especialistas y que fuera adaptado a dependiendo qué rango de edad; entendemos que a menores de 8, 9 o 10 años no se les debe dar la misma formación que a adolescentes de 14 o 15, los riesgos son diferentes.

En este aspecto, quiero comentar también las labores que hacemos en cuanto a contacto con la sociedad, como son los canales de colaboración ciudadana, los cuales desde hace años intentamos potenciar porque la Guardia Civil siempre se ha caracterizado desde su servicio en el ámbito rural por estar cerca del ciudadano y hablar con la gente, que son los que al final te manifiestan sus problemas, sus inquietudes y donde se consigue mucha información para ver qué problemas están teniendo. Pues hay que trasladarlo ya al mundo digital o virtual, y por eso tanto en la página web nuestra con los canales de colaboración, aplicaciones para *smartphones*, teléfonos móviles, así como en redes sociales, lo que hacemos es poder recibir información, y a su vez es un canal de vuelta,

es un canal bidireccional porque de vez en cuando lo que hacemos es publicar lo que se conoce como alertas tecnológicas para que los ciudadanos estén alerta de nuevos modus operandi, nuevas formas que tienen los delincuentes de operar.

En el ámbito de la cooperación, debido a la configuración de la red en general y de cómo operan los ciberdelincuentes, es fundamental; es un fenómeno transversal que afecta a todos los ámbitos, tanto personal como profesional, así como en la globalidad del fenómeno. Ya esos criterios territoriales con los cuales nos movíamos hasta ahora tanto en la investigación policial como judicial, es evidente que las nuevas tecnologías han acabado con ellos.

Por tanto, a nivel nacional entendemos que tanto los órganos públicos como privados que intervienen, sería aconsejable o deseable que hubiese una especie de centro nacional de coordinación, en el cual hubiera órganos tanto de cuerpos policiales, Fiscalía, Ministerio de Industria, etc. pero igual del ámbito privado, tienen que estar las operadoras, tienen que estar las redes sociales, de tal forma que esa información pueda fluir de manera sencilla y de todos para todos, no como hasta ahora, que operamos un poco en el ámbito bilateral, todos tenemos relaciones con todos, pero hacemos reuniones dos a dos, no hay ningún órgano que aglutine todos los actores y sintiendo que somos muchos los que intervenimos en aspectos de la ciberseguridad.

En el aspecto internacional, a nivel policial yo creo que tenemos canales suficientes, ágiles y buenos para la cooperación policial. En el ámbito europeo, vuelvo a incidir, está Europol con el EC3; en el ámbito internacional tenemos a Interpol. Pero sin embargo, lo que vemos es que cuando tenemos que dar el salto judicial, que suele ser casi siempre a la hora de transmitir información que tenga luego validez en un proceso penal, tenemos la limitación de que esos procedimientos no son todavía lo suficientemente ágiles como quisiéramos.

Hay una figura que es la Comisión Rogatoria Internacional por la cual, cuando necesitamos un auxilio o una información de un tercer país, ni nosotros ni el juez español lo puede pedir de forma directa; es necesario que el juez español, con esa Comisión Rogatoria Internacional, pida auxilio a un juez del tercer país para que el juez del tercer país recopile o recabe ese auxilio o esa información y venga de vuelta a España. Estos procesos son procesos que se pueden dilatar semanas o incluso meses,

por lo cual en investigaciones que, sobre todo a través de la red, son hechos que ocurren en cuestión de segundos, entendemos que no está ponderado, y muchas veces a nosotros como investigadores son situaciones que nos retrasan mucho y dificultan la investigación.

Otro aspecto, y yo creo que también es importante a la hora de solicitar colaboración internacional de algunos operadores que prestan servicios en la red, pues no todos, y sobre todo no los grandes, pero sí es cierto que hay multinacionales que, amparándose en que están sujetas a la legislación de su país, donde tiene su sede social, no colaboran todo lo bien que debieran, cuando aun así están prestando servicio a usuarios que están en España. Y ya sin entrar en temas fiscales, que creo que es otro aspecto aunque no atañe a esta ponencia, pero creo que desde España como Gobierno se debería muchas veces, si no obligar legalmente, sí exigir cierto compromiso a esas empresas que al final, son usuarios españoles que están utilizando sus servicios, y que luego cuando les vamos a requerir un auxilio policial o judicial no responden todo lo bien que debieran.

Y ya en el aspecto legislativo, que yo creo que es donde más deberíamos mejorar, porque muchas veces a nosotros nos vienen personas del entorno, de la empresa, incluso de la universidad y nos dicen «¿de qué forma os podemos ayudar para mejorar vuestra situación y vuestras investigaciones?». Y yo siempre les digo lo mismo: más que herramientas técnicas, lo que necesitamos son herramientas legales para poder llegar más y mejor.

La ciberdelincuencia se constituye como una de las amenazas más asimétricas que hay hoy en día; es decir, los delincuentes se aprovechan de técnicas y procedimientos para delinquir que luego nosotros, como fuerzas y cuerpos de seguridad, no podemos utilizar para investigarlos. Y aquí voy a poner dos ejemplos, uno de los cuales ya ha salido, y es la figura del agente encubierto. En el ámbito procesal actualmente se permite para investigación de terrorismo así como para investigación de determinados delitos, pero siempre en el ámbito de la delincuencia organizada. Claro, la persecución tanto de la distribución de la pornografía infantil como del acoso sexual, del *grooming* a menores no es delincuencia organizada, son individuos que de forma individual ejecutan sus acciones delictivas.

Y aquí sí que podría poner un ejemplo de la necesidad de tener esta figura para operar e investigar en Internet, y es el caso de la distribución de

pornografía infantil. Actualmente la difusión de este tipo de imágenes se podría equiparar a una especie de pirámide, en la cual tenemos una base en la cual hay gran cantidad de usuarios que no toman muchas medidas de seguridad en cuanto a la difusión pero que el contenido que intercambian tampoco es de excesiva gravedad o es contenido poco actual o ya muy difundido. Esto, el ejemplo sería el ámbito de las redes *peer-to-peer*, es decir, la gente que a través de redes como Emule o Edonkey intercambian este tipo de material, pero para nosotros, como Fuerzas y Cuerpos de Seguridad, es relativamente sencillo detectarlos por unos sistemas buscadores que disponemos, en los cuales a través del material que ya conocemos, lo introducimos en el buscador, y por así decirlo de forma sencilla nos dice qué personas están compartiendo ese material.

Según vamos subiendo la pirámide, los usuarios toman más medidas de seguridad y el material es más violento, con contenido más grave, o incluso material que se produce ya por redes organizadas que mueven dinero por intercambiar este material. En estos sistemas de intercambio ya entrarían a través de correo electrónico, o incluso en foros cerrados, a los cuales para acceder es necesaria la invitación de uno de los miembros, y el contenido está cifrado. ¿Eso por qué lo hacen? Porque al pedir invitación de alguna de las personas que ya componen ese grupo, se garantizan que nosotros no vamos a poder acceder. Hasta ahora la gran mayoría de las operaciones policiales en el entorno de la distribución de pornografía infantil se hace en las redes *peer-to-peer*, en esa base de que he hablado de la pirámide. Si incidimos solo ahí y no tocamos el techo de la pirámide corremos el riesgo de invertirla, es decir, que la gente ya sabe que gran número de operaciones policiales se hace en redes *peer-to-peer* y digan «esto no es seguro, vamos a migrar a esos foros, a los cuales es más complejo acceder». Si no implementamos figuras como la del agente encubierto, nos vamos a quedar sin herramientas como para poder acceder a esos foros y detectar qué personas están compartiendo ese material, y que normalmente es el más grave. No sé si ha quedado clara la explicación, pero luego en el turno de preguntas podemos matizarlo.

Y luego, la segunda figura que considero que es de bastante importancia para la investigación es la utilización de herramientas de administración remota de equipos. Esto es lo que popularmente se conoce como troyanos, que los delincuentes utilizan para infectar nuestros equipos y robarnos información. Actualmente nosotros no podemos utilizar estos sistemas, lógicamente sería con todas las garantías judiciales, manda-

miento judicial y demás, pero actualmente no podemos utilizarlo para la investigación.

Y muchas veces, incluso yo creo que es más garante que los sistemas tradicionales, y explicaré por qué. Hasta ahora todas las intervenciones de las telecomunicaciones se hacían interviniendo el canal, es decir, todo estaba basado en la telefonía fija, con lo cual se intervenía la línea y te asegurabas de que ibas a intervenir el teléfono que el delincuente estaba utilizando. Hoy en día esto ya no sirve, ¿por qué? Porque yo con mi teléfono, con mi *smartphone* ahora me conecto por 3G, pero dentro de cinco minutos me conecto por la red WiFi de un centro comercial y a los diez minutos me voy al McDonald's y la red es diferente, con lo cual si intentamos interceptar el canal no vamos a conseguir nada porque el canal va cambiando. Por eso entendemos que es muchísimo más efectivo a día de hoy intervenir el dispositivo; independientemente del canal que me conecte, yo voy a tener garantizadas las comunicaciones de ese terminal. ¿Por qué digo también que es más garantista? Porque interviniendo el canal, cualquier persona que utilizara ese teléfono fijo de la familia, van a quedar registradas sus conversaciones. Sin embargo, intervenir un teléfono móvil, normalmente a día de hoy es personal y lo utiliza una sola persona.

Otro aspecto del que quería hablar, y ya lo ha comentado el Director, es el tema de lo sencillo que resulta a día de hoy conseguir anonimato en la red, empezando por lugares públicos, como son locutorios, cibercafés, universidades, colegios, etc. No se puede tener un control total sobre qué personas utilizan cada servicio, pero sí que a lo mejor sería deseable llevar una especie de control administrativo sobre las personas que utilizan un determinado servicio de Internet en los locutorios, por ejemplo, en Internet. De hecho, hace algunos años tuvimos que sufrir las consecuencias de un atentado como fue el 11-M para darnos cuenta de que el que hubiera tarjetas de teléfono prepago anónimas era un grave problema de seguridad. Pues bien, a día de hoy los mismos efectos que se pueden generar con un teléfono móvil por GSM de activar un explosivo o una bomba remota, se puede conseguir igualmente con el mismo teléfono conectado a una red WiFi y de forma totalmente anónima. Entendemos que es una brecha bastante grave de seguridad y que nunca se tiene que confundir con el contenido. Lo que entendemos que hay que controlar es qué persona realiza la conexión en cada momento, independientemente luego del contenido material, que eso en ningún momento se ve afectado, de la comunicación.

Quiero reiterar también, en cuanto a aspectos de legislación, que ya se ha hablado, en materia penal, intentar adaptar a las nuevas realidades los tipos penales, que hasta ahora lo que se iba haciendo era adaptar tipos que ya existían, intentar encajarlos en los nuevos delitos como se cometen en la red. No siempre es efectivo, y entiendo que eso, tanto a las Fuerzas y Cuerpos de Seguridad como incluso las víctimas les genera inseguridad; inseguridad jurídica de ver que los tipos tal y como se están cometiendo a través de las nuevas tecnologías no es equiparable al delito como está tipificado en el Código Penal.

Y ya por acabar, también quería comentar que, a lo mejor, puesto que tenemos un sistema judicial yo creo que un poco saturado, debido a que hay demasiadas conductas que están tipificadas como delito o como falta, pues a lo mejor sería conveniente potenciar el derecho administrativo para las circunstancias menos lesivas o menos graves; quizá, una suplantación de identidad simplemente, sin que vaya acompañada de nada más, que no haya injurias o amenazas, a lo mejor sería más sencillo de resolver simplemente con un procedimiento administrativo, al modelo de como se hace con la protección de datos de carácter personal, que al final para nosotros es casi más efectivo, porque las garantías procesales no son las mismas que en un proceso penal, y la sanción social que recibe es una multa económica, y muchas veces creemos que es casi más efectivo que no un proceso penal que se dilata en el tiempo, y luego la respuesta que se le da a ese delito no está equiparada con la sanción que lleva asociada.

Por mi parte nada más; muchas gracias por su atención, y a su disposición para las preguntas.

COMPARECENCIA DEL CAPITÁN DEL GRUPO DE MENORES Y EXPLOTACIÓN SEXUAL INFANTIL DE LA UNIDAD TÉCNICA DE POLICÍA JUDICIAL (UTPJ) DE LA GUARDIA CIVIL, D. CARLOS IGUAL GARRIDO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 20 DE MAYO DE 2013.

El señor **CAPITÁN DEL GRUPO DE MENORES Y EXPLOTACIÓN SEXUAL INFANTIL DE LA UNIDAD TÉCNICA DE POLICÍA JUDICIAL (UTPJ) DE LA GUARDIA CIVIL** (D. Carlos Igual Garrido): Muchas gracias, señorías; gracias por la invitación y por la oportunidad de estar ante ustedes.

Muchas de las cuestiones que yo venía a comentar ya se han hablado. Primero, quisiera explicarles que el grupo al que pertenezco lleva la coordinación en España de los EMUME de la Guardia Civil, de los grupos que actúan en delitos contra menores y violencia de género, pero en este caso me referiré a delitos contra menores.

El hecho de que los EMUMES hayan asumido también determinadas operaciones de ciberdelincuencia, especialmente en casos de *grooming* y contra la pornografía infantil, es por la evolución que hemos visto en los últimos años; hemos visto delitos que delitos que han existido desde que tenemos conocimiento han evolucionado hacia la red, o en otros casos han modificado su modus operandi; por ejemplo el *bullying*, el acoso escolar que era un problema que existía en el ámbito escolar, hemos visto como en los últimos años —además en concreto en el último año— prácticamente todas todos los casos que hemos tenido de denuncia de *bullying* eran *cyberbullying*, no porque sean exclusivos de la red, sino porque en parte o totalmente se estaban produciendo en Internet.

Y además esto incluso trae consecuencias distintas para las víctimas: en el acoso «clásico» un niño o una niña que era acosada en el colegio, es decir principalmente en el entorno escolar y este acoso se producía en el patio, en las aulas o incluso en la calle; pero, sin embargo, la víctima tenía un lugar seguro, que era su casa. Ahora no; ahora con el *cyberbullying,* incluso cuando la víctima esté en su casa, incluso por la noche, está siendo bombardeada por mensajes amenazantes, por insultos, por

calumnias... a través de las nuevas tecnologías. Con lo cual hacen la vida de estas niñas (niñas y niños) insoportable.

En el *grooming* pasa igual; el *grooming* es la evolución del acoso sexual o abuso sexual de menores. Las nuevas tecnologías han permitido su internacionalización. Antes el acoso sexual a menores, que sigue ocurriendo y especialmente en el ámbito familiar, cuando se producía por extraños, era raro que se produjese hacia un menor de 13 años; ahora no es raro ver niñas víctimas de *grooming* de 11, 12 años que están siendo acosadas incluso por personas de otros países. Luego hablaremos además del problema que presentan estas niñas, especialmente niñas y niños, a la hora de la denuncia.

Y lo mismo ocurre con la pornografía infantil, que era un delito muy minoritario, que existía en círculos de pederastas muy cerrados; pero la proliferación de Internet ha hecho precisamente lo que vemos ahora, que sea uno de los delitos más usuales en Internet. Y además, especialmente en España de una forma más agravada. Hablaba el Comandante De la Cruz, antes, de la pirámide de la pornografía infantil: pues sí es verdad que nosotros disponemos de herramientas desarrolladas por varias universidades, como la Universidad de Vigo y últimamente la Universidad de Alcalá de Henares, que son buscadores que rastrea, las redes p2p; el año pasado detectamos más de 20.000 usuarios en España, personas que estaban descargando y compartiendo vídeos de pornografía infantil.

Un problema que tenemos con la pornografía infantil es que es muy difícil encontrar un lenguaje común entre profesionales. Yo les puedo hablar a ustedes de lo grave que es la pornografía infantil pero no se la puedo enseñar, ni con ustedes ni con psicólogos, ni con juristas, ni con otros profesionales, porque sería un delito. Porque la pornografía infantil no solo son fotos de niños que están posando desnudos; son vídeos de niños abusados por adultos, niños muchas veces menores de 13 años, sufriendo atroces violaciones.

Por suerte la forma como hoy se entienden la pornografía infantil ha evolucionado, cuando empezamos en el año 2001 casi nos costaba convencer de la gravedad de la pornografía infantil a algunos jueces, fiscales o profesionales, especialmente cuando la detención era por posesión de pornografía infantil, en determinados ámbitos no era raro oír «es que este hombre no hace daño a nadie», «¿y por qué este empeño en ustedes de perseguir a la gente que consume «pornografía infantil?». Hoy co-

nocemos el resultado de algunos estudios en otros países que advierten de que la gran amenaza que supone la pornografía infantil, lo primero porque promueve distorsiones cognitivas en las personas que son consumidoras. Y esto lo hemos visto, porque cuando hablábamos con estas personas cuando son detenidas, ante ciertas preguntas clave como por ejemplo «¿tú piensas que ese niño está disfrutando?», ante un niño que está siendo abusado sexualmente, te responden claramente que sí, y lo creen realmente, y que creen que el abuso sexual infantil no es tal sino que es una actividad placentera para los niños. Lo que no sabemos es si esas creencias son previas o son una consecuencia del consumo de pornografía infantil, pero es claro que mantener esas creencias es un peligro para los menores de su entorno.

También hemos constatado que la pornografía infantil está siendo usada por adultos que acosan sexualmente a niños. Esto es así en una de las fases del *grooming*, en la preparación de la víctima, el pederasta envía imágenes pornografía infantil a niños para hacer una especie de educación sexual perversa. Les dice «mira lo que hace este señor con este niño y mira lo bien que se lo pasa, ¿ves como es una cosa normal?», cambia las creencias del niño sobre las relaciones sexuales entre adultos y niños y las pervierte.

Y no menos grave también es que la pornografía infantil crea un círculo de oferta y demanda de tal forma que a medida que más gente demanda estas imágenes, mayor oferta se crea, especialmente en determinados países donde los niños están más desfavorecidos socialmente, aunque también se produce pornografía infantil incluso en España, por el beneficio a veces económico pero mayoritariamente por una motivación pedófila.

Por eso una de nuestras prioridades, y de las que más estamos trabajando, es la identificación de las víctimas. La identificación de esas víctimas, que no porque estén en otros países tienen menos derecho a que se les ponga nombre. Y además es que, hasta que no se identifique a esas víctimas, a esos niños que están siendo abusados, no se va a parar el abuso, no se va a detener a la persona que comete estos abusos, y además esas víctimas no van a recibir asistencia.

Este es uno de los problemas en los que más se han centrado las organizaciones internacionales como Interpol, consciente de que muchos de esos abusos se producen los países, pero por ciudadanos occidentales

españoles, que viajaban a países en desarrollo, en el mal llamado turismo sexual, porque no es turismo, por supuesto, es abuso sexual internacional; y eran los nacionales de la Unión Europea o de países occidentales los que iban a esos países, abusaban de niños, lo grababan, y luego distribuían por internet esas imágenes.

Otro de los problemas que trae también la transnacionalización es la movilidad de los pederastas. El año pasado, por ejemplo, la guardia civil recibió 139 alertas de Interpol de pederastas condenados en sus países, la mayoría británicos y de norteamericanos, que viajaron a España, unos en visita turística, o eso alegaron, pero otros para quedarse a vivir. Todos ellos habían sido condenados en sus países por abusar de niños o relacionados con la pornografía infantil. Pues cumpliendo la legislación de esos países (especialmente países como Reino Unido o Estados Unidos, donde la legislación es muy severa y el control que se ejerce sobre estas personas también), estas personas viajan a España; entonces, las autoridades de esos países nos lo comunican, y cuando llegan a España, desgraciadamente no podemos realizar ningún control sobre la actividad de esas personas. Incluso se ha dado la curiosa circunstancia de que algunas de estas personas han venido a España y han establecido centros educativos, cosa que en sus países tienen prohibido. Y no podemos hacer nada. La legislación española no permite ningún tipo de control ni ningún tipo de seguimiento sobre esta personas salvo que se tenga la sospecha de que han cometido un delito. Y el problema es que se crea una especie de espacio subjetivo de impunidad. Éste problema no es exclusivo de España, es un tema de debate en varios países de la unión europea.

Una de las iniciativas que se han creado en el ámbito internacional para luchar contra la pornografía infantil es el CIRCAM, que es un proyecto para bloquear el acceso a páginas de pornografía infantil, en los países donde está implantado como Bélgica, Suecia, Noruega o Dinamarca, cuando un usuario en esos países intenta acceder a una página de pornografía infantil aparece el siguiente mensaje en su ordenador «está usted intentando acceder a una página de pornografía infantil lo que constituye una infracción penal y por tanto se ha bloqueado su acceso»; en otros países incluso se le avisa que «sus datos pueden ser comunicados a la policía», dependiendo de la legislación del país. Ese proyecto se intentó establecer en España, pero por motivos de la legislación no pudo ser implantado.

Respecto a la prevención, se ha comunicado que una de las formas para mejorar la prevención de este tipo de delitos sería mejorar las vías de comunicación o denuncia de los ciudadanos. Ha mencionado el Director General de la cuenta de correo proteccion-menor@guardiacivil.org, así como del programa «Colabora» del Grupo de Delitos Telemáticos de la UCO como dos iniciativas realizadas para mejorar la comunicación con los ciudadanos. Pero somos conscientes de que no es habitual que un menor que sufre un ciberacoso, o cualquier otro tipo de delitos on-line se ponga en contacto con la Guardia Civil o con la policía para denunciar este hecho, somos muy conscientes de que eso en la mayoría de los casos no ocurre, por desgracia; lo sabemos porque en la mayoría de los casos, cuando tenemos conocimiento de un hecho, ese menor lleva muchos meses sufriendo el acoso, incluso hay quienes han tenido intentos de suicidio o han sufrido consecuencias graves.

Por eso estamos continuamente en contacto con organizaciones que se dedican a ayudar a los niños cuando sufren problemas, por ejemplo con la fundación ANAR, con Protégeles.com y con otra cualquier asociación que trabaje con niños, en un clima de mutua colaboración, de forma que cuando ellos tienen conocimiento de un niño que está siendo acosado o amenazado además de su apoyo o consejo, nosotros complementamos su actuación llegando más allá de donde ellos llegan, identificando a los autores y ofreciendo una protección más completa. También mantenemos contactos habituales con las principales redes sociales, especialmente con Tuenti. La gran ventaja de Tuenti es que es una empresa española. Hablaba antes el comandante De la Cruz, de los problemas que puede haber con ciertos proveedores de servicios que están alojados en otros países; esto no ocurre con Tuenti, y además es la red social mayoritaria en España entre los jóvenes y niños, y con ellos mantenemos una relación muy estrecha y frecuente para intercambiar información sobre amenazas que detectamos nosotros o ellos en esa red.

Hablaba antes también el Director General del Plan Director para la mejora de la convivencia escolar; quiero decirles que mi experiencia cuando voy a los colegios a participar de las clases a los alumnos sobre las amenazas en internet es que la aceptación es dispar dependiendo de a quién se dirijan: cuando son a los padres la asistencia es minoritaria, no suelen superar la decena en un colegio que algunas veces tenía hasta 2.000 alumnos. Nuestra experiencia es que la mejor línea para intervenir en los colegios es a través de los profesionales que se dedican a ello.

Es decir, nosotros preferimos formar a los tutores y demás educadores, porque ellos van a saber transmitir esa información de una forma más pedagógica a los alumnos. Nosotros somos policías, no somos educadores, podemos dar una charla de concienciación a los niños, pero es preferible que sea un profesional de la educación quien trasmita esos conocimientos.

Cuando se creó el Plan Director para la seguridad escolar, hace seis años, en el año 2007, se empezó a ir a los institutos, porque se suponía que los menores que iban a sufrir estas amenazas en internet serían chicos y chicas a partir de 13 o 14 años. Pero en estos seis años hemos visto que cada vez la edad de los menores en internet es menor. En una charla que tuve que dar yo hace unos meses en un colegio de 5º de primaria (estamos hablando de niños de 10, 11 años), la primera pregunta que les hacemos es quién tiene un perfil en Tuenti, y la mayoría de los niños levantaron la mano. Luego pregunté quién tenía una cuenta en Facebook, y cinco niños levantaron la mano, lo que me pareció más grave porque Facebook en principio no es una red concebida para niños tan pequeños. Por su puesto por WhatsApp, ni se me ocurrió preguntar.

Esto nos está haciendo replantearnos la prevención, que debe iniciarse cada vez en edades más tempranas. Además la proliferación de los dispositivos móviles también hace además que incluso en estos últimos años hayamos cambiado los consejos que damos a los padres sobre la utilización de los menores de internet, porque hemos visto que no sirven de nada consejos que se daban hace cinco años como: «tenga usted el ordenador en un sitio público en su casa», porque ahora los niños acceden a internet mayoritariamente desde su móvil; el niño puede estar a tu lado y no sabes dónde está accediendo ni lo que está escribiendo; otro consejo como «evite que los niños publiquen fotos suyas en las redes sociales», hemos visto que esto es lo primero que hacen, que es muy habitual que hagan una foto con el móvil y seguidamente la suben a su perfil. Entonces, siguiendo un poco las recomendaciones de otros países que nos llevan algunos años de ventaja en experiencia en internet (no muchos, ya cada vez menos, como por ejemplo Estados Unidos), los planes de prevención que están haciendo ellos en los colegios es una especie de educación sexual en Internet. Es decir, al igual que se hace educación sexual en los colegios, sería enseñar qué ciertos comportamientos sexuales o de comentarios de contenido sexual serían inapropiados en Internet, igual que lo son en otros ámbitos.

Incluso hemos podido ver programas preventivos en las escuelas donde los alumnos crean perfiles en internet y unos se hacen pasar por acosadores así ven lo fácil que es simular una identidad falsa y hacerse pasar por otra persona que no es, y los demás alumnos aprenden a ser precavidos con las personas que conocen por internet.

Y ya por último, señalar otra serie de problemas que nosotros detectamos en Internet, que estarían más relacionados con los contenidos que no son apropiados para menores, y que además no están penalizados en España: hablamos de páginas que contienen apología de la pederastia o apología de la anorexia, la bulimia, o de la automutilación.

La apología de la pederastia no es un delito es España. Cuando estas páginas se alojan en proveedores españoles, bien las Fuerzas y Cuerpos de Seguridad o las ONG,s que se dedican a la protección de los menores, pueden pedirles que si contravienen la condiciones de contratación de la compañía, las pueden cerrar. Pero si esa página se aloja, como es habitual, en otros servidores en otros países, pese a que sean hechas por españoles y donde se defiende la pederastia como una orientación sexual más. En estas páginas existen foros donde se dan un apoyo mutuo, se dan consejos, con lo cual vemos que puede estar ocurriendo lo que hablábamos antes con la pornografía infantil, que podamos estar reforzando ciertas conductas que luego, más adelante, puedan propiciar incluso en abuso sexual infantil.

También están incluidas en esta categoría de contenidos inapropiados las páginas de apología de la anorexia y la bulimia, páginas especialmente dañinas para los adolescentes, antes mayoritariamente chicas, y cada vez más chicos, donde se crean foros dañinos para la salud física y mental de los menores y donde se hace una apología de la anorexia, la mayoría de las veces por las menores.

Por último en relación con los contenidos inapropiados, una de las últimas tendencias es la apología del *self-injuring*, es decir, de la autolesión y el suicidio; en Reino Unido en el año 2008, tuvieron un caso de siete adolescentes que frecuentaban una de estas páginas y se suicidaron, es necesario mantener una vigilancia sobre este tipo de contenidos, antes que lamentar las consecuencias.

Y como ya se ha preguntado por varios de ustedes qué mejoras legislativas serían deseable, creemos que la actual tipificación penal del *grooming* como aquellos actos de acoso sexual a menores, que exigen,

en concreto dice el código penal «que se acompañe de actos materiales encaminados al acercamiento». El problema es que la provocación del abuso sexual infantil, lo que nosotros llamamos actos preparatorios del *grooming*, por ejemplo, un pederasta que intenta contactar con menores puede enviar un mensaje explícito de querer mantener relaciones sexuales a por ejemplo 500 menores, esperando que si de esas 500 víctimas, con que solo 5 contesten a su solicitud, es un buen porcentaje, además las posibilidades de Internet le permiten que no sean 500 sino que sean 5.000 las víctimas contactadas; ese acto, esa proposición sexual no está penalizada. Esa persona puede intentar invitar a cuantos menores quiera a actos sexuales, que mientras no realice una acción más concreta, posteriores comunicaciones, no sería perseguible. Y esto es difícil explicárselo a los padres cuando nos denuncian, evidentemente escandalizados, de que a su hija o hijo de 10, 11 o 12 años un adulto o una persona que desconocen está haciéndole propuestas sexuales. Pues para nosotros nos resulta muy difícil decir «si no ha habido actos siguientes, algún tipo de acercamiento, se queda el delito tan diluido que no hay delito. Necesitamos instrumentos legales para poder intervenir en los primeros momentos del acoso sexual y no tener que esperar a consecuencias más graves.

Muchas gracias.

COMPARECENCIA DEL DIRECTOR GENERAL DE EVALUACIÓN Y COOPERACIÓN TERRITORIAL DEL MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE, D. ALFONSO GONZÁLEZ HERMOSO DE MENDOZA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 6 DE JUNIO DE 2013.

En primer lugar agradecer la invitación a participar en esta Comisión sobre «Riesgos derivados del uso de la red en menores», un tema que preocupa de manera creciente al conjunto de sociedad y al que las administraciones públicas tenemos la obligación de dar respuesta desde los distintos ámbitos competenciales que nos son propios.

La comparecencia de los responsables del Ministerio de Educación, Cultura y Deporte estará dividida en dos partes: una primera a mi cargo en donde presentaré el marco institucional y normativo, y una segunda parte a cargo de la Directora del Instituto Nacional de Tecnología Educativas y Formación del Profesorado que presentará las acciones concretas que se están llevando a cabo, tanto desde el Ministerios, como desde el resto de administraciones educativas.

Durante las anteriores comparecencias habrán tenido ocasión de escuchar argumentos que atendían con detalle a los aspectos jurídicos, tecnológicos, así como, de mercado en los que se desarrollan las tecnologías de la información, desde el punto de vista de la seguridad y la protección de los menores.

Pocas experiencias pueden ser más desalentadoras sobre el uso de las tecnologías de la información que oír explicar a los expertos la fragilidad de nuestra presencia en las redes, la vulnerabilidad de nuestra identidad digital o la imposibilidad de borrar los rastros, deseados o no, de la presencia en la red.

A poco que escuchemos resulta evidente entender la falsa seguridad con la que, adultos y menores, desde el ordenador, la tableta o el teléfono nos exponemos a la maldad de profesionales del crimen, o de simples aficionados malintencionados que pueden destrozar nuestras vidas.

A los originarios del siglo XX nadie nos ha formado, ni podrían haberlo hecho, sobre los riesgos de Internet. Sólo la experiencia personal y

el aprendizaje informal, unidos al sentido común, posibilitan que vayamos sorteando las amenazas que surgen de manera imprevisible en el uso de las nuevas tecnologías.

Los menores, en el mundo digital como en el mundo analógico, suponiendo que pudiéramos diferenciar entre ambos, por su propia condición se encuentran en una posición de especial indefensión frente a los ataques de desaprensivos, así como en una situación de especial riesgo por su falta de juicio ante la trascendencia de sus propios actos. Nadie discute, y así lo asumen los poderes públicos, que necesitan una especial protección tanto legislativa, como por la actuación de los jueces y cuerpos de seguridad.

Pero a diferencia de lo que nos pasó a nosotros ellos si están en condiciones de aprender las competencias básicas de un ciudadano digital, y de conocer sin disimulo los riesgos a los que se enfrentan en la Red. Que los menores realicen este aprendizaje en paralelo a su inevitable inmersión en el mundo digital, es responsabilidad tanto de la escuela, como de manera fundamental de los padres. La educación es un proyecto que afecta a toda la sociedad. Sin la implicación directa del conjunto de la sociedad, ni en este, ni en ningún otro reto educativo, tendremos posibilidades de éxito.

Dicho esto, el punto de vista de las administraciones educativas, con respecto al uso de Internet por menores, aporta necesariamente una perspectiva distinta al de otras administraciones.

Así, una vez precisado que las administraciones educativas tienen el mayor compromiso por la protección de la seguridad de los menores, y que reclaman al resto de los poderes públicos responsables que actúen con el mayor de los rigores posibles sobre aquellos que dañen o intenten dañar a los menores por cualquier medio, hay que destacar que para los responsables públicos de la educación, el mayor riesgo al que nos enfrentamos como consecuencia de la revolución digital que estamos viviendo, es el de la perdida de igualdad y de competitividad de la sociedad española.

Es, la amenaza de que sólo una parte de la sociedad adquiera las competencias básicas digitales, que son, y serán de manera creciente determinantes de las oportunidades de desarrollo personal y profesional. No adquirir desde la infancia los valores, destrezas y contenidos propios de la cultura digital, en el mundo de hoy, coloca a las personas en una situa-

ción de indefensión, cuando no directamente de marginalidad, inaceptable en un estado social y democrático de derecho.

Es, la amenaza de la separación entre el mundo real en el que crecen, aprenden, se relacionan y se entretienen los jóvenes, y la educación formal que puedan recibir en la escuela. Dejar fuera a aquellos que tienen inteligencias distintas de las tradicionales, y en muchas ocasiones a los más creativos, a los emprendedores, a los que más tienen que aportar a la sociedad, es un derroche que nos podemos permitir y una injusticia inasumible.

Es, la amenaza de no saber integrar el aprendizaje formal de la escuela y las ilimitadas posibilidades de aprendizaje informal que ofertan las tecnologías. En procesos como los que vivimos en los que la educación cada vez se torna más abierta y expandida, mantener y consolidar la organización que supone la escuela es un reto esencial. La escuela es posiblemente la tecnología más potente que ha desarrollado la humanidad para alcanzar cotas más altas de justicia y prosperidad. Pero para ello tenemos que ser capaces de darle un nuevo sentido, propio de la era que nos toca vivir. Nos planteamos las transformaciones que lleva consigo introducir la tecnología en el aula, e ignoramos que muy posiblemente la verdadera revolución es la que viene de la mano de la incorporación de la educación en los dispositivos móviles que nos acompañan, a lo largo de nuestra vida y en todos sus momentos.

Es, la amenaza de entregar, como ha sucedido en otros sectores culturales o económicos, una actividad extremadamente sensible como es la educación a corporaciones internacionales, de convertir la actividad de aprendizaje de nuestros menores en una nueva mercancía de información para los gigantes de la red. Todas las distopías existentes basadas en la manipulación de las personas desde la traza de la privacidad que deja el uso de las tecnologías de la información, quedarían en una historia menor si se pudiera monitorizar y explotar los datos de una persona a lo largo de su aprendizaje desde la infancia. Estos datos suponen una información todavía más sensible y determinante que el conocimiento del código genético.

Es, la amenaza de quedar al margen de las transformaciones de la educación que se están experimentado en las naciones de nuestro ámbito cultural. La incorporación generalizada y adecuada las tecnologías de la información a los procesos de aprendizaje se muestra como el arma más

poderosa de cambio social para responder a los retos de una sociedad cada vez más justa, abierta y global, en donde la única certeza que somos capaces de atesorar es la de la inevitabilidad del cambio. Tecnología, sí. Tecnología para poder responder a los retos de la defensa y la promoción de la cultura propia en un entorno global. Tecnología para alcanzar la personalización en el aprendizaje, para poder aprender a lo largo de toda la vida. Para hacer una sociedad más competitiva, igualitaria y sostenible.

Con el uso de las tecnologías no se pretende resolver un problema de eficiencia del sistema educativo, de hacer más por menos, ni de alcanzar los mismos objetivos por vías alternativas. Hablamos de la oportunidad de transformar qué y cómo se aprende, para dar respuesta desde el sistema educativo a las exigencias de una sociedad en permanente cambio. Hablamos de poder atender a las demandas de una sociedad del siglo XXI. Una sociedad que está viviendo en un brevísimo periodo de tiempo una revolución que, a buen seguro, determinará un cambio de era. Todavía nos falta distancia para poder valorar lo que supone la nueva cotidianeidad que trae consigo la posibilidad de acceder a la información en cualquier lugar, en cualquier momento, de manera ilimitada y casi gratuita. Hablamos de una educación que integre de manera natural la adquisición de las competencias adecuadas para convivir en una sociedad intensiva en el uso de las tecnologías de la información, y por ende, global, abierta y crecientemente competitiva. En definitiva, hablamos de formar a los ciudadanos del siglo XXI. Éste es el desafío al que se enfrentan en la actualidad los sistemas educativos de todo el mundo, y al que nos enfrentamos también en España

En definitiva, el mayor riesgo al cual se enfrenta la sociedad en un momento de cambio radical, como el que vivimos, es el de no disponer de un sistema educativo que garantice, no sólo la escolarización, sino el acceso a una educación de calidad.

Para ello es importante romper los viejos clichés con los que se suelen enfrentar los temas sobre Internet, y en especial en su relación con la educación. No existe la realidad, por un lado, y un mundo virtual, por otro. Vivimos en una única realidad, una realidad emergente que integra plena y naturalmente lo analógico y digital. De la misma manera que sólo existe una educación. Una educación que utiliza todos los recursos disponibles para formar a personas autónomas y responsables, a ciudadanos comprometidos con la justicia, la libertad y la prosperidad de sus

comunidades. Lo digital y lo analógico forman parte de nuestras vidas en un continuo indisoluble. Así sucede en lo positivo, habiéndose desarrollado gracias a las tecnologías de la información cadenas de apoyo mutuo en lo político, empresarial o social que han cambiado el mundo, así como han surgido oportunidades de desarrollo para cualquier persona, sencillamente, imposibles de imaginar hace unas décadas. Pero también, por desgracia, esa integración se ha dado en las miserias y crueldades de las que ninguna sociedad está libre. Internet ofrece un nuevo entorno que abre nuevas e inesperadas oportunidades de desarrollo personal y social, pero que también da nuevas oportunidades de expresión a la maldad humana.

Así, tan importante como es disponer de la adecuada formación para la convivencia democrática en los entornos digitales, lo es no banalizar las consecuencias del mal uso de la tecnología. Cegados por la pasión por el progreso o por la tecnología, en algunas ocasiones, otras veces simplemente llevados por la ignorancia o la codicia, no es infrecuente el que se quiera minimizar la importancia de la inmoralidad o la ilegalidad de un acto por el hecho de que se realice en los entornos digitales.

Cuanto más libre y abierto es un espacio, como sucede con Internet, más importante es perseguir a los antisociales que pretenden apropiarse o beneficiarse de él. El respeto a la dignidad humana no puede subordinarse a incertidumbres tecnológicas. Debemos seguir reservando la sanción más enérgica a aquellos que amenacen la pacífica convivencia, de manera especial si es atacando el bien más preciado de la sociedad, los menores.

La incertidumbre no puede justificar la arbitrariedad. En situaciones de incertidumbre las sociedades miran a la educación. Miran a los valores, a las personas. Por eso nunca como ahora la formación ha sido tan determinante de la riqueza y de la calidad democrática de una sociedad. Gestionar la incertidumbre que genera un mundo en cambio permanente, globalizado, abierto, y crecientemente tecnológico, hace imprescindible garantizar una formación universal y de calidad, arraigada en los principios y valores constitucionales.

Cuando Max Weber, visita Estados Unidos en 1904 no sólo tiene ocasión de experimentar la importancia del protestantismo en la configuración de este país y valorar su naciente organización burocrática y política. También tiene ocasión de sentir ante sí, al subir al piso 12 del

rascacielos en el que se encontraba su Hotel en Chicago, la emergencia de la enorme transformación que para las formas de convivencia se avecinaban al divisar por primera vez en toda su plenitud una gran ciudad moderna. Internet es la gran ciudad del siglo XXI.

Es la obligación de los poderes públicos implicados en la educación el aprovechar esta realidad e, impulsar propuestas formativas que reduzcan el abandono escolar, haciendo intrínsecamente interesante y motivador el estudio y aprendizaje, así como, que atiendan de manera personalizada las demandas de formación de cada alumno, considerando la diversidad de talentos e intereses de cada persona, de igual modo que sus circunstancias socioeconómicas y culturales.

En definitiva, el reto de las administraciones educativas es aprovechar las oportunidades que ofrece la gran ciudad de Internet, para formar a los nuevos ciudadanos, a los ciudadanos digitales. Hoy día una educación igualitaria y de calidad pasa por el uso de las tecnologías, por la formación en competencias digitales. Buscar, jerarquizar, compartir y utilizar información, gestionar la identidad digital o protegerse de la ciberdelincuencia son los atributos básicos de una ciudadanía del siglo XXI.

Antes de pasar a ver la situación en concreto desde el punto de vista normativo, quisiera destacar un aspecto en la transformación de la educación que estamos viviendo, que con frecuencia queda diluido por la preminencia que se concede a la tecnología. El sistema educativo, sin duda, debe tener su centro en el alumno, pero directa e inseparablemente unido a la institución de la escuela y a la figura del maestro. La escuela como espacio de relación e intercambio, entre pares y con la sociedad, y el maestro, por encima de la pedagogía, como tutor y mediador en proceso aprendizaje. El protagonismo de la institución escolar crece en la medida en que nos dirigimos a una sociedad más abierta, compleja y global. La figura del maestro crece en relevancia en la medida en que busquemos la personalización del aprendizaje y el desarrollo de la autonomía personal del alumno. El gran descubrimiento de la transformación educativa que estamos viviendo es, el maestro.

Cambiando de punto de vista de la intervención y para empezar a hablar del marco institucional y normativo de los riesgos de los menores por el uso de las tecnologías de la información, destacar que las políticas educativas son deudoras de las muy abundantes normas generales de apoyo y protección a los menores. De manera especial:

- **La Convención sobre los Derechos del Niño de Naciones Unidas**, de 20 de noviembre de 1989 ratificada por el Estado Español en el año 1990, que en su artículo 19 recoge el derecho del niño o niña a vivir sin sufrir ningún tipo de violencia o maltrato y la obligación de los Estados parte de garantizar este derecho. Contempla, además, como principio básico de las actuaciones de las instituciones competentes el interés superior del niño.
- **La Carta Europea de los Derechos del Niño,** de 21 de septiembre de 1992, que en su apartado 8.19 establece que *«Los Estados miembros…deben otorgar protección especial a los niños y niñas víctimas de tortura, malos tratos por parte de los miembros de su familia…debe asegurarse la continuación de su educación y el tratamiento adecuado para su reinserción social».*
- **La Recomendación del Consejo (98/560/CE)** de 24 de septiembre de 1998, relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana *recomienda establecer marcos nacionales para la protección de menores con la finalidad de promover el acceso y el uso responsable de los medios.*
- **Carta de los Derechos Fundamentales de la Unión Europea (18/12/2000)**. Entre los derechos que se encuentran recogidos en la dicha carta están *el derecho al respeto de la vida privada y las comunicaciones y el derecho a la protección de los datos de carácter personal.* En su artículo 24 se centra en los derechos del menor exponiendo que *«Los menores tienen derecho a la protección y a los cuidados necesarios para su bienestar. Podrán expresar su opinión libremente. Ésta será tenida en cuenta en relación con los asuntos que les afecten, en función de su edad y de su madurez».* También se afirma que *«**En todos los actos relativos a los menores llevados a cabo por autoridades públicas o instituciones privadas, el interés superior del menor constituirá una consideración primordial**».*
- **La Directiva 2000/31/CE** del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el

comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).En ella se hace *referencia a la protección del menor* en su consideración 10 y en sus artículos 3, 16 y 21, relativos a la identificación de delitos y la elaboración de códigos de conducta.

- **La Directiva 2002/58/CE** relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Esta directiva tiene como objetivo garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, *del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales* en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad.
- **La Recomendación del Parlamento Europeo y del Consejo (2006/952/CE)** de 20 de diciembre de 2006, *relativa a la protección de los menores y de la dignidad humana* y al derecho de réplica en relación con la competitividad de la industria europea de servicios audiovisuales y de información en línea. Se recomienda a los Estados la incentivación de acciones que identifiquen contenidos y servicios de calidad para menores y el acceso a ellos. También se recomienda combatir las actividades ilícitas que son perjudiciales para los menores. Por otro lado, se recomienda al sector de servicios audiovisuales y de la información que pongan en marcha medidas que faciliten el acceso a los menores a la vez que se evitan los contenidos perjudiciales, por ejemplo con sistemas de filtrado, etiquetado, etc. En su anexo II *se hace referencia a la formación de los profesores y a la de los menores para favorecer la alfabetización en los medios de comunicación*, y en su anexo III se exponen ejemplos de acciones que pueden llevar a cabo las industrias y partes interesadas en beneficio de los menores.
- **COM(2011) 556 El Informe de la Comisión** al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la aplicación de la Recomendación del Consejo, de 24 de septiembre de 1998, *relativa a la protección de los menores y de la dignidad humana* y de la Recomendación del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006,

relativa a la protección de los menores y de la dignidad humana y al derecho de réplica en relación con la competitividad de la industria europea de servicios audiovisuales y de información en línea « La Protección de los Menores en el Mundo Digital» donde se hace referencia a la necesidad de intensificar los esfuerzos contra los contenidos ilícitos y perjudiciales para los menores y a la denuncia de estos. A este respecto se menciona la existencia del programa de la Comisión «Safer Internet», que ha implantado líneas directas de denuncia en todos los estados miembros, si bien se detectan importantes diferencias entre la efectividad en los distintos países. Se insta también a los Proveedores de Servicios de Internet (PSI) a que supervisen la aplicación de los códigos de conducta y a que, a pesar de ser voluntario, incluyan la protección de menores en sus mandatos.

Se recomienda también un mayor control de la redes sociales, los acuerdos para la cooperación en la protección de menores de los contenidos procedentes de otros países, la continuación de la alfabetización mediática, y la mejoría de los sistemas de clasificación de acuerdo con la edad y el contenido (incluidos los juegos, donde el sistema de clasificación PEGI apenas tiene impacto).

- **COM(2012) 196 El Informe de la Comisión** al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia europea en favor de un Internet más adecuado para los niños. Se presenta la necesidad de un ecosistema para los usuarios específicos que son los menores y de una estrategia que cree un entorno en línea más seguro para ellos. Esta estrategia se apoya en 4 pilares: los contenidos en línea de alta calidad para niños y jóvenes (estimulando la creación de los contenidos y promoviendo las experiencias positivas), intensificar la capacitación y la sensibilización (alfabetización mediática y enseñanza de seguridad en línea en la escuela, actividades para jóvenes y herramientas de denuncia), la creación de un entorno en línea seguro (parámetros de confidencialidad, control parental, clasificaciones por edades y contenidos, protección de la publicidad y de los gastos en línea excesivos) y la lucha contra los abusos y la explotación sexual de los niños (Identificación, denuncia y retirada de la pornografía infantil, cooperación internacional en la lucha contra los abusos y la explotación sexual de menores). Se propo-

nen acciones a La Comisión Europea, a los Estados miembros y a la industria.

- **La Convención sobre los Derechos del Niño de Naciones Unidas**, de 20 de noviembre de 1989 ratificada por el Estado Español en el año 1990, que en su artículo 19 recoge el derecho del niño o niña a vivir sin sufrir ningún tipo de violencia o maltrato y la obligación de los Estados parte de garantizar este derecho. Contempla, además, como principio básico de las actuaciones de las instituciones competentes el interés superior del niño.
- **La Carta Europea de los Derechos del Niño,** de 21 de septiembre de 1992, que en su apartado 8.19 establece que *«Los Estados miembros…deben otorgar protección especial a los niños y niñas víctimas de tortura, malos tratos por parte de los miembros de su familia…debe asegurarse la continuación de su educación y el tratamiento adecuado para su reinserción social».*
- **La Recomendación del Consejo (98/560/CE)** de 24 de septiembre de 1998, relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana *recomienda establecer marcos nacionales para la protección de menores con la finalidad de promover el acceso y el uso responsable de los medios.*
- **Carta de los Derechos Fundamentales de la Unión Europea (18/12/2000)**. Entre los derechos que se encuentran recogidos en la dicha carta están *el derecho al respeto de la vida privada y las comunicaciones y el derecho a la protección de los datos de carácter personal.* En su artículo 24 se centra en los derechos del menor exponiendo que *«Los menores tienen derecho a la protección y a los cuidados necesarios para su bienestar. Podrán expresar su opinión libremente. Ésta será tenida en cuenta en relación con los asuntos que les afecten, en función de su edad y de su madurez».* También se afirma que ***«En todos los actos relativos a los menores llevados a cabo por autoridades públicas o instituciones privadas, el interés superior del menor constituirá una consideración primordial»***.
- **La Directiva 2000/31/CE** del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos

de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).En ella se hace *referencia a la protección del menor* en su consideración 10 y en sus artículos 3, 16 y 21, relativos a la identificación de delitos y la elaboración de códigos de conducta.

- **La Directiva 2002/58/CE** relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Esta directiva tiene como objetivo garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, *del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales* en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad.
- **La Recomendación del Parlamento Europeo y del Consejo (2006/952/CE)** de 20 de diciembre de 2006, *relativa a la protección de los menores y de la dignidad humana* y al derecho de réplica en relación con la competitividad de la industria europea de servicios audiovisuales y de información en línea. Se recomienda a los Estados la incentivación de acciones que identifiquen contenidos y servicios de calidad para menores y el acceso a ellos. También se recomienda combatir las actividades ilícitas que son perjudiciales para los menores. Por otro lado, se recomienda al sector de servicios audiovisuales y de la información que pongan en marcha medidas que faciliten el acceso a los menores a la vez que se evitan los contenidos perjudiciales, por ejemplo con sistemas de filtrado, etiquetado, etc. En su anexo II *se hace referencia a la formación de los profesores y a la de los menores para favorecer la alfabetización en los medios de comunicación*, y en su anexo III se exponen ejemplos de acciones que pueden llevar a cabo las industrias y partes interesadas en beneficio de los menores.
- **COM(2011) 556 El Informe de la Comisión** al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la aplicación de la Recomendación del Consejo, de 24 de septiembre de 1998, *relativa a la protección de los menores y de la dignidad humana* y de la Recomendación del

Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativa a la protección de los menores y de la dignidad humana y al derecho de réplica en relación con la competitividad de la industria europea de servicios audiovisuales y de información en línea « La Protección de los Menores en el Mundo Digital» donde se hace referencia a la necesidad de intensificar los esfuerzos contra los contenidos ilícitos y perjudiciales para los menores y a la denuncia de estos. A este respecto se menciona la existencia del programa de la Comisión «Safer Internet», que ha implantado líneas directas de denuncia en todos los estados miembros, si bien se detectan importantes diferencias entre la efectividad en los distintos países. Se insta también a los Proveedores de Servicios de Internet (PSI) a que supervisen la aplicación de los códigos de conducta y a que, a pesar de ser voluntario, incluyan la protección de menores en sus mandatos.

Se recomienda también un mayor control de la redes sociales, los acuerdos para la cooperación en la protección de menores de los contenidos procedentes de otros países, la continuación de la alfabetización mediática, y la mejoría de los sistemas de clasificación de acuerdo con la edad y el contenido (incluidos los juegos, donde el sistema de clasificación PEGI apenas tiene impacto).

- **COM(2012) 196 El Informe de la Comisión** al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia europea en favor de un Internet más adecuado para los niños. Se presenta la necesidad de un ecosistema para los usuarios específicos que son los menores y de una estrategia que cree un entorno en línea más seguro para ellos. Esta estrategia se apoya en 4 pilares: los contenidos en línea de alta calidad para niños y jóvenes (estimulando la creación de los contenidos y promoviendo las experiencias positivas), intensificar la capacitación y la sensibilización (alfabetización mediática y enseñanza de seguridad en línea en la escuela, actividades para jóvenes y herramientas de denuncia), la creación de un entorno en línea seguro (parámetros de confidencialidad, control parental, clasificaciones por edades y contenidos, protección de la publicidad y de los gastos en línea excesivos) y la lucha contra los abusos y la explotación sexual de los niños (Identificación, denuncia y retirada de la pornografía infantil, cooperación internacional en la lucha

contra los abusos y la explotación sexual de menores). Se proponen acciones a La Comisión Europea, a los Estados miembros y a la industria.

En el ámbito estrictamente educativo la Ley Orgánica 2/2006, de 3 de mayo, de Educación se refiere a la protección de datos del menor en su Disposición adicional vigésimo tercera, relativa a los datos personales de los alumnos. Específicamente se menciona la obtención de datos e información de los alumnos, su tratamiento y la cesión de estos.

En el Preámbulo del Proyecto de Ley Orgánica para la Mejora de la Calidad de la educación, se señala:*»Asimismo, el uso responsable y ordenado de estas nuevas tecnologías por parte de los alumnos debe estar presente en todo el sistema educativo».*

«Artículo 111.bis. Tecnologías de la Información y la Comunicación.

1. El Ministerio de Educación, Cultura y Deporte establecerá, previa consulta a las Comunidades Autónomas, los estándares que garanticen la interoperabilidad entre los distintos sistemas de información utilizados en el Sistema Educativo Español, en el marco del Esquema Nacional de

Interoperabilidad previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

Para ello, se identificarán los tipos básicos de sistemas de información utilizados por las Administraciones educativas, tanto para la gestión académica y administrativa como para el soporte al aprendizaje, y se determinarán las especificaciones técnicas básicas de los mismos y los distintos niveles de compatibilidad y seguridad en el tratamiento de los datos que deben alcanzar. Dentro de estas especificaciones se considerarán especialmente relevantes las definiciones de los protocolos y formatos para el intercambio de datos entre sistemas de información de las Administraciones educativas.

Estas medidas también irán encaminadas a potenciar y a facilitar el aprovechamiento de los registros administrativos en el marco de las estadísticas educativas estatales, para posibilitar la ampliación de la información estadística referida al alumnado, el profesorado, los centros y las gestiones educativas, lo que redundará en la mejora de las herramientas de análisis y de seguimiento de la actividad educativa y de las medidas de mejora de la calidad del Sistema Educativo Español.

2. Los entornos virtuales de aprendizaje que se empleen en los centros docentes sostenidos con fondos públicos facilitarán la aplicación de planes educativos específicos diseñados por los docentes para la consecución de objetivos concretos del currículo, y deberán contribuir a la extensión del concepto de aula en el tiempo y en el espacio. Por ello deberán, respetando los estándares de interoperabilidad, permitir a los alumnos el acceso desde cualquier sitio y en cualquier momento a los entornos de aprendizaje disponibles en los centros docentes en los que estudien, y con pleno respeto a lo dispuesto en la normativa aplicable en materia de propiedad intelectual.

3. El Ministerio de Educación, Cultura y Deporte establecerá, previa consulta a las Comunidades Autónomas, los formatos que deberán ser soportados por las herramientas y sistemas de soporte al aprendizaje en el ámbito de los contenidos educativos digitales públicos con el objeto de garantizar su uso, con independencia de la plataforma tecnológica en la que se alberguen.

4. El Ministerio de Educación, Cultura y Deporte ofrecerá plataformas digitales y tecnológicas de acceso a toda la comunidad educativa, que podrán incorporar recursos didácticos aportados por las Administraciones educativas y otros agentes para su uso compartido. Los recursos deberán ser seleccionados de acuerdo con parámetros de calidad metodológica, adopción de estándares abiertos y disponibilidad de fuentes que faciliten su difusión, adaptación, reutilización y redistribución y serán reconocidos como tales.

5. Se promoverá el uso, por parte de las Administraciones educativas y los equipos directivos de los centros, de las tecnologías de la información y las comunicaciones en el aula, como medio didáctico apropiado y valioso para llevar a cabo las tareas de enseñanza y aprendizaje.

6. El Ministerio de Educación, Cultura y Deporte elaborará, previa consulta a las Comunidades Autónomas, un marco común de referencia de competencia digital docente que oriente la formación permanente del profesorado y facilite el desarrollo de una cultura digital en el aula.»

En cuanto a la situación actual en relación con las competencias digitales en el curriculum. Señalar que l*a formación del alumnado, tanto en el respeto a los derechos individuales como en el buen uso de los medios que la tecnología pone a su alcance* de acuerdo con la normativa vigen-

te deberán estar presentes con carácter transversal en todas las áreas y materias y, además, se desarrollarán de forma más específica en algunas de las áreas y materias que componen el currículo, cuyas enseñanzas mínimas están definidas en los Reales Decretos que se mencionan más adelante y que, a su vez, aparecen recogidas en el desarrollo normativo de las diferentes administraciones y en los proyectos educativos de cada uno de los centros.

En este sentido es preciso destacar, en primer lugar, que la Ley Orgánica 2/2006, de 3 de mayo, de Educación señala que, tanto el respeto a los valores y las normas de convivencia como el conocimiento y el uso adecuado de las tecnologías de la información, constituyen objetivos prioritarios de las distintas etapas de la educación básica y de bachillerato. Así lo recogen respectivamente, los artículos 17.a) y 17.i) para la Educación Primaria, 23.a) y 23 e) para la Educación Secundaria, y 33 a) y g) para el Bachillerato.

Educación Primaria. Objetivos generales de la etapa

En consonancia con lo anterior, el Real Decreto 1513/2006, de 7 de diciembre, por el que se establecen las enseñanzas mínimas de la Educación Primaria, señala en el artículo 3.i) que uno de los objetivos de la etapa será *«iniciarse en la utilización, para el aprendizaje, de las tecnologías de la información y la comunicación desarrollando un espíritu crítico ante los mensajes que reciben y elaboran»,* y más adelante, en el artículo 4.5 se establece que, *«sin perjuicio de su tratamiento específico en alguna de las áreas de la etapa, la comprensión lectora, la expresión oral y escrita, la comunicación audiovisual, las tecnologías de la información y la comunicación y la educación en valores se trabajarán en todas las áreas».*

En el Anexo I del citado Real Decreto se determina que se incorporan las competencias básicas al currículo puesto que permiten poner el acento en aquellos aprendizajes que se consideran imprescindibles. Una de las ocho competencias básicas es *«Tratamiento de la Información y competencia digital»,* competencia que debe haber desarrollado los jóvenes al finalizar la enseñanza obligatoria para poder lograr su realización personal, ejercer la ciudadanía activa, incorporarse a la vida adulta de manera satisfactoria y ser capaz de desarrollar un aprendizaje permanente a lo largo de la vida. El tratamiento de la información y la competencia digital implican ser una persona autónoma, eficaz, responsable, crítica y

reflexiva al seleccionar, tratar y utilizar la información y sus fuentes, así como las distintas herramientas tecnológicas; también tener una actitud crítica y reflexiva y respetar las normas de conducta acordadas socialmente para regular el uso de la información y sus fuentes en los distintos soportes.

Educación Secundaria. Objetivos generales de la etapa

Del mismo modo, el Real Decreto 1631/2006, de 29 de diciembre, por el que se establecen las enseñanzas mínimas correspondientes a la Educación Secundaria Obligatoria, y al Real Decreto 1190/2012, de 3 de agosto, por el que se modifican el Real Decreto 1513/2006, de 7 de diciembre, por el que se establecen las enseñanzas mínimas de la Educación Primaria, y el Real Decreto 1631/2006, de 29 de diciembre, por el que se establecen las enseñanzas mínimas correspondientes a la Educación Secundaria Obligatoria, entre los objetivos de la etapa enumerados en el artículo 3 se encuentran, tanto la formación en el respeto a los derechos humanos y en la convivencia, como la adquisición de una preparación básica en el campo de las tecnologías, especialmente las de la información y la comunicación. Cabe añadir además que entre las competencias básicas que el alumnado debe alcanzar al finalizar la Educación Secundaria Obligatoria y que se recogen en el anexo I del citado Real Decreto figuran tanto *«la competencia digital como la social y ciudadana»* y que ambas resultan fundamentales para la consecución de los objetivos citados.

Desarrollo curricular por materias

Informática. Se establece que ésta tendrá entre sus objetivos: «Adoptar las conductas de seguridad activa y pasiva que posibiliten la protección de los datos y del propio individuo en sus interacciones en Internet». En consonancia con esto, dentro de los bloques de contenidos de la materia el primero está dedicado a la seguridad en Internet y, en el último, que profundiza en Internet y las redes sociales virtuales, se indica que se incluirá como contenido específico la «adquisición de hábitos orientados a la protección de la intimidad y la seguridad personal en la interacción en entornos virtuales: acceso a servicios de ocio».

Bachillerato. Objetivos generales de la etapa

Por último, el Real Decreto 1467/2007, de 2 de noviembre, por el que se establece la estructura del Bachillerato y se fijan sus enseñanzas

mínimas, se refiere también a este aspecto en varios puntos. Así, dentro de los objetivos de la etapa definidos en su artículo 3 se señala que uno de ellos será «utilizar con solvencia y responsabilidad las tecnologías de la información y la comunicación».

Desarrollo curricular por materias

Ciencias para el Mundo Contemporáneo. De acuerdo con lo que establece el Real Decreto 1467/2007, de 2 de noviembre, por el que se establece la estructura del Bachillerato y se fijan sus enseñanzas mínimas, uno de los objetivos de la materia será «*Adquirir un conocimiento coherente y crítico de las tecnologías de la información, la comunicación y el ocio presentes en su entorno, propiciando un uso sensato y racional de las mismas para la construcción del conocimiento científico, la elaboración del criterio personal y la mejora del bienestar individual y colectivo*».

Cultura audiovisual. Según el citado Real Decreto 1467/2007, uno de los criterios de evaluación de la materia será *«Identificar las posibilidades de las tecnologías de la información y la comunicación, con especial atención a los medios de comunicación de libre acceso como Internet.»* Y, a continuación, a este respecto se especifica lo siguiente: *«A través de este criterio se observará la asimilación de la utilidad y oportunidades que ofrecen los medios audiovisuales, evaluando todos sus aspectos positivos y, también, aquellos otros que puedan ofrecer contenidos ilícitos o ilegales.»*

Tecnologías de la información y la comunicación. Conforme a la Resolución de 25 de agosto de 2008, de la Secretaría de Estado de Educación y Formación, por la que se organiza la oferta de materias optativas en el Bachillerato, uno de los objetivos básicos de esta materia será *«adoptar las conductas de seguridad activa y pasiva que posibiliten la protección de los datos y del propio individuo en sus interacciones en Internet y en la gestión de recursos y aplicaciones locales».*

La revisión curricular que traerá consigo la LOMCE es una oportunidad excepcional para profundizar en la plena incorporación del aprendizaje por competencias, tan necesario y tan reclamado por la Unión Europea y por la OCDE, en el sistema educativo español, y dentro de ellas de manera fundamental las competencias digitales.

Otras actuaciones en las que participa el Ministerio de Educación, Cultura y Deporte

Observatorio Estatal de la Convivencia Escolar

Se crea mediante el Real Decreto 275/2007, de 23 de febrero, el *Observatorio Estatal de la Convivencia Escolar*, cuya misión consiste en asesorar sobre todo tipo de situaciones relativas al aprendizaje de la convivencia escolar, elaborar informes y estudios, hacer un diagnóstico en materia de convivencia escolar, y proponer medidas que ayuden a elaborar las distintas políticas estatales.

En 2012 el Observatorio publicó un extenso informe sobre *Actuaciones para el impulso y mejora de la convivencia escolar en las Comunidades Autónomas*, en él se recoge específicamente *a la necesidad de prevenir la violencia en el entorno de las tecnologías de la comunicación.*

Plan Director para la Convivencia y la Mejora escolar.

Dentro del Acuerdo Marco de Colaboración en educación para la mejora de la seguridad, suscrito en diciembre de 2006 por los Ministerios de Educación y Ciencia y del Ministerio del Interior, durante el curso 2012-2013 está implantado el III Plan Director para la Convivencia y mejora de la seguridad escolar.

Dentro de las actuaciones previstas por el plan se incluyen sesiones de formación al alumnado sobre determinados problemas de seguridad que les afectan especialmente como colectivo, entre los cuales figuran como tema destacado *los riesgos asociados a Internet y a las nuevas tecnologías.* Sirva como ejemplo de ello, que en el segundo trimestre del presente curso escolar 2012/13, en el Plan Director para la Convivencia y la Mejora escolar en la Comunidad de Madrid, el 52,6% de las 2.161 actuaciones realizadas de prevención dirigidas a alumnos, han tenido como tema: *Los riesgos en Internet*

Observatorio de la Infancia

Asimismo el Ministerio de Educación, Cultura y Deporte participa en el Observatorio de la Infancia, creado por Acuerdo de Consejo de Ministros de fecha 12 de marzo de 1999, que tiene por objeto la construcción de un sistema de información con capacidad para conocer el bienestar y calidad de vida de la población infantil, integrado como órgano colegiado en el Ministerio de Sanidad, Servicios Sociales e Igualdad.

El Ministerio de Educación, Cultura y Deporte también trabaja y colabora en el II Plan Estratégico Nacional de la Infancia y la Adolescen-

cia 2012-2015 (PENIA II), en el objetivo de la educación en valores y prevención del conflictos: potenciar valores basados en la convivencia, el respeto y el buen trato, evitando las situaciones de conflicto escolar, y en el III Plan de Acción contra la Explotación Sexual de la Infancia y la Adolescencia 2010-2013 (PESI III), concretamente en el desarrollo de campañas de información y sensibilización social dirigidas a niños, niñas y adolescentes sobre riesgos y factores de protección de posibles situaciones de explotación sexual y sensibilización a la sociedad en general y a los niños y niñas en particular, sobre USO SEGURO DE LAS TIC

También, en el Proyecto de Ley Orgánica para Mejora de la Calidad Educativa (LOMCE) se profundiza en la obligación que tienen los centros educativos en elaborar un plan de convivencia y se concreta, que en el caso de *aquellas conductas que atenten contra la dignidad personal de otros miembros de la comunidad educativa, que tengan una implicación de género, sexual, racial o xenófoba o de discapacidad, o que se realicen contra el alumnado más vulnerable por sus características personales, sociales o educativas tendrán la calificación de falta muy grave y llevarán asociada como medida correctora la expulsión, temporal o definitiva, del centro* (nueva redacción del artículo 124 de la LOE).

Las redes sociales en Internet es el medio de comunicación más usado por los alumnos, tanto dentro como fuera del aula. Los padres de los menores y los centros escolares no pueden desconocer los riesgos que conlleva el uso de las redes, pero tampoco pueden ignorar el mundo de oportunidades que se abren con ellas. No hay que olvidar que el menor de hoy en día, es el futuro ciudadano de mañana, que vive y vivirá en un mundo digital. Es importante poner el foco no tanto en los riesgos, aunque no hay que restarles importancia para poder prevenirlos o actuar contra ellos, cuanto en el desarrollo *de las capacidades o posibilidades que ofrecen para los alumnos, profesores o cualquier ciudadano.* Todas las administraciones y especialmente el Ministerio de Educación, Cultura y Deporte deben colaborar en la formación de ese ciudadano en la toma de medidas de prevención ante los posibles abusos que puedan surgir de la utilización de las redes sociales, y por supuesto, en la intervención para salvaguardar los derechos irrenunciables de los menores.

COMPARECENCIA DE LA DIRECTORA DEL INSTITUTO NACIONAL DE TECNOLOGÍAS EDUCATIVAS Y DE FORMACIÓN DEL PROFESORADO (INTEF), DÑA. ANA MARÍA ROMÁN RIECHMAN, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 6 DE JUNIO DE 2013.

La enorme expansión que en los últimos años ha experimentado el uso de las tecnologías de la información, ha convertido a las redes sociales en Internet en uno de los medios de comunicación más usados por el alumnado, tanto dentro como fuera de los centros educativos.

Entre los menores el uso del ordenador es prácticamente universal (95,6%), mientras que el 87,1% utiliza Internet. Esa facilidad de acceso y familiaridad con el uso de los nuevos medios les expone a una serie de riesgos sobre los que no siempre han recibido suficiente formación. No son plenamente conscientes de las consecuencias personales y legales que pueden derivarse de determinadas prácticas, y no toman en consideración el hecho de que cualquier información que se pone a disposición de un tercero, por la facilidad que da el medio, puede terminar siendo usada en un contexto totalmente diferente, incluso para hacer daño a otros o a ellos mismos.

Los riesgos más graves son aquellos que afectan a la integridad, tanto física como emocional, de los menores, en especial el «ciberbullying», el «grooming» y el «sexting». No es fácil evitarlos, no son infrecuentes y, aunque no se produzca agresión física por parte de los acosadores, los efectos sobre la víctima pueden ser devastadores.

Para paliar la situación el Ministerio de Educación, Cultura y Deporte sigue una serie de estrategias, algunas de las cuales han sido expuestas por el Director General en la anterior comparecencia, por lo que me centraré en las restantes, que se refieren a los siguientes ámbitos:

— Acciones del INTEF sobre «Riesgos derivados del uso de la Red por parte de los menores».
— Actuaciones en colaboración con otros ministerios.
— Actuaciones más significativas realizadas por las comunidades autónomas.

— Otras iniciativas de ámbito nacional.
— Iniciativas de ámbito europeo.

1. Acciones del INTEF sobre «Riesgos derivados del uso de la Red por parte de los menores»

El Instituto Nacional de Tecnologías Educativas y Formación del Profesorado, INTEF, como unidad del Ministerio de Educación, Cultura y Deporte responsable de la integración de las TIC en las etapas educativas no universitarias, es muy sensible a las necesidades de formación docente que genera el uso de Internet por los menores.

Los riesgos asociados a ese uso han desencadenado a veces actitudes de prohibición que en realidad no resuelven el problema. Un problema que debe enfocarse mediante la formación de los estudiantes, a los que se debe otorgar un nivel adecuado de competencia digital, que es una de las competencias básicas del currículo, para que tengan los conocimientos, destrezas y actitudes necesarias en relación con el uso seguro de los nuevos medios digitales.

Son encomiables todas las iniciativas que desarrollan para la protección del menor en la Red. Las charlas y actos con participación de representantes de las fuerzas de seguridad, en las que se dan advertencias sobre los peligros que existen, son muy convenientes y cuentan con todo nuestro apoyo. Pero esto aún no es suficiente para que los menores puedan usar la Red de forma habitual y segura. Su logro debe ser un objetivo compartido por padres, profesores y el resto de la sociedad.

El profesorado es el factor clave para que los estudiantes desarrollen las competencias básicas necesarias tanto para su futuro desempeño profesional como en su aprendizaje permanente a lo largo de la vida, y desde el INTEF se acomete el reto de su apoyo mediante distintos proyectos formulados conjuntamente con las CCAA y que se agrupan en dos grandes planes:

— *Plan de Cultura Digital en la Escuela*, en el ámbito de las tecnologías educativas.

— *Marco de Desarrollo Profesional Docente,* en el ámbito de formación del profesorado.

En el primero se incluyen cinco líneas prioritarias:

Conectividad de Centros Escolares
Interoperabilidad y estándares:
Espacio de contenidos en abierto
Catálogo General de Recursos Educativos
Competencia Digital Docente

En esta esta última, la Comisión Europea encargó hace dos años a través de su Dirección General de Educación y Cultura a IPTS (The Institute for Prospective Technological Studies) la elaboración de un marco común europeo de competencia digital, en cuyo borrador final se está trabajando y será publicado en fechas próximas. Una de las cinco áreas de ese marco descriptivo es precisamente «la seguridad», tanto en el uso de dispositivos, como en la protección de datos y la identidad digital.

El INTEF coordina el grupo de trabajo (con participación de las CCAA) que está anticipando la adaptación española a ese marco europeo, desarrollando un Marco de Competencia Digital Docente, que afronta los problemas de la diversidad y escasa especificación de los marcos descriptivos existentes, y de las carencias formativas del profesorado a la hora de integrar la competencia digital en el currículo de los estudiantes.

Además, dentro este Plan de Cultura Digital en la Escuela, la seguridad del menor en su acceso a la red es un tema transversal que es tratado desde distintos ámbitos y perspectivas, en especial desde los relacionados con establecer un entorno seguro de navegación en las redes de los centros escolares y su acceso a Internet.

Dentro del nuevo Marco de Desarrollo Profesional Docente en el que este año se ha comenzado a trabajar en colaboración con las CCAA, se han identificado tres líneas prioritarias:

- *Competencias Profesionales Docentes*:
- *Nuevas Modalidades de Formación*
- *Nueva Regulación de la Formación Docente*.

El INTEF ya ha organizado el presente año escolar un curso de formación docente en red sobre uso de nuevos entornos virtuales de aprendizaje (en inglés, PLE) con el objetivo de fomentar su inmersión digital y el desarrollo de competencia digital aplicada a la docencia y tiene previsto desarrollar nuevas actividades con esos objetivos (incluyendo la nueva

modalidad de cursos masivos abiertos en red o MOOC). Se ha iniciado también la elaboración de los materiales para un curso tutorizado sobre «Educación conectada: redes sociales y escuela», que tendrá una parte importante dedicada al uso seguro de la Red y la prevención de los riesgos asociados a su utilización.

Por último, el INTEF cuenta con espacios web sobre metodologías, información y difusión de medidas para favorecer el uso responsable de las redes sociales y la imagen digital de los alumnos, en donde se aportan recursos y se lanzan iniciativas para promover el uso de un INTERNET seguro. Estos dos sitios webson:

El dedicado a la «Guía de redes sociales para familias»:

Esta guía ofrece a la comunidad educativa y especialmente a las familias, pautas de actuación, consejos prácticos e información básica sobre todo dirigidos a un acceso más seguro por los menores.

El espacio web «Familias conectadas, navegación segura»:

Es un espacio que se encuentra alojado dentro de la Red de Buenas Prácticas del INTEF. Se trata de una red de colaboración entre el profesorado que está coordinada por docentes en activo, especialistas en cada una de las etapas educativas, y que cuenta con un gran número de participantes organizados en distintas áreas o secciones. Dentro de este espacio existe un apartado dirigido específicamente a las familias y una de las secciones recoge un gran número de artículos sobre la temática de la navegación segura y la protección del menor en Internet que reciben decenas de miles de visitas.

2. Actuaciones en colaboración con otros Ministerios

En este cometido de proteger al menor de los peligros del uso de la Red, el Ministerio de Educación, Cultura y Deporte ha puesto en marcha actuaciones en colaboración principalmente con diversos organismos del Ministerio de Industria, Energía y Turismo, y del Ministerio de Justicia.

Con el Ministerio de Industria, Energía y Turismo y con las comunidades autónomas para apoyar la integración de las Tecnologías de la Información y la Comunicación en la Educación. Al amparo de esta colaboración y a través de entidad Red.es se han puesto en marcha diversos proyectos y, en el ámbito que nos ocupa, el espacio virtual de difusión

e intercambio de buenas prácticas educativas Educ@conTIC, en los que se presta especial atención a los temas de seguridad en la red y el uso responsable de las TIC.

El Ministerio también colabora con el Instituto Nacional de Tecnologías de la Comunicación (INTECO), dependiente del Ministerio de Industria, Energía y Turismo, que ha realizado numerosas guías didácticas sobre acoso dirigidas a padres y educadores. Entre ellas destacan la «Guía de actuación contra el ciberacoso» y la «Guía sobre adolescencia y sexting: qué es y cómo prevenirlo», que se pueden descargar a través de la red y que numerosos centros han puesto a disposición de las familias a través de sus páginas web.

También colabora con INTECO en una línea de información para la prevención y la detección de todo tipo de situaciones de acoso a través de Internet, en la que esta entidad ofrece información sobre los problemas a los que pueden enfrentarse los menores en la red y se facilita el acceso a líneas de ayuda.

Además, el INTEF participa con la Agencia Española de Protección de Datos en la creación de un nuevo espacio web dedicado a la protección de los menores. Se trata de un proyecto cuya finalidad es minimizar, en la medida de lo posible, el riesgo para los menores que se deriva de un uso no responsable de Internet a través de acciones (a llevar a cabo fundamentalmente por la comunidad educativa, pero sin prescindir de los padres y tutores) de concienciación, sensibilización y formación sobre la protección de los datos de carácter personal y de la privacidad.

En tal sentido se ha diseñado material y contenidos que abarcan aspectos como: la importancia de la privacidad y el valor de los datos personales, su tratamiento en distintos contextos, el uso de las redes sociales, la mensajería instantánea, la identidad digital y los problemas relacionados con la suplantación de identidad y las situaciones de riesgo (ciberacoso, grooming, sexting), proporcionandose un catálogo de buenas prácticas, consejos y recursos de apoyo o auxilio para liberarse de ellas.

Se trata de un proyecto de carácter integral, que permitirá incorporar, además de los materiales y recursos ya existentes, aquellos otros que se vayan produciendo, así como la actualización de su contenido, y que estará plenamente disponible a través de la web de la Agencia Española de Protección de Datos en 2013.

3. Actuaciones más significativas realizadas por distintas comunidades autónomas

(Pendiente de revisión por CCAA)

4. Otras iniciativas de ámbito nacional

Cabe destacar entre las actuaciones en el ámbito de la seguridad del menor en el uso de la Red, la iniciativa PROTÉGELES dependiente de Safer Internet Programme de la COMISIÓN EUROPEA.

Esta iniciativa está teniendo una acogida muy favorable por parte de las Consejerías de Educación que se están adhiriendo a la misma mediante la firma de convenios específicos, tal como habrán podido observar en la exposición que acabo de realizar de las actuaciones autonómicas.

PROTÉGELES cuenta con Líneas de Ayuda y recursos para que en general todos los ciudadanos puedan encontrar información y consejos para hacer frente a los riesgos de Internet. Realiza también una importante labor de prevención y formación, con talleres sobre seguridad en el uso de internet y las TIC en centros escolares. Cuenta con los siguientes recursos:

a) *Centro de Seguridad en Internet,* que tiene como principal tarea procurar un entorno seguro para los más jóvenes en el uso de internet, la telefonía móvil y las tecnologías de la Información y la Comunicación —TIC— en general, mediante la recepción de denuncias, líneas de ayuda profesionalizadas y la realización de campañas de formación y sensibilización.

b) Espacios web dirigidos a menores la que grupos niños de jóvenes de distintas edades tienen a su alcance recursos formativos y pueden hacen oír su voz, opiniones y propuestas sobre temas concretos vinculados al uso de Internet.

5. Iniciativas de ámbito europeo

El anteriormente mencionado Safer Internet Programme de la COMISIÓN EUROPEA también contempla los siguientes proyectos principales, que nos afectan como miembros de la UE:

- INSAFE es una red europea creada en 2006 y compuesta por 30 ministerios de Educación de la UE y de otros países. Coordinada por *European Schoolnet,* tiene como misión fomentar el uso de Internet por parte de los ciudadanos de una manera positiva, segura y efectiva.
- eNACSO es una red compuesta por 27 organizaciones no gubernamentales de derechos de los niños de toda la UE que tiene como objetivo conseguir un entorno online más seguro para los menores. Para ello promueven y apoyan acciones a nivel nacional y europeo para proteger a los menores y promover sus derechos en relación con Internet y las nuevas tecnologías.
- *EU Kids online,* que actualmente desarrolla un programa —*EU Kids online III*— que cubre el período 2011-2014.

Conclusiones

La influencia de las Tecnologías de la Información y Comunicación (TIC) en la sociedad es extraordinaria, tanto por su intensidad como por su alcance, lo que ha llevado a utilizar la expresión de «Sociedad de la Información y del Conocimiento» como forma de referirnos al momento actual y de diferenciar este nuevo statu quo respecto al de la era industrial. La educación está completamente impregnada de dicha influencia de forma irreversible.

Por un lado nos encontramos frente a una sensación de «aceleración» de los cambios tecnológicos y sus efectos sociales, políticos y culturales. El «factor de multiplicación tecnológica» de las TIC, es decir, la capacidad que tienen de mejorar los resultados y el rendimiento en cualquier sector en el que se empleen, alcanza valores que no se conocieron en la revolución industrial.

Por otro lado, parece no existir ningún ámbito en la vida de los ciudadanos al que no parezca afectar la rápida evolución de las TIC. Esta nueva era informacional se caracteriza por la considerable y creciente capacidad de acumular y procesar conocimiento, que se ha convertido en un factor clave de productividad, y por tanto, de posibilidades de producción de bienes y servicios y de organización del trabajo.

Hasta ahora, las TIC no han transformado de forma significativa la educación. Pero ante los cambios sociales y culturales mencionados, el

sistema educativo necesita adaptarse y transformarse, y las TIC son un elemento clave para la mejora de la calidad educativa: permiten desarrollar una cultura colaborativa y abierta en el entorno escolar, hacen viable la personalización y atención individualizada al estudiante, y facilitan la labor de transmitir el deseo de acceso al conocimiento por los profesores a los alumnos.

Se trata de aspectos positivos del uso de la tecnología que no podemos olvidar, el menor de hoy en día, es el futuro ciudadano de mañana, que vive ya, pero sobre todo vivirá, en un mundo digital envolvente.

Pero este ineludible «Nuevo Mundo» también entraña riesgos para los que nuestra sociedad se debe preparar, haciendo especial hincapié en la protección del menor mediante su formación, otorgándole el nivel adecuado de competencia digital para que pueda aplicarlos conocimientos, destrezas y actitudes necesarias en relación al uso seguro de los nuevos medios digitales.

La política del Ministerio de Educación, Cultura y Deporte está dirigida en una línea coherente con lo anterior, tal como he intentado explicar durante mi intervención. Consideramos necesario poner el foco tanto en los riesgos de la Red, a los que hay que otorgarles la importancia que tienen, para poder prevenirlos y actuar contra ellos; como en potenciar la utilización de las TIC por los alumnos, a través de la mediación de los profesores en las actividades de enseñanza y aprendizaje que se desarrollan en las aulas.

El Ministerio de Educación, Cultura y Deporte, junto a las Consejerías de Educación de las Comunidades Autónomas colaboraran tanto en la formación de ese futuro ciudadano para la Sociedad de la Información y el Conocimiento como para la toma de medidas de prevención ante los posibles abusos que puedan surgir de la utilización de las redes sociales y otros entornos de la Red para salvaguardar los derechos de los menores.

Por su parte los padres y los centros escolares no pueden desconocer los riesgos que conlleva el uso de las Red, pero tampoco deben ignorar el mundo de oportunidades para sus hijos que se abren con ello. Sólo la formación de los menores para un uso adecuado y responsable de la tecnología puede dar solución al dilema.

COMPARECENCIA DEL JEFE DE LA SECCIÓN CENTRAL DE DELITOS EN TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIDAD DE INVESTIGACIÓN CRIMINAL Y POLICÍA JUDICIAL DE LA ERTZAINTZA, D. MANUEL VIOTA MAESTRE, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 17 DE JUNIO DE 2013.

¿Debemos proteger a nuestros menores de Internet?

Si realizamos esta pregunta a la ciudadanía, seguramente el resultado sería un SI claro y contundente, por lo menos es lo que nosotros apreciamos de nuestras comunicaciones con los padres de dichos menores.

Sin embargo, desde mi punto de vista, no debemos proteger a los menores de Internet; debemos proteger a los menores de las personas que hacen mal uso de la red, incluso de ellos mismos. Es decir, Internet no es el enemigo, es únicamente una herramienta y por lo tanto, conceptos tales como la bondad o la maldad le son ajenos. La tecnología es neutra. Es el uso que se haga de la misma lo que determina su catalogación moral. Internet no es más que una lupa en la que se magnifican las características de quienes participan en ella. Así, podemos encontrar brillantes creaciones artísticas, científicas o literarias, cohabitando con pornografía infantil, fraudes y diversas apologías del odio.

Nuestros menores conforman la generación de los llamados «nativos digitales» (terminología utilizada por primera vez por Marc Prensky en su libro «Enseñanza de los nativos digitales»), es decir, niños que han nacido cuando Internet y las tecnologías asociadas ya estaban desplegadas y su uso era común.

Eso les ha llevado a que asuman, desde su más tierna infancia, como algo normal, el uso de estas tecnologías, a las cuales se han ido acercando con naturalidad según iban creciendo. Para ellos, su vida digital es parte integrante de su vida real y en ocasiones no son conscientes del doble plano en el que tienen que moverse, ya que las fronteras entre los mundos virtual y real están muy difuminadas y desleídas.

La principal consecuencia de esta temprana inmersión tecnológica es el establecimiento de una brecha digital entre su generación y la de sus progenitores, quienes a la postre somos «inmigrantes digitales» (según la misma terminología utilizada por Marc Prensky).

Para la generación de sus padres, el acercamiento a Internet y las tecnologías relacionadas, se ha llevado a cabo unas veces de forma voluntaria, y otras de forma forzada, debido sobre todo a la necesidad de utilizar estas herramientas, y casi «por obligación» en muchos casos, lo que implica que su comprensión del «mundo virtual» es muy limitada.

Si a cualquiera de nuestros menores se le entrega un móvil de última generación, en tres minutos lo han desembalado, puesto la tarjeta sim, la batería, lo han conectado a Internet, se han descargado el Whatsapp, han configurado los tonos, los fondos y lo han personalizado. En ese tiempo, sus padres, estarían aún buscando en el manual la sección que viene en su idioma materno.

Esta brecha digital también existe, aunque es cierto que en menor medida, con sus profesores, ya que aunque el Departamento de Educación les forma y les obliga a utilizar en la docencia las nuevas tecnologías (p.e. plan Eskola 2.0), únicamente comprenden aquellas herramientas que utilizan habitualmente y solo en contadas ocasiones realizan una inmersión más profunda en el campo tecnológico. El descubrimiento de nuevas tecnologías no asociadas a la educación es algo que dependerá únicamente del interés personal del docente. (Y estas tecnologías pueden ser tan importantes como el Whatsapp, distintas redes sociales, etc.)

Debido a este desfase, unos y otros, padres y profesores, se sienten, y así nos lo han manifestado en innumerables ocasiones, completamente impotentes a la hora de educar a los menores en el uso responsable de Internet.

Esta pretendida discapacidad formativa, en realidad no es tal, es únicamente una apariencia, y se basa en la demonización de la tecnología, en hacer hincapié en las conductas perniciosas de la Red, frente a las cosas positivas de las mismas. Se ve Internet como un ente del que hay que proteger a los menores. Este enfoque, como se ha apuntado anteriormente, desde nuestro punto de vista es erróneo: no hay que defender a nuestros menores de la tecnología. Hay que defender a nuestros menores de las personas que hacen mal uso de la misma.

Así las cosas, aquellas normas de educación y protección que nuestros padres y abuelos nos inculcaban cuando nosotros éramos pequeños sirven todavía en nuestros días, incluso si se aplican a Internet y sus riesgos. Por ello aconsejamos a los padres que si para la educación de sus hijos la tecnología supone un problema, que la eliminen de la ecuación, no que le prohíban usarla, sino que apliquen los mismos sistemas de protección y educación que utilizan con sus hijos en la vida real. Que conviertan a la tecnología en algo transparente, que se pueda fluir a su través sin que sea un impedimento.

Es cierto que un mejor conocimiento por parte de todos los actores implicados, de las distintas tecnologías, facilitaría enormemente su comprensión y por lo tanto serían mucho más capaces de educar a sus hijos, y por ello no debe aislarse de todo lo que suponen las nuevas tecnologías.

Por otro lado, nuestros menores, aunque muy capaces técnicamente, carecen de la madurez necesaria para comprender las implicaciones y consecuencias que sus acciones tienen, tanto en los demás como en si mismos. Muchas de sus acciones son tomadas por ellos mismos como juegos o bromas carentes de importancia cuando en la realidad es que se trata de delitos, y en ocasiones graves. Todo el mundo sabe que robar es un delito, pero sin embargo el sustraer una cuenta de correo de otra persona no estaría tan claro, por lo menos para cierta parte de la Sociedad, porque al fin y al cabo, las cuentas de correo son gratuitas, al menos la inmensa mayoría de ellas.

Riesgos o conductas erróneas

Pero, ¿cuáles son los peligros más frecuentes a los que se pueden enfrentar los menores al acceder a Internet?

1. **Conexión constante a la Red**. Hace solo unos años, para poder conectarnos a Internet teníamos que utilizar unos ruidosos módems. Estos módems solo se podían utilizar en los hogares desde las 8 de la noche hasta las 8 de la mañana, pues era cuando teníamos la llamada «Tarifa plana», hacerlo fuera de esas horas suponía en muchos casos un «suicidio económico» por los costes asociados que tenían otros horarios. Además al realizar la conexión hacían un ruido espantoso, y han generado más de una discusión porque los

cohabitantes se despertaban y eso además ocurría varias veces por errores en las conexiones.

En esa época, si alguien quería atacarnos, tenía que utilizar ese horario porque fuera de él no estábamos «online». Los menores de edad, disponían de un horario más reducido porque eran enviados a la cama e internet se acababa. Ya no podían hacer uso de ella sin que sus padres lo supieran por el ruido que generaba el módem. Además, como otro hándicap, durante la conexión a la Red no se podía utilizar el teléfono. En algunos casos cuando estabas descargando un fichero grande y estabas próximo a acabar alguien te llamaba y en ocasiones reseteaba la conexión y vuelta a empezar. Por último las conexiones eran extremadamente lentas.

Sin embargo ahora, todos los hogares con conexión a Internet lo hacen mediante la alta velocidad, bien sea ADSL o cable, con tarifa plana real, y sin interferir en el teléfono. Esto supone que muchos equipos están permanente conectados a la Red porque puesto que… «ya que pago la conexión la aprovecho al máximo». Aunque no haya nadie en el ordenador, el mismo suele estar conectado a internet.

Además la mayoría de los routers modernos tienen conectividad wifi, la cual en la inmensa mayoría de los casos se encuentra abierta pese a no tener ningún dispositivo conectado.

Estos avances en la comunicación tienen también su contrapartida y es que aumentamos exponencialmente la ventana temporal de exposición. Ahora nuestros equipos pueden ser localizados y por lo tanto atacados las 24 horas del día. Nuestros wifis pueden ser utilizados por nuestros vecinos a cualquier hora del día, bien sea para navegar por internet gratis (el menor de los males), para hacerlo de forma anónima o bien para atacar a nuestros sistemas.

Si a eso le unimos que en breve se producirá el abandono del protocolo IPV4 y su cambio por el IPV6, que va a permitir que cualquier dispositivo que se alimente de electricidad pueda estar permanentemente conectado a Internet veremos como el riesgo potencial de ser víctimas aumenta de manera considerable.

Por último a nuestros menores a partir casi de los 10 años ya les estamos dando teléfonos móviles con la excusa de «tenerlos localizados y que nos llamen cuando pase algo». Creo que se nos está

yendo de las manos... Un menor de 10 años va de casa a la escuela, y al salir sus padres o la persona designada lo recogen y lo llevan al parque (si tiene suerte) o a actividades extraescolares (si no la tiene). ¿Necesitan realmente un móvil?.

Además, para no gastar, les instalamos el Whatsapp o el Line o programas similares para que puedan chatear gratis. Aumentamos doblemente los riesgos: por un lado, porque estos móviles son nuevas vías de contacto que pueden ser aprovechadas por delincuentes para acceder a nuestros menores y en segundo lugar porque no son pocos los menores, que en la soledad de su cuarto, de madrugada, permanecen chateando con sus contactos mientras deberían estar durmiendo. Esto se traduce en la bajada del rendimiento escolar.

2. **Las webcams y los teléfonos con cámara**. Existen infinidad de malware que pueden controlar remotamente las cámaras instaladas en equipos informáticos. Esto no sería preocupante si nuestros menores no tuvieran el ordenador instalado en su dormitorio con la webcam apuntando hacia dónde duermen o se cambian de ropa. O si tienen portátil, que cuando están chateando y tienen que hacer alguna necesidad fisiológica no se lo llevan al baño, o incluso a la ducha para evitar perderse esos «interesantísimos chats» con sus amistades.

   Hace un tiempo aconsejábamos a los padres que los ordenadores estuvieran situados en un lugar común, pero ahora con la proliferación de los móviles y tablets este consejo se nos ha quedado completamente corto.

3. **No hay cultura de seguridad informática** ya no solo en los menores, sino en la Sociedad en general. Venimos de un ordenamiento jurídico destinado a proteger el mundo físico y ahora ante el mundo digital, intangible pero real, se torna un poco vago y esa cultura tiene su reflejo en muchos ámbitos de la vida.

   Si en un barrio cualquiera una persona abre una tienda de golosinas, lo primero que hace antes de llenarla de género y abrirla al público es poner una persiana y en ocasiones una alarma. Sin embargo si lo que abro es una tienda por internet, ni se preocupan en cumplir las mínimas medidas de seguridad para evitar que alguien ataque a su aplicación. Esta discordancia también se aplica a otros ámbitos de la vida. Como para navegar por la Red únicamente ne-

cesitamos un ordenador y una conexión creemos que esa facilidad es sinónimo de seguridad. ¿Para que me van a atacar a mi si no tengo nada importante?

4. **Contenidos inapropiados.** Dentro de esta catalogación podríamos incluir todas aquellas páginas que alojan contenidos que de ser vistos por mentes en formación pueden tener consecuencias lesivas para el correcto desarrollo cognitivo y emocional. Ejemplos serían las páginas de pornografía en general, las de ensalzamiento de la anorexia y bulimia, las «gore» que muestran escenas escalofriantes en cuanto a su brutalidad, las que hacen apología de los distintos tipos de odio, bien sean xenófobos, políticos, de clases o de sexo.

5. **Depredadores sexuales.** Sujetos que navegan por las redes a la caza y captura de menores a los que embaucar para que les envíen fotogramas eróticos y llegado el caso a obtener contactos sexuales con los mismos. Estos sujetos utilizan sofisticados métodos psicológicos para hacerse con el control de las mentes de nuestros adolescentes, los cuales por sus características de maduración son muy vulnerables a estas técnicas. No debemos olvidar que el paso de la infancia a la adolescencia es un periodo vital caracterizado por incontables problemas psicológicos, desde la falta de autoestima, conductas agresivas, necesidad de reconocimiento, despertar a las conductas sexuales, que si bien en la inmensa mayoría de los casos son superados con el paso del tiempo, no es menos cierto que este periodo hace a los adolescentes especialmente vulnerables.

   Uno de los modus operandi de estos depredadores consiste en que se apropian de la cuenta de correo electrónico de un menor. Teniendo en su poder la cuenta de correo electrónico tienen acceso a toda su vida digital, fotografías almacenadas, perfiles de redes sociales, mensajes, contactos, etc. Haciendo uso de la ingeniería social, mantienen conversaciones con sus contactos para obtener el control de más cuentas.

   Una vez obtenido el control suelen contactar nuevamente con las víctimas para extorsionarles diciendo que si no acceden a activar la webcam, o al envío de fotogramas sexuales, sus secretos, (en algunas ocasiones, bastante sensibles) serán distribuidos entre sus amigos, padres y profesores. Debido a la inmadurez propia de la edad, esta situación de estrés se magnifica y en muchas ocasiones

estos menores sucumben a las amenazas y entran en un círculo vicioso de difícil ruptura, puesto que las imágenes exigidas son cada vez más comprometidas.

Pero no siempre es necesaria la captura de un perfil para la extorsión. En otras ocasiones el delincuente adopta la identidad de un adolescente y se produce un «enamoramiento». Para poder obtener la información necesaria para llevar a cabo su plan, hace años el acosador tenía que estar mucho tiempo sonsacando y conociendo a su víctima hasta que tenía los datos precisos para conocer bien sus gustos y aficiones. Ahora, este paso ya no es necesario. Basta con «echar un ojo» a los perfiles de las redes sociales y allí tenemos toda la información, edad, altura, peso, gustos, deportes que practico, libros que leo, incluso una detallada colección de fotografías, que permite además elegir a la víctima según los gustos de los pederastas.

Con todos esos datos en su poder, lograr el enamoramiento es relativamente sencillo. Una vez obtenido, el acosador va a enviar una fotografía de quien se supone que es él. La victima le va a mandar otra. El pederasta le va a contestar con una foto con el torso desnudo, la victima una en bikini….. y así se va subiendo la intensidad sexual de las imágenes hasta que logra fotografías verdaderamente comprometidas.

Llegado a este punto el delincuente se descubre y empieza la verdadera extorsión, exigiéndole a su víctima nuevos fotogramas o vídeos con la amenaza de que si no los obtiene publicará las que ya tiene en su poder y se las reenviará a sus amigos, padres y profesores.

Debido a la falta de maduración y a la carencia de herramientas psicológicas adecuadas, es muy fácil que estos menores, presas del miedo y la vergüenza, caigan en esta espiral de la que es muy difícil salir.

6. **Acoso entre iguales**, el tristemente famoso ciberbullying. Como su vida transcurre entre los mundos virtuales y reales, este acoso también se libra en ese campo de batalla. Los insultos, vejaciones y demás actos impropios tienen lugar en ambos frentes. Crean perfiles, cuentas, identidades ficticias para suplantar la identidad de la víctima o bien para catalizar el odio hacia ella.

Frecuentemente observamos como los menores son capaces de hacerse con el control de una cuenta de correo electrónico de uno de sus compañeros, suplantar su identidad ante el grupo y leer sus mensajes de correo, en un símil actualizado de lo que en nuestra época era el leer los diarios de los hermanos mayores.

Bien, esta conducta, para la que se encuentran capacitados técnicamente, puede conllevar penas, que de ser mayores de edad, se convertirían en penas de prisión, y por lo tanto al trasladarse al ámbito de la protección del menor también deberían llevar aparejadas sanciones altas.

Además el uso de Internet y del resto de tecnologías para comunicarse entre ellos proporciona un halo de impunidad, de relajo del control social de sus acciones y un pretendido anonimato, lo que deriva en que se atrevan a decir a un compañero cosas a través de la tecnología, que en directo no serían capaces, ya no solo por la posible represalia, sino por la dificultad de afrontar la comunicación «cara a cara».

No tenemos que engañarnos, el acoso como tal, ha existido siempre. Lo que pasa es que antes, la vida escolar y la extraescolar, frecuentemente estaban separadas, es decir, los niños se relacionaban con sus compañeros en el colegio pero al salir de él establecían otras relaciones con otros niños que frecuentemente no tenían nada que ver con la institución escolar. Es decir, existían dos grupos sociales distintos que pocas veces se mezclaban. Por lo tanto, lo que ocurría en uno de estos círculos no solía tener trascendencia en el otro grupo. Sin embargo en la actualidad, estos grupos se hallan generalmente interconectados a través de las redes sociales y es prácticamente imposible mantener privado un suceso ocurrido en cualquiera de nuestros ámbitos de relación: enseguida se extiende hacia otros grupos a los que pertenezcamos.

Además la trascendencia de las acciones realizadas en la vida real y en Internet tienen una muy distinta repercusión. No es lo mismo que dos chavales se insulten en el baño y nadie escuche esa bronca, que mantengan esta discusión a través de las redes sociales. El daño ocasionado en el segundo de los casos es enormemente mayor toda vez que la publicidad de los insultos llega al entorno social de ambos y por lo tanto la sensación de agravio es mucho más grave.

Internet ha posibilitado además una «democratización» del acoso. Antes el acosador generalmente solía ser el típico alumno «polirepetidor» con tendencias delincuenciales que basada en su mayor maduración física imponía su dominio a sus compañeros de clase. Pero ahora, cualquiera de los compañeros puede poner en un «brete» a otro sin más que sacarle una fotografía comprometida y publicarla en internet.

Este acoso se lleva a cabo de muchas formas distintas pero muchas de ellas pasan por la creación de perfiles en las redes sociales, suplantando la identidad de las víctimas, en las que se muestran conductas que buscan minorar su relevancia social y hacer que el grupo «la tome» con la víctima. Esta conducta tiene difícil encaje en nuestro ordenamiento jurídico, puesto que los jueces para considerar este delito como suplantación de personalidad estiman que es necesario que tal usurpación se lleve de manera íntegra en todos los aspectos de la vida de la víctima y que además tenga una permanencia muy amplia en el tiempo. Por lo tanto estas conductas pueden resultar impunes, aunque causen un grave daño psicológico a las víctimas que ven como sus amigos se apartan de él en base a unos comentarios que le son atribuidos pero que no ha generado.

En bastantes ocasiones las víctimas del bullying suelen cambiar de colegio buscando dejar atrás las agresiones, pero estas las persiguen. Este abandono del centro escolar es una victimización secundaria, que lejos de arreglar el problema lo magnifica, porque en el nuevo centro educativo, sus nuevos compañeros van a tener constancia de lo que ha ocurrido en el centro de origen y el acoso, con mucha probabilidad, se va a reproducir. El problema tiene que resolverse en el mismo lugar en el que se genera, bien sea mediante una charla entre los padres implicados, o con la intervención del centro o en último caso con nuestra participación. En cualquier caso, si alguien debe abandonar el centro escolar para restaurar la convivencia, deberían ser siempre los agresores, nunca las víctimas. No es de recibo que a la víctima de una agresión se le imponga además una medida de alejamiento de su agresor, por mucho que consideremos que lo hacemos para su protección. Es una forma fácil de eludir el problema, no de solucionarlo.

7. **Fraudes.** Estos, en principio son muy restringidos, por la escasa importancia de los mismos debido a la limitada disponibilidad monetaria de los adolescentes. La gran mayoría de ellos suelen consistir en compraventas a través de internet, y los mensajes Premium. Sin embargo, en ocasiones se tornan graves cuando se hacen con la tarjeta de crédito de sus progenitores para utilizarlas en sitios de juego online, siendo de ellos los más peligrosos los juegos de apuestas.

8. **Autoexhibición.** Los menores vierten en Internet cantidades ingentes de información sobre su vida e intimidad que puede ser utilizada en su contra. Ya no solo esas fotos «atrevidas» que cuelgan en sus perfiles de las redes sociales, sino el resto de información sobre sus estudios, domicilios, viajes que realizan, etc.

   Hay perfiles que son verdaderos diarios vitales minuto a minuto, la proliferación de los teléfonos móviles con conexión a Internet ha posibilitado una conexión 24/7 y todo lo que le pasa a un menor suele volcarse en su red social. Es triste observar como cuadrillas de adolescentes se reúnen en algún lugar y entre ellos no hablan solo se comunican a través de los móviles, aunque estén a un escaso metro de distancia.

   Además, la inmensa mayoría de los smartphones tienen el servicio gps activado lo que posibilita que las fotografías que se obtienen con estos dispositivos estén geoetiquetadas y pueda realizarse un seguimiento de los lugares exactos dónde han sido obtenidas.

   Otro de los problemas añadidos de la publicación de fotos en las redes sociales es la inmediatez de su publicación, es decir, desde que se obtiene la fotografía hasta que se manda a la red, pasan escasos segundos. Hace relativamente poco tiempo, para subir una foto a la red teníamos que sacarla con una cámara digital, pasarla al ordenador, verla en nuestro monitor, y después enviarla. En cualquiera de estos estadios podríamos arrepentirnos del contenido que íbamos a enviar y abortar su distribución. Además la visualización de la foto en un monitor aporta un mayor control de detalle de lo que realmente se ha captado, cosa que no pasa en la pequeña pantalla de nuestro móvil, donde los detalles del fondo suelen pasar desapercibidos.

En las charlas que impartimos, llegado este punto, solemos hablarles de lo que nosotros denominamos «la prueba del tablón». Para centrar el ejemplo hacemos varias preguntas:

– ¿Quienes de los asistentes han acudido el verano pasado a la playa o a la piscina?. Suelen ser la práctica mayoría los que asienten.

– ¿Os habéis sacado fotografías en bikini o bañador?. Suelen contestar la práctica totalidad de forma afirmativa.

– Ahora nos solemos centrar en las chicas porque su pudor suele ser mayor: les preguntamos si alguna de ellas pondría esas fotografías en un tablón de anuncios que íbamos a instalar en la entrada del centro escolar. Aquí, sin excepción todas contestan negativamente.

– La última pregunta es si han subido esas fotos a las redes sociales. Muchas suelen contestar positivamente.

Curiosamente son muy pudorosas a la hora de colgar las fotografías en un tablón físico por el miedo o la vergüenza de que sus compañeros de clase pudieran verlas y sin embargo no tienen ningún reparo en colgarla en sus perfiles donde curiosamente tienen agregados, a todos sus compañeros de clase, además de el resto de contactos ajenos al centro escolar.

Además se da la circunstancia, todavía más grave, de que si alguien le gusta la fotografía física del tablón y la coge solo habría una foto circulando, sin embargo puesta en Internet, cualquiera que la vea puede realizar una copia. Si me arrepiento de haberla colgado físicamente, cuando la retire, nadie más la podrá ver, pero en el mundo virtual, aunque la retire, nadie puede saber cuantas copias hay almacenadas en los discos duros de los que la hayan visualizado.

Y no hablemos del conocido como sexting que consiste en el envío de fotografías pretendidamente sexys a las parejas sentimentales. Cuando las parejas se rompen no de forma consensuada, curiosamente a uno de ellos siempre le «entran en el ordenador», le roban las fotos y las distribuyen.

9. **Sacarse fotos con el teléfono móvil**. Aunque no tengan intención de subirlas a la Red. Esas fotografías que empiezan siendo atrevidas y

en muchas ocasiones llegan hasta ser pornográficas, se almacenan en el teléfono móvil y estos pueden ser robados o simplemente perdidos. Si a esto unimos que muchos adolescentes no tienen contraseña en el móvil en la creencia de que de este modo si se les pierde el que lo encuentre llamará a sus padres y se lo devolverá…. El acceso a estas fotografías no está restringido. Y aún en el caso de que tengan clave de acceso estas fotos se guardan en la tarjeta sd y por lo tanto puede ser extraída y vista en cualquier ordenador o en otro móvil sin ninguna restricción. Además, para acabar de rematar la faena, las fotografías previamente borradas pueden ser recuperadas muy fácilmente mediante programas gratuitos, con lo que aquellas fotos que eran demasiado escandalosas para enviarlas e incluso para guardarlas en el móvil, siguen estando latentes en la tarjeta sd a la espera de como decía Bécquer … «una mano de nieve sepa arrancarlas…».

10. **Aceptar a desconocidos como contactos en las redes sociales**. Existe una especie de competición entre los menores para ser el que más contactos tenga en su perfil, como símbolo de popularidad y estatus. Es imposible que si tengo 500 contactos pueda conocer físicamente a todos y cada uno de ellos con lo que las posibilidades de que entre estos haya alguien que es quien no dice ser se multiplican de forma exponencial.

11. **Facilitar contraseñas.** En su inocencia, los menores confían en exceso en sus contactos y es muy frecuente que faciliten sus contraseñas a sus conocidos cuando les son requeridas. Esta es una de las formas en las que los acosadores se hacen con el control de cuentas de correo y perfiles.

    Una vez han logrado la primera de las cuentas, contactan con los amigos de la primera víctima y, suplantando su identidad, les pide sus contraseñas pretendiendo que necesita enviar un mensaje, bajar una foto o lo que sea y no le funciona su perfil.

    Hay que señalar que todos nuestros secretos, toda nuestra vida digital únicamente está separada de los delincuentes por una palabra, la contraseña y si la damos alegremente, cualquiera podrá acceder a mis recuerdos y vivencias.

    Estamos sufriendo una transformación en el almacenamiento, no hace demasiados años, las fotografías las guardábamos en los álbumes de fotos, pasamos a las cámaras digitales y los discos duros

y los cds y ahora estamos en los smartphones y el almacenamiento en la nube. La información ya no está (solo) en nuestros dispositivos hay copias de la misma en páginas web, perfiles, en sitios de almacenamiento online, etc.

Pretendidas soluciones

Analizados los principales problemas vamos a ver cuales son las soluciones más utilizadas

1. **Control parental tipo filtro.** Los filtros de navegación se basan en que un programa informático determine la idoneidad del contenido al que el usuario está accediendo y que puede ser configurado para que permita o impida ver determinados contenidos. Desde nuestro punto de vista, este tipo de control parental debería ser pactado por padres y menores de forma que estos supieran que no se les va a permitir acceder a determinados lugares porque son peligrosos para su desarrollo psicológico. Sin embargo esta medida tiene una limitada eficacia, toda vez, que estos menores estarán protegidos, únicamente cuando accedan a la Red a través del ordenador en el que se haya instalado el software. En cuanto vaya a casa de un amigo, un cibercafé, o haga uso de tablets, móviles, etc. será completamente ineficaz.
2. **Control parental tipo espía**. Existen muchos desacuerdos sobre la legitimidad de instalar este tipo de software, que lo que hace es realizar un exhaustivo informe sobre lo que el menor está viendo. Por un lado los tutores son responsables de la educación y de las acciones que sus hijos realicen y por lo tanto deben tener algún tipo de control sobre sus conductas, pero por otro lado los menores también deben tener derecho a cierta intimidad. Además la maduración de los jóvenes no se realiza de forma cuántica, sino de forma progresiva y secuencial. Sin embargo para la Ley tan menor es alguien de 17 años y 364 días como uno de 13 años, aunque su nivel evolutivo sea completamente distinto. Además, siempre desde nuestro punto de vista, la instalación de este control parental espía, supone un riesgo importantísimo con respecto a la relación entre padres e hijos. El instalar un software de este tipo, a la larga va a suponer que debido a alguna actualización del antivirus sea re-

portado como instalado en el sistema y el menor se va a dar cuenta de ello.

Por otro lado está una reflexión sobre la necesidad e idoneidad de estas conductas. Es cierto que muchos padres se sienten tentados a instalar estos programas de control para saber que es lo que sus hijos hacen en internet. Como se ve, son solo chivatos, es decir no impiden que se accedan a los contenidos, sino únicamente avisa de lo que se ha visto. Además estos padres, tan proclives a este sistema de control en Internet, ni se plantearían contratar a un detective privado para controlar a sus hijos cuando salen de fiesta. ¿Es que Internet es más peligroso para los menores que la vida real?.

Además este sistema adolece de los mismos problemas que el anterior, solo que en el primero de los casos ha sido aceptado por el menor y en el segundo ha sido impuesto, con lo que si lo descubren, además de la pérdida de confianza en sus progenitores, el menor, con toda seguridad va a ser capaz de soslayarlo, pues en la mayoría de los casos, la competencia técnica de ellos supera con mucho la de sus tutores.

3. **La educación**. Internet es para nuestros menores, una parte indisoluble de su vida y por lo tanto tenemos que orientarles en ella de la misma forma que lo hacemos en la vida real.

   Si en nuestra infancia los padres despreocupados, dejaban a sus hijos viendo durante horas la televisión, ahora los dejarán desprotegidos navegando en Internet.

   Aunque ambas conductas parezcan similares hay que tener en cuenta que por muy mala que sea la programación de la cadena televisiva que estén viendo, detrás de la misma hay una serie de personas que filtran de alguna forma su contenido y sus horas de emisión, en base a una autorregulación, y sin embargo esto no pasa en Internet donde les permitimos un acceso ilimitado para buscar lo que quieran e incluso que puedan ser contactados por extraños.

   Este es el único sistema verdaderamente eficaz para prevenir los delitos en Internet. Es cierto que no podremos impedir que los acosadores nos tomen como víctimas, pero si que podremos detectar estos riesgos con anticipación y poder evitar el agravamiento de la conducta.

Hemos de enseñarles hábitos saludables de navegación, que herramientas utilizar, que páginas web visitar y cuales no, que protejan su intimidad, su identidad, que no agreguen ni charlen con desconocidos, etc. De esta manera, cuando lo interioricen serán capaces de navegar autónomamente sin la supervisión de un adulto y estarán más seguros en su uso de Internet.

En esta educación deberían participar varios estamentos, por un lado los padres, quienes deberían encauzar las conductas desde la más tierna infancia realizando la navegación conjunta, posteriormente permitirles el acceso a sitios seguros para al final ir dándoles mayor libertad. Es cierto que esto implica una dedicación de los padres para aprender como funciona Internet y en muchas ocasiones estos se muestran reacios a tal formación.

Además estaría la escuela, que como parte de la preparación de nuestros jóvenes para la vida no pueden dejar de lado las nuevas tecnologías, porque no estamos hablando del mañana en lo tocante a las TIC, estamos ya hablando del ayer.

Otros estamentos también deben colaborar, las empresas de Internet, las policías, medios de comunicación, asociaciones, los legisladores, en fin toda la Sociedad para llevar a cabo una concienciación sobre el uso responsable de Internet.

Conscientes de que la inmersión de los menores en las Tecnologías de la Información y Comunicaciones (TIC) es un proceso completamente automático, irrefrenable e irreversible al que no puede ponerse trabas ni obstáculos, desde hace ya tres años, en la Ertzaintza, venimos desarrollando un proyecto de colaboración con distintas escuelas, colegios, institutos y universidades del País Vasco consistente en la impartición de charlas formativas sobre los peligros de Internet y las consecuencias que el mal uso de las tecnologías pueden acarrearles a los menores.

Este proyecto está teniendo una magnífica acogida, entre otras cosas, porque no es lo mismo que una cosa te la diga tu «profe», tu padre, o un policía que trabaja en «delitos informáticos». El peso que los menores otorgan a nuestras aportaciones es muy alto y nos es más fácil llegar hasta ellos porque son muy receptivos a nuestros consejos, sobre todo porque nos basamos en casos reales que hemos investigado.

4. **Medidas represivas.** Cuando estas medidas preventivas fallan tienen que existir las medidas represivas. Si bien es cierto que sería deseable no tener que hacer uso de estas, resulta de todo punto imposible evitarlas. Es entonces cuanto hacemos acto de presencia, policías, fiscales y jueces.

   Para poder investigar estos delitos que se comenten a través de Internet se necesitan básicamente tres cosas:

   – Conocimientos. Los ponemos nosotros.
   – Recursos técnicos: Los ponen los desarrolladores.
   – Herramientas legales: Las ponen los legisladores.

   En el caso del conocimiento se trata de que los policías vayamos lo más cerca de los delincuentes que sea posible. Adelantarlos va a resultar imposible porque cuentan con mayores recursos económicos, mayor formación y mejor cooperación internacional y además no están constreñidos por reglas que cumplir.

   Los recursos técnicos, pese a no ser completamente indispensables si que son interesantes puesto que facilitan enormemente la labor de los investigadores. Es una cuestión de números, hay más delincuentes que policías.

   La labor de investigación de un delito informático en muchas ocasiones topa con que es necesaria la visualización de una ingente cantidad de archivos que ha de realizarse por parte de un policía sentado detrás de un ordenador, con las incomodidades y posibilidades de error que ello conlleva. También la búsqueda de evidencias conlleva mucho tiempo. Cuanto mejores sean los protocolos y las herramientas más facilidades tendremos para la investigación.

   Pero son las herramientas legales, las que a mi parecer pueden dar un impulso definitivo a la lucha contra el cibercrimen. Se nos tiene que dotar de instrumentos ágiles que podamos utilizar para emplearlos en esta lucha, porque de otro modo, por mucho conocimiento que tengamos, por mucha tecnología que hayamos desarrollado, no podremos localizar a ningún delincuente. Tendríamos un Formula I encerrado en una plaza de toros.

   Aspectos que podrían modificarse:

   – Definir correctamente la usurpación de personalidad. Dotarle de relevancia jurídica a estas suplantaciones consistentes en crear

perfiles en redes sociales para hacer creer a la gente que es otra persona.

- Convertir en delictiva la distribución de material «sensible» aunque el mismo haya sido entregado voluntariamente por su titular.
- Aumentar la edad legal de consentimiento sexual. Se están barajando los 16 años, pero debería establecerse de forma adicional un nuevo aspecto a tener en cuenta de cara a no culpabilizar unas relaciones sexuales consentidas y debería ser la diferencia de edad entre la pareja. No es lo mismo que un menor de 15 años mantenga una relación sexual con un adulto de 18, que el mismo menor de 15 años la mantenga con un adulto de 60 años.
- Determinar como delictivo el intento de mantener contacto sexual con un menor de 16 años sin que este tenga que ser consumado.
- Regular definitivamente la figura del agente encubierto.
- Permitir como parte de las condenas que el material informático ocupado con relación a cualquier delito pueda pasar a manos de la policía para utilizarlo en sus investigaciones en un símil de lo ya permitido para los casos de narcotráfico.
- Agilizar las identificaciones de los usuarios de direcciones Ips. No es de recibo que para obtener el titular de una dirección IP haya que pedir un oficio judicial y sin embargo cualquier persona va a Tráfico y abonando unas tasas de 8.10 euros le aportan «vida y milagros» del titular de un vehículo.
- Agilizar los procedimientos de asistencia jurídica internacional.
- Crear la figura del juez especialista en Delitos Informáticos, a semejanza del Fiscal Especialista.

COMPARECENCIA DEL JEFE DE LA DIVISIÓN TÉCNICA DE PLANIFICACIÓN DE LA SEGURIDAD CIUDADANA DE LOS MOSSOS D'ESQUADRA, D. JOAQUIM BAYARRI I NOGUERAS, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 17 DE JUNIO DE 2013.

El señor **JEFE DE LA DIVISIÓN TÉCNICA DE PLANIFICACIÓN DE LA SEGURIDAD CIUDADANA DE LOS MOSSOS D'ESQUADRA** (D. Joaquim Bayarri i Nogueras): Mi presentación o mi ponencia hará más peso, básicamente, en el ámbito de la prevención; aparte es de los servicios de los que yo tengo la responsabilidad, y porque entiendo que también habrán venido otros expertos más del ámbito de la investigación, que la investigación, al fin y al cabo, las problemáticas ya se conocen.

Los riesgos que nos presenta Internet para los menores, pues ya son los conocidos: el de la libertad sexual, contra la intimidad (y ahí estaríamos con el *cyberbullying* y el *grooming* y la libertad sexual), contra el patrimonio (que también afecta de manera, aunque poco relevante de momento, a menores, en temas de compras, en juegos como el Habbo, o en juegos en línea por Internet, pues consiguen tarjetas de los padres o a través de los móviles); y el último apartado, que sería lo que nosotros clasificamos como el normal desarrollo social... sí, la primera.

Otra parte que aquí nos cuesta mucho trabajar, que sería cuando acceden a páginas que promueven medidas que hacen referencia a la anorexia o pro bulimia. Aquí tenemos denuncias de padres, se dan consejos que no están regulados médicamente, y que algunos menores los siguen para mantener la línea o para mejorar su físico, y aquí es muy difícil que los servidores que alojan estas páginas, como tampoco hay ninguna actividad ilegal, pues aunque haya denuncias, no se descuelgan ni se interrumpe su consulta.

En referencia a esto, la apuesta que hace Mossos d'Esquadra para trabajar todo este ámbito es trabajar la formación y el acompañamiento. ¿Por qué la formación y el acompañamiento? Luego se puede hablar de las medidas policiales, las de prevención, las de cooperación policial, las normativas en que los reguladores y empresas privadas que dan servicios están obligados y que hay una normativa que los contempla. Internet

es global, y la respuesta a cualquier ilícito es compleja y dilatada en el tiempo. Por lo tanto, nosotros en lo que apostamos ya desde 2008 es en informar a las personas que van a navegar por ese mundo, por la red. Es la máxima: si prevenimos, no habrá ilícitos, y aseguramos que la incidencia de la víctima sea el mínimo posible.

La formación, ¿en qué dos aspectos nos centramos? En el primero, que es el valor que adquiere la información personal. Aquí lo que intentamos es complejo en menores, porque al fin y al cabo un menor es una personalidad que se expande y necesita conexión. Es que desde pequeños, desde ocho o nueve años empiecen a plantearse el valor de lo que van a colgar en Internet —para que nos entendamos— y el uso que se puede dar. Sí que son expansivos, pero intentamos que recapaciten, tanto los de ocho, los de trece, los de catorce, y los adultos, en pensar qué va a pasar con esa información: una imagen, unos datos que dan a un desconocido, pues que se lo vayan preguntando, porque una cosa compartida con un compañero, eso puede ir a la nube e internacionalizarse.

Y la segunda parte es en el respeto entre los internautas: en los talleres que hacemos, y esto el año pasado lo empezamos a introducir a partir de que explosionó esto de la red, es que se vayan valorando ellos mismos, pues eso, el denunciar o el acosar o el insultar a un compañero por Internet, o colgar una imagen desde los tres puntos de vista: como víctima, que lo puede sufrir, como autor que lo hace, y luego, que es donde intentamos buscar y que se motiven, es en el mero espectador. O sea, él y yo, o nosotros nos estamos insultando, ellos son meros espectadores y miramos que el menor se ponga en los tres papeles. Y empiecen a decir qué harían, si está bien o está mal o qué piensan, para intentar recapacitar en este ámbito.

El acompañamiento: ahora se define a los jóvenes o a los menores como las generaciones digitales. Bueno, esta generación digital, lo que no puede ser es que se convierta en un huérfano digital porque los mayores están ausentes. Por eso el acompañamiento tanto de padres como, en este caso, de profesores, porque al final son los que están muchas horas con ellos, sobre todo en la etapa de formación.

Y este acompañamiento de los adultos, de mayores, de padres o profesores, ¿cómo se hace? Los expertos dicen: con mediación activa. No es prohibir Internet, no es controles parentales y restricción de páginas, que

también, sobre todo en edades menores, pero sí que lo que fomentamos en las charlas y en las sesiones formativas es que el padre y, en su caso, el profesor, pero sobre todo los padres desde temprana edad tienen que empezar a navegar y a acompañar a sus hijos en esa nueva experiencia. Y hacemos el símil: cuando uno es muy pequeño, coge al hijo, lo acompaña por la escalera del tobogán, lo sube arriba y lo deja poco a poco que se lance por el tobogán, primero un tobogán pequeño y otro día un tobogán más grande. Pues aquí hay que hacer lo mismo, porque tenemos que hacer que esa navegación familiar, esa cosa compartida desde edades pequeñas sea una cosa habitual, rutinaria. Es una manera de ir poniendo a los mayores en Internet, porque es que no están. Y los chavales, los jóvenes, o los menores, pues muchos de ellos son huérfanos, podríamos decir, digitales.

¿Por qué adoptamos esta estrategia de prevención? Cuando en 2008 ya empezamos a incidir en todo el ámbito este de la prevención, ¿qué vimos? La red es global, es lo que decía, cualquier cosa pasa y no puedes controlarlo porque es internacional, no llegas. La fuerza que tiene que permite una afectación exponencial de víctimas: antes, y si nos vamos a un caso muy concreto de un pederasta o de pornografía, eran fotografías que se pasaban en mano, tenías que revelarlas. Ahora un pederasta o una persona que tenga capacidad para intercambiar fotos, los intercambios son a miles, la red multiplica exponencialmente las víctimas de cualquier hecho.

La red evoluciona constantemente. Y aquí siempre hay que estar siempre a la última. Y quien está siempre a la última es el que navega más. Y hoy en día la realidad es que son los menores los que están más en la red y están a las últimas. Y eso nos lleva a un paradigma que no ha pasado nunca, pero ahora los menores son más hábiles que los adultos en las tecnologías de la información. Por lo tanto, tenemos que estar con ellos desde el primer momento. A nivel global los menores, comparados con los adultos, tienen un dominio mucho más amplio, se intercambian experiencias, nuevas maneras de hacer, trampas, ingenios, y comparten todo lo que pueden compartir.

¿Cómo podemos trabajar esto? Pues formando al usuario; cuanta más prevención tenga el usuario, menos víctimas potenciales tendremos, cuanto más conozca Internet y sus riesgos, menos víctima será.

Implicar a los adultos, padres y profesores, en lo que les decía: no puede ser que haya dos mundos, los padres en el físico y los menores o

los jóvenes en el virtual. No habrá conexión, Internet no puede ser una barrera, sino que tiene que ser un puente entre generaciones.

O es necesario un esfuerzo sobredimensionado: ¿qué quiero decir con esto? Cuando nos planteamos trabajar el ámbito de la prevención, tuvimos claro que nuestra presencia, nuestra acción de prevención en este ámbito, de todas las charlas, formaciones que hacemos, iban a requerir un sobreesfuerzo. ¿Por qué? Porque hay que actualizar a la sociedad. Sí que hay otros actores que van trabajando en este ámbito, pero, bueno —ahora lo veremos—, nosotros tenemos un plan en las escuelas y vimos que aquí teníamos que invertir. Como hemos hecho en violencia de género o en otros ámbitos, teníamos que prevenir y, por tanto, formar a las posibles víctimas para que dejaran de ser posibles y no fueran víctimas.

Beneficios de esta prevención que hicimos en el Plan de Internet Segura: empoderar a los menores, padres, madres y docentes. Si vamos a las escuelas a enseñar a los menores, implicamos a los padres, a las madres y a los docentes, porque también se tienen que implicar.

Esto que nos daba también un punto de encuentro, una facilidad en estar en medio de los menores y de los docentes, en este caso en las escuelas, detectar las alertas que podían pasar en cualquier momento, los *informers*, cualquier hecho de *grooming* o cualquier problemática que hubiera, el menor y en más medida el profesor o maestro, para él nosotros éramos un referente. Y nos llegan y nos transmiten información.

¿Qué queríamos? Posicionarnos como referentes ante los menores, padres, madres, ante cualquier problema futuro: que la policía también esté en el mundo digital a través de los menores y de los adultos. Y esto nos ha permitido establecer una red de contactos que nos abre vías de comunicación con los centros y con los menores en cualquier temática que nos vaya apareciendo en el ámbito de Internet.

Un poquito, y aquí voy un poco rápido, cómo planteamos esta prevención: esta prevención, en el año 2006 se empezó lo que nosotros llamamos un plan operativo en centros educativos. Hay charlas de muchos ámbitos: de violencia de género, grupos juveniles, bandas juveniles, riesgos con las drogas... Y aquí es donde —mutilación genital— en 2008 incluimos lo que es Internet segura para jóvenes.

Para que nos demos una idea, este plan operativo de prevención en los centros, en el periodo escolar 2011-2012 se hicieron 7.200 presentacio-

nes y hubo 200.000 asistentes. De estos, alumnos son 200.000; docentes, 4.000; y de padres y madres, unos 8.900 asistentes. Esto sería en todas las dinámicas. En el ámbito de Internet: serían unas 3.000 presentaciones, y llegamos a unos 95.000 menores; unos 50.000 padres, aquí los padres nos fallan, yo discrepo del compañero de la Ertzaintza, pero los padres no están. Y unos 10.000 profesores, que aquí sí que... Esto el año pasado, 2012. Aquí a los profesores, al ir a las escuelas, pues los implicamos. A los padres sí que realmente no están, porque 10.000 padres sobre 95.000 menores es poquito.

En el año 2008 se activó el Plan de Internet Segura. Los objetivos eran: promover la seguridad en el uso de la red, identificar las prácticas que nos son seguras y facilitar consejos. Pero sobre todo, sobre todo, lo que se quería era que Internet fuera un entorno seguro para el menor. Y para eso había que empoderarlo y darle conocimientos y formación.

Un poquito lo que nos hemos encontrado desde 2008, en que las primeras charlas que hacíamos con menores, maestros y padres, era que tuvieran un sitio, que fuera un sitio común donde el menor navegara por Internet. Y bueno, esto desde 2008 a 2013, sobre todo yo diría que a partir de 2011, y 2012 ya fue exponencial, el menor o el joven dejó el comedor, y no se sabe dónde está. Está pero no se sabe... A ver, con cariño, aún están en el comedor, pero las posibilidades de interconexión en un ámbito no controlado, o sea, que tienes el terminal, esto es el futuro y el reto que los padres y todo el mundo tenemos que afrontar.

Por lo tanto, delante de esta estrategia de no ubicación, nos esforzamos más por trabajar lo que es la responsabilidad del menor. Ya sabemos que son menores y jóvenes, pero hay que hacerles en este ámbito responsables de lo que hacen, de sus actos y de lo que van colgando en Internet porque al final luego eso se les vuelve en su contra.

Las líneas de trabajo que desarrollamos en los centros educativos: hay tres ámbitos. Yo aquí no me extenderé mucho. Bueno, hacemos las presentaciones, que serían las típicas de Internet, de navegar, de las contraseñas, todo lo que hace falta en Internet.

Las cápsulas: eso va ya un poquito a demanda del grupo que tenemos, se puede trabajar más las redes o las contraseñas u otros niveles.

Y al final, lo que impulsamos el año pasado, y un poquito es lo que quiere dar respuesta a la red, son los talleres. Y aquí es donde sí que si-

tuamos al menor, con un relato con historias, en situaciones reales que se puede encontrar, o que le cuelgan la foto o que él es el que está insultando, o él es uno de los compañeros que ve cómo se insultan dos, o él es el insultado, y a ver cómo reaccionan para que recapaciten. Se van poniendo diferentes historias y aquí lo que queremos es que el menor, tanto el menor de menos de 13 años como el de más de 13 años, pues se vayan concienciando, que eso es importante, de que les va a marcar el futuro.

En principio serían estos tres tipos de técnicas. Están pensadas, se adecuan al nivel de lo que son los niños hasta los 13 años, jóvenes que están en la ESO y en los institutos, y luego, sobre todo a padres, madres y docentes; sobre todo, focalizados los talleres y las charlas de padres, madres y docentes a esa mediación activa del menor. Hay que acompañarlos en la navegación cuando son muy jóvenes, para que vayan cogiendo los hábitos, y sobre todo para que haya ese puente entre generaciones y que no vayan por libre o que se confíen más en otros menores o en extraños.

Un poquito, desde que se activó el plan de Internet, que se hizo a mediados de 2008: en estos cinco años más o menos hemos llegado a 500.000 asistentes. Prácticamente lo que les decía: unos 50.000 padres, unos 10.000 profesores, y el resto son alumnos en los diferentes ámbitos.

Los talleres —aquí lo verán, es de 2013—, es cuando los hemos empezando a impulsar: se diseñaron a finales del curso docente del año pasado. Es lo que está teniendo más éxito, porque realmente es donde los padres ahora sí que están más concienciados del riesgo que hay para los menores.

Cuando acabamos las charlas, pasamos unas encuestas, tanto a los niños, que son de 8-12 años, cuando tienen 13 ya pasamos a jóvenes. Y hacemos una serie de preguntas para ir dándonos la idea de cómo evoluciona el fenómeno.

Yo lo paso, lo pasaremos rápido. Pero un poquito, si a los chavales de 8 a 12 años les preguntamos si conocen los riesgos de Internet, antes de hacer la primer charla, un 24% nos dicen que sí, un 70%, alguno, y un 7% no tenían ninguna idea.

¿Cómo navegan? Esto nos va cambiando con los años, porque esto es una encuesta acumulada. Aún hay un 30%, y va evolucionando, que ya lo hacen —no es una parte común— en su habitación, en el estudio, en el comedor, que sería un sitio donde pueden estar controlados, estamos

hablando hasta 12 años (un 21%), y un 15% ya estaríamos con los portátiles o las tabletas o los *smartphones*, que ya no se pueden ubicar.

¿Mantienes conversaciones —abajo— con personas desconocidas? Un 1%, siempre; 3%, muchas veces; y 17% a veces. Por tanto, tenemos un 21% de menores que de alguna manera están contactando con desconocidos.

¿Cuántas personas tienes de agregadas en el correo electrónico o red social? Estamos hablando de chavales de 8 a 12 años. De 0 a 50, la mitad de los menores; de 50 a 100, el 19%; y más de 100, un 25%. Y estamos hablando de menores de 12 años.

Antes de tener contactos en la red, ¿ya conoces a las personas? Un 25% dice que a algunos sí o no; y un 6%, a ninguno. O sea, establecen contactos con gente que no conocen.

¿Por qué te conectas a Internet? Un 11%, para contactar con gente.

¿Cuántas horas a la semana te conectas? Un 5%, más de 20 horas.

Y cuando te encuentras con algo en Internet... ¿a quién acudes? De momento a los padres, un 62% (luego veremos que eso baja); a nadie, que eso es lo preocupante ya, un 13%. Estamos hablamos de menores hasta 12 años.

O sea, hay que fomentar estos vínculos, porque si no...

En la franja de los 13 a 17 años: ¿conoces los riesgos de Internet? Aquí hay un poquito más, un 33% algunos riesgos, y un 3%, no. Aquí hay una diferencia de dos, tres puntos con los menores.

¿En qué estancia te conectas? Aquí «mi habitación» ya sube a un 47%, estábamos en un 33%. Ya hay más autonomía, el comedor baja, un 18%. Y el 12%, en otro sitio, más o menos sería igual.

¿Con quién contactas o contactas con personas desconocidas? Un 2%, siempre; un 5%, algunas veces; y un 26%. Aquí nos iríamos al 33%. También que son adolescentes que en un momento determinado contactan con gente que no conocen.

¿Cuántas personas tienes agregadas? Aquí ya nos disparamos, porque más de la mitad de los jóvenes tiene a más de 100 personas, que es imposible. Siempre decimos nosotros que un amigo no es un contacto y un contacto no es un amigo; un contacto es un contacto de Internet, no se sabe quién es. Ya les damos consejos, claves, palabras para que se entre-

crucen, pero es imposible controlar agregados de agregados de agregados, pues cuentas con 200 o 300 personas, quién es cada uno.

Antes de tener contactos con la red, ¿ya los conoces personalmente? La mitad dicen que sí, y la otra mitad —prácticamente un 4%, no, en menores era un 6%, aquí es un 4%—, pero entre que sí y no, un 42%, que es más elevado. O sea, más o menos la mitad de los contactos no nos ofrecen fiabilidad.

¿A qué edad se empezaron a conectar? Y eso también hay que tenerlo en cuenta: antes de los 8 años, un 25% de menores. Y aquí lo dicen ellos, seguro que no se lo inventan. Aquí los padres tenemos una gran responsabilidad, porque aquí ni escuela ni maestros, aquí son los padres. Es decir, un 25% de menores se conectan antes de los 8 años. Aquí no discriminamos si tutelados o no, ya están en Internet el 25%; entre 9 y 10, el 47%; y el resto con más de 11 años.

¿Por qué se conectan? Un 18% para contactar con gente. Puede haber contenidos, pero para contactar.

Y más de 20 horas, pues el 20%.

Cuando te encuentras algo en Internet que te incomoda, ¿a quién se lo explicas? Un 21%, a nadie, se lo resuelven solos, o lo dan de baja, o se lo pasan; a los padres, aquí ya baja hasta el 36%; y aquí los amigos ya toman un rol de consultor o de acompañar en estos casos. A los profesores, aquí tampoco tenemos éxito, un 3%. Es lo que intentamos buscar, esa complicidad en el aula y en la familia.

¿Ha sido provechosa esa actividad? Esta es para ver cómo nosotros lo hacemos... bueno, en principio un 60% entienden que lo que vamos contando o explicamos, pues... Y el 7%, entendemos que ya tiene que estar o con mucho conocimiento, o es un irresponsable.

Referente a los padres, madres, estaríamos hablando de esas 60.000 personas que nos han escuchado, o a quienes nos hemos dirigido.

¿Conocía los riesgos de Internet antes? Un 25% nos dice que sí; un 72%, alguno; y un 3%, ninguno.

¿Conoces las ventajas de Internet? Más o menos quedaría equiparado.

¿Ha detectado usted algún riesgo para sus hijos en Internet? Un 30% podemos decir que son padres concienciados; el 50%, algunos; y un 21% que no, por lo tanto, estos no están ni se les espera, como decían...

¿Conoce a las personas con quien contacta habitualmente su hijo? Un 30%, sí; algunas, 50%; y ese 8% que no sabe con quién conecta su hijo en Internet. Aquí estaríamos hablando tanto de los de 8 hasta..., en cualquier edad, porque esto va dirigido a padres.

¿Comparte las conexiones con Internet con sus hijos? Un 23%, sí; un 51%, alguna vez; y el 20%, nunca.

¿En qué estancia tienen colocados los ordenadores? Esta ya nos va menguando: el comedor, un 25%; en las habitaciones del hijo, 22%.

¿Utilizaría alguno de los consejos dados por los Mossos? Bueno, en este caso, nosotros, el 60%, sí. Y si ha sido provechoso, pues aquí los padres son más agradecidos, y un 75%. A ver, supongo que también les ayuda y realmente también ven un poquito más toda esta trama.

Un poquito, bueno, de las encuestas ya hemos hablado.

El correo electrónico: aparte de la formación en las escuelas, también abrimos un correo electrónico, que esto lo tienen todas las policías, de Internet segura, porque ya que estábamos en los centros, pues nos llegaran noticias o lo que sea.

El año pasado, en 2012, tuvimos 627 correos. De estos más o menos se mantienen. En 2011 hubo 645. Sí ha habido alguno menos. De lo que nos llega por correo, que luego las denuncias también nos lo corroboran un poquito, aquí es desde una denuncia, una consulta, una página web que alguien dice que ha visto que le parece pornografía infantil... o una persona que denuncia su hijo que ha sufrido un robo de la identidad. Luego ya presenta una denuncia, pero nos llega por aquí.

Es que de estas 627, unas 42 del año 2012 serían en referencia a pornografía infantil. Lo que sí ocurre es que, comparado con 2011, eran 61. O sea, hemos detectado un descenso en este ámbito delincuencial.

Sí aumenta exponencialmente lo que es el tema de patrimonio. Todo lo que es falsificaciones, estafas, que afectan al patrimonio, este año 2012 eran 357, y en 2011 fueron 265. O sea, el ámbito del patrimonio es el que se incrementa exponencialmente porque cada vez hay más gente, lo que no afecta tanto a los menores. Pero lo que es en el ámbito del menor, y en ese caso en pornografía infantil, hemos reducido un 30% lo que nos ha llegado por correo, que también un poquito nos lo relaciona con las denuncias que tenemos.

Tráfico. El correo lo que nos permite es tener una línea directa con los centros, y nos llegan algunas noticias y algunas denuncias relevantes.

Las líneas de trabajo son: contra el honor, todo este tipo de delitos, que esto ya es... bueno, es lo que pasa, sobre todo contra el patrimonio y el orden socioeconómico.

En el ámbito de los ilícitos ya más concretos, yo suelo aquí comentar que de lo que es el *grooming*, que estaríamos relacionando, tanto hasta los 18 años como de menos de 13 años, aquí tuvimos 75 casos el año pasado, de los cuales 38 eran menores de 13 años. Y aquí sí que es preocupante porque los padres aquí..., sí que había algunos que, bueno, no lo acabaron de controlar, pero en otros estábamos hablando de huérfanos digitales, porque son muchos. Que de los 75 casos, más de la mitad, 38, fueran menores de 13 años, esto es que el control parental o estar un poquito encima de lo que hace el menor, pues no se estaba haciendo.

De todos estos delitos, lo que realmente afecta a personas, de los 7.693 que nos denunciaron a nosotros, que afecten a personas, y dentro de esto sería el *grooming*, las amenazas y estas cosas, son un 5%: 358. O sea, es un 5% de lo que se denuncia en el ámbito de actividad ilícita en Internet. En 2012 tuvimos estas 7.693 denuncias.

Para ver un poco la evolución: en 2008 tuvimos 600 casos que nos denunciaron. El 2008 es el año en que podemos decir que la policía autonómica se fue desplegando gradualmente en Cataluña, y en 2008 ya éramos responsables de todo lo que era el territorio catalán. Por lo tanto, los datos fiables, hasta ese momento se presentaban también denuncias en Guardia Civil o Policía Nacional. Pero a partir de 2008, todo esto, o al menos somos la policía ordinaria a la que se denuncian todos estos hechos; tuvimos 602. En 2009 hubo un aumento del 100%, pasamos a 1.600 casos. En 2010 hubo un aumento del 85%, pasando a 2.800. En 2011, 5.200; y llegamos a 2012 con esos 7.693 casos.

Aparte de esta línea del correo y de las denuncias, también queremos estar presente, tenemos, como todo el mundo, trabajamos el Facebook y el Twitter como elementos para estar presentes en Internet. Aquí también activamos campañas, o cuando hubo el tema de los *informers*, pues consejos, qué hacer, denunciar en la página para que el servidor o el que gestiona el servidor las dé de baja. Y en principio entendemos que como policía tenemos que estar en la red, tenemos que estar

presentes para mantener los vínculos entre menores, mayores, adultos, afectados, porque es otra realidad que hay, y en esa también tenemos que estar presentes.

De toda esta experiencia en el ámbito de la prevención, nosotros trabajamos tres elementos: uno es novedoso, lo estamos haciendo este año: los contenidos, con este trabajo que hacemos y con el Centro de Seguridad en Internet de Cataluña, CESICAT, preparamos los contenidos. Tenemos que insistir en formar a los docentes y a los padres, por supuesto. Y lo que estamos haciendo, en el plan este de seguridad en los centros ya hicimos alguna experiencia de trabajar profesores, alumnos, alumnos que hacen de mediadores y nosotros en determinados conflictos que no tienen nada que ver con Internet.

Y este año lo que hemos hecho, una experiencia piloto, que en principio se les preguntaba y nos dicen que va muy bien, es que hemos formado a alumnos de 4º de ESO para que hagan de formadores a los de 1º y 2º de ESO. Es otra faceta para ver si podemos conseguir más complicidad en el ámbito de que entre menores, si se lo explica el profesor o el policía, y se lo explica uno mayor, de 4º, «no, no hagas esto, porque mira a mí qué me pasó». Miramos a ver si así podemos incidir en los alumnos más pequeños, menores de 13 años, que los mayores de 13 años hagan de formadores de los 12 años.

Estamos haciendo una experiencia piloto en dos institutos de la zona del Vallès Oriental oriental. Y en principio, bueno, pues los que están interviniendo nos dicen que la cosa promete y que están muy contentos con esta actuación.

Esto ya son las direcciones.

Con el CESICAT trabajamos muy transversalmente, con el Departament d'Ensenyament, con el Centro de Seguridad de la Información de Cataluña que nos asesora, y si nos llega alguna cosa al correo, pues nos dan respuesta y nos ayudan a preparar las formaciones.

Y un poquito, yo sería..., este ámbito el que explicaría y, si hay alguna pregunta u observación crítica, lo que sea, aquí estamos abiertos a todo.

COMPARECENCIA DE LA FISCAL DE SALA COORDINADORA CONTRA LA CRIMINALIDAD INFORMÁTICA, DÑA. ELVIRA TEJADA DE LA FUENTE, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 27 DE JUNIO DE 2013.

La señora **FISCAL DE SALA COORDINADORA CONTRA LA CRIMINALIDAD INFORMÁTICA** (Dª Elvira Tejada de la Fuente): Muchísimas gracias señoría. En primer término, en nombre del Ministerio Fiscal español, en el de mi compañera doña Consuelo Madrigal Martínez-Pereda, como Fiscal de Sala Coordinadora en materia de Menores, y en el mío propio, quiero agradecer la oportunidad que nos dan de comparecer en esta interesantísima ponencia.

Primeramente quisiera recordar, como sus señorías saben, que el Ministerio Fiscal español es una institución de relevancia constitucional, que tiene unas funciones asignadas por la propia Constitución entre las cuales están la defensa de la legalidad, de los derechos de todos los ciudadanos y del interés público tutelado por la ley. El Ministerio Fiscal se rige por cuatro principios fundamentales, que también recoge el artículo 124 de la Constitución, que son los de legalidad, imparcialidad, unidad de actuación y dependencia jerárquica.

Y creo que es importante hacer referencia a los dos últimos porque, aunque son principios en torno a los cuales se articula, digamos, la estructuración y organización interna de la Fiscalía, tienen una proyección externa muy importante ya que, gracias a la vigencia de esos principios, el Ministerio Fiscal actúa de acuerdo con una unidad de criterio y ello contribuye a garantizar la seguridad jurídica y la igualdad de todos los ciudadanos ante la ley, que son valores que también proclama nuestra Constitución.

Los Fiscales tenemos encomendadas muchas funciones, numerosas atribuciones que concreta nuestro Estatuto Orgánico y que comprenden no solamente la actuación que asumimos en el ámbito jurisdiccional penal sino también en otros ámbitos jurisdiccionales. Así, entre otras, desempeñamos funciones muy importantes de carácter tuitivo en relación con los más desvalidos, con los discapaces y con los menores de edad.

Para poder desarrollar adecuadamente todas estas funciones nos hemos ido estructurando, sobre todo en estos últimos años, en áreas de especialización. Precisamente por ello, teniendo en cuenta que el objeto de esta ponencia es analizar la problemática que entraña la ciberdelincuencia, concretada especialmente en los riesgos que genera en los menores de edad, la comparecencia del Ministerio Fiscal en este acto se lleva a efecto a través de las personas que coordinamos las dos áreas de especialidad que confluyen en este tema: por una parte el área de criminalidad informática y, por otra, el área que se ocupa de protección y responsabilidad de los menores de edad.

Después de esta pequeña presentación, y entrando de lleno en la materia propia de mi competencia que es el área de criminalidad informática, me van a permitir que para centrar el tema haga primero unas valoraciones de carácter general: estamos ante un fenómeno criminal que no se circunscribe a delitos concretos, es decir, a un catálogo previamente determinado de delitos, sino que el concepto, en realidad, hace referencia a un fenómeno criminal que afecta a bienes jurídicos muy diversos y que puede servir de soporte a conductas delictivas muy variadas. De hecho más que ante un grupo de delitos estamos ante una forma de cometer ilícitos de muy distinta naturaleza que, no obstante, presentan todos ellos una serie de características comunes que, para dar una visión de carácter general, podrían resumirse fundamentalmente en tres apartados.

Primero la complejidad técnica que ofrecen estas investigaciones y el enjuiciamiento de estas conductas, lo cual genera unas dificultades significativas para los que carecemos de una formación especifica en la estructura y funcionamiento de las tecnologías, digamos, para los que tenemos una preparación eminentemente jurídica. En relación con estas actividades ilícitas resulta más complicado descubrir el delito, encontrar las pruebas ó determinar quiénes son los delincuentes, porque en muchas ocasiones ello exige el conocimiento de unas técnicas, instrumentos o herramientas en cuyo manejo, en principio, no somos expertos. Por contra ¿qué nos encontramos?, frente a nosotros tenemos a unas personas que suelen ser unos expertos manejando estas tecnologías y que saben utilizarlas para multiplicar las consecuencias de la actividad criminal y, lo que es más importante a efectos de persecución penal, para ocultarse y dificultar su identificación. Internet ofrece múltiples mecanismos para anonimizar las conductas y ello supone un primer problema para actuar ante esta forma de delincuencia.

La Fiscalía, está dando respuesta a esta situación basándose en dos parámetros que son fundamentales y que están muy relacionados entre sí: formación y especialización (luego me referiré un poquito más en detalle a este último aspecto).

Segundo tema, segunda característica común a estas actividades ilícitas, la especial vulnerabilidad en la que se encuentra cualquier ciudadano, y en especial los que son más débiles, los que están más desprotegidos, como los menores, ante esta forma de delincuencia. ¿Por qué? Porque se ha generalizado el uso de estas tecnologías entre todos los ciudadanos; porque ha penetrado en todas las facetas de nuestra vida, en nuestras relaciones a nivel personal, a nivel profesional, a nivel de ocio; porque sin querer, consciente o inconscientemente, estamos continuamente volcando en la red información sobre nosotros mismos que nos identifica perfectamente y que facilita que nos convirtamos en blanco de actividades ilícitas que pueden cometerse por personas que no conocemos, y con las que posiblemente jamás hubiéramos llegado a tener contacto fuera de la red: o sea, a veces, con nuestra propia actuación, nos colocamos un poco en el «punto de mira» de los ciberdelincuentes. Esto es especialmente llamativo, grave y peligroso en referencia a los menores de edad.

¿Qué ocurre además? Que el delincuente tiene a su favor un instrumento de fácil manejo que le permite potenciar los efectos de la actividad ilícita. Centrándonos en el tema de los menores de edad piensen, por ejemplo, que el daño que se le puede realizar a un niño con un trato degradante ó humillante a través de las redes es mucho más grave que el que se le puede originar en un contexto del mundo real porque a través de las redes sociales la ofensa se expande en cuestión de minutos a todo el haz de relaciones de la víctima y, en consecuencia, el perjuicio puede ser mucho más grave.

Y finalmente la tercera característica, que estimo muy importante y de especial relevancia en esta sede, es la necesidad de los ordenamientos jurídicos, de absolutamente todos los Estados, de mantener un proceso de adaptación permanente para ir dando respuesta a las situaciones nuevas que se van generando. Nos hallamos ante una realidad cambiante, ante una realidad que evoluciona muy, muy deprisa al hilo del desarrollo tecnológico, y que continuamente nos enfrenta a situaciones nuevas no previstas por la norma jurídica. Refiriéndome concretamente al ámbito que me corresponde, en mi responsabilidad como Fiscal encargada de

criminalidad informática, incidiría en dos grandes campos: el del derecho penal sustantivo y el de la investigación y el derecho procesal.

En el marco penal sustantivo es fundamental ir generando tipos penales que den respuesta a las nuevas conductas que se están produciendo, o ir adaptando los tipos ya existentes a la comisión de las correspondientes conductas a través de las tecnologías de la información y la comunicación, con el objetivo de disponer de una norma que haga posible la persecución y sanción de estos comportamientos capaces de lesionar bienes jurídicos merecedores de protección. Hay en curso ahora mismo un importante proyecto de reforma del Código Penal, al que luego me referiré específicamente, que aborda justamente la regulación de algunos tipos penales relacionados con el uso de las TIC´s y que nos interesan especialmente por afectar a menores de edad.

Y por otra parte el aspecto procesal, el aspecto de investigación, es también esencial. Porque estamos ante una forma de delincuencia en la que no sirven en términos generales como mecanismos de investigación muchas de las técnicas policiales de carácter más tradicional. Quiero decir con ello que, para investigar un delito cometido a través de la red, de poco van a servir, en muchos casos, técnicas como, por ejemplo, los seguimientos o las vigilancias policiales sino que este tipo de investigaciones exigirá, generalmente, utilizar en la indagación los propios sistemas informáticos. Y el problema es que en la actualidad no disponemos en nuestro ordenamiento jurídico de una regulación específica sobre muchos de los instrumentos legales que serían necesarios para ello.

Además esta cuestión es de especial importancia si tenemos en cuenta que tanto los ordenadores como los sistemas informáticos son herramientas —vamos a llamarlos así— capaces de almacenar una gran cantidad de información de carácter personal, y aptos para canalizar todas nuestra comunicaciones con terceros y a dicho fin están siendo utilizados de forma generalizada. En consecuencia muchas de las investigaciones que tienen por objeto estas herramientas pueden incidir de forma clara y evidente en derechos fundamentales de la persona y especialmente en los derechos a la intimidad personal y al secreto de las comunicaciones, amparados en el artículo 18 CE. Como ustedes bien saben cualquier investigación que afecte a derechos fundamentales exige unas garantías, unos cuidados muy especiales en la adopción de las medidas, en la realización de la investigación, para no lesionar los citados derechos. Es por ello que

resulta fundamental que cuanto antes se aborde una regulación adecuada de nuevas técnicas de investigación que permitan una actuación más eficaz frente a esta forma de delincuencia, garantizando, al tiempo, los derechos de los ciudadanos y la integridad y autenticidad de las evidencias que se vayan obteniendo.

No obstante he de aclarar que no estamos trabajando en vacío. Existen preceptos en la vigente Ley de Enjuiciamiento Criminal que pueden ser aplicados, y de hecho están siendo aplicados, en estos supuestos y disponemos de una Jurisprudencia y una doctrina del Tribunal Constitucional muy constante, muy consolidada y muy clara acerca de los parámetros que deben observarse en cualquier actividad de investigación que incida en derechos fundamentales. Y todo ello está sirviendo de base y fundamento en las actuaciones en curso. Pero sería bueno, como he indicado, que a la mayor brevedad posible se establecieran legalmente mecanismos específicos que ya están siendo necesarios para llevar adelante estas investigaciones con eficacia y con total seguridad y garantía.

Ante esta situación, el Ministerio Fiscal español se ha encontrado ante el reto por una parte de dar respuesta a estas situaciones y conseguir ser cada vez más eficaces ante esta forma de criminalidad y, por otra parte, de no ceder ni un ápice en nuestra función de defender los derechos y las libertades fundamentales. En esta circunstancia nuestra apuesta ha sido por la especialización: articular un área de especialización en esta materia que, sobre la base de una formación permanente y continua, permita mejorar y potenciar nuestras habilidades y destrezas en este ámbito.

Ello ha dado lugar a la constitución de una red de Fiscales, especialistas en la materia, que tengo el honor de dirigir en estos momentos y que se despliega por todo el territorio nacional. En la actualidad contamos con una unidad central, radicada en esta capital, y un servicio de criminalidad informática, en todas las fiscalías provinciales, que se integra por el delegado de la especialidad auxiliado de uno o más compañeros en atención a la actividad de la respectiva fiscalía (volumen de procedimientos, plantilla orgánica, dimensión territorial provincial etc.). A partir de esta estructura trabajamos en equipo, a través de una comunicación interna fluida y constante, poniendo en común nuestras experiencias y nuestras opiniones que, valoradas conjuntamente, nos permiten ir elaborando esos criterios comunes que son los que posteriormente, una vez refrendados

por la Fiscalía General del Estado, aplicamos en el desarrollo de nuestra actividad y en nuestra actuación ante los órganos judiciales.

Este trabajo en equipo, bajo los principios de legalidad y de imparcialidad, hace de esta área de especialización la *punta de lanza* del Ministerio Fiscal en la lucha contra este fenómeno criminal, porque esa experiencia compartida, y la preparación y conocimientos de los que nos vamos dotando, aprovechan a los restantes Fiscales, a la Institución en su conjunto, de tal modo, que nuestra labor es la de ir abriendo camino, ofreciendo soluciones ante este complejo fenómeno con tres objetivos fundamentales: potenciar las investigaciones por hechos de esta naturaleza, ejercer la acción penal contra los responsables criminales cuando tengamos pruebas suficientes para ello (y para eso intentar conseguir pruebas válidas y útiles para acreditar los hechos) y defender los intereses y los derechos de las víctimas y, en general, de los perjudicados por este tipo de delitos.

A partir de este planteamiento es un honor informarles acerca de nuestra experiencia (llevamos trabajando como red aproximadamente año y medio) en aquellos delitos vinculados al uso de las TIC´s que más afectan a los menores de edad. Y de paso aprovecharé, si me lo permiten, para hacer algunas sugerencias de modificaciones legislativas en relación con este tema.

Indudablemente el primer aspecto que hay que abordar es el de los delitos contra la libertad e indemnidad sexual de los menores, dentro de los cuales es obligada la referencia a los delitos de pornografía infantil. Es esta una tipología delictiva que se ha visto extraordinariamente potenciada con el desarrollo de las tecnologías de la información y de la comunicación (también ocurre con los delitos de estafa, pero ello excede del área de trabajo de esta Ponencia). De hecho un porcentaje elevadísimo de las investigaciones que se incoan cada año por hechos asociados a la pornografía infantil son actividades ilícitas cometidas a través de estas tecnologías.

No me extenderé en cifras sobre la dimensión de este fenómeno, pues sus señorías contarán con información suficiente sobre ello, pero estimo de interés destacar que, según la Memoria de la Fiscalía General del Estado correspondiente al año 2011, un 12,52% de los procedimientos judiciales incoados en España por conductas asociadas al uso de las TICs tuvieron por objeto delitos de pornografía infantil y/o en relación con

personas discapacitadas y el numero de acusaciones presentadas por el Ministerio Fiscal por hechos ilícitos de esta naturaleza se eleva a 368 en el mismo periodo anual.

Los tipos penales que sancionan los delitos de pornografía infantil están en permanente evolución porque todos los Estados están esforzándose por adaptar sus legislaciones internas a una normativa internacional que, a su vez, también va avanzando a medida que la propia Comunidad Internacional toma conciencia del peligro que Internet supone, en la proliferación de estos ilícitos y en la expansión de sus efectos, en un ámbito en el que tan gravemente se ven afectados los derechos e intereses de los menores de edad. El esfuerzo de armonización normativa es especialmente importante dada la dimensión transnacional de estas conductas, lo que hace imprescindible que los Estados adopten una estrategia legislativa común para facilitar la cooperación en la investigación y enjuiciamiento de estos delitos.

Precisamente uno de los temas en que incide el Anteproyecto de reforma del Código Penal actualmente en curso es el relacionado con estás tipologías delictivas, que en su vigente regulación pueden verse afectadas en aspectos importantes, sobre los que estimo oportuno llamar la atención de sus señorías en atención a la función que posteriormente han de desempeñar en el proceso legislativo.

Consideramos importante y positivo que el borrador incluya en el Código Penal un concepto de pornografía infantil, hasta ahora no contemplado en nuestro ordenamiento jurídico. La razón de ello es que nos hallamos ante un materia que puede verse afectada, digamos, por matices de carácter ético, moral, religioso, de carácter ideológico. Y es bueno que la propia ley, el legislador, defina qué ha de entenderse por material pornográfico, por pornografía infantil, para así ganar seguridad jurídica y garantizar que todos los operadores dispongamos, al respecto, de una referencia perfectamente definida. Lo que hace el proyecto es tomar el concepto de pornografía infantil que se recoge en la Directiva 2011/92/UE, relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil que, a su vez, hace suyo el que ya se contemplaba en la Convención de Budapest del Consejo de Europa.

Una segunda novedad destacable en el Anteproyecto es la tipificación como delito del acceso *on-line* a archivos con pornografía infantil. Permitan que me explique: en la actualidad en España son constitutivas de deli-

to, y así se sancionan en el artículo 189 del código penal, no solamente las actividades de producción, fabricación, venta, exhibición, distribución y difusión de pornografía sino también la posesión de material de esta naturaleza para el propio consumo. La tipificación de esta última conducta, tal y como viene definida por el código penal y tal y como se está interpretando por los tribunales, requiere, para que pueda apreciarse la existencia de delito, que se haya producido no solo el acceso al material sino también la descarga efectiva y la posesión del mismo durante un cierto periodo de tiempo por parte de autor del hecho. Por el contrario no es delito, hoy por hoy, en nuestro país, el visionado *on-line*, lo que es conocido como *streaming*, de pornografía infantil, circunstancia que no deja de resultar una incoherencia en la medida en que actualmente el consumo de pornografía infantil generalmente se realiza *on-line* sin que lleguen a efectuarse descargas directas. Por otra parte es evidente que la lesión al bien jurídico protegido es muy similar en uno y otro caso, es decir en los supuestos de posesión para propio uso y los de visionado *on-line.*

En consecuencia el Anteproyecto opta por sancionar también esta conducta de acceso *on-line*, siguiendo también en este aspecto la Directiva antes citada del año 2011 de la Unión Europea, sobre explotación sexual de los menores y pornografía infantil.

Finalmente, y en relación con este mismo tema, destacaría una tercera aportación muy interesante del Anteproyecto que puede tener una gran eficacia. Me refiero al hecho de que se contemple expresamente en el Código Penal la posibilidad de que el juez, en el curso de un procedimiento criminal, acuerde el cierre de páginas web con contenidos de pornografía infantil cuando ello sea posible, por encontrarse ubicadas en servidores radicados en nuestro país, o, en su caso, el bloqueo de la posibilidad de acceso desde España a estas páginas cuando las mismas se encuentren alojadas en servidores ubicados en otros Estados. La medida es importante para combatir este tipo de actividades ilícitas y en esa misma dirección apunta la última directiva europea. El Anteproyecto de reforma del Código Penal se refiere a la posibilidad de que el órgano judicial acuerde esas medidas con carácter definitivo, una vez dictada sentencia, y también, a petición del Ministerio Fiscal, con carácter cautelar, es decir antes de dictarse resolución sobre el fondo.

Actualmente estamos solicitando, y se están adoptando, medidas similares con apoyo en el artículo 13 de la Ley de .Enjuiciamiento Crimi-

nal y en los artículos 8 y 11 de la ley 34/2002 de servicios de la sociedad de la información y del comercio electrónico, pero es bueno que el Código Penal las contemple expresamente en su articulado, porque será una forma de potenciar el uso de las mismas y de soslayar cualquier duda acerca de su utilización.

En esta materia, relativa a los delitos contra la libertad e indemnidad sexual de los menores, es de interés la referencia a otro tipo de conductas, que desgraciadamente detectamos se están incrementando, y que son aquellas, vulgarmente conocidas como *child grooming*, en las que el agresor se aprovecha en general de las TIC y en particular de Internet para contactar con menores que no hayan alcanzado la edad para prestar el consentimiento para actos de contenido sexual y mantener con ellos una relación de esta naturaleza. Este comportamiento fue objeto de una tipificación específica en el artículo 183 bis del Código Penal, con ocasión de la reforma llevada a efecto por Ley Orgánica 5/2010 de 22 de junio, implementando en ese sentido la Convención de Lanzarote del Consejo de Europa.

Sin embargo, como ya alertó la Fiscalía General del Estado en su Memoria del año 2011, la rígida articulación de este tipo penal ha determinado que su aplicación práctica resulte escasa. La circunstancia de que el tipo penal contemple como victimas únicamente a los menores de 13 años (esto es porque en España actualmente la edad para prestar el consentimiento sexual está ahí, en los 13 años) y la exigencia de que la propuesta de mantener un encuentro con el niño deba acompañarse de actos *materiales encaminados al acercamiento* —que parece interpretarse como de carácter físico— limitan considerablemente la posibilidad de aplicación de este nuevo precepto. Como hemos podido constatar, en muchas ocasiones el autor de los hechos no pretende un encuentro físico con el menor, sino un encuentro virtual a los fines de lograr material pornográfico obtenido directamente o bien de inducir al menor a realizar ante la webcam actos de contenido sexual, circunstancia que determina que estas conducta —no incardinables, en principio, en este tipo— hayan de reconducirse, en su caso, a otros preceptos penales.

El Anteproyecto de reforma del Código Penal da respuesta a ambas limitaciones: por una parte eleva la edad de consentimiento sexual a los 15 años, lo que amplia el ámbito de aplicación de la norma en lo que se refiere a posibles victimas de estas actividades ilícitas. Esta medida, ade-

más, puede considerarse acertada porque España es, actualmente, uno de los países europeos que tiene fijado un límite de edad más bajo para prestar consentimiento sexual pues en los países de nuestro entorno el límite está en los 14, 15 e incluso 16 años, como es el caso el Reino Unido y Bélgica. Y por otra parte, y esta es la segunda aportación de la reforma, se tipifica también como delito esta misma conducta cuando el agresor no pretende el acercamiento físico sino la obtención de material pornográfico, con lo cual el nuevo texto saldrá al paso, si llega a ser aprobado, de los supuestos antes referidos y que actualmente quedan al margen de la aplicación del artículo 183 bis del Código Penal.

Resta reflexionar sobre una cuestión que dejo para el análisis y valoración por parte de mi compañera doña Consuelo Madrigal: me refiero a los supuestos en los que el agresor es un menor de edad, es decir, cuando estas conductas se producen por parte de menores respecto de otros menores. Al respecto ha de recordarse que tanto la Convención de Lanzarote del Consejo de Europa como la Directiva del año 2011 de la Unión Europea, antes citada, circunscriben la persecución y sanción de estas conductas a los supuestos en que el agresor es una persona adulta que contacta con menores para este tipo de actos, no cuando los actores son también menores de edad.

Las actividades ilícitas vinculadas al uso de las TIC´s que afectan a los menores de edad no son solamente aquellas que atentan contra su libertad e indemnidad sexual sino que hay otro ámbito en el que la incidencia es también muy importante, concretamente el de los delitos contra la libertad, la intimidad y la seguridad. El incremento de las amenazas, coacciones, humillaciones y en general de los actos que suponen un trato degradante a menores a través de estas tecnologías es también llamativo. Y esta circunstancia es perfectamente lógica, porque los menores —y con esto me permito citar datos del Defensor del Menor de la Comunidad de Madrid, según los cuales un 90% de nuestros menores hacen uso con asiduidad de las redes sociales— utilizan esos mecanismos habitualmente para comunicarse entre si, por lo que están todo el día interactuando en el mundo virtual. Por ello canalizan también por esta misma vía este tipo de comportamientos de carácter injurioso, ofensivo o humillante, cuyos efectos además se agudizan por la capacidad expansiva de la red y porque al agresor le es más fácil actuar de esta forma más despersonalizada y que le ofrece cierta sensación de anonimato.

Hay muchas formas de agredir a un menor a través de estas tecnologías. Se pueden utilizar mensajes SMS de contenido humillante o degradante; puede elaborarse o poner en funcionamiento páginas web en las que posteriormente se vierten mensajes ridiculizantes o que ofenden al menor; puede suplantarse la identidad del menor y atribuyéndole determinadas manifestaciones o expresiones, perjudicar sus relaciones con terceros; es posible también grabar al menor en situaciones comprometidas o que ofenden su dignidad para difundirlas luego en las redes sociales, o por mensajes de teléfonos móviles, etc. Es decir, las acciones concretas susceptibles de lesionar los bienes jurídicos que nos ocupan pueden ser muy variadas.

El Ministerio Fiscal está persiguiendo, calificando y sancionando estas conductas en base a distintos tipos penales: como delitos de amenazas ó coacciones, delitos contra la intimidad, delitos de descubrimiento y revelación de secretos e incluso, en los casos más graves, como delitos contra la integridad moral. La casuística a la que nos enfrentamos es muy rica y variada por lo que es imprescindible atender a cada supuesto concreto para valorar cual es la tipificación más correcta en atención a la dinámica delictiva y a las circunstancias específicas de cada una de las conductas.

Y como, además, a medida que van avanzando las tecnologías se van produciendo variaciones en las manifestaciones criminales, en ocasiones se van generando zonas de impunidad, en el sentido de que van surgiendo nuevas conductas, cuya sanción no esta prevista penalmente pese a que son susceptibles de lesionar bienes jurídicos merecedores de protección y ello determina la necesidad de abordar modificaciones legislativas en el sentido antes indicado. Y al respecto estimo oportuno referirme a una conducta concreta que es la de la suplantación de identidad, que se está produciendo con relativa frecuencia entre adultos y también entre menores de edad y que no tiene hasta el momento presente una respuesta especifica en vía penal. La Fiscalía General del Estado, en su Memoria del año 2011, alertó acerca de este comportamiento y abogó por su tipificación penal en determinadas circunstancias.

¿En qué consiste básicamente? Pues en suplantar la identidad de otro en todas sus comunicaciones *on-line* con carácter de permanencia y con unas connotaciones que aporten credibilidad, es decir, que la suplantación se haga en unas condiciones que induzcan realmente a error. Si se

hace en esas condiciones esta conducta puede implicar un atentado grave contra la privacidad y puede tener una seria incidencia en las relaciones de la víctima con terceros en la medida en que permite atribuir, a aquella, opiniones, planteamientos ó manifestaciones que no son suyas y afectan a su consideración pública. Todo ello sin perjuicio de los efectos de esa suplantación cuando se realiza con fines criminales específicos.

En relación con los menores este tipo de conducta se está detectando en distintas manifestaciones. En ocasiones se utiliza para suplantarles y perjudicarles en su relación con terceros, es decir, el delincuente se interpone en el haz de relaciones del menor con amigos y conocidos generándole situaciones conflictivas con el grupo. En otros casos la suplantación tiene por objeto acceder a información ó a datos íntimos del menor. En este último caso cuando el atacante es una persona adulta la finalidad, normalmente, es obtener algún beneficio de carácter sexual y para ello se engaña al niño, haciéndole creer que el interlocutor es un amigo, para así conseguir de la victima el envío de fotografías o videos o que realice, o deje de realizar, determinadas conductas. De hecho muchos de los supuestos de acoso a menores a través de la red se llevan a efecto utilizando este tipo de engaño en las fases iniciales de la actividad ilícita.

Por todas estas razones el área de especialización en criminalidad informática ha abogado por la tipificación de estos comportamientos. En relación con ello y como información complementaria parece oportuno comentar a sus señorías que algunos países, como Argentina y Perú, están trabajando en proyectos legislativos en esa misma dirección.

Y finalmente —cinco minutos y ya término— desearía hacer algunas aportaciones que considero importantes en el ámbito de la legislación procesal. Como les decía al principio nos encontramos con la circunstancia de que los instrumentos de investigación que tenemos legalmente articulados están pensados para ser utilizados ante una realidad delincuencial muy diferente a la que nos ocupa en este acto, ello hace que muchas veces estos instrumentos se nos queden cortos para investigar este tipo de actividades ilícitas, porque la tecnología ha ido proyectándose mucho más lejos.

Una de las figuras, por ejemplo, respecto de la que estamos percibiendo la necesidad de que sea objeto de una regulación complementaria, adaptada a la problemática que generan las investigaciones *on-line,* es la del agente encubierto. Es esta una técnica de investigación policial, regu-

lada en el artículo 282 bis de la Ley de Enjuiciamiento Criminal, que está siendo muy útil en la lucha contra la delincuencia organizada pero que, en la normativa actualmente vigente, esta planteada en atención a las necesidades de actuación ante grupos criminales de carácter convencional y con existencia en la vida real (es decir, en la realidad física) y que se dedican a actividades ilícitas como el tráfico de drogas, el terrorismo o la trata de personas.

La experiencia práctica nos enseña que esta técnica podría ser muy efectiva en el ámbito de la investigación tecnológica. Así piensen, por ejemplo, en las conductas que hemos comentado de acoso a menores a través de la red y en las ventajas que podría ofrecer la posibilidad de utilizar un agente policial que pudiera hacerse pasar por el menor, —una vez iniciado el delito para evitar supuestos de provocación—, y de esta forma facilitar la identificación del acosador. Sin embargo hay que admitir que la investigación *on-line* presenta peculiaridades propias que hacen que la normativa actual sobre esta materia resulte insuficiente a estos efectos.

A nuestro entender una regulación específica para esta materia habría de mantener las líneas básicas y esenciales de la figura, como son la exigencia de autorización judicial o del Ministerio Fiscal, dando cuenta de ello inmediatamente al juez; el control y seguimiento pleno y completo de la actuación del agente encubierto por parte del juez y la adecuación de la medida a criterios de necesidad y proporcionalidad, pues no hay que olvidar que no toda clase y categoría de delitos justifica el empleo de medios de investigación de esta naturaleza, ya que no se pueden matar moscas a cañonazos, permítanme la expresión. Pero sería necesario adaptar la normativa, en determinados aspectos, a las características de la investigación tecnológica.

Así, una primera dificultad que ofrece la actual regulación es que esta figura está planteada solamente para la investigación de determinados delitos y en todo caso en el marco de la delincuencia organizada. Al respecto hay que recodar en primer término que, en muchas ocasiones, las actividades ilícitas vinculadas al uso de las TIC´s nada tienen que ver con la delincuencia organizada sino que se presentan como actuaciones individuales e independientes unas de otras —insisto en la referencia a los acosadores de menores—. En segundo lugar, un buen número de los delitos enmarcables en el campo de la criminalidad informática no se encuentran incluidos en el listado del artículo 282 bis de la Ley de En-

juiciamiento Criminal, como es el caso de algunos de aquellos a los que me he referido anteriormente: las amenazas, las coacciones ó los delitos contra la integridad moral. Por ello sería bueno que se ampliaran las posibilidades de aplicación de esta figura a la generalidad de los delitos que se cometen a través de las TIC´s, sin renunciar en ningún caso —insisto en ello porque esto es importante— ni a criterios de proporcionalidad, ni al debido control de la actuación del agente por parte de la autoridad judicial y del Ministerio Fiscal. Es decir, en la concesión de autorización habría de valorarse, en cada caso, la necesidad y la proporcionalidad en función de los bienes jurídicos que entren en conflicto.

Otra cuestión que plantea la utilización de esta figura, en las investigaciones *on-line*, es la de determinar el momento a partir del cual es preciso obtener autorización judicial para la utilización de una identidad supuesta y actuar como agente encubierto. En el entorno de la realidad física es para todos evidente cual es el momento en que un agente se introduce en un grupo de delincuentes —que le identifican físicamente— utilizando un nombre y apellido que no son los propios y que justifica generalmente con documentación identificativa preparada al efecto. Pero no puede obviarse, cuando nos referimos a la navegación *on-line* —no ya a la actividad delictiva— sino a la navegación *on-line* en términos generales, que es frecuente y habitual el uso de *nicknames* o identidades supuestas por la generalidad de los usuarios sin que ello genere preocupación alguna en los restantes internautas.

Por tanto habría que plantearse si es exigible autorización judicial para usar, en esos términos, una identidad supuesta, ó al menos que no es la propia, cuando el agente policial, en el ejercicio de sus funciones, está llevando a efecto una navegación libre por la red, es decir, cuando no busca un objetivo plenamente determinado, en atención a hechos y personas, sino que está accediendo a *sitios* de información pública. Cuestión distinta sería si la navegación tuviera como objetivo el acceso a foros concretos, cerrados, ó si la pretensión, al efectuar una *navegación encubierta*, fuera precisamente la de ocultar la cualidad de agente policial, a través de un engaño deliberado, o prolongar una investigación que en otras circunstancias no hubiera sido posible. En estos últimos casos parece evidente la necesidad de autorización al juez. Lo que queremos poner de manifiesto es que esta es una materia que precisa de regulación específica en orden a establecer criterios acerca de las posibilidades de

actuación policial en Internet utilizando *nicks* o identidades imaginarias o supuestas así como de las circunstancias que harían exigible autorización judicial para ello.

Finalmente he de referirme a la tercera de las cuestiones que se plantea en relación con esta materia, y que se centra en las posibilidades de actuación del agente encubierto en determinadas investigaciones. Es un hecho constatado que en ocasiones para acceder a determinados foros, y en concreto a foros muy restringidos como son los de fabricación de pornografía infantil o aquellos en que se están gestando y organizando ataques informáticos muy serios, es preciso que quien pretende ingresar de alguna manera demuestre una cierta sintonía con la actividad ilícita que ahí se desarrolla. Es una medida de seguridad que adoptan quienes participan directamente en estas actividades para evitar ser descubiertos. Y ello obliga a plantearse la conveniencia de regular la autorización por parte del órgano judicial, a quien vaya a actuar como agente encubierto, para realizar actos concretos que en sí mismos serían constitutivos de delito pero que resultan imprescindibles para acceder a esos foros y continuar la investigación iniciada. Es una materia que habría que ir abordando legalmente, valorando en que supuestos sería posible esta actuación, cual sería el alcance de la conducta autorizada así como la forma y garantías con que llevar a efecto el control judicial de esta actividad.

Otra modificación que estimamos de interés, y que no puedo dejar pasar la oportunidad de trasladar a sus señorías, se refiere a determinados aspectos de la ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación. Hay que recordar al respecto que en la investigación tecnológica el punto de arranque de casi todas las indagaciones son los datos conservados por los operadores de servicios de comunicación pública, ya que, como bien saben, cada vez que accedemos a la red, o nos comunicamos a través del teléfono, el operador de comunicación pública que nos da la conexión registra y anota el dato de tráfico así generado. Esta información es esencial para averiguar, por ejemplo, quien ha proferido una amenaza a través de la red pues la determinación de la IP de conexión permite llegar a conocer, a partir de los datos almacenados, la procedencia de dicha amenaza y la identificación del autor.

La ley 25/2007 de 25 de octubre antes citada, que incorpora en España la Directiva 2006/24/CE, establece la obligación de los operadores

de servicios de comunicación pública de conservar toda la información sobre datos de tráfico (no de contenido), generados por telefonía móvil, telefonía fija e Internet, durante un año, para tenerla —dice la ley— a disposición del órgano judicial que necesite usar de ella en investigaciones criminales —y aquí viene el problema— por delitos graves.

El concepto de delito grave puede entenderse en dos sentidos; en sentido estricto delito grave es aquel que está castigado con pena grave, es decir, superior a 5 años, bien de privación de libertad o bien de privación de derechos. Pero también puede asumirse un concepto más amplio de lo que es delito grave, entendido como aquel que afecta a bienes jurídicos muy trascendentes (como los que afectan a menores), ó los cometidos por organizaciones criminales, ó los que generan grave alarma social, con independencia de la pena que corresponda al delito. Tradicionalmente la Fiscalía ha venido sosteniendo, y así era asumido por los órganos judiciales, que la referencia a delito grave que se efectúa en el artículo 1º de la Ley 25/2007 había que interpretarla en sentido amplio y ello ha permitido acceder a los datos de tráfico de comunicaciones, conservados por los operadores, en las investigaciones de los delitos cometidos a través de las TIC´s. Al respecto hay que recordar que casi todas las actividades ilícitas que han sido objeto de cometario en el curso de esta intervención son delitos menos graves y, por tanto, tienen prevista una sanción inferior al límite antes indicado.

Pero últimamente está tomando cuerpo una línea jurisprudencial que entiende que la expresión delito grave del artículo 1 de la Ley 25/2007 hay que interpretarla en sentido estricto, es decir, referida únicamente a delitos de pena superior a 5 años, lo que puede determinar que se cieguen las vías de investigación en muchos de estos casos.

La Fiscalía ya remitió hace varios meses al Ministerio de Justicia una propuesta de reforma legislativa, en la que trasladamos esta problemática y solicitamos la modificación, o, en su caso, la aclaración del concepto cuestionado en la Ley 25/2007, adecuándola al espíritu de la propia disposición legal y también al sentido de la Directiva del año 2006 y del resto de la normativa europea —como la Convención de Budapest del Consejo de Europa— que es el de potenciar la investigación de todos los delitos que se cometen a través de las TIC,s.

Aprovecho, por tanto la oportunidad que nos ofrece esta comparecencia para trasladar a sus Señorías nuestra preocupación por este tema,

dado los problemas que se están generando en las investigaciones de esta naturaleza.

Y finalmente, no más de un minuto, en referencia a otro tema de especial interés relacionado con esta misma disposición legal. La norma que nos ocupa solamente obliga a los operadores de servicios de comunicación pública, no así a los restantes operadores, a los prestadores de servicios de Internet que sustentan las redes sociales. Esto genera un vacío legal y tal vez fuera conveniente abordar la regulación de las obligaciones que se estimaran oportunas sobre conservación de datos y facilitación de datos a las autoridades competentes por parte de todos los prestadores de servicios de Internet, e incluso por parte de todas las personas físicas y jurídicas que realizan tratamiento de datos electrónicos, es decir, de datos derivados de estas tecnologías.

A ello se refiere específicamente la Convención de Budapest del Consejo de Europa sobre ciberdelincuencia que fue ratificada por España en el año 2010. Dicha Convención en su artículo 16 se refiere concretamente a ello, al instar a todos los países a regular legalmente la posibilidad de ordenar a cualquier operador de Internet la conservación de datos en supuestos determinados y su cesión a la autoridad competente cuando resulten necesarios en una investigación. En la legislación española todavía no se ha incorporado esta exigencia y sería bueno aprovechar las reflexiones que se están efectuando en este ámbito para abordar la implementación de la citada Convención en nuestra normativa interna.

Y nada más; lamento haberme alargado un poquito. Muchísimas gracias por su atención y quedo a su disposición.

COMPARECENCIA DE LA FISCAL DE SALA COORDINADORA DE MENORES, DÑA. CONSUELO MADRIGAL MARTÍNEZ-PEREDA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 27 DE JUNIO DE 2013.

La señora **FISCAL DE SALA COORDINADORA DE MENORES** (Dña. Consuelo Madrigal Martínez-Pereda): Muchas gracias por esta invitación y disculpen porque no tengo muy bien estos días la garganta.

Yo quisiera aprovecharme de la intervención que ha realizado mi compañera, Elvira, para ya dar por sentadas algunas cosas, aunque realmente aquí hay muy poco que dar por sentado. Solo querría decirles que el ámbito de actividad del Ministerio Fiscal que yo coordino expresamente es un ámbito bifronte, porque por un lado es la actividad del Ministerio Fiscal en la persecución de los delitos que cometen los propios menores, es la justicia juvenil. Y en este sentido, la experiencia de nuestra especialización es muy antigua, porque ya procede de la ley de 1992. Y luego, por ley, en el año 2000 se crearon las secciones de Menores en todas las fiscalías provinciales de España. De manera que los fiscales se dedican a la justicia juvenil de una manera especializada desde hace ya varios años.

Pero luego tenemos una actividad también, dentro de las secciones de menores, que es la protección de los propios menores de edad, la protección jurídica. Y esto inicialmente se refería fundamentalmente a la supervisión de la actuación de la administración en la protección de los menores de edad que se encuentran en riesgo de exclusión social, riesgos distintos, y los que se encuentran en desamparo. Esto es lo que sus padres, o por ausencia de padres o porque estos no se portan suficientemente bien, pues están desprovistos del necesario sustento moral y material. La administración interviene y el Ministerio Fiscal supervisa esta actuación protectora de la administración.

Pero junto con esta supervisión, las fiscalías cada vez han tenido una mayor intervención en la protección de los derechos de la infancia, no solo de los derechos fundamentales, al honor, a la intimidad y a la propia imagen, sino en cualquier situación en que un derecho de menores de edad pueda estar comprometido, bien a veces por riesgos muy puntuales, y pueden ser variadísimos, desde la ablación de clítoris y los matrimo-

nios forzados hasta el compromiso de la imagen de menores discapaces en los medios de comunicación, hasta los posibles perjuicios que puede sufrir un menor por la adscripción de sus padres a una secta o a una asociación peligrosa. De manera que tenemos un campo de actuación que muchas veces ha podido quedar, digamos, no orillado, pero silenciado en el ámbito de la actividad del Ministerio Fiscal, pero que cobra cada día mayor importancia debido a la mayor sensibilidad a los derechos de los niños en nuestro mundo.

Y en esto quisiera hacerles una precisión, si me permiten, y es que en mi experiencia, la atención a los derechos de los niños no solamente es una cuestión ética y jurídica, y además un interés social, evidenciado en la sensibilidad que existe hacia este tema. Es también algo que produce un efecto colateral en los derechos de los adultos. Y esta reflexión creo que es muy interesante en el ámbito de la protección de los usuarios de Internet, porque la protección de la infancia es el mínimo del mínimo ético, hay que proteger a toda la sociedad, pero por lo menos a los más desvalidos (a los niños, a los discapaces… a las personas que no pueden defender por sí mismos sus propios derechos. Y toda la teoría, la práctica y la dogmática respecto de esa protección van a redundar en la protección que todos los usuarios, también los adultos, necesitan, aunque sea matizada, pero abre camino para una protección más afinada, más completa de la sociedad en general. Y yo creo que esta reflexión, aunque sea interesada, puede abrir el camino e iluminar lo que debe ser la protección de los menores, en todos los ámbitos y en concreto en el que hoy nos trae aquí, que es el de Internet.

Y quisiera enlazar, antes de referirme a los temas que personalmente atañen a mi trabajo, con lo que dijo en una de sus intervenciones el senador Chiquillo, y también el senador Sendra, que hablaban de sus propios hijos; porque el Memorándum de Roma, que elaboró un grupo de trabajo a iniciativa de la Comisión Europea en el año 2008, distingue entre lo que son *inmigrantes virtuales* o inmigrantes en la red, que somos nosotros, personas ya adultas que en nuestra vida adulta, y con suerte, hemos accedido a las nuevas tecnologías y nos manejamos con ellas para nuestro trabajo y a veces para la diversión también, de lo que son *nativos virtuales*; los nativos digitales son nuestros hijos, que no es que accedan a Internet, sino que en la expresión gráfica del senador Sendra, viven en Internet, viven en las redes sociales y viven en el WhatsApp. Ahora mismo el WhatsApp, a falta de ordenador, incluso cuando los padres pueden

privar a sus hijos del uso de ordenador o supervisarlo, el WhatsApp queda exento de control e irrestricto frente a todo tipo de supervisión del uso que pudiera ser perjudicial para personas menores de edad.

También, si me permiten, aunque sea una reflexión un poco literaria o filosófica, puede apreciarse que las nuevas tecnologías, y concretamente la web 2.0, con las redes sociales y la telefonía móvil han realizado lo que es un golpe de Estado virtual, un golpe de Estado informático en el avance de la suplantación de la realidad por el mundo virtual. Se suplanta la realidad por lo que son sus apariencias. Como decía antes el senador Chiquillo en el futuro y ya ahora mismo una buena parte de los delitos se cometen de manera virtual. No todos los delitos, pero parte de los mismos se comete de forma virtual.

La suplantación de la realidad por sus apariencias ha sido el objetivo del arte occidental a través de la historia, pero de una manera rudimentaria, artesanal, local, muy concreta, ahora se produce de tal forma que puede ser cierta la anécdota de una persona que no sabía si le había ocurrido una cosa o la había visto por la televisión. Esto parece que es un chiste, pero cuando se trata de los niños, no lo es tanto. Y hay un cuento, el de *Alicia en el país de las maravillas* no, su continuación, que es *Alicia a través del espejo*, hay un momento dado en que la protagonista entra en el sueño del Rey Rojo. Y entonces se empieza a sentir muy incómoda, a sentir que se cae, que pierde el equilibrio, porque no controla su propia existencia. Y yo creo que esto es interesante a la hora de abordar la protección que debemos dar a nuestros hijos en Internet y la que deberíamos darnos a nosotros mismos, porque cuando uno vive en el sueño de otro, y esto es lo que ocurre a nivel planetario, porque las industrias de lo imaginario, de la publicidad y del mercado han colonizado completamente el planeta, cuando uno vive en el sueño de otro, no es libre, y mucho menos cuando ni siquiera es consciente de ello.

Y esto es lo que les ocurre a nuestros hijos, y a nosotros mismos en menor medida, porque vivimos menos en Internet, pero no porque seamos más conscientes, del rastro que dejamos de nosotros mismos cuando hacemos un clic o cuando conectamos, cuando llamamos por teléfono, cuando hablamos, cuando subimos una foto nuestra, de otro, etiquetada con su nombre...

Bien, esto es lo que buscan que hagamos las redes sociales a las que pertenecen nuestros hijos, o tal vez nosotros mismos. Las redes sociales,

puesto que son gratuitas, buscan algo, no ofrecen ese servicio benéficamente, buscan datos personales. Porque los datos personales que se consiguen con cada clic, con cada tecla que nuestros hijos y nosotros tocamos en Internet, tienen un enorme y un inmenso valor de mercado, es el valor de la publicidad, permiten a las redes sociales o las plataformas servidoras de Internet hacer rastreos, segmentar, localizar eventuales destinatarios e identificándolos con la dirección IP, segmentar la publicidad y distribuir convenientemente los mensajes publicitarios que envían a cada tipo de usuario. Esto tiene un valor en el mercado muy alto, o lo suficientemente alto como para que para obtenerlo las plataformas presten sus servicios de manera aparentemente gratuita.

Entonces, ¿desde dónde debe venir la protección? Desde las obligaciones de las plataformas respecto del tratamiento de esos datos personales que nosotros y nuestros hijos, en concreto, les ofrecemos a veces tan confiadamente.

¿Cuáles son los riesgos específicos que al ofrecer nuestros datos personales, o sus datos personales nuestros niños, tienen en Internet? En primer lugar, los riesgos son los mismos, pero incrementados porque la neuropsiquiatría nos indica cómo el cerebro adolescente, el cerebro de los niños, sobre todo el de los adolescentes, más aún que el de los niños pequeños, valora de una forma muy diferente el peligro, lo afronta de una forma diferente porque no tiene los recursos —no sé si empleo la palabra más adecuada— del sistema límbico que permiten al adulto reaccionar más defensivamente frente al riesgo.

Los números —tampoco les voy a agobiar con esto— cantan cuando el 77% de los usuarios de redes sociales en España no tiene su perfil cerrado. Esto puede parecernos extraño, pero el 77% de los usuarios jóvenes, adolescentes, entre 14 y 18 años tiene su perfil abierto, cuando los principales riesgos pueden concretarse precisamente por el fácil acceso a los perfiles abiertos en Facebook, en Tuenti ….

Los padres se pueden preocupar de que sus hijos cierren ese perfil, pero yo me pregunto: ¿lo hacen, lo hacemos, las padres conocemos las claves de suscripción a Tuenti de los niños más pequeños, o a Facebook de los que son mayores? ¿Nos preocupamos de que lo tengan cerrado? En fin, este sería un aspecto.

Otro aspecto es el de que rara vez leen las instrucciones o las condiciones de privacidad de los servidores y de las plataformas, Sobre todo de las

redes sociales. Es verdad que estas tienen unas condiciones de privacidad mayores, menores, más o menos amplias o restrictivas, pero no las tienen por defecto, y este es el principal inconveniente. Por defecto es el perfil abierto, por defecto se ofrece el acceso público a los datos personales del usuario. Hay que leer una letra pequeña, que es comprensible pero no siempre fácil de localizar, para configurar la opción de privacidad. A partir de ahí vienen los riesgos de ser víctima de una serie de delitos, etc.

Pero no quisiera centrarme exclusivamente, porque ya lo ha hecho Elvira, sobre todo, y porque podemos hacerlo también al final, en la protección frente a los delitos que existen y que son los más graves, y que es donde nosotros, los Fiscales, actuamos fundamentalmente. Pero yo creo que debemos actuar previamente en una protección civil de los datos de carácter personal que no se quede en la defensa frente a los ataques a bienes jurídicos más importantes que protege el Código Penal (la integridad moral, la libertad sexual, la dignidad, el honor);

Se trata de redefinir, valorar y proteger la privacidad. El concepto de privacidad que es mucho más amplio. También aquí, en último lugar, usted ha hecho referencia a esta idea, aunque sea de una manera colateral, porque no es solamente los delitos que se pueden comentar en nuestro nombre, o respecto de nosotros, sino el mero hecho de que se nos atribuyan opiniones absurdas, estúpidas y tontas, aunque eso no sea un delito, a un político o a cualquiera, es algo perturbador. Ahí tenemos cantidad de riesgos, sencillamente porque se nos conozca, aunque solo sea porque se nos conoce.

Entonces, nosotros intentamos defender a los niños, y a los niños frente al uso indiscriminado de sus datos por esta menor percepción del riesgo y menores posibilidades de reacción ante el riesgo. Pero también por otra cuestión, no solamente porque le pueden victimizar o restringir su libertad sexual sino porque todos los datos que un joven vierte en Internet, sus propias palabras, sus propias actuaciones, su vida virtual, es una vida que está descontextualizada, porque es la apariencia de la realidad, pero no es la propia realidad. Ese mismo niño a sus padres, a sus abuelos, en su trabajo, a su profesora, le hablaría de una forma muy distinta de lo que le puede hablar en Internet, porque la barrera virtual inhibe los frenos psicológicos, descontextualiza la relación, y puede dirigirse a sus profesores, a sus compañeros, a sus padres, de una forma muy diferente de lo que lo haría en la vida real.

Entonces, la cuestión nosotros la orientamos en un doble sentido: en una protección que pudiera ser puramente civil el tratamiento de los datos, la protección de los datos de carácter personal de los niños. Y aquí nos encontramos con que hay una protección que procede de los propios sistemas informáticos, de Internet, pero es muy insuficiente en nuestro país, porque tenemos —y de esto Elvira quizá pueda hablar mejor y sepa más que yo—, pero los filtros, la encriptación, los cortafuegos... Bueno, la encriptación de los mensajes es tan complicada que solo la utilizan las redes de pederastia y las redes de narcotráfico, porque se necesitan profesionales tan cualificados para desencriptar que no es un recurso doméstico de padres y familias. Y los filtros y cortafuegos no requieren toda esa especialización, ¿pero qué ocurre?: que quedan inmediatamente superados por los programas cambiantes y constantemente dinámicos que ofrece la propia red. Entonces, un filtro puede quedar obsoleto en cuestión de semanas prácticamente. Y quedan también desvirtuados por el hecho de que los propios niños son mucho más expertos que sus padres y que los técnicos que han instalado el filtro, en muchas ocasiones, y aunque esto sea un chiste, pero en Fiscalía muchas veces tenemos un problema, tenemos el ordenador mal y decimos «que venga el técnico, por favor, que venta el técnico». Y yo digo: «no, no llamemos a un niño». Porque el niño te puede solucionar a veces tus propios problemas mucho mejor. Entonces, ponerle el cortafuegos al equipo es pan para hoy y hambre para mañana.

Están los ciberpolicías, que son entidades como FIRST o CERT que ofrecen servicios de investigación en tu propio ordenador, en tu propio programa, en los contactos sobre los propios hijos.

En esta línea, la propia Agencia Española de Protección de Datos ha dirigido unas recomendaciones en el año 2009, y en 2008 y en 2010.

La primera de esas recomendaciones es la navegación conjunta de los hijos con los padres. Es una recomendación excelente pero que tiene muy poco seguimiento. Pocos padres tienen tiempo para dedicar a sus hijos en todos los órdenes de la vida, aunque este me parece que sería el tiempo mejor invertido, pero la realidad es que vuelven tarde del trabajo y están tan cansados que si el hijo está en Internet, bendito sea Dios, ¿no? Bueno, yo creo que esto es la experiencia de las fiscalías y de las secciones de menores, que cuando ya vemos a ese niño o adolescente cometiendo otros delitos, el padre no sabe nada de lo que ha hecho su hijo

durante muchísimo tiempo. Esto es una digresión, pero esta sí sería una buena recomendación si pudiera hacerse efectiva.

También se recomienda que los niños utilicen Internet en entornos siempre personalizados.

Y se recomienda —y esto, creo que es muy importante— que los propios padres adultos, educadores, profesores respeten la privacidad de los niños, y que salvo casos muy excepcionales (que yo creo que deberían estar en el ámbito de la justicia juvenil y de las sospechas de la comisión de algún delito por parte de los niños), no debe nunca monitorizarse el ordenador a un chico no ponerle sistemas de geolocalización en el móvil ni videovigilancia, porque si queremos transmitir aprecio por la privacidad, lo que hay que demostrar es aprecio por la privacidad de los propios niños a los que queremos hacer esa transmisión de valores.

Pero desde el año 2009 la Agencia Española de Protección de Datos hace hincapié en una autoprotección, en realidad, del usuario, y llama al usuario a tener respeto por la privacidad ajena, a tener siempre la precaución de que cuando se sube una foto etiquetada nunca sea con el nombre verdadero de la persona que aparece en la imagen, sea propia o sea de otros. Y esto sobre todo tiene importancia cuando subimos fotos de terceros, porque en alguna ocasión... A mí misma me pasó: un hermano mío encontró unas fotos en Internet con el Facebook de otra persona, porque había estado yo en una fiesta campestre, y yo no tengo Facebook siquiera, ni he subido jamás una foto mía. Pero esto, mientras no tiene trascendencia, porque es una cosa que, aunque sea familiar, pero no deja de ser riesgo, porque no todos estamos en fiestas campestres. La fiestas de nuestros hijos, rara vez son campestres, suelen ser nocturnas, y no son siempre bonitas. E incluso, aunque las fiestas sean —entre comillas— bonitas, la foto no es bonita, con los ojos rojos, las botellas, las copas en la mano, poca ropa... Hablo en el mejor de los escenarios. Por desgracia, ¿no? Estoy hablando solo de lo que pudiera ser una protección civil.

¿Pero qué nos encontramos también? Pues nos encontramos con algo que es la realidad, y la ley recoge la realidad: la edad para consentir el tratamiento de datos de carácter personal, en el reglamento del año 2007 de la Ley de Protección de Datos de 1999 se fija en 14 años; de manera que el menor de edad pero de más de 14 años puede consentir la cesión y el tratamiento de sus datos de carácter personal.

Esto me lleva a anticipar lo que hubiera querido hacerles como recomendación final: yo creo que la protección penal es imprescindible, pero la protección penal está para los supuestos más graves, que como ha dicho Elvira y podemos ver, son muchos y muy variados y afectan particularmente a las personas menores de edad. Pero es la mínima. Antes debe hacerse una prevención. Quiero decir que es la *ultima ratio*, es la última intervención de los poderes públicos; antes, las intervenciones deben ser preventivas. Y creo que es esencial la prevención a través de la educación: educar en la privacidad, en el valor de la privacidad.

Y mi propuesta en este sentido es la de inclusión en los repertorios curriculares del bachillerato y de la educación general obligatoria de asignaturas sobre privacidad: tanto como valor ético, como sobre los mecanismos de protección, de respeto, del valor social y personal de la privacidad como componente inherente de la propia personalidad. Y por supuesto, en los valores éticos de su respeto cuando es bien jurídico de otras personas.

Pero también sería muy interesante, de cara a otros atentados más graves, una asignatura sobre la comunicación en Internet, que no es tanto sobre materias tecnológicas o informáticas, sobre las que los niños sí que saben, sino sobre el tipo de comunicación, el tipo de vida y el tipo de relación que se establece en Internet. Yo creo que la gramática es siempre necesaria, y nuestros hijos ahora mismo no la conocen suficientemente bien ni la manejan bien, pero es mucho más necesario lo que pudiéramos llamar lenguaje virtual, los análisis de la estructura de la comunicación en internet, la identificación y el análisis de los textos de Internet, del tipo de lenguaje que no es un lenguaje gramático ni es el lenguaje de la vida real, sino el lenguaje virtual. La significación; en realidad no sería gramática, sería semiología virtual, porque esto dotaría a los niños de mayores recursos a la hora de identificar contenidos, identificar procedencias de esos contenidos. Puedo poner un ejemplo que es muy gráfico, aunque por supuesto reduccionista: si yo les envío a ustedes un mensaje de correo electrónico de WhatsApp sabrán perfectamente que tengo más de 50 años y que estudié en un buen colegio, porque pongo acentos, porque pongo todas las palabras, saben que soy una señora mayor, como mínimo; este sería el abecé de la asignatura que yo estoy diciendo, porque por el correo electrónico puede uno saber muchísimas más datos del interlocutor.

En definitiva, creo que esta sería quizá la principal autoprotección a la que se refiere la Agencia Española de Protección de Datos, aunque no lo menciona de esta manera.

Pero luego existiría también la posibilidad de una protección civil de los derechos fundamentales que pudieran verse comprometidos, que está vinculada a la protección con el derecho al honor, la intimidad y la propia imagen. Y aquí encontramos una paradoja: en la vida real, en los medios de comunicación (las cadenas de televisión, la radio, pero sobre todo las cadenas de televisión y los periódicos) existe una gran cantidad de cautelas y garantías y una protección muy fuerte de la imagen de los niños y de sus propios datos personales, sobre todo cuando es inconsentida. Y nuestras leyes, la Ley Orgánica 1/1982, de protección de estos derechos tienen unos contenidos específicos respecto de los menores de edad, y la Ley de Protección Jurídica del Menor de Edad también; incluso el fiscal puede actuar de oficio en casos en que han sido consentidos por el propio niño y sus propios padres, si él considera que el contexto en que salen es negativo, es perjudicial para los derechos del niño.

Sin embargo, esta protección en los medios de comunicación habituales del mundo real no se da en el ámbito de Internet. No conocemos ningún caso en que se haya planteado una demanda del honor o la intimidad desde el punto de vista civil. Sí que ha habido una sentencia del ámbito de resoluciones vinculadas al trágico caso de Marta del Castillo, porque unos padres actuaron contra, primero era contra un medio de comunicación, que eran Canal Sur y Telemadrid, porque habían publicado en sus programas imágenes de amigos de Marta del Castillo que ellos mismos habían subido a YouTube. Estas cadenas de televisión las cogieron de YouTube y las publicaron en su programación habitual, en la época en la que el interés por el asunto estaba más álgido. Los padres dijeron: no hemos autorizado la aparición de nuestros hijos en Internet... En Internet sí, pero los propios chicos mayores de 14 años; pero las cadenas dijeron: pero como las hemos cogido de YouTube hay un consentimiento tácito. Un Juzgado de primera instancia de Sevilla;, condenó a Canal Sur y a Telemadrid al pago de unas indemnizaciones porque se entendía que el consentimiento para el tratamiento de los datos en Internet no abarcaba el tratamiento de los datos en televisión.

¿Qué quedaría para una posible acción de responsabilidad civil? Pues el tratamiento inconsentido, el que puede darse cuando se trata de niños que no tienen 14 años que se han inscrito o registrado como si

los tuvieran, porque la suplantación del perfil realmente es muy fácil en las redes sociales; es fácil porque las propias redes sociales —hay que decirlo claramente— no se cuidan de esto. Porque mecanismos tecnológicos para comprobar luego o para impedirlo hay muchos más de los que ponen en marcha.

Cabría plantearnos si se podría realizar algún tipo de acción civil por esta vía cuando se tratase de datos o no consentidos (no consentida su instalación en la red) o consentidos por menores de 13 años. Y podríamos plantearnos (y yo creo que esto deberíamos hacerlo) la responsabilidad civil de la plataforma, del servidor por no haber tenido la diligencia debida en el registro de menores de 14 años. Hasta ahora no se ha hecho, pero yo creo que podría hacerse. ¿Por qué no se ha hecho? Pues porque la mayor parte de los ataques que llaman la atención de los padres (porque los hijos están más bien desprevenidos) es ya constitutiva de delitos. Y entonces, la reacción va por la vía del delito, que permite exigir una responsabilidad civil subsidiaria. Pero yo creo que deberíamos extender la protección civil, porque estamos en un ámbito; el usuario ordinario de es víctima de delitos, pero sí es víctima de atentados a su intimidad que son atentados civiles y que deberíamos tener una mayor movilidad en el ámbito de la responsabilidad civil por la exigua protección de los datos de carácter personal de nuestros hijos, y extensivamente, y por extensión, después finalmente también de los nuestros.

Entonces, podemos pasar también al ámbito de la protección penal, que es, digamos, el ámbito de mayor incidencia de la actuación del Ministerio Fiscal. En el ámbito civil, no digo en mi fiscalía, en las secciones de menores estamos trabajando ahora con la protección de la imagen de menores discapaces, tanto en medios de comunicación (y estos sobre todo) como también en el ámbito de la red. Porque no se trata solo de los atentados que los discapaces pueden padecer, fundamentalmente a su integridad moral, estos son por supuesto constitutivos de delito cuando son objeto de vejaciones, de injurias, de insultos; no, me refiero también al tratamiento de la discapacidad contrario a lo que debe ser la imagen social de la discapacidad según la Convención de los Derechos de Personas con Discapacidad, convención de Naciones Unidas del año 2006. Y esto también merece una protección y una reacción desde el punto de vista civil a la que las plataformas no deberían ser ajenas.

Aquí nos encontramos, tanto en este ámbito como en cualquier otra actividad ilícita —paso ya con ello a hablar de la posible exigencia de

responsabilidades penales—, con que las plataformas de redes sociales y los servidores son en principio irresponsables por los contenidos ilícitos. Y esto es así porque lo dice la propia ley. Los artículos 13 a 17, creo que son, de la Ley de Servicios de la Información y de Comercio Electrónico establecen que los servidores y las plataformas de redes sociales no responden por los contenidos ilícitos que puedan albergarse en Internet a través de sus servicios. Esto es lógico, porque es imposible imponer un control al ingente o infinito mundo virtual. Pero, sin embargo tiene la contraprestación de que deben cooperar activamente con la autoridad competente, normalmente la autoridad judicial, y a veces, muchas veces basta la sugerencia del Ministerio Fiscal) en la retirada de esos contenidos ilícitos, en el bloqueo de las páginas que las albergan y, por supuesto, en la suspensión del servicio cuando afecte a servicios más amplios que una mera página de Internet.

La verdad es que sí cooperan en esto una vez que son advertidos. Aquí nos encontramos con que la cooperación es real, pero a veces lenta, por lo que ha dicho antes Elvira: los servidores y las plataformas de redes sociales radican normalmente en Estados Unidos. Facebook se remite siempre para cualquier conflicto a las leyes de California y a los tribunales de Santa Clara, y MySpace siempre a las leyes y tribunales de Nueva York. Google es, yo creo, más receptiva, aunque nos dificulta un poco la trayectoria, tenemos que ir por unos vericuetos de advertencia y tal que, como sabe muy bien Salomé por alguna intervención que hemos tenido conjuntamente hace poco tiempo, es lento; está previsto para que esa comunicación y esa actuación sean en cuestión de horas o días, pero en realidad requiere un tiempo mayor. Pero finalmente prestan esa colaboración. Incluso ha habido una reunión de varias redes sociales americanas, Facebook y otras 19 más, con 49 fiscales generales de Estados Unidos, en la que la mayor parte de esas redes se comprometieron a realizar una mayor protección, sobre todo de los menores, en Internet, estableciendo —esto no lo han hecho por defecto— el sistema de privacidad con la inscripción —esto no se ha hecho—, pero sí bloqueando el acceso de mayores de 18 años a los perfiles de menores de edad cuando no están aceptados. Esto sí lo han hecho algunas más, por lo menos está más hecho.

Pero tanto estas recomendaciones en Estados Unidos como las iniciativas europeas han tenido un seguimiento muy desigual. La propia Unión Europea, que instó las iniciativas del Grupo 29 en el año 2009, y en el

año 2011 hizo un seguimiento investigando a 14 sitios, sobre todo de redes sociales, vio que de esas 14 investigadas solo 2 tenían la privacidad por defecto (Bebo y otra, no me acuerdo cuál era), y que solo 4 tenían limitado el acceso de mayores de 18 años a perfiles de menores de edad no consentidos; de forma que es bastante grave porque hay muchas otra redes sociales (en España Tuenti) que esto todavía no lo tienen limitado, el acceso de mayores de 18 años a perfiles de menores de edad cuando no están voluntariamente abiertos por el menor; si el menor lo abre, ya no se podría hacer nada. Pero incluso cuando lo tiene cerrado no está garantizado que a través de la amistad de la amistad de la amistad, un mayor de 18 años pueda acceder al perfil cerrado de un usuario menor de 18 años.

Y para terminar con alguna pincelada sobre los riesgos de Internet para los menores en el ámbito de la justicia juvenil, quiero decir, aquellos riesgos que son constitutivos de delito y que proceden de otros usuarios menores de edad, y que se examinan primero en las fiscalías y por los juzgados de menores.

Son varias las conductas, aunque sí que es cierto que encajan en su mayor parte en el repertorio de delitos que hay en el Código Penal. Ocurre muchas veces que es difícil, y tenemos que acostumbrarnos —digo tanto la policía como los fiscales como los jueces— a la descripción de los hechos. Porque una vez identificado el hecho y bien descrito, encaja en uno o en otro tipo penal, salvo la suplantación del perfil informático, que ese sí que es verdad que nos plantea mayores problemas, si una vez que se ha suplantado la identidad informática no se cometen, tras esa suplantación, otros delitos. La mera suplantación del perfil informático, yo creo que no es en sí misma delictiva, como no es, dejó de serlo en el Código de 1995, el uso indebido de nombre supuesto. Decir que eres otra persona, ahora no. Ahora bien, hacer actos inanes, intrascendentes a nombre de otra persona en Internet, yo creo que hoy no tendría tipificación penal, aunque nadie quiere que otro actúe por él, pero si es un acto intrascendente («hoy me he levantado, hoy he bebido»); yo creo que vale la pena tipificar con distintos matices y distintas gravedades. Nunca vale la pena imponer excesiva penalidad a las conductas, porque es mucho más posible la aplicación del tipo penal cuando la pena señalada es proporcional, pero por lo menos la tipificación de esta figura.

Las demás sí que están tipificadas. La primera sería el *cyberbullying*. Ya sabemos que el acoso escolar ha cedido terreno, pero no es que haya

cedido terreno, sino que ha cedido el espacio escolar, los patios y las aulas y se ha trasladado al WhatsApp, a las redes sociales, y en definitiva, a la vida en el ciberespacio del que estábamos hablando antes. Y aquí por eso se ha hecho en cierto sentido más grave. Se ha hecho más grave porque está mucho más alejado del control de los adultos, más alejado de los profesores y de los padres, sobre todo en el WhatsApp, donde los padres, precisamente por la volatilidad de las imágenes, que pueden ser borradas (y los contenidos) inmediatamente, pues no tenemos ya los padres ni los educadores ningún control. Y además se ha hecho más grave porque la difusión de las ofensas, del escarnio se concentra; hay una concentración del universo relacional del menor a través de las redes sociales. Porque tiene unos pocos amigos (digamos pocos o no tan pocos, 50 o 60), pero esos lo saben todo de cada uno de ellos. Y si alguien sube una fotografía, a veces nos preguntamos: una condena porque unos amigos subieron una fotografía de un tercero y le han hundido entre sus redes, ¿esto qué es? Hombre, hay que ver la fotografía. A lo mejor la fotografía era él, pero salía comiendo a dos carrillos o salía feo o salía desnudo o salía...

Entonces, este ciberacoso otras veces se nutre también de otros delitos, como son peleas, golpes, palizas, situaciones de escarnio que se graban con los móviles y se difunden entre el grupo de amigos, entre el grupo del colegio, etc.

En el *cyberbullying*, sin embargo, las posibilidades de reacción son múltiples. Ya tenemos una instrucción del año 2006, cuando era más que nada fundamentalmente el acoso escolar; y solo han pasado seis, siete años y ya no es solo acoso escolar sino *cyberbullying* lo que más nos preocupa. Pero en esta instrucción del año 2006 sí que tenemos criterios para afrontarlo, y sobre todo en el ámbito de la justicia juvenil, para atajarlo, y siempre y cuando se cuente con las propias redes y servidores para bloquear los contenidos o eliminarlos del ámbito del ciberespacio.

Otra de las conductas es el llamado *sexting*; esto es el contacto, que puede ser de un adulto o de otro menor, con un niño o con un joven, normalmente en el ámbito de relaciones sentimentales o de relaciones de amistad, facilite imágenes íntimas con o sin ropa, o de contextos sexuales, que luego son utilizadas (no siempre, pero son utilizadas) como chantaje para obtener otro tipo de favores de carácter sexual o más imágenes, bien para nutrir acopios de pornografía infantil o para cualquier otro tipo de chantaje.

Del *sexting* pasamos a la «sextorsión». Y esta figura ya es más grave por los efectos devastadores que puede causar en el ofendido, y normalmente la encajamos en el de los delitos contra la integridad moral, como delito. En los casos menos graves, como el ciberacoso, también en algunos casos menos graves podría ser falta. Y aquí la jurisprudencia no es del Tribunal Supremo. Tenemos jurisprudencia, porque estos hechos no llegan al Tribunal Supremo, sino que se quedan ordinariamente en las audiencias provinciales, y puede ser muy variada. El hecho de que muchas audiencias provinciales utilicen el argumento de que el hecho no es tan grave porque ha sido realizado en la red, para calificarlo como falta, y al mismo tiempo en otros casos, que es más grave porque ha sido realizado en la red, para calificarlo como delito, nos revela o nos indica la indeterminación o la confusión que incluso en el ámbito de nuestra propia jurisprudencia puede existir todavía y existe todavía respecto del alcance de la suplantación que decíamos antes de la vida real por sus apariencias, que yo creo que es mucho más importante de lo que a veces los adultos, inmigrantes y no nativos en Internet, nos damos cuenta.

Luego están las amenazas, las coacciones, que adquieren esta mayor trascendencia por realizarse en el ciberespacio. Y está la pornografía infantil, de la que ha hablado ya Elvira, no voy a incidir en esto, pero que a veces nos encontramos con que realizan o cooperan en su realización las propias personas menores de edad. Es frecuente que en las redes de pornografía infantil haya algún menor de edad que tanto por sus conocimientos informáticos como por su mayor proximidad a menores puede aportar el material o elaborarlo técnicamente.

Sin embargo, cuando hablamos de este caso que estoy comentando, pues es verdad que la reacción de la justicia juvenil contempla mecanismos, digamos, de cierto rigor, aunque siempre la justicia juvenil tiene intervenciones educativas. Pero hemos recomendado y seguimos recomendando la prudencia cuando se trata de los mismos comportamientos realizados por menores de edad. Porque a veces el comportamiento realizado por un adulto, cuando lo realiza un menor de edad tiene una trascendencia, un significado en su propia vida y en su contexto muy diferente. Es imprescindible analizar las causas, el contexto, la educación, la propia relación del menor con los contenidos pornográficos, para adaptar la respuesta, normalmente pedagógica o educativa, o de tratamiento psicológico, si es que lo precisara, al menor.

Y la propia Fiscalía General del Estado, en una de las últimas circulares, la 9/2011, recomienda ir a las soluciones alternativas, a la desjudicialización, que permite no juzgar y estigmatizar al menor, que a lo mejor puede tener algunos contenidos pornográficos, muchas veces realizados con niños de su misma edad. Y con esto quisiera ya terminar. En estos casos vale la pena adaptar, para evitar el estigma que puede suponer el proceso y el juicio, dar una solución alternativa por la vía de las tareas educativas o la sumisión a tratamiento sin necesidad de un juicio y una condena.

Pero sí quisiera hacer, antes de terminar esta exposición, desde el punto de vista de las propuestas legislativas, incluso en relación con el borrador del nuevo Código Penal, la idea de que tanto los delitos de pornografía infantil como los delitos de abusos sexuales, en definitiva, todos los delitos relacionados con la libertad y la dignidad, hay que tener en cuenta que el Código Penal se aplica también a los menores de edad; en la justicia juvenil aplicamos el Código Penal para la definición de las conductas, aunque luego las consecuencias sean distintas, no son penas, son medidas, y tenemos un repertorio de medidas diferentes, todas educativas y tal, e incluso la privación de libertad se enfoca siempre con esa finalidad educativa. Pero la conducta, la tipificación, el hecho es el mismo.

Y aquí nos encontramos con un grave problema, si el legislador no adopta la cautela de establecer una asimetría de edad como presupuesto de muchos de los delitos. El abuso sexual es abuso sexual también aunque lo cometa una persona de 17 años con un menor de edad, que puede tener también 17 años. Y cuando no hubiera mediado engaño y el único fundamento para el abuso sexual sea la disimetría de edad (uno de 30 con uno de 14), se entiende; pero la misma conducta realizada entre dos personas de 17 años, o de 17 y 14 o de 17 y 15, incluso ya de 14 y 13, que es el abuso sexual siempre y sistemáticamente, porque la edad de consentimiento sexual ahora mismo está fijada en los 13 años, pues yo creo que las reformas de los tipos penales deben contemplar también que se van a aplicar a menores de edad, y que cuando se aplican a menores de edad tendrían que tener por lo menos ese presupuesto mínimo de una disimetría de edad que como mínimo, como mínimo, fuera de 5 años.

Porque el tema guarda relación también con la edad de consentimiento sexual, que es verdad que la española está muy baja en relación con

otros países europeos, pero tampoco debemos llevarlo a una altura que quede fuera de la realidad social en que nos movemos. Nuestros niños se mueven en un ámbito en el que están constantemente viendo imágenes sexuales, películas con contenidos sexuales, relaciones sexuales normalizadas en el ámbito escolar y académico (pensemos en las series como *Física y Química*, o *Al salir de clase*, sobre todo *Física y Química* o el internado de tal), donde los profesores, con profesores, con profesoras, con alumnos y tal... Es verdad que esa es una realidad también virtual, pero es la realidad en la que viven nuestros niños, y aunque no sea cierto, porque entonces nadie podría dedicarse al trabajo, pero sí que están en un mundo altamente sexualizado, y luego criminalizar todos los comportamientos que se realicen con personas de menos de 16 años, incluso el matrimonio a partir de los 14 años, por supuesto que hay que elevar esa edad, pero sin criminalizar la vida social.

En fin, esto es un poco lo que, dentro del espacio que se me ha concedido, podría decirles, pero estoy a su disposición para cualquier cuestión o pregunta o sugerencia que quieran plantear.

COMPARECENCIA DE LA DIRECTORA GENERAL DE SERVICIOS PARA LA FAMILIA Y LA INFANCIA, DÑA. MARÍA SALOMÉ ADROHER BIOSCA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 27 DE JUNIO DE 2013.

La señora **DIRECTORA GENERAL DE SERVICIOS PARA LA FAMILIA Y LA INFANCIA** (Dña. María Salomé Adroher Biosca): Muchísimas gracias, señor presidente, miembros de la Mesa, señores senadores, les doy las gracias por habernos invitado y dado la oportunidad para participar en esta ponencia conjunta de estudio sobre riesgos derivados del uso de la red por parte de los menores.

La infancia, como saben, es uno de los colectivos prioritarios para el Gobierno, y por ello en la Dirección General y el Ministerio de Sanidad, Servicios sociales e Igualdad estamos trabajando intensamente en favor de los niños, de la infancia; de ahí la importancia de poder compartir con ustedes las líneas de trabajo y también las reflexiones que estamos llevando a cabo en torno al objeto de esta ponencia.

A lo largo de mi intervención haré alusión al tándem de menores y nuevas tecnologías desde una doble perspectiva: primero, como oportunidad, las nuevas tecnologías como oportunidad formación de apertura al conocimiento, de generar igualdad de oportunidades. Pero también, en segundo lugar las nuevas tecnologías como riesgo; como riesgo para todas las personas pero también para los niños.

Quería comenzar con lo que puede ser un buen resumen de la hoja de ruta de nuestro Gobierno y en general de los poderes públicos de España, y me refiero a las observaciones que nos hizo llegar el Comité de Derechos del Niño de Naciones Unidas a España en 2010, y una concretamente referida al tema que nos trae hoy aquí. Se nos animaba a que prosiguiéramos nuestra labor «de promover la existencia de medios de comunicación de calidad que contribuyan a la alfabetización digital de los niños, garantizar que la televisión pública tome la iniciativa y ejerza una función de liderazgo en la creación de programas responsables durante las horas de máxima audiencia de los niños, dando prioridad al desarrollo de estos y no a los beneficios económicos, contando con la participación de los niños en la elaboración del contenido y del diseño

de los programas infantiles; alentar también a las empresas que operan en el sector de Internet a que adopten códigos de conducta adecuados; y alentar la capacitación de niños y adultos para navegar con seguridad por Internet».

Mi intervención va a tener fundamentalmente tres partes. En primer lugar, quiero resaltar el interés de la Dirección General a la que sirvo en esta materia; en segundo lugar, aportar brevemente algunos datos en torno a cuatro grandes ejes temáticos; y finalmente, exponerles las líneas de trabajo que estamos llevando a cabo en nuestra Dirección General.

1. Interés de la Dirección General de Servicios para la Familia y la Infancia en esta materia.

Es evidente que la enorme expansión de Internet y de otros medios en la última década supone una revolución en las comunicaciones, y también supone en positivo nuevas posibilidades y nuevos retos para el ciudadano, tanto en el acceso a la información como en el acceso a la comunicación.

La infancia, también los mayores, pero la infancia está muy presente en la red; su gran capacidad de aprendizaje, su gran capacidad de adaptación hace que gran número de niños sean usuarios de Internet, y naturalmente muchos de ellos con habilidades superiores a los adultos. El *quién socializa a quién*, en este caso simboliza muy bien la situación actual, porque al final son nuestros hijos los que muchas veces nos enseñan a nosotros, los padres, a utilizar estas nuevas tecnologías.

Otra cuestión es el contenido de la red. Nadie duda que es un buen instrumento para difundir información, opinar, debatir y comunicarnos, pero también que puede tener sus riesgos; riesgos de importancia, por contenidos, en alguna ocasión, éticamente reprobables (aparecen contenidos de discriminación racial, de violencia de género, de manipulación psicológica, de incitación al consumo de bebidas alcohólicas, entre otros); oportunidades y riesgos de estas nuevas tecnologías que aparecen además recogidas en la Convención de Naciones Unidas de Derechos del Niño, que por una parte reconoce el derecho de los niños a buscar y difundir información, pero les reconoce también el derecho a ser protegidos contra toda la información y material perjudicial para su bienestar, así como contra cualquier injerencia arbitraria o ilegal en su vida privada,

su familia, domicilio, correspondencia, y cualquier ataque a su honra y reputación.

Y también la Convención de Naciones Unidas de Derechos del Niño subraya la responsabilidad de los padres, tutores, representantes legales y educadores a la hora de proporcionar a los niños y niñas directrices y orientaciones apropiadas para que ejerzan los derechos que les son reconocidos.

Por ello, ahí tienen los tres ámbitos de trabajo, entiendo que para todas las administraciones públicas, singularmente también para la Dirección general a la que me honro en servir.

En primer lugar, el primer reto es garantizar el acceso a esta importante herramienta de comunicación; el objetivo es reducir la brecha digital entre menores con acceso y sin acceso a Internet, de cara a garantizar la igualdad de oportunidades en el ámbito educativo, social, cultural y, desde luego, para su futuro desarrollo profesional.

Pero el segundo reto es el buen uso, la necesidad de proteger a la infancia de contenidos inapropiados, como lo señalaba y lo recordaba hace un momento en relación con la Convención de Naciones Unidas de Derechos del Niño y a todas las iniciativas que voy a compartir con ustedes tendentes a una cada vez más adecuada utilización de Internet, para lo cual son agentes fundamentales padres, educadores, y los propios niños; hablaremos de la responsabilidad de los propios niños en el conocimiento y buen uso de estas herramientas, y el utilizarlas con valores y pautas y comportamientos socialmente aceptables, advirtiendo de los posibles riesgos.

Riesgos respecto de los cuales subrayo particularmente la explotación sexual como más preocupante.

2. Algunos datos.

Generalización del uso de las TICs.

En primer lugar, debemos destacar la generalización del uso de las TIC por los menores. Según la encuesta sobre equipamiento y uso de tecnologías de la información y comunicación en los hogares del INE de 2012, el uso de ordenadores entre la población infantil de 10 a 15

años es prácticamente universal: el 96% de los niños tiene acceso a los ordenadores en nuestro país, y el 91,2% utiliza Internet. Hay diferencias por sexos: el número de niños usuarios y de niñas no es exactamente el mismo, pero el acceso es, como vemos, universal.

Estos resultados suponen que el uso de Internet, y especialmente del ordenador, es una práctica frecuente en edades incluso anteriores a los 10 años. También es interesante subrayar que la disposición al teléfono móvil aumenta de forma considerable con la edad, hasta el punto de que a los 15 años el 91% de los niños ya dispone de un teléfono móvil. Por tanto, es una herramienta a la que tiene acceso una parte importante de nuestros niños.

El papel de las familias

¿Y qué papel tiene las familias en el uso o abuso de las nuevas tecnologías por los menores? Aunque hay muchos estudios publicados sobre esta materia, voy a referirme a dos.

En la Universidad Pontifica Comillas, en la que he trabajado durante 26 años, hicimos en 2008 un estudio, en el cual entrevistamos a 15.000 niños de toda España sobre cuestiones diversas: ha sido la mayor muestra de una encuesta realizada directamente a los menores que se ha hecho en España y que ha dado lugar a dos publicaciones.

Una de las conclusiones que arroja sobre este punto es cuanto más solos están los niños, cuanto menos tiempo pasan con sus padres, más tiempo pasan frente a aparatos electrónicos, sean estos los que sean, a los cuales tienen acceso de una forma generalizada; y en consecuencia cada vez se produce un mayor aislamiento y soledad, y por tanto una mayor influencia del grupo de iguales, que a veces es buena y a veces no tanto.

Pero también da la situación inversa: los niños que por diversas razones tienen más fácil acceso a estos medios acabarán renunciando paulatinamente al contacto social, incluso familiar, a medida en que su gusto o adicción por el uso de las nuevas tecnologías vaya haciendo mella en ellos.

Podría profundizar sobre esa idea del papel de la familia, de la conexión entre el uso y abuso de las TIC y la conciliación de la vida laboral y familiar de nuestras familias pero esta correlación supone una llamada de atención.

El otro estudio al que quiero referirme lo llevó a cabo INTECO en el año 2009 titulado *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y la e-confianza de sus padres*. Este estudio muestra cómo padres e hijos nos aproximamos a las TIC de forma diferente. Los padres solemos ser usuarios con una finalidad concreta (transacción bancaria, comprar *online*, consultar noticias, mandar un WhatsApp); los niños se aproximan con un interés de una forma más global, más natural, más total y lo usan para todo: estudiar, charlar, escuchar música, etc.

Curiosamente, lo que más preocupa, según este estudio, a padres y madres, es el riesgo de dependencia o uso abusivo, muy por delante de otras situaciones más problemáticas, como acoso, *sexting,* etc….

Los padres, los adultos, necesitamos herramientas que nos ayuden a valorar objetivamente la gravedad de las situaciones a las que se enfrentan nuestros hijos y reaccionar de una forma adecuada ante una situación de riesgo.

¿Cómo reacciona el menor ante una situación de riesgo? El 85% de los niños manifiesta que no ese capaz de dar respuesta; y de ellos, solo un 1% declara que si se encontrara en una situación de riesgo se lo contaría a sus padres, pediría ayuda a sus padres. En cambio, cuando les preguntan a los padres «¿crees que tu hijo, ante una incidencia de seguridad o de peligro, acudiría a ti?», más del 30% de los padres creen que sus hijos recurrirían a ellos como primera opción. Luego no existe correspondencia entre lo que contestan los niños y lo que contestan los padres en relación con la confianza o al acceso a sus padres en caso de peligro. Eso apunta también alguna cuestión que sería importante tener en consideración y tomar en consideración en nuestras políticas familiares y en nuestras políticas de formación a padres.

Conductas disfuncionales y adicciones

La literatura científica ha puesto de manifiesto cómo los nuevos sistemas de comunicación aumentan nuestras posibilidades de contacto social pero generan efectos perniciosos cuando su uso se vuelve desmedido. Y eso nos pasa a mayores y a pequeños, hay un peligro de adicción, y por ello desde la Delegación del Gobierno para el Plan Nacional sobre Drogas está atendiendo también a esta nueva situación.

Son tantas las posibilidades de acceder a información, estar permanentemente conectado, no sentir la amenaza de la proximidad física para insultar o para hacer un comentario negativo hacia otra persona, que lo que paradójicamente es una oportunidad puede transformarse fácilmente en una conducta disfuncional o en una adicción.

Cabe mencionar un estudio reciente, *Conductas adictivas a Internet entre jóvenes europeos*, de 2012, financiado por la Comisión Europea, que no da buenas noticias para España. La relación entre redes sociales y conductas disfuncionales e Internet alcanza su mayor proporción en España, de tal forma que el 39,2% de los adolescentes que pasan más de 2 horas al día en redes sociales presentan conductas disfuncionales en Internet, frente al 13% de aquellos que pasan menos de 2 horas diarias. Por tanto, el peligro de la adicción, del consumo desmedido de estas nuevas tecnologías, es cierto.

En cuanto al consumo de televisión, también ahí podría darles datos, no voy a hacerlo, televisión, videojuegos, etc., que apuntan también en esta línea.

TICs y comportamientos violentos

Un escalón más en riesgo de las nuevas tecnologías es la incidencia de la violencia en los medios de comunicación y en los comportamientos violentos de menores. La adicción era el primer riesgo; el segundo es la violencia. Desde hace más de treinta años diversas de investigaciones, relacionan directamente comportamientos violentos y actitudes agresivas con la violencia, primero en la televisión, y ahora también en los videojuegos, en Internet, en las nuevas tecnologías en general. Los niños expuestos a muchas horas de televisión o de otros medios acaban «disfrutando» de un alto nivel de violencia.

Pornografía infantil, ciberacoso y ciberbullying e internet

Y el último escalón de riesgo, el más problemático ya roza directamente el ámbito penales cuando las nuevas tecnologías desembocan en pornografía infantil, ciberacoso y otras formas de violencia.

Según datos presentados el 14 de enero de este año, de 2013, en la sede de la Comisión Europea en Madrid: el 13% de los adolescentes

españoles entre 14 y 17 años ha sufrido situaciones de acoso en Internet o *cyberbullying*; el 9,4% de los adolescentes reconoce haber acosado a alguien a través de Internet; el 68,3% de los adolescentes, que ha sometido a alguien a ciberacoso reconoce acosar a otras personas; y el 47,8% —fíjense en esto— de los adolescentes que ha sufrido ciberacoso ha terminado acosando alguna vez, esto es como el que ha sido maltratado de niño, que maltrata. Parece que estas conductas se reproducen cuando uno las sufre, y esto nos tiene que hacer pensar a los que tenemos que tomar decisiones.

Hay que considerar que el 74% de los menores en nuestro país está registrado en una red social antes de los 14 años; de entre los menores de edad, un 15% afirma haber subido fotos o vídeos para perjudicar a alguien; un 13% se había sentido mal por lo que otros subieron a la red; entre el 40% y el 55% de los escolares están implicados de algún modo como víctimas, agresores u observadores; entre el 3% y el 10% de los jóvenes sufre victimización grave; el 88,6% de los menores españoles con móvil entre 10 y 16 años hace fotografías con su móvil; el 48,2% las envía a otras personas, y el 20% las publica en Internet.

Podía hacer alusión a más datos sobre pornografía, ciberacoso o *cyberbullying*, pero creo que los tenemos a nuestra disposición en diversas investigaciones, y solo quería poner la atención en esta cuestión.

3. Líneas de trabajo de la DGSFI (Msssi).

Si el punto de partida es considerar las TIC como oportunidad y como riesgo, si los datos de las diversas investigaciones y encuestas nos ofrecen las conclusiones a las que acabo de referirme, desde la Dirección General de Servicios a la Familia y la Infancia con competencias transversales, ¿cuáles son las acciones que estamos llevando a cabo y en qué estamos embarcados?

Las he agrupado en cuatro grandes líneas: primero, planificar en planes estatales, nacionales lo que se hace por parte de la Administración General del Estado, y también de las comunidades autónomas, en este ámbito, la planificación como herramienta fundamental para que todos rememos en la misma dirección.

Segundo, la prevención: esto quizás es lo más característico de una Dirección General de Servicios para la Familia y la Infancia, dado que

nuestro acceso al ciudadano está mediado a través de ONGs, Comunidades Autónomas, Corporaciones locales, etc…

En tercer lugar, la participación; y en cuarto lugar la coordinación administrativa como tarea fundamental.

Planificación

Comienzo por lo más reciente: Plan Estratégico Nacional para la Infancia y la Adolescencia (PENIA) 2013-2016, que ha aprobado recientemente el Consejo de Ministros. Uno de los objetivos del plan, el 3, se dedica precisamente a esta cuestión: impulsar los derechos y la protección de la infancia con relación a los medios de comunicación y a las tecnologías de la información en general.

Debe tenerse en cuenta que además de la consulta a todos los centros directivos de la Administración General del Estado con competencias en esta materia, y naturalmente también a comunidades autónomas y a ONG, este tema fue tratado de forma monográfica durante la elaboración del plan en un seminario de preparación organizado en el observatorio de la infancia en colaboración con Red.es.

Yo agruparía las medidas de este objetivo (hay otras medidas incluidas en otros objetivos que están también relacionadas directamente con esta cuestión) en torno a esos tres ejes. El primero, el fomento del uso responsable de estos medios a través de la sensibilización y formación a los niños, familias y profesorado, es decir, buen uso, buen uso de Internet, visión crítica de la televisión, etc. La segunda es la promoción de unos medios de comunicación de calidad y responsables, para lo cual se regularán contenidos a los que acceden los niños y se promoverá la educación en valores.

El tercer grupo de medidas tiene que ver con el control y sanciones, y contiene medidas dirigidas a establecer controles sobre contenidos de programación en televisión y franjas horarias, mejorar niveles de seguridad en la red, diseñar códigos de autorregulación relacionados con el uso de Internet y naturalmente, incluir nuevos tipos delictivos en el Código Penal en estrecha colaboración, como así hemos hecho, con el Ministerio de Justicia.

Una vez aprobado este plan en el Consejo de Ministros, la Dirección General de Servicios para la Familia y la Infancia, y a través suyo el obser-

vatorio de la infancia, somos los encargados de impulsar que estas medidas vayan llevándose a cabo a lo largo de todo el periodo de vigencia del plan.

En relación con este último aspecto del plan, control y sanciones, estrechamente relacionado con él debo mencionar el tercer Plan contra la Explotación Sexual de la Infancia, el PESI 2010-2013, que contiene varias medidas que tienen que ver fundamentalmente con la parte de control y sanción: potenciar la colaboración con Fuerzas y Cuerpos de Seguridad del Estado con la base de imágenes de pornografía infantil de Interpol, sensibilizar a la sociedad en general y a las familias sobre el uso seguro de las nuevas tecnologías, crear áreas específicas para niños y niñas en establecimientos cibernéticos, etc.

Estamos elaborando también un plan integral de apoyo a la familia. Hemos realizado ya toda la fase de diagnóstico del plan y estamos comenzando ya con grupos de trabajo para diseñarlo; este plan recogerá también medidas específicas en el ámbito de las nuevas tecnologías para potenciar servicios, medidas y políticas que ofrezcan un entorno favorable y positivo para la vida familiar, incluyendo medidas directamente vinculadas a padres y madres para facilitarles el ejercicio de las responsabilidades de educación, cuidado y supervisión de sus hijos.

Prevención y formación

La segunda línea de trabajo de la dirección general es lo que hemos querido denominar prevención, formación a pares y profesores. Es quizás esta el área más característica de una Dirección General de Servicios para la Familia y la Infancia, pero que necesariamente debemos llevar a cabo a través de la colaboración institucional, tanto con otras instituciones públicas como con el tercer sector de acción social.

En relación a la colaboración pública la Dirección General ha venido colaborando con Red.es y otras instituciones para desarrollar campañas y jornadas de sensibilización tanto a padres como a otros profesionales sobre el buen uso de Internet y medios de comunicación por parte de los menores. La plataforma para canalizar todo esto es la plataforma del Observatorio de la Infancia.

En relación con la colaboración con el tercer sector de acción social, debemos poner en valor y destacar la labor de apoyo técnico y financiero que prestamos a las ONG de infancia, y también de familia, que desarro-

llan su labor en este ámbito, a través fundamentalmente de la convocatoria anual de subvenciones con cargo al 0,7% del IRPF, y también las de ayudas al tercer sector.

Si bien es difícil cuantificar exactamente la cuantía que se ha destinado a estas acciones, en 2012 se han subvencionado con unos 453.000 euros a ONGs que desarrollan proyectos de formación y campañas de sensibilización para padres, madres y educadores; formación para la divulgación de los derechos de la infancia a través de la web, creación de redes sociales educativas para la participación infanto-juvenil; herramientas prácticas para padres y educadores en relación con la navegación segura de los menores por la red y prevención del abuso sexual infantil a través de las nuevas tecnologías.

Finalmente merece la pena hacer una alusión final a la parentalidad positiva, es decir, el apoyo a padres y madres en el ejercicio de nuestras responsabilidades de crianza, cuidado y educación de nuestros hijos. Ya saben que es un nuevo enfoque de intervención psicosocial, más basado en potenciar las capacidades que en actuar frente a las carencias y de forma reactiva. Y en los programas de parentalidad positiva, en los que ha sido líder siempre esta Dirección General durante muchísimos años, se ha estado trabajando, con comunidades autónomas para identificar buenas prácticas en esta materia, con las corporaciones locales a través de la FEMP y con el tercer sector a través de la línea de programas de parentalidad positiva en el IRPF.

Participación

La tercera línea sería la referida a acciones de participación infantil. Y en este punto, hacer una muy brevísima alusión a esta red, a ciberresponsables, financiada desde el año 2010 por la Dirección General. Es una red creada en el marco de la plataforma Organizaciones de Infancia para servir como plataforma donde los chicos y las chicas entre 12 y 17 años, organizados en grupo, que publican sus propios blogs o espacios personales a través de una información suficientemente contrastada. Es decir, no se trata solo en esta segunda y tercera línea de ayudar a que padres y educadores sepamos manejar esta situación de la brecha digital y de los riesgos y oportunidades de Internet, sino de que los propios protagonistas, que en este caso son los niños, sean responsables —y la palabra lo dice bien— en el buen uso de las nuevas tecnologías.

Coordinación administrativa

Y finalmente, la cuarta línea de trabajo de la dirección general es la coordinación administrativa en labores de prevención, control y sanción a través de grupos generales de trabajo. Saben ustedes que hay un comité de expertos que bajo el marco de la Comisión Europea y promovido por la asociación Protégeles está integrado por los ministerios competentes en la esta materia (Educación, Sanidad, Interior, Industria, etc), además de por representantes de comunidades autónomas, ONG especializadas, operadores en telefonía móvil, redes sociales... Este es un grupo fundamental.

Pero además, como saben bien, se ha creado recientemente, en mayo, un grupo de trabajo, Internet y Menores, con el objetivo de favorecer la coordinación de actuaciones y aunar esfuerzos para evitar duplicidades entre administraciones públicas garantizando los derechos de la infancia en Internet. En este grupo de trabajo participamos nosotros junto con la Dirección General de Evaluación y Cooperación Territorial del Ministerio de Educación, Cultura y Deporte, la Dirección General de la Policía, el Grupo de Delitos Telemáticos de la Guardia Civil y Ministerio de Interior, Secretaría de Estado de Telecomunicaciones para la Sociedad de la Información, Dirección General de INTECO y Dirección General de Red.es, del Ministerio de Industria, Energía y Turismo, y la Fiscalía General de Menores del Ministerio de Justicia. Este grupo es liderado por INTECO, y la secretaría recae en Red.es.

Además debemos reseñar la colaboración bilateral, que naturalmente se plantea a todos los niveles en todos los ministerios. Quiero reseñar particularmente, nuestra colaboración con el Ministerio de Justicia en el anteproyecto de ley de reforma del Código Penal en el cual se va a trasponer la Directiva relativa a la lucha contra los abusos sexuales, la explotación sexual de los niños y la pornografía infantil.

Hay otras acciones del ministerio que ya va terminando el tiempo, simplemente señalo: el código PAOS y el *No Hate Speech Online* (no al discurso al odio en la red), que va a liderar en nuestro ministerio del Instituto de la Juventud, el INJUVE, con varios objetivos para evitar el uso de Internet como instrumento de fomento del discurso del odio, el racismo, etc.

Conclusiones

Los desafíos a los que nos enfrentamos son claros. El primero es garantizar la igualdad de oportunidades: las administraciones públicas deberíamos promover el acceso de los menores a las nuevas tecnologías como instrumento de conocimiento, formación y socialización, impulsando su buen uso a la vez que tomando medidas de protección de los riesgos y vulneración de derechos. La alfabetización digital sigue siendo un reto que tiene que ver con la igualdad de oportunidades..

El segundo desafío es que las TIC tengan calidad y se haga un buen uso de ellas, y de ahí se deriva la necesidad de la formación a padres y educadores reduciendo la brecha digital generacional, y desarrollando acciones que permitan incardinar las políticas de prevención de las adicciones en el ámbito escolar dentro de una estrategia más amplia de atención a la problemática de los centros educativos, dadas las bases comunes que subyacen en fenómenos aparentemente inconexos como la violencia en la etapa adolescente, el consumo de sustancias con potencial adictivo y el abuso de las nuevas tecnologías de información y comunicación, y el juego.

El tercer desafío son los necesarios controles y sanciones: no podemos olvidar la necesidad de hacer más efectiva la labor de los Cuerpos de Seguridad del Estado en la lucha contra los delitos vinculados a estas nuevas tecnologías, y la próxima trasposición de la directiva a la que antes aludía.

Herramientas fundamentales para afrentar estos tres desafíos son los que creo estamos poniendo en marcha. Por una parte, fundamental, la colaboración interadministrativa: esta es una cuestión transversal, compete a diversos departamentos del Gobierno y compete a diversas administraciones de diverso ámbito territorial; y por tanto, generar espacios de colaboración interadministrativa involucrando a las diversas instituciones y remando todos en la misma dirección y con los mismos principios, parece una herramienta absolutamente imprescindible.

Pero, en paralelo, se plantea como esencial la alianza público-privada, no solo con el tercer sector de acción social sino también con el empresarial, promoviendo que los derechos de la infancia se asuman como responsabilidad social corporativa en las empresas.

Muchísimas gracias por su paciencia, y estoy a su disposición para cualquier observación que tengan a bien hacerme.

COMPARECENCIA DEL DIRECTOR EJECUTIVO DE UNICEF COMITÉ ESPAÑOL, D. FRANCISCO JAVIER MARTOS MOTA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 12 DE SEPTIEMBRE DE 2013.

El señor **DIRECTOR EJECUTIVO DE UNICEF COMITÉ ESPAÑOL** (D. Francisco Javier Martos Mota): Muchísimas gracias por la invitación. Vengo acompañado de Gabriel González Bueno, que es más especialista que yo en estos temas y en otros relacionados con la Convención de los Derechos del Niño. Les agradezco la oportunidad. Creo que ha venido bien el retraso, por otra parte, porque nosotros colaboramos con Protégeles, y entonces, para no repetir algunas cosas y tener una perspectiva un poco diferente, propositiva y desde la perspectiva que en UNICEF vemos de estos problemas, no solo de los problemas, sino de las oportunidades.

Un tema clave para nosotros en esta visión global es vincular toda la Convención de los Derechos del Niño, que es nuestro mandato como organización y por tanto la base fundamental de nuestro trabajo. Y en esta línea también quiero incidir en algunas de las cosas que son esenciales en ese mandato y que están vinculadas también al uso de las nuevas tecnologías, redes sociales, etc.

Un elemento clave es el concepto de ciudadanía: los niños son ciudadanos, con una autonomía progresiva y una serie de condiciones distintas a un adulto, pero un elemento clave es que entendemos que se está tratando a los niños únicamente como consumidores, y el elemento esencial en redes sociales, nuevas tecnologías y en todos los estudios que hemos hecho. Por ejemplo, en el año 2004, que ya se nos ha quedado obsoleto pero algunas de las ideas creo que son válidas, lo que veíamos es que todo el tratamiento a los niños en web y en todos los entornos estaba muy vinculado a ese concepto de utilizar el niño únicamente como un consumidor más; y ahora el compañero de Protégeles, creo que insistía en algunas de estas ideas, como esto último que comentaba del WhatsApp, no entender que el niño es un sujeto en formación, un sujeto de derechos, y que por tanto debemos ser más cuidadosos, pero también darle un tratamiento como a un ciudadano en formación. Y ese es un elemento clave a la hora de tratar estas cosas.

Porque para nosotros el entorno y todo lo que tiene que ver con Internet y las nuevas tecnologías es también una oportunidad; y es una oportunidad de desarrollo de ese concepto de ciudadanía. Nosotros y muchísimos compañeros de otras ONG (Save the Children, Cáritas), muchos compañeros están utilizando también las redes sociales, las nuevas tecnologías para trabajar el concepto de ciudadanía social, educación para el desarrollo, temas medioambientales... O sea, verlo también como una oportunidad, porque si no, llega un momento en que estamos obsesionados por todos los riesgos que hay en la red, y al final hay una membrana muy fina entre lo que es la realidad real y la realidad virtual, al final las dinámicas son muy similares.

Entonces, en eso sí me gustaría insistir, y es un elemento que para nosotros es clave: estamos viendo muchísimas oportunidades para trabajar; temas que están vinculados también con lo que comentabais anteriormente en los temas de educación, cómo podemos mejorar la calidad educativa del país, algunos elementos claves para nosotros como son todos los temas en todos los informes internacionales que hacemos en relación a España (el fracaso escolar), algunos temas de pobreza infantil. Es decir, la brecha digital también profundiza los temas de pobreza infantil; cómo salvar esa brecha digital, cómo dar más acceso a Internet... Lo vemos realmente como una oportunidad y una necesidad.

Yo vengo de Helsinki, estuve hace dos semanas en una reunión internacional, y más allá de lo que se habló, lo que me sorprendió muchísimo y uno comprende es por qué su sistema educativo es tan bueno y realmente ayuda tanto al sistema productivo. Te das cuenta de que la concepción que hay sobre la infancia va más allá del mero sector educativo. Es un proyecto de país en el que nada más llegar al país recibes una carta del primer ministro hablando del informe PISA y diciendo que la prioridad absoluta del país es la infancia. Y eso, claro, es muy distinto, porque los profesores de la primaria son los mejores graduados; el acceso a Internet es un derecho y está recogido en la ley. Es decir, es una visión un poco más holística de todo esto que nos atañe que está vinculado a nuevas tecnologías, educación, riesgos y oportunidades. Y para nosotros es un poco la idea que queremos trasladar en esta sesión.

En relación con el entorno protector, hablamos de la regulación en el sector público —lo que comentaba el anterior ponente—, la necesidad de que el Estado tenga la responsabilidad, que no sea únicamente una autorre-

gulación del sector privado, que como decía, nosotros también colaboramos con Google, colaboramos con Tuenti, con varias empresas en este concepto de la autorregulación, la formación de las personas en temas de derechos de la infancia, pero no dejarlo solo en el ámbito de la autorregulación.

Y la educación: el elemento clave, para nosotros, en la protección a los niños en todos los temas de Internet y el acceso a las nuevas tecnologías es que en muchísimos casos, cuando hay una situación de acoso al último que acuden es al papá o a la mamá; o sea, están acudiendo a otras personas, incluso a maestros o a amigos. Entonces, romper un poco esas dinámicas en las que muchos niños entienden que el papá no tiene ni idea de esto de las redes sociales, que no tiene ni idea de Internet y por tanto hay como un *gap*, una diferencia enorme entre lo que el niño, el adolescente siente que su papá sabe. Y es verdad que también es clave la comunicación interna, el trabajar conjuntamente, el tener una cercanía, y que nosotros también nos impliquemos como padres en lo que es el conocimiento de todas estas cosas y de todas estas herramientas.

Dar poder a los niños y promover su capacidad de afrontar riesgos: la responsabilidad de los padres, como les comentaba; acabar con la impunidad de los abusadores, también es clave para nosotros. En el último estudio que ha hecho UNICEF en relación con estos temas, por ejemplo solo 45 países tienen una legislación realmente acorde con la Convención de los Derechos del Niño y con todo lo que son los tratados de derechos humanos, en la persecución de este tipo de abusos. La persecución transnacional, porque, claro, estos elementos están vinculados no solo a aspectos locales o domésticos; los sistemas de seguridad, el acceso a material nocivo, que en la mayoría de los casos, en algunos países —me decía Gabriel—, por ejemplo en Gran Bretaña a partir de 2014 todos los dispositivos de banda ancha van a ir, desde el momento en que tú lo contratas, con una serie de filtros para los niños; y ya es por ley, no es algo de autorregulación ni nada, sino que es una obligación legal.

Porque es de las pocas cosas que tenemos. Es verdad que en muchos casos se puede quitar el filtro, etc., pero ya le estás dando de partida una situación distinta. También en el acceso fundamentalmente en móviles, que está cambiando. Para que se hagan una idea, el 40% de las personas que acceden a nuestra página web ya lo hace a través de dispositivos móviles. Es un ejemplo pequeño pero que da una escala de cómo está cambiando esto.

Y también el trabajo que nosotros hacemos como UNICEF y con otros compañeros de otras ONG en la recuperación y rehabilitación de los niños afectados, que para nosotros también es un aspecto clave.

En recomendaciones, y por centrar un poco lo que entendemos que podríamos trabajar, sería en instituciones públicas, la constitución del consejo audiovisual dotándole de competencia y capacidad sancionadora sobre los contenidos en Internet, y la protección de los niños en este ámbito. Seguir apoyando la persecución policial de los delitos: estamos totalmente de acuerdo con lo que ha dicho el señor Cánovas anteriormente, o sea, las unidades españolas son de primer nivel y trabajan muy bien. La brigada policial tiene un premio de UNICEF, nuestro, de hace dos o tres años. O sea, realmente estamos encantados de ese trabajo y entendemos que, dadas las condiciones en las que trabajan también y las dificultades de este trabajo, el apoyo no solo económico, sino moral, porque las cosas que tienen que ver y sobre las que trabajan son realmente... cualquier apoyo, sea emocional o como sea, ayuda también, porque realmente estas personas están en una situación de estrés bastante grande.

Regular o corregular algunas prácticas comerciales poco respetuosas con los menores, como las que incitan a proporcionar datos (lo que hablaba antes de WhatsApp), sin una autorización paterna, o la publicidad engañosa o intrusiva; y promover el acceso seguro a Internet.

También lo que venía en este informe, y continúa, es que por ejemplo muchísimas palabras, si tú pones en Google «juguetes» te van a salir juguetes sexuales, te van a salir muchos contenidos; entonces, en los estudios que hemos hecho del acceso de los niños se pueden encontrar con cualquier cosa; entonces, procurar en lo posible, ir trabajando en que existan esa serie de filtros de tal manera que estas cosas no ocurran. Aunque es realmente difícil, por esa concepción de los niños también como consumidores.

A las familias, informar y comunicarse con los hijos estableciendo líneas de confianza, educar en un uso positivo de la red, de los contenidos y herramientas; el uso de las tecnologías, procurar también tasar que haya límites en el uso. Y en algunos casos, como en los dispositivos de ordenadores, también siempre hemos dicho de ponerlos en el salón, de tener un control, aunque cada vez es más difícil por el uso de los teléfonos móviles y las tabletas.

Educar e informar sobre usos adecuados o peligrosos, que lo mismo menores pueden hacer de la red, y la importancia de no proporcionar datos personales a terceros; en realidad, cosas que hacemos en el mundo real, trasladarlas también al mundo digital. Es decir, tener una confianza absoluta con los niños, e igual que les avisamos de «no te vayas con un adulto extraño», pues en el entorno digital también tener esa relación.

Y luego, evitar la intromisión excesiva en las comunicaciones personales, concediendo progresivos espacios a la autonomía y desarrollo de los niños. En esta visión también de que es una herramienta, de que es una posibilidad y de que tenemos que educar en el uso de esa herramienta, pero no constreñir o estar únicamente pensando en ponerle puertas al campo, porque es imposible. La realidad, en este caso, yo creo que es educación, confianza, trabajo conjunto de los padres y los hijos, también en el entorno educativo, ir formando cada vez más a los maestros, y que en este espacio haya la confianza de tal manera que los niños puedan acercarse a los adultos en el caso de que haya una situación de acoso, *mobbing* o cualquier otra situación en la que se vean violados sus derechos.

Con las operadoras también estamos trabajando: trabajamos con Orange, ahora estamos trabajando con Movistar. O sea, estamos en un trabajo de autorregulación, de trabajo con ellas, pero realmente sí entendemos que es necesario que la legislación española esté acorde con esa protección y que no sea un elemento única y exclusivamente de autorregulación.

Medidas internas: cláusulas con proveedores, definir políticas y protocolos de actuación de protección de menores conocidos por todos los empleados, el establecimiento de una persona de referencia, por ejemplo, en las empresas en estos temas sería un elemento también clave a la hora de dirigirte, igual que hay una oficina de atención al cliente, o en el caso de reclamaciones, que ya haya una serie de mecanismos, que en esto también se introduzca alguna medida.

Realizar un análisis previo de los nuevos productos, herramientas y contenidos, previniendo consecuencias negativas para la infancia, y seguir promoviendo guías y herramientas para niños y familias sobre el uso de Internet, más vinculado con esto que hablábamos de la educación, la sensibilización y el poder trabajar con las familias.

Continuar la promoción de campañas de sensibilización e información a todos los actores (familias, niños, educadores, empresas y autoridades públicas), e introducir formalmente la seguridad y la protección en Internet en el currículo escolar, además de otras competencias comunicativas generales. O sea, que esto esté en el ámbito, un poco como decía el compañero, también en la formación, incluso en los currículos universitarios, sería un elemento clave de tal manera que los maestros en el espacio educativo puedan conocer los riesgos y las oportunidades —sí me gustaría insistir en esta parte— que nos brinda Internet.

Y esto es un poco nuestra visión, vinculada fundamentalmente a los temas que desde la organización entendemos que son esenciales, que son derechos de la infancia, educación, protección, y ser capaces de construir un entorno más amigable, entendiendo que hay una parte que tiene que ver con la protección de los niños, pero que hay otra que tiene que ver con las oportunidades de desarrollo, construcción de ciudadanía, educación, vinculado a las nuevas tecnologías.

Muchísimas gracias.

COMPARECENCIA DEL DIRECTOR Y FUNDADOR DE PANTALLASAMIGAS, D. JORGE FLORES FERNÁNDEZ, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 12 DE SEPTIEMBRE DE 2013.

El señor **DIRECTOR Y FUNDADOR DE PANTALLASAMIGAS** (D. Jorge Flores Fernández): Muchas gracias, Sr. Presidente, Señorías. En nombre de quienes hemos trabajado desde 2004 en esta aventura de las Pantallas, que queremos hacer cada vez más Amigas, me gustaría agradecerles el privilegio de compartir con ustedes y el resto de comparecientes esta ponencia de estudio así como la oportunidad de dejar testimonio, constructivo, de nuestra visión al respecto.

Ruego me permitan apoyarme en un texto para tratar de ceñirme al tiempo asignado sin que se queden fuera ninguna de las ideas a transmitir ni roben protagonismo otras que me suelen asaltar, siempre, a modo de hiperenlaces.

Evitaré dar cifras y citar estudios. Prescindiré también, por agilidad, de ser estricto en el uso de lenguaje sensible a las cuestiones de género.

En primer lugar, una breve y obligada presentación. PantallasAmigas cumplirá el año próximo su décimo aniversario, década que habrá dedicado a la única misión para la que surgió: hacer de las pantallas aliadas, amigas, en el desarrollo saludable de la infancia y adolescencia. Con vocación internacional, nace en Bilbao con el impulso de EDEX, entidad de acción social que cumple este 2013 su aniversario número cuarenta.

Nuestra misión en relación a la infancia y la adolescencia se concreta en dos objetivos: la promoción del uso seguro y saludable de las TIC y el fomento de la ciudadanía digital responsable.

Entre nuestras labores están:

— La creación y desarrollo de guías, materiales y recursos didácticos en los más variados formatos: impreso, CD-ROM y DVD audiovisual interactivo, sitios web multimedia, juegos para móviles…
— La información y sensibilización, en especial mediante la organización de sesiones divulgativas y congresos así como participación en los mismos y en medios de comunicación.
— La realización de estudios e investigaciones.

— La formación de personas adultas (educadoras, mediadoras sociales, docentes, padres y madres…) y de niños, niñas y adolescentes.
— El diseño de planes de intervención integral o de acciones específicas para determinados colectivos, contextos o problemáticas.

El ámbito de actuación supera el territorio español con intervenciones, bajo demanda, en países como Colombia o México y, con el nombre de TelasAmigas, en Brasil.

Como dato significativo, mencionar que disponemos de un canal de YouTube creado con animaciones didácticas para todos los públicos de elaboración propia que supera, a día de hoy, los 3.350 suscriptores y las 2.100.000 visualizaciones y donde más de un 75% son provenientes de fuera de España, especialmente de México. Cada día, 4.500 vídeos son visualizados desde nuestro canal. No se cuentan en esta cifra aquellos que fueron descargaron y reproducidos offline. Sin duda, varios millones de personas, especialmente adolescentes, han sido perceptores de nuestra intervención, de forma directa o intermediada.

Tras esta presentación, nuestra exposición se articula en cinco momentos:

— En primer lugar, un par **reflexiones**, para tomar dimensión.
— En segundo lugar, compartiré con ustedes nuestro **posicionamiento** basado en acuerdos y desacuerdos con comparecencias anteriores.
— Posteriormente, haremos algunas **propuestas** para la acción.
— Luego trataremos los riesgos **emergentes y de especial relevancia**.
— Y, por último, hablaremos del verdadero reto, el Plan y sus características deseables y de cómo desde PantallasAmigas hemos interpretado y hecho posible nuestro camino.

Consideraciones previas

Simplemente para tomar dimensión de la relevancia de lo que estamos tratando, dos reflexiones:

— Hace apenas unos años la sociedad se armó de franjas de horario infantil de televisión para proteger a los menores de contenidos considerados nocivos por los expertos. Hoy, esos contenidos, en cantidad y virulencia inimaginables, están siendo consumidos a

cualquier hora del día desde cualquier lugar… e incluso portados en el bolsillo. Siendo coherentes, cabe esperar efectos nocivos proporcionales, esto es, grandes, que creo ya se están dando con la consiguiente y evidente trivialización, por ejemplo, de ciertas conductas de carácter sexual o violento o, en algunos casos, sexual y violento.

— La segunda reflexión es tanto o más evidente que la anterior, pero no menos importante. Nuestros menores están utilizando una de las más revolucionarias y potentes tecnologías que hayamos conocido nunca… para lo bueno… y para lo malo. ¿No es demasiado el riesgo? Son menores lo cual es sinónimo de inexpertos y vulnerables

  Las grandes oportunidades de Internet vienen con riesgos proporcionales, esto es, enormes y, sin embargo, abrazamos con ansia estas posibilidades de la Red, sin aumentar de manera equivalente las actuaciones que permitirían evitarlos o reducir sus consecuencias.

Opiniones

Tras estas dos apuntes previos, fieles a uno de nuestros pilares como es la **aportación de valor,** hemos leído todas las comparecencias previas disponibles para no repetirnos y, aunque no es un debate sino una exposición, comenzaré refiriéndome a algunas de las ideas expresadas en otras sesiones para lo que ruego me permitan una cita vaga, pero suficiente, de los interlocutores u organismos referenciados. Es una forma de manifestar nuestra posición abreviando la exposición.

Coincidimos en la mayoría del contenido vertido durante las comparecencias previas que, por suerte, es bastante alineado y apenas contradictorio. Quizás destacar alguna *apreciación compartida especialmente* y que nos toca de cerca…

— Las observaciones y recomendaciones desde Red.es, con excepciones expuestas más adelante sobre experticia de los adolescentes y el etiquetado de contenidos.

— La visión integrada, agregada, de personas menores y adultas en una sociedad que convive también en la Red. Se trata de ciudadanos y ciudadanas que deben adquirir las competencias necesarias para vivir en el contexto digital, expuesta desde Inteco.

— El análisis de los riesgos realizado por la Ertzaintza y las medidas propuestas.
— La importancia de la privacidad, destacadas desde Fiscalía y Educación.
— La necesidad de aglutinar agentes y realizar un enfoque transversal manifestado desde el Cuerpo Nacional de Policía y la Guardia Civil.
— La asimetría existente entre agresor y agredido o perseguidor, expuesta por Fiscalía y Guardia Civil.
— Y, por último, la necesidad de estimular las competencias básicas de un ciudadano digital así como las oportunidades del aprendizaje informal, observadas desde Educación.

Sin embargo, voy a señalar algunos aspectos que se han mencionado en la ponencia y sobre los que tenemos opinión diferente:

— En primer lugar, señalar que vida online no es vida virtual, es vida real siempre. Aun siendo impostada, simulada, es vida real pero interpretada. Hay muchas vidas impostadas a pie de calle como también las hay online. Claro está que la Red, como medio de socialización, tienen sus propios códigos, vicios y virtudes, al igual que los tienen la familia, el barrio o el centro educativo. Las y los adolescentes se muestran diferentes en cada uno de esos contextos.
— En segundo lugar, tenemos que decir que no estamos de acuerdo con el presupuesto generalizado de que los nativos digitales «controlan», para nada. Saben o consiguen saber, si acaso, qué botones apretar para conseguir lo que quieren, pero no suelen conocer todos los efectos resultantes de apretar esos botones, al mismo tiempo que ignoran muchas otras cosas que podrían hacerse o cómo hacerlas. Y si acaso saben más que nosotras las personas adultas no quiere decir que sepan lo suficiente. No son usuarios avanzados, son usuarios intensivos y a veces hasta compulsivos. Sacan cientos de fotos y no consta que sean, por ello, buenos fotógrafos ¿verdad?
— Otra cuestión a matizar por nuestra parte: no confiamos en el etiquetado de contenidos. Ya fue una iniciativa europea poco exitosa cuando la red era aún más acotada. Hoy en día hay aún más dificultades con un ancho de banda mayor para descargar y cargar, con contenidos audiovisuales más abundantes y difíciles de catalogar, donde cualquiera puede ser «creador de contenidos» sin etiquetar y con variedad creciente de formatos, canales y dispositivos. Existe un precedente en los videojuegos que cuentan con un código

de clasificación autogestionado (PEDI y POSC) que resulta ser en muchas ocasiones insuficiente y engañoso y que, por supuesto, no alcanza mas que a una mínima parte de los juegos posibles.

Propuestas

Nos gustaría ahora, como adelantaba al inicio, realizar propuestas más o menos concretas que pueden ayudar a reducir los riesgos de los menores en Internet, con independencia de que estén en la calle, en la escuela o con su familia.

Cuando hablamos de ***prevención***, estas serían algunas líneas de acción:

En el plano social, familiar y educativo

1) Estimular la **ciudadanía digital**, esto es, el sentimiento de pertenencia a una comunidad y la corresponsabilidad en la misma y para con las demás personas, especialmente en lo relativo a la custodia de la privacidad ajena. Promover en este marco los valores universales cuales son la solidaridad, la cooperación, el respeto…
2) Potenciar el cuidado de la **privacidad**. Tan importante como el cuidado de los datos personales es el cuidado personal de los datos, un cuidado que debe ser proactivo.
3) Fomentar la necesidad de **autoprotección** mediante la sensibilización sobre los riesgos y sus consecuencias.
4) Considerar a los y las menores como **agentes activos** en la solución y no tanto como objetos a proteger. Nuestra experiencia llamada «Cibermanagers» iniciada hace más de tres años es un ejemplo claro de educación entre iguales, rotura de brecha generacional y beneficios de las prácticas de aprendizaje-servicio solidario.
5) Trabajar de forma preventiva en la **disminución del daño** en lo relativos a los contenidos nocivos. Es un hecho que no pueden ser evitados y, sin embargo, tampoco se ponen medios para minorar los efectos de esta exposición. No se trata con los menores pero tampoco se capacita a los mayores que les educan.
6) Advertir de forma suficiente a padres y madres sobre los riesgos y la **responsabilidad** que supone proveer a sus hijos de dispositivos conectados a internet, de manera particular en el caso de las tabletas para los más pequeños o los smartphones para preadolescentes.

7) Hacer saber a padres, madres y educadores las limitaciones y las oportunidades de los diversos **sistemas de control parental** así como la necesidad de respetar la privacidad de los menores en tanto que son sujetos con derechos y no tanto objetos a proteger.
8) Realizar una aproximación integral en relación a los menores e Internet desde la perspectiva de la Convención de los Derechos del Niño que contempla además de la **protección**, la **participación** y la **promoción** de la infancia. Por otro lado, y en esta línea, tener más presente el **principio del interés superior de la infancia**.
9) Proporcionar a la población, personas menores pero también adultas, conocimientos suficientes para determinar la **legalidad o ilegalidad de una acción** en la Red puesto que de esta manera se evita la comisión de supuestos ilegales por desconocimiento, al mismo tiempo que se identifican aquellos de los que se es víctima y que habilitan una denuncia.
10) Difundir los **servicios de control de conductas inadecuadas** de que ya disponen algunas de las aplicaciones y redes sociales en que se producen los problemas con el fin de abordar desde ese primer momento incidencias que pueden llegar más lejos, descargando al mismo tiempo otras vías de intervención que pudieran ser en ese momento prescindibles como, por ejemplo, la policía.
11) Potenciar prácticas de **parentalidad digital positiva**.
12) Estimular las **habilidades para la vida** (definidas por la Organización Panamericana de la Salud) enfocadas al entorno digital con especial énfasis en la empatía y el espíritu crítico.
13) Fomentar el desarrollo de la **resiliencia**.
14) Incluir de forma clara **espacios en la enseñanza formal** para que la educación en esta temática se convierta en obligatoria y, por ende, posible. Existen recursos didácticos de calidad, tenemos aulas equipadas, el alumnado recibe con interés las sesiones… con estas premisas no debe haber impedimento.
15) Utilizar las bondades de la **educación informal** y experimentar nuevas metodologías que se adecúen a las renovadas formas de ser y vivir en la infancia y la adolescencia.

Ya en el campo de la acción policial y judicial:

16) Realizar un **registro** y comunicación periódica y frecuente al resto de agentes intervinientes sobre las denuncias recibidas como indi-

cador de tendencias que permita habilitar un ciclo preventivo más eficiente y ajustado a la realidad cambiante.

Y para terminar, dos puntos con relación a la industria y la autorregulación:

17) Establecer **indicadores objetivos** que midan la participación y proactividad en las acciones de autorregulación de la industria de forma que su exposición pública condicione la dedicación de las compañías por su repercusión en la imagen entre la sociedad y clientes. Estos indicadores habrían de penalizar, por ejemplo, las condiciones cambiantes de funcionamiento de la plataforma que inhabilitan para tener un dominio de la misma a quienes las usan. Otro ejemplo de indicador podría ser la falta de agilidad o diligencia en los requerimientos policiales o legales.
18) Como último punto, primar mediante **reconocimiento público e incentivos fiscales** específicos actuaciones de empresas tendentes a paliar el reto de los riesgos en la Red: formación de empleados, patrocinios…

Hasta aquí, nuestras sugerencias para la prevención. A la hora de la ***intervención***, esto es, cuando el problema ya ha acontecido, consideramos que es importante realizar un ajuste que optimice los resultados obtenidos en lo relativo a la reducción del daño y el uso de los siempre críticos recursos policiales. Por ello, es preciso trabajar en las siguientes líneas:

1) La ciudadanía debe tener claro a quién y, no menos importante, cuándo y con qué documentación o pruebas, acudir.
2) La ciudadanía debe contar con unas expectativas que se ajusten a la realidad para que pueda obrar en consecuencia.
3) La ciudadanía debe estar capacitada para contribuir de forma activa a la resolución del problema (conservación de pruebas y datos, omisión de acciones ilegales…) y a la reducción del daño. Para ello es importante la definición y difusión de protocolos de autogestión de incidencias en los casos que, según los mismos, sean de aplicación.

Riesgos emergentes y de especial consideración

Me gustaría ahora destacar parte de algunos riesgos de especial relevancia y aquellos que están creciendo especialmente.

— Ciberbullying: el **ciberbullying** o **ciberacoso entre iguales**, sin duda, es y seguirá siendo el principal quebradero de cabeza en el marco escolar pero también fuera del mismo.
— Violencia de género digital: nos preocupa especialmente la **ciberviolencia de género** que se ceba en mujeres cada vez más jóvenes debido al repunte de las conductas machistas en la adolescencia. Mujeres menores son doblemente victimizadas.
— Uso abusivo y adicción: consideramos que aumentará el **uso abusivo** de las tecnologías por el simple aumento de la oferta en cantidad y calidad, la reducción de los precios, el aumento de la conectividad y especialmente por la portabilidad de los terminales de acceso: tabletas, móviles, portátiles... Aquí es preciso dejar claro que no se trata de adicciones a Internet o al smartphone sino a los diferentes servicios que desde estos dispositivos se puede acceder.
— Juegos con apuestas: dado que apenas han sido mencionados una vez, creemos que merece la pena poner de manifiesto el reto que presentan los **juegos de apuestas y azar** a los que acceden los menores sin ningún tipo de control.
— Colectivos diversos en mayor riesgo potencial: otro aspecto pendiente es el de colectivos de personas que carecen de capacitación en materia de uso seguro de Internet adecuada a sus características personales. Se trata de personas menores o adultas con **diversidad funcional o algún tipo de necesidad especial** que, por un lado, son potenciales usuarias intensivas de Internet y, quizás también, por otro, especialmente vulnerables.
— Videojuegos multijugador online: los **videojuegos online** vienen haciendo la función complementaria de redes sociales que escapan a casi todo tipo de escrutinio y regulación. Son además entornos muy dinámicos que, por su esencia y apariencia lúdica, se convierten en caladero de pedófilos debido a que tanto los propios jugadores como sus padres bajan la guardia. En estos entornos la identidad y edad de un compañero o contrincante no se considera algo importante.
— Sextorsión: la **sextorsión** es un problema en clarísimo aumento. No se trata ya del chantaje de una expareja o una acción para dominar a la víctima en un caso de Internet grooming. Lo venimos advirtiendo durante meses y hoy queda escrito aquí: se trata de crimen organizado, de redes, de un negocio a escala que busca

obtener dinero (300, 500 euros… depende de lo que se considere que puede disponer la persona sextorsionada). Las víctimas son, por lo general, adolescentes, jóvenes u hombres adultos de los que ha sido grabada una imagen íntima desde su propia webcam tras haber sido seducido por una falsa novia, ahora sí, completamente virtual.

— Uso inadecuado de Twitter: el uso que realizan los menores adolescentes de **Twitter** es una verdadera preocupación por el carácter abierto y horizontal de esta aplicación que facilita amplio alcance y rapidez de propagación de las comunicaciones. Su presencia en este entorno refleja un fenómeno que puede acentuarse o remitir: los adolescentes están abandonando las redes sociales. En este caso, y simplificando, porque Tuenti está lleno de niños y Facebook lleno de viejos.

Un plan, el verdadero reto

Con este compendio de riesgos y necesidades está claro que se precisa un plan, un buen plan, un plan integral, eficiente y flexible.

¿Es posible? La capacidad para las tareas de diseño y realización del plan hemos de suponerla garantizada. Sin embargo, el alcance está limitado por los recursos, siempre escasos, más ahora. Además, la flexibilidad compromete la eficiencia… así que deben añadirse tres virtudes:

— Determinación, que significa también constancia en el tiempo.
— Coordinación y optimización, como condiciones necesarias de eficiencia.
— Y, por último, rapidez de adaptación.

¿Están la Administración y los Poderes Públicos en condiciones de ofrecer una determinación prolongada con recursos ajustados, una coordinación adecuada y una ágil adecuación a un entorno cambiante? Este es, entendemos, el verdadero reto, la condición necesaria.

El modus operandi de PantallasAmigas

Para cerrar esta intervención, me gustaría contarles cómo hemos vivido este reto desde PantallasAmigas, cómo hemos desarrollado nuestra actividad, cuál ha sido y seguirá siendo nuestro plan.

La innovación y la prevención temprana, la anticipación a las necesidades y la realización de actuaciones de alto valor añadido son algunas de las señas de identidad de nuestro trabajo. Trabajo que ha dejado frutos como los que a continuación les señalo:

En 2005 buscamos quien tuviera experiencia en lo que aquí iba a suceder. La prestigiosa Parry Aftab, asesora de Facebook en la actualidad, escribió para PantallasAmigas una guía para ayudar a los adultos, primeros implicados, a comprender el fenómeno de Internet y sus riesgos asociados. Es una guía que lleva por título: **Internet con los Menores Riesgos**
En **2006** ya preparamos el primer recurso dirigido a niños de 8 a 12 años. Se trata de un CD-ROM interactivo: **Las 10 Claves para usar Internet con Seguridad**
Supimos, del conocimiento adquirido en el trabajo con la experta Parry Aftab que el ciberbullying sería el gran reto y, también en **2006,** publicamos la primera guía, de nuevo, tratando de sensibilizar y formar a padres, madres, docentes, educadores... Se tituló «Ciberbullying. Guía para padres, madres y personal docente».
En Febrero de 2008, de la mano del Ararteko, vio la luz nuestra siguiente apuesta, un recurso interactivo contra el ciberacoso entre iguales, de nuevo dirigido al último ciclo de primaria.
A principios de 2009 presentamos con INTECO el primer juego para móviles que abordaba de forma educativa el tema de la seguridad en Internet: Secukid.
Parece que el sexting es algo reciente ahora, en 2013, una moda o quizás una práctica de riesgo con tintes de plaga. YouTube da fe de que en mayo de **2009** pusimos a disposición de la ciudanía una serie de vídeos preventivos que desde el inicio tuvieron notable aceptación. También construimos la web www.sexting.es para ayudar a conocer el fenómeno.
Veíamos con preocupación que los adolescentes cometían delitos por osadía o por negligencia, pero en muchos casos también por ignorancia de las consecuencias posibles. Mediado el año **2009** presentamos de la mano del Defensor del Menor la «Guía e-Legales, para la gente legal de Internet».

Las noticias han hecho que tapar la webcam se convierta desde mediados de 2012 en un consejo recurrente. PantallasAmigas desarrolló un site preventivo al efecto en **Junio de 2010** llamado www.CuidadoconlaWebcam.com e invitó para su mayor difusión a compartirlo con Foro Generaciones Interactivas.

También es en 2010 cuando vio la luz un arduo trabajo del equipo multidisciplinar EMICI.

Se presentó en Euskadi, en el marco del I Congreso Internacional Ciudadanía Digital coorganizado por PantallasAmigas, el primer Protocolo de Actuación Escolar ante el Ciberbullying, proyecto impulsado y coordinado también desde PantallasAmigas.

A finales de 2011, estudios respaldados entidades de referencia concluyeron que en este asunto la participación de los propios adolescentes es clave. También este mismo 2013 grupos de trabajo europeos han concluido que es una buena metodología contra el ciberbullying.

De nuevo, años antes, **en 2010**, PantallasAmigas, había presentado una metodología llamada Cibermangers fundamentada en esas bases ya observadas por nuestra experiencia cotidiana.

Se insistió en el Día Europeo de Internet Segura del presente 2013 sobre aspectos de ciudadanía y netiqueta bajo el lema «Conéctate y respeta».

Nuestra apuesta clara por ello data de septiembre de 2010. Tres años y medio antes ya teníamos en la calle un instrumento para potenciar la ciberciudanía: www.netiquetate.com

El pasado año 2012 centramos nuestra lucha en llamar la atención sobre los efectos perniciosos para la privacidad y la convivencia que podía tener el uso de etiquetas en las fotografías de las redes sociales sin permiso previo y expreso.

Lanzamos dos campañas en forma de recursos multimedia online, una de sensibilización y otra de denuncia:

www.etiquetassinproblemas.com y www.etiquetassinpermisono.com

A principio de 2013 vio la luz un simulador de privacidad, como herramienta para el entrenamiento y la reflexión, en este caso en relación a Tuenti.

Desde 2012 comenzamos a advertir sobre la sextorsión y creamos un vídeo de sensibilización y una página informativa www.sextorion.es completando así nuestro recurso didáctico interactivo «Amy_16, una historia de sextorsión».

Es por lo tanto una historia jalonada de acciones anticipadas como requiere toda acción preventiva. Esta es nuestra forma de trabajar, con un equipo de profesionales muy cualificados y extraordinariamente generosos en el esfuerzo. Ahí está Internet para dar testimonio de los resultados. Es duro, pero muy gratificante y, sobre todo, es posible si se ponen los medios. PantallasAmigas no tenía ninguno y lo hemos hecho durante casi diez años.

Sabíamos que para aportar valor de verdad a la sociedad en este terreno no podíamos esperar a que un estudio midiera un problema, alguien (en un ayuntamiento, en una comunidad autónoma... o en Europa..) lo tomara en cuenta, habilitara los recursos e impulsara el desarrollo de medidas preventivas. Son otros tiempos, rápidos y cambiantes, repito, y nos enfrentamos al reto por excelencia.

Salvo un único caso, nunca un proyecto tuvo presupuesto de una administración pública de forma previa a su ejecución.

Muchos de estos y otros proyectos no recibieron ninguna financiación externa ni privada ni pública, aunque algunos de ellos lleven otros logotipos.

Creemos que la Administración y los Poderes Públicos deben dejar de lado sus limitaciones operativas para esta importante misión, para que el PLAN con mayúsculas alcance sus objetivos con éxito, como lo hacen con otras causas que lo requieren por suponer una amenaza importante para la ciudadanía. ¿acaso esta no lo es?

Deseamos desde PantallasAmigas haber aportado una visión suficientemente completa y constructiva respecto a este imponente asunto.

Quedo pendiente de sus cuestiones. Muchas gracias por su atención.

COMPARECENCIA DE LA COORDINADORA DE LOS DERECHOS DE LA INFANCIA DE LA ORGANIZACIÓN SAVE THE CHILDREN, DÑA. LILIANA ORJUELA LÓPEZ, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 26 DE SEPTIEMBRE DE 2013.

1. *Introducción*

Las Tecnologías de la Información y la Comunicación (TIC) son elementos cotidianos de la vida de los niños y las niñas que, en general, les resultan beneficiosas pero también les exponen a riesgos y formas específicas de violencia. Los usos de las TIC por parte de niños y niñas, deben ser observados desde una perspectiva de derechos de infancia, desde el marco que establece la Convención sobre los Derechos del Niño y el conjunto de normas internacionales de protección y promoción de los derechos humanos de los niños y las niñas.

Internet está presente en la vida de todos y cada uno de nosotros. Los niños y las niñas comienzan a acceder a una edad cada vez más temprana a una amplia variedad de dispositivos electrónicos y cada vez pasan más tiempo en línea[1].

En España, el acceso y uso a estas tecnologías de los niños y las niñas no solo tiene lugar en sus hogares, sino también en los colegios y en lugares públicos. Hay diferencias significativas en cuanto al género, ya que las niñas tienden a utilizar más mensajería instantánea y los niños tienden a utilizar más los videojuegos.

Save the Children realizó en 2010 un estudio cualitativo[2] con niños y niñas sobre los usos y riesgos que percibían en relación a las TIC. Entre los resultados obtenidos cabe destacar:

---

[1] La encuesta sobre equipamiento y uso de TIC en los hogares (INE 2011) refiere que el uso de ordenadores entre la población infantil de 10 a 15 años es prácticamente universal (95,6%) y que el 87,1% utiliza Internet. Por sexos, los datos sobre el número de niños y niñas usuarias de ordenador y de Internet, son muy parecidos. Los resultados sugieren que el uso de Internet y especialmente del ordenador es una práctica frecuente en edades anteriores a los 10 años. La disponibilidad de Internet móvil ha tenido en el último año un incremento notorio.

[2] Save the Children (2010). La tecnología en la preadolescencia y adolescencia: usos, riesgos y propuestas desde los y las protagonistas. Estudio llevado a cabo para recoger las propuestas y principales conclusiones e incluirlas en la propuesta del III Plan de Acción contra la explotación Sexual Infantil 2010-2013.

- La familiaridad de los niños y las niñas en la utilización de las TIC y la capacidad para enseñar a los adultos a utilizarlas.
- El uso más habitual es el acceso a las redes sociales.
- Los niños y las niñas tienen conocimiento de los riesgos asociados al contacto online con personas extrañas, sin embargo no siempre los ponen en práctica.
- Falta de conocimiento sobre los límites de la privacidad de la información personal que comparten.
- Perciben que la preocupación de sus padres está centrada más en el tiempo que permanecen conectados a Internet, que en los contenidos que manejan y el uso que hacen de las TIC.
- Los niños y las niñas tienen la percepción errónea del dominio y el control sobre posibles riesgos.

Es fundamental tener en cuenta que desarrollo tecnológico, las aplicaciones para su uso y la generalización del mismo en la sociedad avanzan más rápido que las leyes que los regulan y articulan la protección de los niños y las niñas. En España la edad mínima legal para acceder a una red social es de 14 años, sin embargo estudios demuestran que gran parte de niños y niñas entre los 9 y los 13 años tienen un perfil creado en alguna de ellas.

2. *Beneficios*

Las TIC proporcionan beneficios relacionados con el acceso inmediato a la información y a la comunicación. Su accesibilidad ha generado una nueva forma de establecer relaciones entre las personas, algo que incide de manera directa en el desarrollo de los niños y las niñas que crecen y se socializan en un contexto tecnológico. Por ello cuentan con una gran habilidad en el manejo de dichas herramientas que les posibilitan ser productores y receptores de contenidos que traspasan la frontera de lo privado.

Sin duda alguna, Internet es un canal fundamental para la participación, la educación, el acceso a la información, la creatividad, el ocio y el juego, la comunicación y la libre expresión.

3. *Riesgos*

Sin embargo, Internet también conlleva un espectro de riesgos a los que los niños y las niñas son más vulnerables que los adultos.

Esos riesgos están vinculados a la vulneración de sus derechos fundamentales como la libertad, la dignidad, la intimidad y el derecho a ser protegidos contra la violencia. La protección, la prevención y la atención de los niños y las niñas víctimas de violencia, desde una perspectiva de sus derechos, requiere adoptar «un paradigma basado en el respeto y la promoción de su dignidad humana y su integridad física y psicológica como titulares de derechos»[3].

Desde esta perspectiva las TIC presentan varios riesgos para los niños, se recogen aquí algunos basados en los planteamientos de la Observación Nº 13 del Comité de los Derechos del Niño:

1. Abusos sexuales cometidos para producir y difundir imágenes a través de TIC

2. Posesión y distribución de fotografías o pseudo fotografías que se han tomado, o retocado con fines sexuales o fines de hostigamiento a través del ciber acoso

3. Utilización de las TIC por parte de los niños y las niñas:

   a) Exposición a publicidad, correos no deseados, contenidos violentos, incitación al odio, al racismo, contenidos sexuales inapropiados.

   b) El contacto entre niños a través de las TIC posibilita la intimidación o acoso incluso de tipo sexual o puede favorecer que sean víctimas de engaños o coacción para participar en actividades sexuales.

   c) Los niños pueden «intimidar u hostigar a otros, jugar a juegos que afecten negativamente su desarrollo psicológico, crear y publicar material sexual inapropiado, dar información o consejos equivocados y/o realizar descargas y ataques piratas y participar en juegos de azar, estafas financieras y/o actividades terroristas[4].»

Los niños y las niñas deben ser protegidos frente a todos los riesgos y formas de exposición a la violencia porque las habilidades técnicas, personales y sociales para enfrentarlos se adquieren y desarrollan con el paso de los años, con un proceso de aprendizaje que debe iniciarse desde

---

[3] Comité de los Derechos del Niño. Observación General Nº 13 (2011). Derecho del niño a no ser objeto de ninguna forma de violencia. 18 de abril de 2011. CRC/C/GC/13 Naciones Unidas.

[4] Íbidem, párrafo 31.

la primera infancia para que ellos mismos sepan identificar los riesgos y pedir ayuda cuando no puedan manejarlos.

La forma de contacto entre víctimas y agresores en el caso de las TIC, introduce factores de riesgo específicos, como el anonimato del agresor, la gran difusión social de la situación y las dificultades prácticas para detener la agresión y, por extensión, terminar con el sufrimiento de la víctima.

Evidentemente, el daño que pueden producir estos riesgos depende de diferentes factores propios del niño o la niña y de su entorno. Los factores de riesgo y de protección están asociados a:

> **Factores individuales** de los niños y las niñas como la edad, el género, el acceso a las TIC, los vínculos afectivos y la comunicación con los adultos de referencia, la madurez psicológica, entre otros.
> **Factores sociales** como el entorno familiar, escolar y las amistades, las concepciones sociales del niño y la niña como sujetos de derechos, los estereotipos de género, la tolerancia social en el uso de niños y niñas para imágenes de pornografía y la aceptación social del acoso entre pares.
> **Factores institucionales y normativos** como la legislación vigente, la regulación de las empresas proveedoras de servicios de Internet y móviles; los recursos institucionales y la coordinación intersectorial para promover la prevención, la detección y la atención de las víctimas de ciberdelitos o de los menores de edad que los cometen.

4. *Protección*

Las familias son el núcleo de referencia donde se debe educar y proteger a los niños y las niñas, en este caso de los riesgos derivados de Internet. Aunque la brecha digital entre padres e hijos sea grande, en la medida que sus vínculos afectivos sean positivos, es mayor la probabilidad de que los niños y las niñas pidan su ayuda o la de un adulto de referencia, cuando se encuentran en una situación de riesgo.

Pero además, abordar los riesgos online que enfrentan los niños y las niñas es una obligación que emana de los compromisos adquiridos por el Estado para la protección efectiva de sus derechos. Esta debe ser una prioridad política.

El Estado tiene la obligación de prohibir, perseguir y castigar cualquier forma de violencia contra los niños y las niñas que se cometa a través de las TIC mediante su sistema penal tipificando y procesando estas formas de violencia y velando porque las víctimas sean adecuadamente atendidas y reparadas.

El Estado también tiene la responsabilidad de proteger a la infancia de contenidos perjudiciales a los que pueden verse expuestos los niños y las niñas a través de las TIC y de los medios de comunicación, regulando los mecanismos de control, la responsabilidad de los agentes de estos medios en el bloqueo de contenidos inapropiados, la aprobación de códigos de conducta y las normas para evaluar los contenidos y poner quejas sobre ellos.

Para cumplir con estas obligaciones el Consejo de Europa propone que en las estrategias nacionales contra la violencia para la protección de los niños y las niñas deben contener medidas eficaces y multidisciplinares centradas en las necesidades de los niños y las niñas, sus familias y la sociedad en general. Las directrices para la elaboración de estas estrategias proponen el avance para crear una cultura de respeto de los derechos de los niños y las niñas a través de:

La educación y la sensibilización social de medios de comunicación. Que incluya programas escolares, campañas públicas de información y de sensibilización social. También el trabajo con padres y madres para la promoción de la parentalidad positiva es fundamental para promover formas de relación y de resolución de conflictos no violentas.

La formación de los profesionales que trabajan con niños y niñas ya que deben estar cualificados para prevenir, detectar y actuar de manera eficaz frente a la violencia contra la infancia.

La participación de los medios de comunicación y las nuevas tecnologías. Es importante señalar que los medios de comunicación y las empresas relacionadas con las TIC tienen un papel para promover la cultura de respeto de los derechos humanos. Las regulaciones de gestión de contenidos y acceso a las TIC deben considerar la perspectiva de derechos de infancia.

El compromiso de los proveedores de Internet. Para lograr unos «servicios de Internet accesibles, seguros y fiables, se debería mo-

tivar a estos proveedores para que proporcionen información sobre los riesgos potenciales que pueden vulnerar los derechos, la seguridad y la privacidad en línea de sus clientes. Debería reforzarse la cooperación con las autoridades del orden público en la investigación de delitos cometidos mediante la utilización de las tecnologías de comunicación»[5].

El ámbito educativo es esencial en esta tarea, tanto Naciones Unidas[6] como los estudios especializados en el tema[7] subrayan la importancia fundamental de adoptar medidas educativas claves para trabajar con los niños y las niñas:

- Facilitar información veraz, accesible y apropiada para su edad.
- Formar en medidas de autoprotección ante los riesgos relacionados con las TIC.
- Desarrollar programas de prevención del acoso escolar y del ciberacoso.
- Establecer una relación positiva entre los compañeros de clase y combatir las intimidaciones.
- Concienciar sobre los derechos de la infancia y específicamente el derecho a ser escuchados y a que su opinión se tenga en cuenta.
- Desarrollar habilidades sociales importantes para la convivencia libre de violencia: solidaridad, asertividad, empatía y control de las emociones.

5. *Dos situaciones que requieren especial atención*

Imágenes de abuso sexual infantil

Como señalan las cifras que presenta el Ministerio del Interior, en 2006 se registraron 392 denuncias vinculadas a pornografía infantil, y en 2011: 704 denuncias. La Guardia Civil informa que el número de dete-

[5] CoE. Una Estrategia Integral. Directrices del Consejo de Europa sobre las estrategias nacionales integrales para la protección de los niños contra la violencia. Council of Europe Policy Guidelines on Integrated National Strategies for the Protection of Children from Violence (2009), página 17. Disponible en: http://www.coe.int/t/dg3/children/news/ guidelines/Recommendation%20CM%20protection%20of%20children%20_ESP_BD.pdf

[6] Comité de los Derechos del Niño. Observación General Nº 13 (2011)... Óp. Cit.

[7] Ver próximo informe sobre acoso escolar y ciberacoso que ha realizado Save the Children.

nidos vinculados a operaciones contra la pornografía infantil, aumentó en el año 2012 a 97, respecto a 2011 donde fueron 8. Estas operaciones han implicado la coordinación con el FBI, la Europol y los servicios de seguridad de otros países, ya que por la naturaleza de las TIC, este tipo de delitos traspasan las fronteras de los Estados.

En el ámbito del derecho internacional de derechos de la infancia, para hacer referencia a la llamada pornografía infantil, es decir a las imágenes, videos o audios que representan actividades de abuso sexual de niños y niñas se emplea el término imágenes de abuso sexual infantil, ya que describen mejor la situación de vulneración de derechos.

Save the Children considera preocupante la exposición y visualización de este tipo de material por parte de niños y niñas, porque contribuye a la normalización de esas situaciones y puede incluso dificultar que las propias víctimas que lo sufren lo reconozcan como tal y lo denuncien. Recordemos aquí, dos noticias recientes, una se refiere a la detención de menores de edad por tenencia y difusión de imágenes de abuso sexual infantil a través de sus móviles con las aplicaciones de mensajería instantánea como Whatsapp[8]. En otro caso, se produjo la detención de un chico de 16 años como presunto autor de una de las agresiones que se difundía[9].

Algunas páginas suelen pasar desapercibidas, por ejemplo aquellas que contienen imágenes de niños y niñas posando semidesnudos o desnudos, sexualizando así a la infancia y la adolescencia directa o indirectamente.

Save the Children alerta sobre la preocupante dificultad para la identificación de las víctimas: las bases de datos de INTERPOL en 2010 señalaban más de 550.000 imágenes de niños y niñas víctimas de abuso sexual descargadas de Internet, a partir de las que tan solo se habían identificado 1.453 víctimas.

Ciberacoso

El ciberacoso –en inglés cyberbullying– es una nueva forma de acoso escolar o bullying, es decir es una forma de violencia entre pares que implica el uso de las TIC –teléfonos móviles, Internet, videojuegos– para

[8] http://www.policia.es/prensa/20130526_1.html.

[9] http://www.policia.es/prensa/20130514_1.html.

acosar, amenazar o intimidar deliberadamente a alguien. Entre sus características está la desigualdad de poder, la intencionalidad y el anonimato del agresor en muchos casos y la repetición entendida en términos de la amplia posibilidad de difusión.

Un estudio del Defensor del Pueblo y UNICEF de 2007, reflejó que el 5.5% de los escolares se declaraban víctimas de ciberbullying y el 5.4% de los entrevistados se proclamaban agresores de otros usando medios cibernéticos. También se señala que una cuarta parte de los escolares había sido testigo de fenómenos de ciberbullying, ya sea de forma eventual (22%), como de forma prolongada (3%).

Las TIC también ofrecen en las víctimas oportunidades para responder y defenderse, incluso en ocasiones de manera violenta también, respuesta que probablemente no sería la misma cara a cara[10].

Aunque la violencia sea ejercida entre niños o niñas, los adultos responsables tienen un papel fundamental para combatir y prevenir de manera adecuada el acoso escolar y el ciberacoso.

Es esencial tener en consideración los derechos de todos los menores de edad implicados en esas situaciones. En este sentido resulta relevante hacer referencia a la Observación 14[11] sobre el interés superior del niño, que señala que si hay un conflicto entre el interés superior de un niño con los de otros niños, es importante sopesar los intereses de todas las partes y estudiar caso por caso;

– Las actuaciones para atender a los niños y las niñas víctimas deben tener en cuenta las Directrices de Naciones Unidas sobre niños y niñas víctimas y testigos[12] que reconocen los derechos a un trato digno y comprensivo, a la protección contra la discriminación, a ser informado, a ser oído y a expresar opiniones, a una asistencia eficaz, a la intimidad, a ser protegido de sufrimientos durante el

[10] Ortega- Ruiz R, Casas José A. Knowing, building and living together on Internet and social networks: The ConRed cyberbullying Prevention program. International Journal of conflict and Violence: Vol6(2) 2012, pp. 303-313.

[11] Comité de los Derechos del Niño. Observación General Nº14 (2013) sobre el derecho del niño a que su interés superior sea una consideración primaria, 29 de mayo de 2013, CRC/C/GC/14, párrafo 39.

[12] Directrices sobre la justicia en asuntos concernientes a los niños víctimas y testigos de delitos, aprobadas por el Consejo Económico y Social de Naciones Unidas el 10 de agosto de 2005.

proceso de justicia, a la seguridad, a la reparación y a medidas preventivas especiales.

– Con los niños o las niñas agresores es necesario evaluar caso a caso para establecer medidas sancionadoras y educativas a partir de los derechos que reconoce la Convención, «(...) la represión o el castigo, deben ser sustituidos por los de rehabilitación y justicia restitutiva (...)»[13]. Por lo que es conveniente resaltar que «las políticas de mano dura para combatir la violencia contra la infancia tiene efectos muy destructivos en los niños, en particular los adolescentes, porque su enfoque punitivo victimiza a los niños al responder a la violencia con más violencia»[14] como señala el Comité de los Derechos del Niño.

Save the Children presentará próximamente un informe sobre acoso escolar y ciberacoso que recogerá el marco de derechos, los resultados de una investigación sobre este tema y la propuesta de un protocolo marco de actuación.

6. *Avances en el contexto español*

En los últimos años el Estado español ha llevado a cabo avances significativos en materia de legislación, sensibilización y formación para abordar los riesgos y la violencia en las TIC a que están expuestos los niños y las niñas.

Cabe destacar entre los más importantes:

— La aprobación del **III Plan de Acción contra la Explotación Sexual de la Infancia y la Adolescencia 2010-2013**, que recoge medidas concretas y puntuales sobre el modo de abordar las imágenes de abuso sexual infantil a través de las TIC referentes al conocimiento de la realidad, prevención, protección, revisión del marco jurídico y medidas de cooperación internacional.

---

[13] Comité de los Derechos del Niño. Observación General Nº14 (2013) Óp. Cit... párrafo 28.

[14] Comité de los Derechos del Niño. Observación General Nº 13 (2011) Óp. Cit... párrafos 15 y 27.

— La aprobación del **II Plan Estratégico de Infancia y Adolescencia 2013- 2016**, entre cuyos objetivos está impulsar los derechos y la protección de la infancia con relación a los medios de comunicación y a las tecnologías de la información en general. Este plan establece una serie de medidas que han sido acordadas por los Cuerpos y Fuerzas de Seguridad del Estado, las Comunidades Autónomas, las instituciones públicas, la sociedad civil y la academia.

En este marco, gracias al apoyo de las instituciones públicas Save the Children y otras ONG de infancia, han desarrollado varios programas de prevención de los riesgos de violencia contra niños y niñas a través de las TIC. Igualmente muchos actores institucionales promueven actividades de sensibilización y formación de profesionales y de niños y niñas en relación a los riesgos de las TIC y de propuestas de protección. Por ejemplo, en muchas ciudades, actores locales como los agentes tutores, hacen una labor importante, en el tema de las TIC y del acoso escolar. Los estudios académicos y las estadísticas permiten deducir que la conciencia social sobre estos riesgos va en aumento.

Actualmente se está debatiendo una **reforma del Código Penal** que avanza en la definición de diferentes formas, algunas de ellas novedosas, de violencia ejercida contra los niños y las niñas a través de las TIC. Cabe destacar entre las reformas contenidas en la propuesta aprobada el pasado 20 de septiembre por el Consejo de Ministros:

— El endurecimiento de las penas y la definición de pornografía infantil, abarca no sólo el material que representa a un niño participando en comportamientos sexuales, sino también las imágenes realistas de niños participando en conductas sexuales explícitas aunque no reflejen un abuso real.

— El castigo de los actos de adquisición, uso, producción y difusión o la asistencia a espectáculos pornográficos donde participen menores de edad.

— Se propone facultar a Jueces y tribunales para bloquear o retirar webs que difundan pornografía.

— En cuanto al grooming, se incluye un apartado nuevo con el fin de sancionar a quien contacte a un menor de 15 años a través de TIC y que lo engañe o presiones para que facilite material pornográfico.

— Se incluye un nuevo tipo vinculado a la divulgación contra su voluntad de imágenes o grabaciones de otra persona sin su consentimiento, cuando se haya producido en el ámbito privado y su difusión lesione su intimidad.

Las medidas anunciadas en esta reforma constituyen un notable avance en la adecuación de las normas penales españolas al contexto europeo, fundamentalmente de la Directiva de la Unión Europea 2011/93/UE, relativa a la lucha contra los abusos sexuales y la pornografía infantil. Algo fundamental teniendo en cuenta que la naturaleza transfronteriza de muchas conductas exige normas homogéneas para su persecución a partir de la colaboración policial entre varios estados. Es esencial que, además, las modificaciones de las normas procesales penales que actualmente hay planteadas o anunciadas (Código Procesal Penal, Estatuto de la Víctima) prosigan en esta senda de adaptación del marco legal español al contexto normativo internacional en dos ámbitos fundamentales: **la adecuada protección y atención a las víctimas menores de edad de estos delitos y reforzar las garantías legales del trabajo de investigación de estos delitos por parte de los Cuerpos y Fuerzas de Seguridad del Estado.**

Para ello es fundamental profundizar en un mejor conocimiento de la realidad actual, debatir entre los actores fundamentales y coordinar la actuación desde todos los ámbitos a todos los niveles de la administración.

Muchos actores están implicados en la responsabilidad de la protección: los gobiernos, la legislación, la sociedad civil, el sector privado (en particular los proveedores de servicios online), las escuelas, las familias, y los propios niños y niñas. Nos encontramos frente a un tema complejo y, por ello, es necesaria la implicación de todos los actores.

7. *Recomendaciones*

Para reforzar el marco de protección de los niños y las niñas frente a los riesgos y la violencia a que se pueden ver expuestos a través de las TIC, es necesario que las autoridades públicas adopten medidas entre las que Save the Children destaca dos recomendaciones fundamentales para abordar los dos temas a los que se ha prestado mayor atención en este documento:

En torno a las imágenes de abuso sexual infantil

Avanzar en la adaptación del marco jurídico español a la normativa europea e internacional. Las reformas del Código Penal, de la Ley de Enjuiciamiento Criminal (Código Procesal Penal) o la ley que establezca el Estatuto de la víctima, deben prever medidas que no solo tipifiquen y agraven las penas de estos delitos, sino brindar las garantías y el apoyo necesario al trabajo que realizan los Cuerpos y Fuerzas de Seguridad del Estado en la persecución de delitos informáticos. Debe también preverse un enfoque adecuado para la atención y protección de las víctimas.

En relación al ciberacoso

Desarrollar un protocolo marco de actuación en casos de acoso escolar y ciberacoso, que unifique, actualice y recoja las experiencias de las diferentes Comunidades Autónomas que han desarrollado protocolos de actuación. Este protocolo debe fundarse en un enfoque preventivo que permita igualmente actuar de manera urgente ante casos de acoso o ciberacoso, posibilitando y facilitando la actuación coordinada de las instituciones claves para la protección contra esta violencia.

Actualizar y debatir en torno al modo de abordar el ciberacoso a nivel judicial. La Fiscalía General del Estado desarrolló en 2005 el marco aún vigente para orientar su actuación ante el acoso escolar desde el sistema de justicia juvenil, desde una perspectiva de derechos de la infancia en la Instrucción 10/2005.Es evidente que desde 2005 hasta la actualidad los comportamientos de acoso entre pares han cambiado y van en aumento por su vinculación a las TIC.

Con carácter general, las recomendaciones de Save the Children para completar un marco de protección integral frente a la violencia a la que se pueden ver expuestos los niños y las niñas a través de las TIC reclaman:

- Elaborar una **Ley Integral de protección de los niños y las niñas contra la violencia** garantizaría una respuesta integral a todas las formas de violencia incluyendo la violencia de la que pueden ser víctimas los niños y las niñas a través de las TIC[15].

[15] Por ello Save the Children retoma la recomendación que ha hecho el Comité de los Derechos del Niño a España del desarrollo de una Ley Integral de protección frente a todas las formas

- Impulsar y desarrollar investigaciones para conocer formas específicas de violencia contra la infancia relacionadas con el acoso y ciberacoso por motivos de género, por discapacidad y por discriminación étnica.
- Fomentar políticas de promoción de la parentalidad positiva que respalden a las familias en sus responsabilidades de educar a los hijos e hijas con pautas educativas no violentas que promuevan el desarrollo integral y respondan a sus necesidades específicas.

Un factor clave del éxito en la protección de los niños y las niñas frente los riesgos y la violencia a la que se pueden ver expuestos a través de las TIC es la prevención, para ello es fundamental:

- Preservar los recursos públicos destinados en los presupuestos estatales y de las Comunidades Autónomas a la realización de programas de sensibilización y prevención de riesgos a través de las TIC en diferentes grupos de población.
- Avanzar hacia un modelo educativo inclusivo, participativo y dialógico que promueva los derechos fundamentales de la infancia y que se base en el desarrollo de valores como la solidaridad, la justicia, la colaboración y la igualdad de oportunidades y resultados.
- Desarrollar programas de formación de profesionales[16]. Es fundamental que los profesionales –incluidos los profesores– que trabajan con niños y niñas tengan formación en desarrollo infantil, derechos de infancia y que conozcan los protocolos de actuación frente a la violencia a través de las TIC.
- Desarrollar programas de formación de padres y madres. Promover los vínculos afectivos y la educación no violenta en el hogar, a través de programas de promoción de la Parentalidad positiva. Actualización en los temas TIC. Concienciación sobre pautas de protección contra los riesgos de violencia en la escuela y a través de TIC.

---

de violencia contra los niños y las niñas. Ver Más allá de los golpes: ¿Por qué es necesaria una ley?. Informe sobre la violencia contra los niños y las niñas. Save the Children, 2012.

[16] Como señala la Observación Nº 14 del Comité de los Derechos del Niño (CRC/C/GC/14) de 2013, los Estados deben garantizar la buena formación de los docentes y profesionales de los ámbitos que están en relación.

- Centrar en la autoprotección de niños y niñas los esfuerzos en materia de prevención, fundamental para fortalecer las estrategias de protección ante los riesgos a través de las TIC para prevenir la victimización y la comisión de delitos. La forma de abordarlo no puede estar basada en la restricción,la censura o la usurpación de su intimidad a partir de la vigilancia de sus actividades online, esta perspectiva no aborda directamente los riesgos.
- Fomentar la regulación de las empresas proveedoras de Internet, y empresas que diseñan dispositivos y aplicaciones –apps– en relación a la protección de datos, el derechos a la intimidad, la protección del consumidor, la seguridad y el derecho a la información de los niños y las niñas usuarios.
- Promover campañas de concienciación y sensibilización dirigidas a población en general. Inclusión de módulos formales de usos y prevención de riesgos a través de las TIC, dentro del currículo escolar.

8. *Documentos clave*

Consejo de Europa

CoE (2007). Convenio 201 del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual. Convenio de Lanzarote. Ratificado por España en julio de 2010, publicado en el BOE de 12 de noviembre de 2010.

CoE. Una Estrategia Integral. Directrices del Consejo de Europa sobre las estrategias nacionales integrales para la protección de los niños contra la violencia. Council of Europe Policy Guidelines on Integrated National Strategies for the Protection of Children from Violence (2009). Disponible en: http://www.coe.int/t/dg3/children/news/guidelines/ Recommendation%20CM%20protection%20of%20children%20_ESP_BD.pdf.

España

Plan Estratégico Nacional de Infancia y Adolescencia 2013 – 2016. Aprobado por el Consejo de Ministros el 5 de Abril de 2013. Disponible en: http://www.observatoriodelainfancia.msssi.gob.es/documentos/PENIA_2013-2016.pdf.

Plan de Acción contra la explotación sexual de la Infancia y la Adolescencia (2010- 2013). Ministerio de Sanidad, política social e igualdad, 2011.

Fiscalía General del Estado. Instrucción 10/2005 sobre el tratamiento del acoso escolar desde el sistema de justicia juvenil. Disponible en: http://bit.ly/16wzs9r

Naciones Unidas

Convención de los Derechos del Niño. Aprobada por la Asamblea General de Naciones Unidas el 20 de noviembre de 1990. Disponible en: http://www2.ohchr.org/spanish/law/crc.htm

Comité de los Derechos del Niño. Observación General Nº 13 (2011). Derecho del niño a no ser objeto de ninguna forma de violencia. 18 de abril de 2011. CRC/C/GC/13 Naciones Unidas.

Comité de los Derechos del Niño. Observación General Nº 14 (2013) sobre el derecho del niño a que su interés superior sea una consideración primaria, 29 de mayo de 2013, CRC/C/GC/14. Comité de los Derechos del Niño.

Observaciones finales del Comité de los Derechos del Niño a España. Octubre de 2010. CRC/C/ESP/CO/3-4.

Directrices sobre la justicia en asuntos concernientes a los niños víctimas y testigos de delitos, aprobadas por el Consejo Económico y Social de Naciones Unidas el 10 de agosto de 2005.

Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía. Resolución A/RES/54/263 del 25 de mayo de 2000.

Save the Children

Agenda de Infancia (2010-2015). Save the Children, septiembre de 2011. Disponible en: http://www.savethehcildren. es/ver_doc.php?id=121

Más allá de los golpes: ¿Por qué es necesaria una ley?. Informe sobre la violencia contra los niños y las niñas. Save the Children, 2012. Disponible en: http://www.savethechildren.es/ver_doc.php?id=133

Save the Children (2010). La tecnología en la preadolescencia y adolescencia: usos, riesgos y propuestas desde los y las protagonistas. http://www.deaquinopasas.org/docs/estudio_riesgos_internet.pdf

Save the Children (2012). Violencia sexual contra los niños y las niñas. Abuso y explotación sexual infantil. Guía de material básico para la formación de profesionales.

Save the Children (2012). Guía de recursos para la prevención y atención del abuso y la explotación sexual infantil. Ver especialmente el capítulo: material de sensibilización sobre abuso sexual infantil y TIC, pp- 64-69.

Unión Europea

Directiva del Parlamento Europeo y del Consejo de 20 de septiembre de 2012 por la que se establecen las normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos.

Directiva 2011/92/UE de 13 de Diciembre relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

Algunos estudios recientes sobre ciberacoso

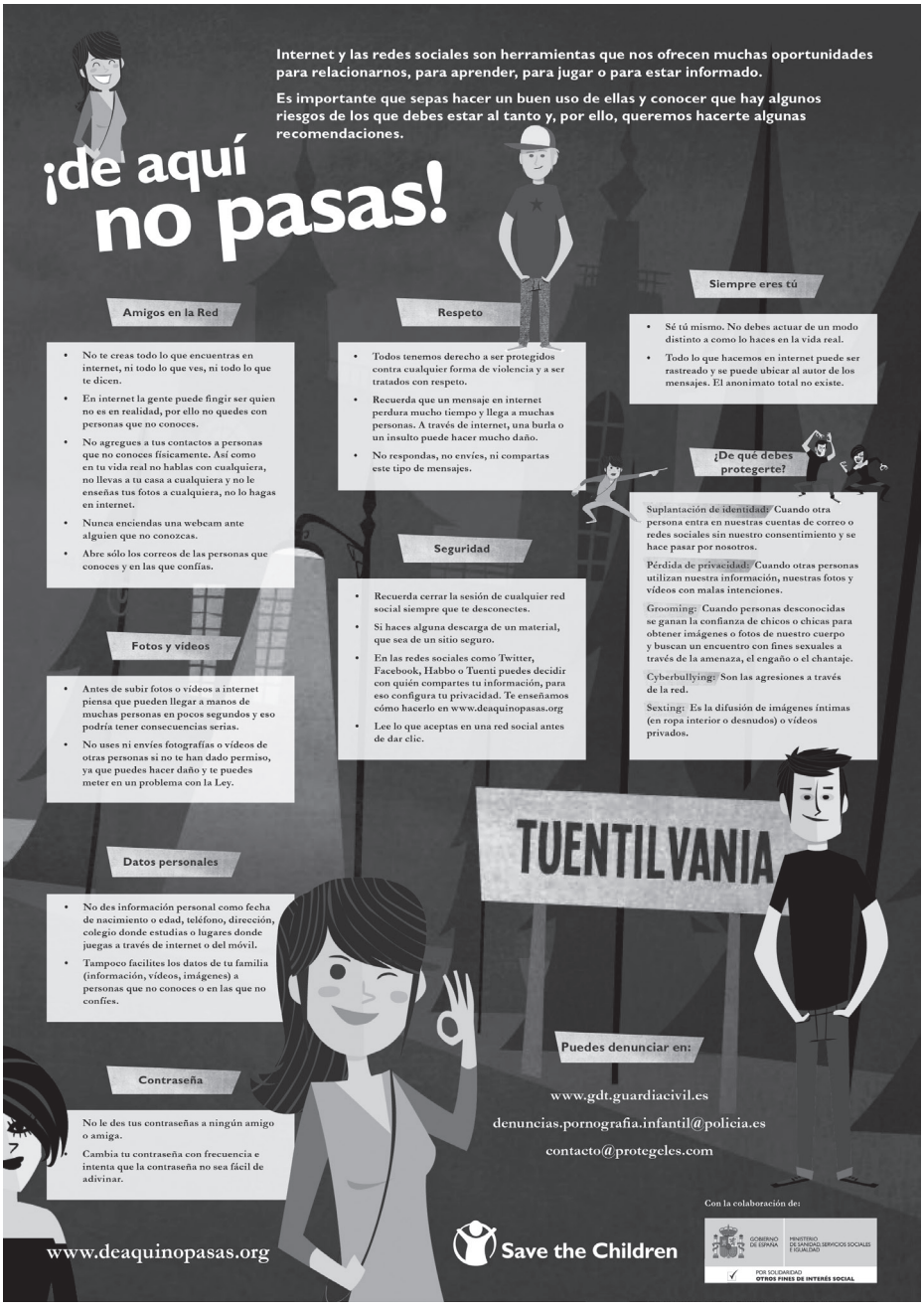
Calmaestra, J. (2011). Cyberbullying: prevalencia y características de un nuevo tipo de bullying. Universidad de Córdoba.

Ortega- Ruiz, R; Casas, José A. (2012). «Knowing, building and living together on Internet and social networks: The ConRed cyberbullying Prevention program». International Journal of conflict and Violence: Vol. 6 (2), pp. 303-313.

Álvarez- García, et. al. (2011). Violencia a través de las tecnologías de la información y la Comunicación en estudiantes de secundaria. Anales de psicología. 2011, vol. 27,nº 1 (enero), pp. 221-231.

León del Barco, B.; Felipe Castaño, E.; Fajardo Bullón, E. & Gómez Carroza, T. (2012). «Cyberbullying en una muestra de estudiantes de Educación Secundaria: Variables moduladoras y redes sociales» Electronic Journal of Research in Educational Psychology, 10 (27), pp. 771-788.

Navarro, R.; & Yubero, S. (2012). «Impacto de la ansiedad social, las habilidades sociales y la cibervictimización en la comunicación online». Escritos de Psicología, 5 (3), 4-15. doi: 10.5231/psy.writ.2012.2009.


Internet y las redes sociales son herramientas que nos ofrecen muchas oportunidades para relacionarnos, para aprender, para jugar o para estar informado.
Es importante que sepas hacer un buen uso de ellas y conocer que hay algunos riesgos de los que debes estar al tanto y, por ello, queremos hacerte algunas recomendaciones.
¡de aquí no pasas!
Amigos en la Red
No te creas todo lo que encuentras en internet, ni todo lo que ves, ni todo lo que te dicen.
En internet la gente puede fingir ser quien no es en realidad, por ello no quedes con personas que no conoces.
No agregues a tus contactos a personas que no conoces físicamente. Así como en tu vida real no hablas con cualquiera, no llevas a tu casa a cualquiera y no le enseñas tus fotos a cualquiera, no lo hagas en internet.
Nunca enciendas una webcam ante alguien que no conozcas.
Abre sólo los correos de las personas que conoces y en las que confías.
Fotos y vídeos
Antes de subir fotos o vídeos a internet piensa que pueden llegar a manos de muchas personas en pocos segundos y eso podría tener consecuencias serias.
No uses ni envíes fotografías o vídeos de otras personas si no te han dado permiso, ya que puedes hacer daño y te puedes meter en un problema con la Ley.
Datos personales
No des información personal como fecha de nacimiento o edad, teléfono, dirección, colegio donde estudias o lugares donde juegas a través de internet o del móvil.
Tampoco facilites los datos de tu familia (información, vídeos, imágenes) a personas que no conoces o en las que no confíes.
Contraseña
No le des tus contraseñas a ningún amigo o amiga.
Cambia tu contraseña con frecuencia e intenta que la contraseña no sea fácil de adivinar.
www.deaquinopasas.org
Respeto
Todos tenemos derecho a ser protegidos contra cualquier forma de violencia y a ser tratados con respeto.
Recuerda que un mensaje en internet perdura mucho tiempo y llega a muchas personas. A través de internet, una burla o un insulto puede hacer mucho daño.
No respondas, no envíes, ni compartas este tipo de mensajes.
Seguridad
Recuerda cerrar la sesión de cualquier red social siempre que te desconectes.
Si haces alguna descarga de un material, que sea de un sitio seguro.
En las redes sociales como Twitter, Facebook, Habbo o Tuenti puedes decidir con quién compartes tu información, para eso configura tu privacidad. Te enseñamos cómo hacerlo en www.deaquinopasas.org
Lee lo que aceptas en una red social antes de dar clic.
Siempre eres tú
Sé tú mismo. No debes actuar de un modo distinto a como lo haces en la vida real.
Todo lo que hacemos en internet puede ser rastreado y se puede ubicar al autor de los mensajes. El anonimato total no existe.
¿De qué debes protegerte?
Suplantación de identidad: Cuando otra persona entra en nuestras cuentas de correo o redes sociales sin nuestro consentimiento y se hace pasar por nosotros.
Pérdida de privacidad: Cuando otras personas utilizan nuestra información, nuestras fotos y vídeos con malas intenciones.
Grooming: Cuando personas desconocidas se ganan la confianza de chicos o chicas para obtener imágenes o fotos de nuestro cuerpo y buscan un encuentro con fines sexuales a través de la amenaza, el engaño o el chantaje.
Cyberbullying: Son las agresiones a través de la red.
Sexting: Es la difusión de imágenes íntimas (en ropa interior o desnudos) o vídeos privados.
TUENTILVANIA
Puedes denunciar en:
www.gdt.guardiacivil.es
denuncias.pornografia.infantil@policia.es
contacto@protegeles.com
Save the Children
Con la colaboración de:
GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

COMPARECENCIA DEL PRESIDENTE DE LA CONFEDERACIÓN CATÓLICA NACIONAL DE PADRES DE FAMILIA Y PADRES DE ALUMNOS, D. LUIS CARBONELL PINTANEL, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 26 DE SEPTIEMBRE DE 2013.

Buenos días, Sr. Presidente/a de la Comisión, Excmas. Sras. y Sres. Senadores:

Preámbulo

Como probablemente vds. ya conocerán, la Confederación de Padres de Alumnos CONCAPA representa a más de tres millones de familias, padres de alumnos, preocupados por la formación de sus hijos. De ahí que para nosotros un tema de vital importancia sea la relación de los menores con internet y las redes sociales, y les felicitamos por la puesta en marcha de esta Comisión tan necesaria.

Los menores pasan la mayor parte del tiempo conectados a las redes sociales, fundamentalmente a través del smartphone, y los riesgos de esta exposición son evidentes y requieren de una serie de medidas cada vez mayores para minimizar estos riesgos. Medidas de formación, información y en algunos casos de sanción.

Es evidente el éxito de las redes sociales, debido en buena parte a la multifuncionalidad de la herramienta: mensajes, fotos, vídeos, chat, juegos, etc. Un mundo muy atractivo, que facilita el ocio y posibilita una mayor rapidez de la información y comunicación, así como la relación en comunidades virtuales.

El problema no es, por tanto, el medio o herramienta sino el uso que se puede hacer del mismo, del mal uso de las redes sociales, especialmente cuando los usuarios son menores y hay que velar por su seguridad e intimidad.

Internet es muy útil y los niños lo utilizan a menudo: los datos (Encuesta de EU Kids Online. 2010) indican que el entorno más común de utilización de Internet en Europa es el doméstico (85%) seguido por el escolar (10%); si bien el acceso se está produciendo cada vez más a través del teléfono móvil, y los menores cada vez se incorporan a Internet a edades más tempranas. Actualmente el 57% de los chavales de entre 9 y 16 años tiene perfil en una red social.

Hoy sabemos que la mitad de los ciudadanos españoles está poco o nada informado sobre los riesgos de proporcionar sus datos personales. Según el barómetro del CIS del pasado mes de junio, un 52% de los españoles no sabe a qué se enfrenta cuando consiente en dar sus datos, aunque más de la mitad (un 54%) reconoce que es bastante probable que estos vayan a ser usados sin su consentimiento.

Con respecto a los menores, un 25% de la población es favorable a restringir completamente el acceso a Internet a menores, y un 51% de los ciudadanos se muestra favorable a que las compañías que usen de forma fraudulenta datos de personas sean multadas.

Por otra parte, casi un 90% de los encuestados considera que deberían existir bastantes restricciones y controles para el acceso de los niños a la Red, y para un 25% los menores deberían tener completamente prohibido el acceso al ciberespacio.

También existe un gran consenso social en cuanto a quienes deben ejercer esa vigilancia. Más del 85% de los ciudadanos consideran que son los padres los que tienen la responsabilidad principal a la hora de establecer controles en el uso de Internet por parte de los menores; lo que sucede es que nos faltan medios y formación.

Según el 52% de los encuestados, la difusión de fotos y videos comprometidos, así como ofrecer demasiada información sobre sí mismos, son los riesgos más frecuentes a los que los menores se enfrentan en Internet.

Los principales problemas son el acceso de menores de 14 años a redes que no están permitidas, porque se considera que no están en con-

diciones de asumir las consecuencias; pero estas redes a su vez carecen de un sistema eficiente de verificación de la edad del usuario, por lo que los menores acaban entrando en ellas. Esto significa que, además, es fácil la usurpación de una identidad.

Otro problema son los datos que piden las redes, ya que en muchos casos se trata de datos privados tales como las creencias personales o el nombre del colegio o centro académico al que asisten. Basta con facilitar un dato para que los grandes buscadores se pongan en marcha sin nuestro conocimiento ni consentimiento.

Con respecto a las imágenes, en las redes sociales figuran unas condiciones de uso que a menudo no son leídas, y entre ellas está la cesión de derechos sobre las imágenes que se cuelgan. Los chavales suelen colgar a menudo imágenes suyas, de sus amigos, de sus familiares, que después van a correr por las redes sociales y no van a poder controlar, y que les pueden ocasionar más de un disgusto.

Las autoridades europeas ya están tomando cartas en el asunto, dedicando fondos a trabajar en la seguridad de los menores o reformando los sistemas educativos para hacer frente a las necesidades de las nuevas tecnologías de la información y de la comunicación en el aula. Además, se está trabajando en ámbitos de seguridad, ayuda y denuncia, incluso con problemas relacionados con las tecnoadicciones.

En el proyecto de investigación eu.net.adb, de la Comisión Europea, que promueve el uso seguro de Internet y de las nuevas tecnologías, se ha realizado una encuesta con 13.284 adolescentes, de edades comprendidas entre los 14 y 17 años, de 7 países europeos (Grecia, Alemania, Holanda, Islandia, Polonia, Rumanía y España). En la encuesta se incluían preguntas acerca del acceso de los adolescentes a Internet y de su uso, experiencias positivas y negativas, conductas adictivas, redes sociales y comunicación online, y juegos.

Uno de los datos que más llama la atención es con respecto al ciberbullying. El resultado de la encuesta ha sido que el 21,9% de los adolescentes españoles ha sufrido este tipo de acoso en alguna ocasión, porcentaje

muy similar al de países como Alemania o Polonia. Dos de cada diez es una cifra muy elevada.

Otra encuesta europea, la realizada por EU Kids Online en 2010 sobre el mismo tema —riesgos y seguridad online— entre más de 23.000 menores de toda Europa, de entre 9 y 16 años, indica que el 12% de los encuestados se ha sentido molesto o disgustado por algo ocurrido en Internet, y que entre los niños que han experimentado algún riesgo es frecuente que los padres no se den cuenta: el 41% de los padres cuyo hijo ha visto imágenes sexuales online dicen que su niño no las ha visto; el 56% de los padres cuyo hijo ha recibido mensajes desagradables o dañinos dice que no ha ocurrido tal cosa; el 52% de los padres de niños que han recibido mensajes sexuales niega que eso le haya sucedido a su hijo o hija…

En definitiva, los padres no hemos sido verdaderamente conscientes de la situación.

Pero la realidad es que el 22% de los niños de entre 11 y 16 años se ha expuesto a uno o más tipos de contenidos creados por otros usuarios potencialmente lesivos: odio (12%), proanorexia (11%), autolesión (8%), consumo de drogas (7%), suicidio (5%).

El 14% de los niños de entre 9 y 16 años ha visto online imágenes «sexualmente explícitas», el 23% pornografía, el 15% ha recibido a través de algún amigo esas imágenes. Pero sólo el 38% borró el mensaje no deseado y el 36% bloqueó a la persona que lo envió.

Por otro lado está la mala utilización de los datos personales. El 9% de los niños ha sido víctima de una mala utilización de sus datos personales (contraseñas, información personal, etc.). Recordemos que estos datos son de hace tres años, lo que significa que seguramente el porcentaje ha aumentado tanto como el consumo de nuevas tecnologías.

Pero básicamente, hay dos situaciones que merecen una especial atención para los padres: el ciberbullying o acoso escolar en internet y el grooming o acoso sexual a menores; dos situaciones de riesgo que han provocado y vienen provocando serios debates y, sobre todo, pueden po-

ner en un serio riesgo la vida de los menores, como se ha podido comprobar por las últimas noticias sobre el tema con casos de suicidio.

En relación con el ciberbullying, el 5% de los niños ha recibido mensajes desagradables o dañinos, y el 3% ha enviado a otros mensajes de este tipo.

Con el parapeto de la red social es fácil entrar en dinámicas de insultos y calumnias, lanzar piedras que otros reproducen y de las que es complicado defenderse. Se ataca con frases, imágenes, etc., atentados contra el honor y la intimidad que luego no hay quien restituya, máxime si se producen en grupo y en el ámbito escolar, donde el alumno tiene que convivir con los acosadores.

Otro de los problemas es el del acosador adulto a menores a través de las redes, particularmente cuando mediante el chantaje y la amenaza consigue atemorizar al menor para que le haga llegar fotografías inadecuadas.

Parece que los riesgos aumentan con la edad (13% entre los 9 y 10 años, 32% entre los 11 y 12 años, y 49% entre los 15 y 16 años) y que los chicos están más expuestos a las imágenes sexuales, mientras que las chicas reciben más mensajes desagradables o lesivos online.

Pero tampoco hay que dejar de lado otros problemas nuevas que van surgiendo en el ámbito escolar como el llamado ciberbaiting o acoso a los profesores, que empiezan como una gamberrada y acaban perjudicando seriamente a los profesores, a su honor y a su intimidad.

Vanessa Van Petten, autora de «Radical Parenting» dice que los jóvenes «necesitan padres, profesores y otros modelos de conducta que les ayuden a descubrir hacia dónde ir, qué decir, cómo actuar y más importante aún, cómo no actuar. Situaciones negativas online pueden tener repercusiones en el mundo real: desde acoso hasta pérdida de dinero en fraudes donde se proporciona información personal».

Es decir, que a la hora de hablar de la seguridad de los menores en Internet, no debemos centrarnos sólo en protegerlos de amenazas de terceros, sino también de ellos mismos, mostrándoles los riesgos de comportamientos como el acoso.

Así que tenemos ciberbullying, grooming, ciberbaiting, sexting….todos ellos serios peligros para nuestros jóvenes, pero esto va en aumento y van surgiendo nuevas formas de acoso.

Finalmente, habría también que afrontar como un riesgo importante el tema de las conductas adictivas, pues el porcentaje de menores que están en riesgo de desarrollo por su uso inadecuado de Internet ya alcanza en España el 21,3%. Se ha comprobado que el uso diario de las nuevas tecnologías está afectando a la rápida transformación del cerebro y a su forma de funcionamiento, con el fin de procesar la gran cantidad de información de estamos recibiendo, pero la adicción puede generar serias dificultades para la vida del niño y para su desarrollo, con trastornos de conducta y tendencia al aislamiento.

Otro problema es que el aumento de las horas dedicadas a Internet supone la consiguiente reducción del tiempo de estudio y diálogo familia, con las repercusiones que esto puede tener tanto en el fracaso escolar como en la calidad de tiempo para la convivencia familiar.

El lado positivo, con respecto a las tareas escolares, es que según el Foro de Generaciones Interactivas (datos de 2010) más de la mitad de los estudiantes de entre 10 y 18 años utiliza el ordenador e Internet como apoyo para las tareas escolares. No sólo como fuente de información, sino también para poner en práctica métodos de aprendizaje cooperativo, mediante la realización de proyectos o la resolución de problemas en grupo.

Es una nueva forma de aprender, que posibilita la relación y la diversión, fomenta la creatividad y facilita la solidaridad y la globalización.

Hay un libro de Fernando García Fernández, director pedagógico del Foro Generaciones Interactivas, sobre «Internet en la vida de nuestros hijos», en donde señala: «da la impresión de que durante algún tiempo los educadores nos hemos fijado excesivamente en la pantalla, en la propia tecnología, sin percatarnos de que lo realmente importante estaba al otro lado de ella, en el ser humano que la usaba. Por eso, se ha invertido mucho en dotar de hardware y de software tanto a los colegios como a los

hogares. Lo que, dicho sea de paso, está muy bien y merece todo nuestro elogio. Pero se echa en falta un esfuerzo similar para conseguir educar en el buen uso. Aunque no es tarea sencilla porque faltan referentes educativos: es difícil educar sobre aquello para lo que no has sido educado».

Y plantea cuatro factores a tener en cuenta por los padres a la hora de mediar educativamente entre nuestros hijos y las pantallas: «el tiempo, el lugar, la compañía y el contenido», cuatro aspectos que vamos a señalar entre nuestras propuestas.

Para los padres es fundamental la formación y la prevención de situaciones de riesgo en los menores de edad, así como la necesidad de recursos, líneas de ayuda por parte de los profesionales para orientarles y ayudarles.

Por ello, desde CONCAPA, venimos animando a los padres a:

— hablar con los centros educativos para asesorarse y conocer cómo se trata el tema en la escuela

— colocar en casa el ordenador a la vista de toda la familia

— tener cortafuegos y antivirus actualizado para proteger el ordenador

— establecer reglas básicas como pactar un horario de utilización, etc.

— enseñar a los hijos a navegar por Internet: distinguir contenidos no recomendables, aspectos legales, normas de uso, no dar datos personales, no aceptar archivos de personas desconocidas, etc.

— hacer de Internet una actividad familiar, abierta a todos los miembros de la familia, donde buscar datos, hacer reservas, hablar con familiares que viven lejos, etc., incluso ayudar en las tareas escolares.

Nos preocupa tremendamente el acoso que se puede producir a través de las redes, producto de ese mal uso de las nuevas tecnologías, y nos preocupa que el niño no sepa distinguir entre mundo real y mundo virtual, entre realidad y ficción, entre la herramienta y la persona.

El único modo de prevenir comportamientos de riesgo y un uso inadecuado de las TIC pasa por involucrarse en la educación de los hijos y potenciar las ventajas que aportan.

Y, por supuesto, que los padres tengan en cuenta que si los menores están siendo víctimas de delitos como el acoso, chantaje sexual, estafa, suplantación de identidad, etc. es necesario denunciarlo. Muchos padres no son conscientes de que el hecho de que le roben la cuenta de correo de la red social a su hijo es un delito, pero las consecuencias pueden ser graves, ya que a través de ella acceden a todos sus contactos y a las imágenes almacenadas propias y de terceras personas. Con esta información y estos datos pueden hacer daño a otras personas y también pueden hacerse pasar por el menor al que le robaron esa cuenta. Es decir, la persona que ha hackeado o robado esa cuenta, tiene en sus manos un arma que puede ser muy peligrosa para muchas personas. Por eso es importante denunciar el hecho. Así estaremos también contribuyendo a aumentar la seguridad de la Red.

Nuestras propuestas

Nuestras propuestas en torno al uso de la Red por parte de los menores se basan en:

1. La necesidad de una formación en los centros escolares sobre el uso seguro y responsable de las redes sociales, una materia que puede ser impartida de forma transversal o con charlas específicas en los centros, contando con profesionales adecuados para ello, como los de Protégeles.
2. Consideramos necesario promover en los colegios las Líneas de Ayuda, de manera que los menores, sus familias y los colegios conozcan los recursos que existen para afrontar los problemas que puedan surgir en torno a este tema.
3. Es preciso facilitar formación a los padres, una formación que debe ser subvencionada por los organismos oficiales y que debe ir precedida de una campaña de concienciación a las familias.
4. Hay que incidir en la formación de los profesores en este ámbito, tanto desde las escuelas de formación del profesorado como desde la universidad y los centros educativos, para que sean capaces de

trabajar con las necesidades actuales, eliminando así la llamada brecha digital.

5. Las empresas responsables de las redes sociales tienen que poder garantizar que sus usuarios son mayores de 14 años (sólo Tuenti se preocupa en estos momentos de ello, buscando y eliminando perfiles de menores y, en todo caso, pidiendo por escrito el permiso de los padres para su utilización).
6. Es necesario agilizar los procesos de atención a las denuncias, ya que cuando se producen las denuncias de contenidos inadecuados se tarda demasiado tiempo en retirarlos (a veces semanas).
7. Los perfiles de los menores deben ser siempre privados, sin excepción.

Confiamos en que la puesta en marcha de estas medidas pueda llevar a minimizar los riesgos que actualmente padecen nuestros hijos, porque en este sentido tenemos la suerte de ser pioneros, los primeros que nos acercamos al mundo digital y tenemos que ir aprendiendo teniendo en cuenta los errores y experiencias que vamos acumulando.

Muchas gracias.

Luis Carbonel Pintanel. Presidente Nacional de CONCAPA

COMPARECENCIA DEL PRESIDENTE DE LA FEDERACIÓ D'ASSOCIACIONS DE PARES I MARES D'ESCOLES LLIURES DE CATALUNYA (FAPEL), D. JOSEP MANUEL PRATS MORENO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 10 DE OCTUBRE DE 2013.

Madrid, 10 de octubre de 2013

Muy buenos días, Sr. Presidente de la Comisión, Excelentísimas Señoras y Señores Senadores:

En primer lugar, como no puede ser de otro modo, quiero agradecer a esta comisión la invitación y la oportunidad de comparecer ante ustedes para compartir la visión que tenemos en Fapel, como padres y madres de alumnos. La última vez que estuve en esta institución fue hace, exactamente, 30 años. Yo era uno de los menores de los que hoy hablaremos. De esos que todavía jugábamos en la calle a las chapas, y al fútbol si había balón. Los riesgos eran otros, más tangibles y sencillos. Hoy mis hijos juegan a las chapas virtuales y pueden tener acceso a todo lo que quieran a través de Internet. La calle es inabarcable, vivimos una revolución educativa, en el modo de educar a nuestros jóvenes, de mayor impacto que la imprenta de Gütemberg. Padres, escuelas, administraciones, legisladores, medios de comunicación, la sociedad en general, tenemos la responsabilidad de afrontar con seriedad un reto de tal magnitud. Por ello me siento muy honrado de poder aportar a esta Comisión la experiencia y las inquietudes de casi un millón de padres y madres que están representados en FAPEL.

Comparezco ante ustedes como Presidente de la Federación de Asociaciones de Padres y Madres de Alumnos de escuelas Libres de Catalunya (FAPEL). Pero también tengo la fortuna de tener algo más de perspectiva, por ser vicepresidente de la Confederación de Federaciones de Asociaciones de Padres de Alumnos (COFAPA), así como miembro del consejo directivo de la European Parents Association (EPA).

Como saben, tengo formación jurídica, especializado en tecnologías y redes. He tenido responsabilidades directivas en esas áreas en la administración pública, y también en el sector educativo privado concertado. También soy educador, porque soy profesor pero, fundamentalmente, porque soy padre de siete hijos. Y lo que hace casi 18 años (la edad de mi hijo mayor) me parecía fundamental, la tecnología, hoy me parece baladí a los efectos que nos ocupan hoy. Desde hace más de 10 años me parece fundamental educarles para que puedan utilizar bien y para bien todo cuanto el mundo tiene y les ofrece, y aporten a la sociedad lo mejor de sí mismos.

En Fapel tenemos como misión fundacional (1) concienciar y defender el derecho de las familias a la libertad de educación, (2) fomentar el buen entendimiento entre familias y colegio, entre familias y AMPA, entre AMPA y colegios. También (3) dialogar con la administración, y dialogar con otras federaciones de padres que crean que la educación es lo más importante. Todos formamos parte del proceso de educar a nuestros hijos. Lógicamente, (y 4) también prestamos servicios de asesoramiento a AMPAs y familias, organizamos, asesoramos y proveemos escuela de padres y una central de compras de libros de texto y gestión de reutilización. Y no dependemos de la subvención pública.

Es por nuestra experiencia a nivel autonómico, estatal y europeo, que me permito constatar que en todas partes de Europa y probablemente del mundo, los padres y madres estamos preocupados por los riesgos que entrañan las redes sociales para los menores. Porque son nuestros hijos...

Me puedo equivocar, pero estoy seguro de que quienes han comparecido antes y lo harán después en esta comisión, y quienes me escuchan hoy, también son padres y madres (alguno de ustedes quizá abuelos jóvenes). Para todos nosotros, pues, más allá de nuestras responsabilidades profesionales, políticas o institucionales, nuestra primera preocupación es, o debería ser, la educación de nuestros propios hijos, y luego los de los demás, por su propio bien y por el bien de nuestra sociedad.

La educación de una persona, dice una cita atribuida a Napoleón, empieza cien años antes de su nacimiento. A mí al menos, como padre, se me presenta por delante un panorama y una responsabilidad que va

más allá de mí mismo e incluso trasciende de mi propio hijo, porque tal como lo eduque yo, educará él a la siguiente generación. Tal es nuestra responsabilidad.

Hay quien sabía muy bien esto cuando hizo las leyes educativas (y en otras muchas no educativas) de nuestra entonces jovencísima democracia, quitándonos la autoridad a los padres y rebajando la de los profesores. Trivializando la educación y, en cierto modo, también la instrucción. Entre dos y tres generaciones sufren y sufrirán sus tremendas consecuencias.

En la tan admirada Suecia ya lo pasaron a principios de los 70 y todavía no se han recuperado; y, aunque hace ya algunos años que han cambiado el rumbo, les está costando mucho. Me remito en este tema a todo cuanto se expuso en la Ponencia de estudio sobre buenas prácticas y estrategias pedagógicas positivas, constituida en el seno de la Comisión de Educación, Política Social y Deporte, para informar sobre los retos de la sociedad del conocimiento y su afectación en el ámbito escolar en el año 2009. Pero estamos ya en 2014 y seguimos casi igual. Desde hace años estamos intentando arreglar un sistema deficiente que ha difuminado la exigencia y los contenidos. Aunque en su haber podemos poner, que no es poco: es mucho!!, la universalización, la equidad y la cohesión. Pero estarán conmigo en que tener a todos los menores en el colegio y ser muy equitativos no resuelve la excelencia educativa en actitudes y contenidos, sobre todo cuando la equidad se logra igualando a todos con objetivos de mínimos, generando mediocridad. Vayamos más allá.

¿Acaso alguno de Vds. piensa que la educación de Vds. y la mía, la del BUP y el COU (alguno habrá del sistema bachillerato y reválida) fue peor que el actual en contenidos y exigencia? De ser así, creo que Vds. y yo hubiéramos sido barridos literalmente, de la política y otros trabajos por generaciones de jóvenes LOGSE mucho más preparados. Me temo que no es así, salvo honrosas excepciones, y estos seguramente a causa del tesón, del esfuerzo y la vocación. ¿Casualidad?

Disculpen esta digresión, aunque apenas había iniciado, pero no crean que me voy del tema, puesto que ya he lanzado uno de los ejes funda-

mentales de los riesgos de las redes sociales y los menores; es una de las ideas que quisiera poner de manifiesto: la necesidad, la obligación, la urgencia que tenemos los padres y madres de apoyarnos en la educación y en la formación para educar a nuestros hijos e hijas. Formación en muchas áreas, pero especialmente en comprender, asimilar e interiorizar que el mundo cambia a una gran velocidad y que las «eras» de la antigüedad, hoy pueden ser meses, si no semanas.

No entraré en considerar ni exponer cifras, que sus Señorías ya tienen sobradamente por anteriores comparecencias. Solamente quisiera exponer una serie de ideas para contextualizar mi discurso, aunque forma parte casi del acervo popular, y a pesar de ello no seamos del todo capaces de comprender su profunda realidad y sus consecuencias.

Y ahora pasaré a hablar de lo que se espera que hable un padre de familia, a quienes represento: **de educación.**

Las redes sociales están y estarán. Como dice el latiguillo que habrán oído sus señorías ya muchas veces: han venido para quedarse. Pero no solamente para eso, sino que evolucionan rápidamente y se adaptan e insertan y quedan imbricadas en nuestra persona porque nosotros, los usuarios, somos quienes las configuramos. Somos el contenido. Y estamos solamente al principio.

Y son unas herramientas buenas, un medio estupendo para poder realizar un sinfín de cosas que habíamos pensado, ideado o imaginado pero nunca habíamos podido realizar. Todos los sectores se han visto sacudidos, y beneficiados, por la incorporación de la ciencia y la tecnología. Se ha potenciado la labor de creativos y emprendedores, de educadores, de las fuerzas de seguridad, de la administración, de innovadores que han implantado ideas en beneficio de la sociedad. Es maravilloso...

Las TIC (tecnologías de la información y la comunicación), las TAC (tecnologías del aprendizaje) y las TEP (tecnologías del empoderamiento y la participación) se han extendido y enraizado a una velocidad y una profundidad de vértigo. Y la velocidad de los cambios que impactan tan profundamente en la persona y sus relaciones son complejos de asumir y

de incorporar. Tendremos estudios dentro de unos años de ese impacto y de sus consecuencias.

La capacidad de influencia de estas redes es espectacular. Jamás habíamos pensado en la capacidad de comunicarnos tanto individualmente como masivamente, en privado y en público, y hacer llegar nuestras ideas a uno o a miles o millones de personas. Han visitado las webs de algunos youtubers? Su popularidad y el modelo de negocio generado han sido una revolución. Aunque quizás en demasiadas ocasiones sólo digan tonterías y aportan un valor escaso. Otros no, y pienso en el impacto de poder seguir las conferencias del TED, o bien las clases magistrales de profesores del MIT o de Harvard... Una quimera hace pocos años.

Habrán comparecido ante esta comisión, y comparecerán aun personas que saben muchísimo de técnica y tecnología, mucho más que yo, cifras, datos, estadísticas de todo tipo. Soy usuario intensivo de tecnologías y redes desde 1994, y esos 20 años me dan una cierta perspectiva: empecé a navegar con Mosaic, gopher, chateaba con IRC, ICQ... Y creo que he llegado a una conclusión sencilla, que pienso que es la clave de todo esto.

Los árboles no nos dejan ver el bosque. Los chips y los aparatos, las redes y las antenas... no nos dejan ver la realidad. Creo que casi todo se podría reducir, como siempre, a la conducta humana. Cierto es que algunos de los que me han precedido han hecho hincapié en la expresión «nuevos delitos», y que el Código Penal los recoge quizás tengan razón desde el punto de vista estrictamente jurídico: el tipo cambia o se adapta... Pero la conducta humana es muy simple, y a todos, a mí y a ustedes, nos dominan siete conocidas tendencias que nos hacen actuar y luego, a lo mejor, pensar; en lugar de pensar y, luego tal vez, actuar. Pura antropología humana, sin más.

Les propongo hacer un ejercicio teórico, solamente un momento; un planteamiento maximalista y poco realista. A veces imaginar ciertos escenarios puede aclararnos las ideas: Supongamos que los menores no estuvieran presentes en la red, muchos delitos asociados a sus conductas, fundamentalmente el ciberacoso, o con las de terceros relacionadas con

ellos, como las que se han citado en otras comparecencias y que nos horrorizan a todos, no se producirían, o apenas... Si no existieran los límites y las normas (recordemos que los menores suelen ser personas en proceso de formación), probablemente los problemas se multiplicarían por el número de usuarios e interacciones.

A mi, y creo que a todos, nos gustaría que nuestros hijos pudieran circular por las redes con tranquilidad, libertad y seguridad. Y responsabilidad... Pero las conductas de algunos usuarios lo impide...

Y si lo que tenemos dentro, en nuestro cerebro y en nuestro corazón, no nos ayuda a pensar en lo correcto para los demás y para uno mismo, actuaremos erróneamente, sea digital o analógicamente, presencial o a distancia, con un chip o con un palo...

¿Es un riesgo conducir mientras se habla por teléfono?: prohibámoslo (a ver para cuando prohíben hablar con el copiloto).

¿Es un riesgo tener armas de fuego? Regulémoslo.

¿Es un riesgo que los menores estén en la red? Eduquémosles!!

Propongo estos ejemplos de prohibición, regulación y educación, porque creo que son los estadios que han venido sufriendo muchas de las innovaciones de la humanidad. Primero las prohibimos, luego las regulamos y finalmente optamos por dar formación, porque hemos estimado insuficiente ambos estadios previos.

A prohibir ya no estamos a tiempo. Los menores ya están en la red y la dominan.

La regulación entraña una gran complejidad: distintos estados, distintas regulaciones, distintas culturas y sensibilidades... y también distintos intereses, especialmente de la grandes empresas y corporaciones tecnológicas y mediáticas. En este sentido, puedo aportarles que en mi calidad de miembro del consejo directivo de la European Parents Association (EPA), tenemos problemas para establecer una posición común acerca de este tema, porque mi colega holandés tiene una perspectiva, experiencia y cultura distintos del italiano, la húngara del francés o la danesa, etc.

Yo les estoy contando la mía, que es un mínimo común denominador de todos mis colegas de EPA: familia, educación, acompañamiento, libertad y responsabilidad.

Por eso la oportunidad la tenemos en la educación, en la formación de padres y en un marco de referencia (antes se llamaban principios), sólidos y reconocidos por la cultura Europea, que es donde estamos. Y en un entorno de libertad, donde cada familia pueda educar a sus hijos e hijas como crea conveniente, según sus propias convicciones, como establece nuestra Constitución en el artículo 27 y, teóricamente, deberían respetar todas las leyes educativas. Y yo añadiría, en igualdad de condiciones...

Los expertos en comunicación ya han escrito, y más que escribirán, acerca de la potencia de la red, de las maravillas de las herramientas TIC, TAC y TEP... Pero falta por saber las consecuencias de haber puesto estas herramientas en manos de niños y adolescentes menores en proceso de formación. Como sociedad somos capaces de los proyectos más vastos para protegerles en algunos ámbitos: En el de la salud porque son un bien digno de protección y, si me permiten la expresión economicista, «un bien escaso». Y también nos esmeramos en otros programas, normas, reglamentos, etc. que tienden a su protección en un mundo físico que los adultos conocemos bien y, por tanto, sabemos adelantarnos a los acontecimientos. Pero nos limitamos a eso, y por otra parte (yo creo que en su mayoría o bien por inconsciencia, ignorancia, o bien por simple esnobismo) les permitimos acceder a información, recursos, contenidos y herramientas que gestionan con muy poco criterio (no son culpables!! Son menores en fase de formación).

Por otra parte, ustedes y yo, como padres o madres, seguiremos acompañando (eso espero) a nuestro hijo de 5 ó 6 años a comprar el pan, le indicaremos los cruces, los peligros, la educación con la que debe pedir el pan, pagar y estar atento al cambio, decir buenos días o buenas tardes, hola y adiós, y que no se pare con desconocidos... Pero deberíamos ser un poco más coherentes... porque resulta que luego les dejamos que se abran una cuenta en facebook ya que ni siquiera sabemos (o sí!!) que hasta los 14 facebook no lo permite, y les «obliga» a mentir. Y accederán a personas y contenidos que jamás nos encontraríamos camino de la panadería.

¿Para qué utilizan los menores las redes? Parece que para comunicarse, eso es obvio... y algo aparentemente tan sencillo como la comunicación humana tiene una complejidad extraordinaria que requiere un proceso de aprendizaje y maduración.

Me decía un experto en comunicación y redes que para poder crear contenidos y mensajes eficientes no es necesaria la tecnología. Es suficiente con haber desarrollado previamente cuatro hábitos esenciales: a) reconocer las fuentes de información b) leerlas y contrastarlas c) tener la capacidad de escribir con el objetivo de hacer abstracciones d) tener la facultad de dialogar una vez confrontados dos mensajes.

Y hoy, eso hay que hacerlo en 140 caracteres....

¿Y cómo andamos de lectura, comprensión lectora y expresión escrita en España? Pues basta echar un ojo a los estudios de PISA para ver que hemos perdido el tiempo en nuestro sistema educativo. De los cuatro hábitos esenciales citados antes, en general nuestros chicos y chicas adolecen gravemente de dos... y es evidente que la comunicación se hace muy difícil sin ellas. Y solamente estamos hablando de nuestras lenguas maternas (castellano, catalán, galego y euskera), así que obviaré el tema del inglés.

Y si nos saltamos el primer paso, dejamos de interiorizar el conocimiento teórico. Entonces abordamos la tecnología huérfanos, además de analfabetos. Y aparece la gran agresividad en los mensajes y expresiones, porque no se domina lo esencial, no se hace un proceso intelectual y expresamos una idea sin sustrato. Y eso sucede en las redes sociales, y en la mayoría de casos de acoso o ciberacoso.

Todo esto no sería tan peligroso, si no existiera una grave brecha entre los padres (y educadores) y los hijos (y alumnos). La formación en la familia y en el colegio son fundamentales para ello, para generar un entorno, una cultura de la relación, una cultura de la conducta. Pero el absentismo de los chicos en la escuela y en casa es de escándalo: y es un absentismo mental, no físico. Puede que estén en el aula, en su habitación o en el salón, o, en el mejor de los casos, comiendo en familia..., pero tienen su cabeza y su corazón en otra parte, en algo que les engancha, les sobreestimula, porque allí pueden ser alguien...

Creo que ya lo conocerán, pero fue muy ilustrativo para mí la lectura, ya en 1999,de un libro muy interesante: Homo Videns, de Giovanni Sartori. Este politólogo italiano, premio Príncipe de Asturias 2005, analizaba ya entonces el impacto de la sociedad audiovisual (las redes sociales no existían), en la educación de las personas y en la política. Creo que debería formar parte de los documentos de esta ponencia de estudio, si no lo es ya.

Muchos padres ni entienden ni quieren entender que las redes sociales serán la forma de organizarnos en un futuro, que es casi presente: relacionarnos, gestionar personas y grupos, comprar, informarnos, identificar y evaluar soluciones para el trabajo o la vida personal, etc.). Muchos de ellos dicen que es una pérdida de tiempo. Y los que las utilizan no han invertido ni un minuto en decodificar con sus hijos el uso de esta tecnología. Les propongo que se den una vuelta por los twitters o Instagrams de menores, niños y adolescentes, y verán qué contenidos vierten, qué comunicación construyen. Lo bueno de cuando ustedes y yo teníamos esa edad, nuestras conversaciones y tonterías quedaban en el aire. Hoy quedan en la red para siempre. Todavía no hay un derecho al olvido, como hemos gozado ustedes y yo. Y a lo mejor habría que exigirlo para los menores de edad...

Por un lado tenemos padres despreocupados de una realidad de futuro por, quizás desidia ignorancia o pereza, y por otro una sociedad sin conocimientos de las reglas básicas de comunicación, utilizando unos recursos que ellos mismos aún deben definir.

El problema no es que les estemos dando a nuestros hijos un vehículo de potente cilindrada. El problema es que no les estamos explicando nada sobre ello. Lo vemos en las competiciones, por ejemplo, de MotoGP: adolescentes que van a 300 km/h y, a pesar de que se caen muchas veces, se levantan de nuevo. Porque saben perfectamente qué están haciendo, y lo saben porque alguien les ha explicado el QUÉ, POR QUÉ, PARA QUÉ, CÓMO, sus riesgos y, sobre todo, que es una herramienta para ganar carreras, no para hacer daño a nadie.

En otras palabras, el principal problema no es «mi hijo se pasa muchas horas ante el ordenador o el teléfono». El problema es que «no sé qué hace, ni por qué lo hace, ni cómo lo hace... pero sobre todo para qué lo hace».

Los padres debemos comprometernos con nuestros hijos. Pero no en si debe tener el ordenador en el salón o unas horas de uso... Compromiso en educarles y en apoyarnos en sus educadores, aquellos que deberíamos haber elegido: maestros y profesores, monitores o entrenadores deportivos, gestores de tiempo libre... Son nuestra responsabilidad. Y ya podemos trabajar mucho para tener una economía muy saneada y potente, que si educamos inútiles emocionales, una sociedad no tira, no progresa.

Los padres, una vez informados, debemos pasar al estado de conciencia y compromiso. Tres motivos para renunciar a ello sería la pereza, el miedo o la ignorancia. Todo ello es más o menos vencible con formación.

Por ejemplo. Es importante saber que nuestros hijos menores están en proceso de educación. Y parece evidente que quienes deben haber influido más en sus hijos sean los padres y educadores que los padres hayan elegido, bajo el ejercicio de su responsabilidad de primeros educadores...

Pero realmente ¿somos conscientes de que todo educa a una persona en proceso de educación? Parece que los expertos en marqueting y ventas sí que lo saben, y ellos no pierden el tiempo. Una máxima que utilizan las industrias de los media y redes sociales para tener claro como influirles: Si pagas por ello, eres el cliente; si no pagas por ello eres el producto. Y nuestros menores (y los mayores también) se están convirtiendo en el producto de las redes sociales, con o sin nuestro consentimiento, el de los padres y de todos los fantásticos defensores de los derechos del niño, que a veces parece que solamente estén para enfrentar padres e hijos. Y eso no les ha preocupado demasiado.

Nuestros hijos, sus hijos también, se convierten en el contenido, en el producto que aporta valor económico a esa red social o herramienta web 2.0. Pero ni vd ni yo veremos siquiera un céntimo de ello, sino que al contrario, le habremos cedido la imagen, nuestra y de nuestros hijos, sin limitación alguna y sin el derecho al olvido.

Como he establecido mi exposición alrededor de una idea, me permito sugerir a sus señorías alguna propuesta concreta, que podría ayudar en algo a cuanto nos preocupa en tanto que el futuro de nuestro país:

1. Educar requiere tiempo. Los padres y madres necesitamos más tiempo para educar, para estar con nuestros hijos y para formarnos. Escuchen y apoyen cuanto dice la Comisión Nacional para la Racionalización de los Horarios en España. Necesitamos tiempo para conciliar el trabajo con la familia. Hay soluciones para conseguirlo. Abramos la mente y no nos instalemos en la frase «toda la vida se ha hecho así», porque, además de que no es cierto, hacer siempre lo mismo garantiza los mismos resultados.
2. Educar requiere saber qué se está haciendo, por qué y para qué. Los padres y madres necesitamos información, pero mucha mucha formación. Ya tenemos algo de sentido común, pero se nos olvida. Y lo más fácil es que se nos apoye desde dos frentes: la televisión y la escuela. Utilicémoslos para mejorar nuestra sociedad. Promuevan y sugieran a los gobiernos acciones basadas en la familia, en la educación y tendremos personas mejores (mejores personas), y en consecuencia una sociedad más culta, más respetuosa, más solidaria. Nunca va al revés.
3. Familia y escuela es la tercera clave. Es en las escuelas donde las familias nos debemos sentir comprometidos con los maestros, y en positivo, para que ellos nos ayuden a educar a nuestros hijos. Ello trae una derivada lógica: si como familia hemos elegido un colegio, nuestro compromiso aumenta y se puede consolidar. Ayudar a las AMPAs y colegios a dar formación a los padres. Pero no solamente en TIC, TAC y TEP, sino para educar mejor a nuestros hijos, que son lo importante.

Es tan simple como que cada uno de los que estamos aquí, hagamos una lista de cómo querríamos que fueran (o que son ya) nuestros hijos al llegar a su edad adulta. Estoy convencido de que en esa lista aparecen en primer lugar una larga retahíla de valores y virtudes. Seguro que hacia el final aparecen aspectos materiales o instrumentales que hagan su vida fácil, segura y confortable: idiomas, trabajo, bienes... Pero su felicidad y la de la sociedad está en la primera parte de la lista y es ahí donde los padres debemos concentrar nuestros esfuerzos: tiempo de familia, educación y formación.

¿Recuerdan aquellos antiguos anuncios de electrodomésticos? Nos aseguraban que la incorporación de los avances científicos y tecnológicos al hogar nos dejaría más tiempo disponible para los nuestros: hijos y cónyuges, y tiempo propio para nuestras aficiones y para «cultivar el espíritu»... Pero parece que lo hemos sabido gestionar muy mal, porque nuestra vida está llena de cosas que nos ahorran tiempo, y cada vez tenemos menos, y encima tendemos a dedicarlo a lo que no es importante.

Me han llamado para hablar sobre los riesgos derivados del uso de la red por parte de los menores, y parece que he preferido hablar de qué debemos hacer en el estadio anterior: la educación de la familia del menor y del menor.

Y es que el problema de la red no es, desde mi punto de vista, tecnológico, sino humano y por ello educativo. Y es por ello que hablamos mucho de riesgos y muy poco de oportunidades. Si educamos bien (a la familia, en familia), tendremos oportunidades. Si no lo hacemos, todo son riesgos.

Y si me permiten, el coste es muchísimo mayor si solamente asumimos los riesgos, en lugar de incidir en la educación, que nos da oportunidades.

Necesitamos TIEMPO para los hijos y para los padres: HORARIOS.

Para EDUCAR a los hijos necesitamos FORMACIÓN para a los padres y COLABORAR con el colegio que libremente hayamos ELEGIDO.

Internet y las redes sociales y las conductas humanas mejorarán si mejoramos a las personas que las utilizan. Alguna vez me han dicho que mi discurso no es realista, que es muy difícil cambiar. Pero lo que es seguro es que tal como estamos haciendo las cosas hasta la fecha, no vamos bien. Pero como en mi tierra decimos: «Mica en mica, s'omple la pica», por algo hay que empezar, como el comer y el rascar...

La brecha digital que se está abriendo entre nosotros y la sociedad del futuro porque muchos padres de este país no saben cómo entrar a formar parte de este partido. Y este partido, Señorías, se está jugando hoy mismo.

Las administraciones tienen una gran capacidad operativa y de influencia. Y les cito un buen ejemplo: Les animo a entrar en la web de la Generalitat de Catalunya, llamada Familia i Escola (familia y escuela). No conozco, si la hay, otra iniciativa desde una administración pública con tanto contenido, con tanto sentido común. Hay muchas seguramente en el sector privado, porque quizás somos más conscientes de lo que nos jugamos, pero no tenemos el poder de la administración para incidir.

Realicen en nuestro nombre estas recomendaciones para mejorar la sociedad. Estamos convencidos que incidir en estos aspectos esenciales es la clave:

Cambiar los horarios para (1) **fomentar el tiempo de familia** y así facilitar la (2) **formación de los padres y madres** a través de AMPAs y colegios, (3) **facilitar la libre elección de centro educativo** y (4) **fomentar la relación**, buena y estructurada, entre **la familia y el maestro**.

Muchas gracias por su atención, y quedo a su disposición para dialogar con Vds. hoy y cualquier otro día y para responder cualquier aspecto que quieran plantearme a continuación.

COMPARECENCIA DEL VICEPRESIDENTE DE LA CONFEDERACIÓN ESPAÑOLA DE ASOCIACIONES DE PADRES Y MADRES DE ALUMNOS (CEAPA), D. JESÚS SALIDO NAVARRO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 10 DE OCTUBRE DE 2013.

Las redes sociales desde la familia

Madrid, 10 de octubre de 2013

Ser padre y madre en el siglo XXI conlleva atender nuevas realidades de la crianza y la educación familiar. Una de ellas es la inclusión de las nuevas pantallas en el día a día de las familias.

Nuestros hijos e hijas son nativos digitales y para ellos el teclado y el ratón son objetos que forman parte de su entorno desde su infancia. Para nosotros esta realidad es una novedad, pues nos encontramos educando en el uso de unas tecnologías que no conocíamos de niños e incluso, en muchas ocasiones, no dominamos de adultos.

Las Redes Sociales en Internet han sido integradas de forma rápida en la vida cotidiana de muchos adolescentes y jóvenes crecidos en la era de la informática y han encontrado en ellas una plataforma donde satisfacer ciertas necesidades personales, convirtiéndose por tanto en una de las marcas de identidad de esta generación. Ellos usan Tuenti, Facebook o Bebo para comunicarse y de esta manera se instala un sentimiento de identidad entre ellos, que los diferencia de las generaciones anteriores.

El uso de estas tecnologías de la información genera entre padres y madres sensaciones a veces contrapuestas. Por un lado, como progenitores hacemos un esfuerzo para que nuestros hijos e hijas dispongan de esas herramientas informáticas que sentimos importantes en el mundo que les espera.

Por otro, nos sentimos poco seguros a la hora de tutelarles o educarles en su uso, porque sentimos que es un mundo propio y distante del nuestro. A la vez, como adultos, somos conscientes de que, como otras tecnologías, la informática e Internet conllevan una serie de riesgos y problemas potenciales sobre los que hay que actuar educativamente.

Desde CEAPA, consideramos que las redes sociales en Internet son un escenario más en el proceso educativo de los hijos e hijas por lo que nuestro papel ha de ser el mismo que en los demás temas educativos, es decir, acompañarles en su proceso de desarrollo y seguir manteniendo el equilibrio entre ofrecer apoyo afectivo y establecer unos límites adecuados a través de una comunicación positiva.

Debemos recordar que seguimos siendo su pilar de confianza y su principal referente y consideramos importante educarles en el uso responsable, seguro y adecuado de las redes sociales.

En concreto, desde CEAPA, consideramos importante tener en cuenta las siguientes pautas en el uso y disfrute de las nuevas tecnologías y las redes sociales.

1. **Ser afectuosos, acompañarles y apoyarles, lo que significa confiar en ellos y potenciar su autonomía.**

   Es necesario fomentar su libertad y responsabilidad de forma gradual, lo que significa que son ellos, en función de su madurez, los que han de tomar sus propias decisiones, vivir y asumir sus consecuencias y aprender de sus errores.

   Ellos deben tener plena libertad a la hora de elegir la red social de la que desean ser miembros, cómo configurar su perfil, qué amigos escoger, etc., aunque nuestro trabajo será asesorarles sobre ello.

   Si sienten que confiamos en ellos y que pueden ser autónomos, se sentirán respetados y será más fácil que nos escuchen y que comprendan y asuman mejor los límites sobre su uso.

2. **Regular ciertos límites relacionados con las redes sociales, al igual que hacemos en cualquier otro ámbito educativo.**

   Es importante acordar un horario y un tiempo límite de uso, que no interfiera en su horario de estudio ni en sus tareas de casa ni supla sus relaciones sociales de calle. No hace mucho se recomendaba que el ordenador ocupase espacios comunes para evitar el aislamiento que se produce cuando está ubicado en su habitación, pero ahora hay que tener en cuenta que el acceso a la red se hace sobre todo a través de ordenadores portátiles y teléfonos móviles lo que supone un nuevo reto para reforzar las habiliddes de comunicación familiar y las actividades conjuntas para el ocio y el tiempo libre.

3. **Comunicarse con nuestros hijos e hijas, creando un entorno de confianza donde todos puedan hablar y ser escuchados, se intercambien ideas, se valoren y se respeten**.

   Si desde que son pequeños hablamos con ellos de su vida cotidiana, de las cosas que les gustan, de cómo se sienten, de sus amistades, etc., de forma natural, cuando lleguen a la adolescencia las redes sociales será un tema más de conversación y no un interrogatorio.

   Estas conversaciones en tono natural, nos van a facilitar la labor para conocer cómo son y cómo se relacionan a través de la web y, que confíen y sientan que pueden contar con nosotros, lo que facilitará que compartan cualquier tema que les interese, les preocupe, etc., incluido todo aquello relacionado con las redes sociales.

   Además, las redes sociales podemos usarlas también nosotros como una herramienta para reforzar nuestra comunicación con ellos, por ejemplo, como vía para intercambiar opiniones, organizar actividades, etc. Para que esto funcione, es imprescindible que nuestro objetivo no sea controlares ni invadir su intimidad. El respeto a su intimidad y a su espacio privado es siempre fundamental y, aún más, en la adolescencia.

4. **Potenciar sus valores y su sentido crítico para que los apliquen cuando usen las redes sociales.**

   La mayoría de nuestros hijos e hijas dominan el uso técnico de las redes sociales pero es necesario que les eduquemos en cómo usarlas de forma positiva, debemos dotarles de un marco ético donde prime el respeto a los demás, la responsabilidad y el sentido común, tanto en sus relaciones en la red como en el resto de relaciones sociales.

   Hemos de enseñarles pautas tales como no ridiculizar a los demás a través de comentarios o fotografías y reprobar esa conducta cuando otros la llevan a cabo, compartir información con los demás, ser sinceros, solidarizarse con aquellas personas que lo necesitan, respetar la privacidad de los demás, etc. Nuestro papel es seguir acompañándoles en su proceso de desarrollo y hacerles capaces de enfrentarse y solucionar sus problemas de una forma ética.

5. **Tratar de entender las redes sociales desde la adolescencia.**

   La adolescencia es una etapa de búsqueda de identidad propia, por lo que necesitan conocerse mejor, diferenciarse de los adultos incluidos sus progenitores, explorar, experimentar, cuestionar las normas, etc., siendo este un proceso en el que su grupo de amigos adquiere un gran protagonismo.

   Por ello, las redes sociales se han convertido en algo casi imprescindible para ellos, porque satisfacen y facilitan su necesidad de relacionarse, de sentirse miembro de un grupo, de mostrarse, de verse reforzado por los demás, de expresarse y, en definitiva, de crecer.

   Actualmente la mayoría de los adolescentes se relacionan a través de las redes sociales, por lo que impedirles su uso les mantendría al margen de una realidad que no debemos evitar porque no les permitiría aprender a relacionarse en este nuevo contexto.

   Por tanto, es necesario tratar de entenderles desde ahí, asumir que están cambiando y adaptarse a sus nuevas necesidades. Aunque pudiera parecer que no necesiten nuestra ayuda o la rechacen, nuestro papel sigue siendo prioritario, ellos sí nos necesitan ya que seguimos siendo su referente y su pilar de confianza.

   Si mantenemos una actitud de respeto hacia el uso que hacen de las redes sociales, es mucho más probable que acudan a nosotros cuando tengan un conflicto surgido en este contexto que no sepan cómo afrontar.

6. **Conocer cómo funcionan las redes sociales**, **para saber de primera mano de qué estamos hablando.**

   Para ello no hace falta que sepamos usar cada herramienta, basta con que nos acerquemos a ellas con interés, curiosidad, sin miedo y reconociendo que en este campo nuestros hijos e hijas nos pueden enseñar muchas cosas: qué son, cuáles son, cuál utilizan, cómo funcionan, qué posibilidades y ventajas tienen, cuáles son las condiciones e implicaciones del servicio, sus riesgos, etc.

   Además, al compartir algunos momentos ante el ordenador podremos aprovechar para revisar con ellos algunos temas que, aunque son importantes, los adolescentes suelen obviar. Temas tales como

las condiciones de uso de la red social en concreto, que la mayoría de las veces conllevan opciones automáticas que probablemente nuestros hijos e hijas desconocen, las opciones de privacidad y otros aspectos que señalamos a continuación.

7. **Supervisar juntos cómo usan las redes sociales y ayudarles a controlar sus riesgos**.

   Las redes sociales generan un tipo de relaciones con unas características muy específicas; la ausencia del contacto cara a cara, el carácter permanente e imborrable de todo lo que se publica, la inexistencia de una sistema de selección que te informe sobre quienes pasan a ser «tus amigos» ofreciéndote unas garantías mínimas sobre cómo es la persona con la que estás manteniendo una relación, etc.

   Estas características singulares pueden generar algunos riesgos que es importante conocer y controlar. Cada red social tiene sus propias características y condiciones de uso y algunas establecen recomendaciones y pautas para usarlas de forma segura, por lo que, para poder actuar con más eficacia, es importante conocer qué red en concreto está usando nuestro hijo o hija.

   De forma general, las pautas básicas que es necesario supervisar para que usen las redes de de forma segura y responsable son:

   - Cuando acepten amigos, no hacerlo automáticamente, y valorar si los conocen bien.
   - No es recomendable aceptar a desconocidos, a simplemente conocidos ni a amigos de amigos. Debemos enseñarles a que no se sientan presionados para agregar a personas que apenas conocen y, en caso de hacerlo, que conozcan las opciones para bloquear y restringir el acceso a su información. Hacerles ver que lo más importante no es la cantidad de amigos que tengan sino la calidad de la relación que tengan con ellos.
   - Restringir con ellos lo máximo posible las opciones de privacidad generales y específicas, controlando así qué personas pueden tener acceso a su información.
   - Es conveniente que sólo sean sus amigos/as los que puedan ver todo lo que cuelgan en su página. También es recomendable que

configuren su privacidad para no recibir mensajes de personas no aceptadas como amigo.

- Respecto a su contraseña de acceso, es importante que escojan una que no sea fácil de intuir, que no la compartan con nadie y que no marquen la opción para que el ordenador recuerde. En caso de que sospechen que alguien ha accedido a su página con su contraseña, es necesario que la cambien.
- Resaltarles la importancia de cuidar la imagen personal que muestran en la red, porque es la forma en la que todos les verán.
- Insistirles que piensen bien en todo aquello que escriben y cuelgan en la red, evitando especialmente comentarios y fotografías que puedan ser comprometidas. Han de ser conscientes de que todo lo publicado queda ahí y puede ser utilizado y manipulado fácilmente por cualquiera. Incluso borrándolo de su perfil puede aparecer en el de los demás. Además, es fundamental que sean conscientes de que todo aquello que quede por escrito es algo que, si fuera necesario, puede ser utilizado como prueba contra ellos.
- Tener cuidado con la información personal que muestran en la red, intentando evitar toda aquella información que sea opcional y, especialmente, aquella personal y familiar que permita localizarlos como son el teléfono, la dirección, etc.
- Recomendarles que no queden con personas desconocidas, y que si lo hacen deben citarse en un lugar público y deben informar siempre a algún amigo o familiar. En definitiva, ante estas situaciones, aplicar el sentido común y la prudencia.
- Conocer cómo podrían otras personas acceder a su información sin ser sus amigos (a través de comentarios sobre los contenidos de sus amigos, etiquetas en las fotos, etc.) para poder evitarlo.
- Concienciarles de que han de publicar contenidos sólo de su autoría, sin copiar contenidos de otros para colgarlos en su página. Además, antes de colgar fotos donde aparezcan otras personas, han de solicitar su permiso y, en caso de no obtenerlo, respetar su decisión.
- Está prohibido darse de alta suplantando la identidad de otra persona. Por ello, si alguien crea una cuenta haciéndose pasar

por ellos, es necesario que lo denuncien por las vías habilitadas para ello en las propias redes sociales y a los cuerpos y fuerzas de seguridad del Estado.

- Ayudarles a expresar sus emociones a través de la red y también a relativizarlos. Muchas veces los sentimientos aparecen magnificados en la redes y hay que aprender a situarlos y relativizarlos valorándolos en su justa medida.
- Concienciarles que es importante que contribuyan a un buen ambiente digital, respetando a los demás y a sí mismos.
- Pedirles que denuncien y nos comenten cualquier anormalidad o abuso que hayan visto en la red.

Es necesario hacerles comprender y ser conscientes de las posibles consecuencias de no protegerse con estas pautas.

Asimismo, es importante que sientan que ellos son los responsables de sus decisiones y conductas pero que, ante cualquier problema, pueden contar con nosotros si ocurre algo que consideren extraño o les haga sentir mal.

8. **Mantener una actitud positiva ante las redes sociales, conociendo sus ventajas y potenciándolas, controlando los riesgos y usándolas de forma positiva.**

   Conociendo y controlando los riesgos, usando las redes de forma positiva, y aprovechando sus ventajas, estas se convierten en un medio de comunicación y aprendizaje con un gran potencial que permiten estimular el desarrollo de habilidades, de la creatividad, de las relaciones sociales, del crecimiento personal, etc.

   Por ejemplo, las redes sociales son un instrumento que permite de forma ágil y fácil organizar eventos sociales, recaudar fondos para un proyecto, expresar diferentes opiniones, comentar la realidad social, comunicarse con un gran número de personas a la vez, realizar convocatorias públicas, etc.

9. **Ser conscientes y facilitar que las redes sociales no han de sustituir ningún otro aspecto de la vida social de nuestros hijos e hijas, si no que ha de complementarlo**.

   En ningún caso se deben convertir en la única forma de relacionarse con los iguales. Mantener unas buenas relaciones a través de las

redes ha de ser compatible con actividades tales como: salidas con los amigos, con la familia, hacer deporte, pasear, leer un libro, ver una película, salir al campo, etc. Desde CEAPA consideramos que es un elemento más para comunicarse, divertirse y relacionarse del que se puede disfrutar en su justa medida y que la clave es mantener el equilibrio entre todo ello.

Por último, me gustaría añadir que desde CEAPA consideramos que es necesario evitar algunos aspectos concretos que podrían suponer pasos hacia atrás en su proceso educativo:

1. **Demonizar las redes sociales**, culpándolas de la mayoría de los problemas de jóvenes y adolescentes. La red social es una herramienta que en sí misma no es ni beneficiosa ni perjudicial, todo dependerá del uso que le den nuestros hijos e hijas.

   Como en cualquier aspecto de la vida serán el abuso y la falta de una visión crítica los que puedan convertirla en un problema. Por el contrario, un uso adecuado puede facilitar y contribuir a su desarrollo. Si surge una complicación, debemos saber cuál es la causa, sin culpar a la herramienta, para poder encontrar la solución adecuada.

   Las redes sociales son un reflejo de la vida, en ellas podemos encontrar cosas buenas y malas. Debemos ver más allá del temor que conlleva todo lo nuevo.

2. **Espiar las páginas de las redes sociales de nuestros hijos e hija**s. Por ejemplo, entrando en ellas sin su permiso, dándonos de alta y haciéndonos pasar por sus amigos para controlarles, etc. Estas conductas supondrían una invasión de su intimidad, algo similar a leer su diario, que rompería su confianza, siendo muy difícil volverla a recuperar. El respeto a su intimidad y a su espacio privado es siempre fundamental y, aún más, en la adolescencia.

En resumen, desde CEAPA consideramos que las redes sociales en internet son un escenario más en el proceso educativo, por lo que nuestro papel como padres y madres ha de ser el mismo que en los demás temas educativos, es decir, seguir manteniendo el equilibrio entre ofrecer apoyo afectivo y establecer unos límites adecuados a través de una comunicación positiva.

Debemos recordar que somos su pilar de confianza y su principal referente, por lo que debemos ser modelos en aquello que queremos transmitir.

Así mismo, desde CEAPA consideramos que debemos educar a nuestros hijos e hijas en el uso responsable, seguro y adecuado de las redes sociales.

COMPARECENCIA DEL DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), D. JOSÉ LUIS RODRÍGUEZ ÁLVAREZ, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 10 DE OCTUBRE DE 2013.

El señor **DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)**: (D. José Luis Rodríguez Álvarez): Me limitaré a apuntar algunos elementos generales que me permitan contextualizar y centrar mi intervención.

En este sentido, querría comenzar recordando que dentro de la espectacular evolución que las nuevas tecnologías han experimentado en los últimos años, el desarrollo de Internet, la red de redes, es sin lugar a dudas uno de los fenómenos que más han transformado nuestra sociedad. La red ha creado un nuevo paradigma de comunicación y de tratamiento de la información, facilitando el intercambio y el desarrollo del conocimiento en unos términos que hasta ahora eran desconocidos en la historia de la humanidad. Y no necesito glosar sus enormes beneficios porque son bien conocidos, y todos en el día a día participamos de ellos.

Pero al mismo tiempo, Internet está planteando problemas de gran trascendencia para la protección de la vida privada; problemas cuyo alcance todavía no estamos en condiciones de evaluar plenamente. Porque vivimos por primera vez en la historia de la humanidad en un momento en el que el desarrollo de la memoria digital permite conservar todo tipo de informaciones con un coste muy reducido. Dándose incluso la paradoja de que a veces es más costoso borrar la información que conservarla.

Por otra parte, Internet permite conectar todas esas memorias digitales entre sí con independencia de cuál sea su ubicación geográfica, y permite transmitir y compartir la información en tiempo real. Y a ello hay que añadir la prodigiosa capacidad que tienen los motores de búsqueda para recopilar y para proporcionar acceso a la información en virtud de los criterios libremente elegidos por cada uno, criterios que pueden ser el nombre y apellidos para obtener información adicional sobre una personas, o que puede ser simplemente una fotografía para identificar a esa persona. Y claro, como consecuencia de ello Internet ha derrumbado ya

definitivamente dos barreras que hasta hace muy poco eran muy eficaces para la protección de la privacidad: la barrera del espacio y la barrera del tiempo. Hoy, con la suma de las memorias digitales que todo lo guardan, Internet que todo lo comunica, y los buscadores que todo lo encuentran, las informaciones personales, con independencia de que sean recientes o pertenezcan a un pasado lejano, están al alcance de cualquiera que solo tenga un dispositivo conectado a Internet, con esta única condición se pueden encontrar informaciones que antes había una dificultad, variable pero siempre una dificultad, de localizar si estaban situadas en un espacio lejano o si pertenecían al pasado. Estas dos barreras que han sido muy eficaces en la protección de la esfera privada, hoy han sido derrumbadas por la suma de memorias digitales, Internet y la actuación sobre ella de los buscadores.

Y esta difusión y esta accesibilidad universal de la información y de los datos personales en Internet generan, claro, nuevos riesgos y nuevas amenazas para la protección de la vida privada y de los derechos fundamentales. Riesgos y amenazas que alcanzan un mayor grado en el caso de los menores. Porque los menores además, según todos los estudios, hacen un uso cada vez más intensivo de Internet, un uso cada vez más intensivo de las redes sociales, de la mensajería instantánea y de las diversas aplicaciones que continuamente van surgiendo.

Las encuestas del Instituto Nacional de Estadística sobre equipamiento y uso de tecnologías de la información en los hogares españoles reflejan una continua expansión del uso de los ordenadores y de Internet por parte de los menores, que ya está casi a punto de convertirse en universal. De hecho, la encuesta de 2012 revela que el uso de ordenadores por menores de entre 10 y 15 años alcanza ya el 96%; y la utilización de Internet ha pasado del 97,1% en 2011 al 91,2% en 2012. Y a ello hay que añadir la incidencia que tienen los dispositivos portátiles, que están desplazando a los clásicos ordenadores personales fijos y sustituyéndolos por tabletas o por teléfonos inteligentes, que incluyen la posibilidad de acceder a una multitud de aplicaciones y de servicios avanzados fuera del hogar y fuera del entorno de protección, que también ha cumplido un papel importante en relación con los menores.

Y en este sentido, resultan significativos también los datos que aportan los estudios. Según el estudio realizado por INTECO y Orange en 2011, que probablemente conocerán, la edad media de inicio en telefonía

móvil estaba en 2011 (y digo «estaba» porque probablemente ya ha cambiado también) en 11,2 años; y el acceso a un *smartphone*, a un teléfono inteligente, se producía en la media de los 13 años en España.

Y es cierto que los menores tienen mayores capacidades técnicas para desenvolverse en este entorno digital, mayores capacidades técnicas que muchos adultos, sin duda, son nativos digitales. Pero no hay que olvidar que se trata de personas que están en proceso de formación; que por lo tanto no conocen plenamente el valor de la privacidad, el valor de los datos personales, la importancia que tiene proteger los datos de carácter personal. Y ello les lleva en muchos casos a un mayor grado de exposición, a hacer un uso más arriesgado o menos responsable de los datos personales. En parte también debido a que, según ponen de manifiesto los neuropsiquiatras, el cerebro de un adolescente valora de forma muy diferente los peligros que el de un adulto, y consecuentemente, los afronta también de una manera distinta de como los afronta un adulto.

Al mismo tiempo, la deficiente configuración de la privacidad en muchas ofertas y servicios que se hacen en la red, que además resultan sumamente atractivos, se presentan como muy atractivos para los menores, y la falsa sensación que tienen los menores de estar entre iguales en la red y de sentirse protegidos, les mueve a actuar con cierta despreocupación, facilitando la información y los datos personales que les hacen aún más vulnerables y más propensos a ser víctimas de conductas no deseadas, que incluso pueden ser constitutivas de delito. Sin desconocer tampoco los casos en los que son los propios menores los autores de conductas infractoras. Esta es otra perspectiva que no debemos perder de vista.

Y estos riesgos, lógicamente, están generando una creciente preocupación por la protección de los menores en Internet que está justificada a tenor no solo de nuestra experiencia cotidiana, sino también de los datos que arrojan los estudios. En la comunicación de la Comisión Europea de 2012 sobre una estrategia en favor de un Internet más adecuado para los niños, se señala que 4 de cada 10 menores europeos manifestaron haberse encontrado con algún riesgo en Internet, 4 de cada 10, como podía ser la comunicación con desconocidos, el uso indebido de datos personales, encuentros reales con personas conocidas en la red, o haber sido víctima del *cyberbullying* (nunca sé muy bien cómo decimos estas palabras, porque las medio castellanizamos, pero ni lo decimos en inglés ni en castellano).

Por mencionar solo otro estudio reciente que probablemente también conocen, hay un informe del Gobierno Vasco sobre maltrato en los colegios de 2012 que revela que 10 de cada 100 alumnos han sido acosados a través de las redes sociales; y en el 2% de los casos son casos graves. En este informe se pone de manifiesto que en primaria lo más habitual son los ataques a través de redes sociales, y en la ESO son más frecuentes los ataques basados en grabación y difusión de imágenes humillantes y comprometidas.

Y casi todos los días nos encontramos en los medios de comunicación con noticias relativas a las consecuencias de un uso inadecuado, un uso irresponsable o incluso malintencionado de las redes, que repercute sobre los menores.

Pero a pesar de la naturaleza de los riesgos, que no se deben minimizar, y la gravedad de algunos casos concretos, como hemos podido ver también los casos que han llegado a suicidio, a mi juicio no resulta procedente, no es conveniente ni oportuno criminalizar la tecnología ni criminalizar los avances sociales. Es necesario encontrar fórmulas para compatibilizar los grandes beneficios de estos avances tecnológicos con la protección de los derechos fundamentales de las personas en general y con la protección de los derechos de los menores en particular. Y este es el gran reto que tenemos planteado. Un reto que por su magnitud y por su complejidad ha de ser abordado desde diversas perspectivas y con la intervención de todos los implicados en la protección de menores, desde los poderes y las instituciones públicas hasta los educadores, padres, tutores; y buscando además, lo que considero muy importante, la participación activa de los propios menores implicándoles en este proceso.

Y en este sentido, considero muy acertada la constitución de esta ponencia de estudio, que permite analizar estas cuestiones desde múltiples perspectivas y formular propuestas teniendo en cuenta esta naturaleza poliédrica de los problemas.

La Agencia Española de Protección de Datos es muy sensible a toda esta problemática, y desde hace tiempo venimos desarrollando diversas actuaciones en el marco de nuestras competencias y dentro de nuestras modestas capacidades y recursos, que lo son. Como bien saben, la Agencia Española de Protección de Datos es un ente de derecho público con personalidad jurídica propia que actúa con independencia de las admi-

nistraciones públicas y que se rige por la Ley Orgánica de Protección de Datos, que le atribuye una serie de funciones que pueden resumirse en velar por el cumplimiento de la legislación de protección de datos y controlar su aplicación. Es decir, la agencia es una autoridad de supervisión y de control en materia de protección de datos; en materia del derecho fundamental de la protección de datos, porque no debemos perder de vista que estamos ante un derecho fundamental, que como saben, la normativa española en este ámbito está constituida básicamente por la Ley Orgánica de Protección de Datos del año 1999, y el reglamento de desarrollo aprobado en el año 2007. Ambas normas desarrollan las previsiones del artículo 18.4 de la Constitución y también incorporan a nuestro ordenamiento la Directiva 95/46, que es la que establece el marco normativo común armonizado en la Unión Europea, directiva que actualmente se encuentra además en un proceso de revisión tras la presentación el año pasado por parte de la Comisión de una propuesta para sustituirla por un reglamento general de protección de datos, y actualmente se encuentra en el trámite legislativo con la intervención de las tres instituciones en Europa.

Obviamente, menciono esta normativa porque tanto la ley como el reglamento se aplican íntegramente al tratamiento de los datos de menores. Pero el reglamento contiene una regulación específica en su artículo 13 que viene a concretar las previsiones generales de la ley en relación con los menores. Se aplica toda la ley, se aplica todo el reglamento, pero hay un artículo que es especialmente relevante, y por eso me voy a detener en él, que es el artículo 13 del reglamento, porque es donde se operan las concreciones en relación con los menores de algunas disposiciones generales. En este artículo, en primer lugar, por lo que se refiere a la prestación del consentimiento para el tratamiento de datos de menores, limita la capacidad de otorgarlo, de otorgar el consentimiento para el tratamiento de sus datos personales a los mayores de 14 años, disponiendo que en el caso de menores de 14 años, para tratar datos personales se requerirá el consentimiento de los padres o tutores.

En otros países la edad es algo inferior. Y de hecho —este es un aspecto que debemos tener en cuenta también—, en la propuesta de reglamento que actualmente se está tramitando en la Unión Europea, esta edad se fija en 13 años; pero en nuestro ordenamiento tenemos actualmente la edad en 14 años.

Además, el apartado 4 de este artículo 13 establece que el responsable del tratamiento, es decir, aquel que recaba y utiliza los datos, el que trata los datos deberá articular procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor, procedimientos que acrediten que se ha comprobado de modo efectivo la edad del menor, y la autenticidad del consentimiento prestado en el caso de que sean los padres o los tutores los que han prestado el consentimiento.

Por otra parte —sigo con el artículo 13 del reglamento—, se prohíbe expresamente recabar de los menores datos que permitan obtener información sobre sus familiares, ya sean características del grupo familiar, sea actividad profesional, información económica, datos sociológicos o cualquier otro, con la única excepción de los datos identificativos de los padres, con el fin de poder dirigirse a ellos en su caso y recabar el consentimiento cuando se trata de menores de 14 años. Pero nuestro ordenamiento prohíbe recabar datos de menores sobre el grupo familiar.

Por último, este mismo precepto, el artículo 13, concreta la obligación general de informar del tratamiento, que está establecida con carácter general en el artículo 5 de la Ley Orgánica de Protección de Datos, y establece que cuando la información esté dirigida a menores deberá expresarse en un lenguaje que sea fácilmente comprensible por ellos. Aquí hay una concreción específica del deber general, que siempre ha de informarse del tratamiento de los datos personales al titular, pero cuando sean menores, el lenguaje ha de estar adaptado a la condición de menores, y por lo tanto ha de hacerse en unos términos que sean fácilmente comprensibles por ellos.

Desde la entrada en vigor de estas disposiciones del reglamento, la agencia ha desarrollado toda una serie de iniciativas y de actuaciones encaminadas a asegurar su cumplimiento. Y en este sentido venimos haciendo requerimientos periódicos a los proveedores de las redes sociales y manteniendo reuniones frecuentes con ellos con la finalidad de conocer cuáles son las medidas que están adoptando para dar cumplimiento a las obligaciones que impone el artículo 13 del reglamento, en especial las dos que he mencionado: la de informar a los menores teniendo en cuenta su grado de madurez, y la de articular procedimientos que garanticen que se está comprobando la edad de los usuarios.

Por lo que respecta a los responsables de las redes sociales, que es donde más impacto tiene esta normativa, las actuaciones de la agencia

se están centrando principalmente en las dos empresas que gestionan las redes sociales más utilizadas por menores en España, que son Tuenti y Facebook. Y me complace decir que, aunque con distinto alcance, en los dos casos se han producido avances. Estos avances son particularmente relevantes en el caso de Tuenti, que como saben es una empresa española y está sometida, por tanto, plenamente a la supervisión de la agencia en materia de protección de datos.

En este caso, aparte de mantener la no indexación de los contenidos en los buscadores de Internet, lo cual ya proporciona de por sí un alto grado de protección de la información personal, incluso de los mensajes intercambiados, ha modificado recientemente sus políticas de privacidad para mejorar la información de modo que resulte más comprensible a los destinatarios, adultos y también especialmente cuando son menores. Y ha revisado las condiciones para permitir el alta en la red a menores de 14 años con la autorización de los padres, estableciendo un procedimiento específico para acreditar que se cuenta con el consentimiento de los padres cuando son menores de 14 años los que se dan de alta en la red.

Y un aspecto que considero muy relevante: ha establecido el máximo nivel de privacidad por defecto para sus usuarios, dando así aplicación al principio de privacidad desde el diseño y privacidad por defecto, que las autoridades de protección de datos venimos recomendando reiteradamente. Es decir, que cuando se entregue una aplicación venga configurada en los términos más respetuosos con la privacidad de los destinatarios, de tal manera que luego sean ellos los que puedan tomar decisiones conscientes y voluntarias sobre si quieren ampliar el acceso a la información a terceros, y a quiénes y con qué grado.

Este principio de privacidad por defecto debería ser una exigencia en relación con los menores. Y al menos hemos conseguido que la empresa española que se dedica a las redes sociales haya implantado —obviamente por decisión propia, pero en el marco de estas conversaciones, requerimientos, intercambio de información que mantenemos—, que haya dado este paso que considero muy importante.

Esta empresa ha implantado también un procedimiento interno para depuración de perfiles de menores de 14 años, que según la información que nos proporcionan, porque les pedimos regularmente informes sobre qué están realizando en este ámbito, les ha permitido en 2012 revisar 400.000 y borrar una media de 1.650 semanalmente, son datos propor-

cionados por la propia empresa, que no estamos en condiciones tampoco de constatar íntegramente.

Y también en Facebook, aunque con distinto alcance, dada también su naturaleza, se han introducido cambios recientemente que suponen un avance en relación con la protección de los menores. En primer lugar, en España, a requerimiento de la agencia, han elevado la edad de acceso de 13 a 14 años para adecuarla a la normativa española; y han arbitrado procedimientos técnicos que impiden a quienes se identifican como menores de 14 años crear una cuenta. Además, como complemento han establecido sistemas comunitarios para revisar la edad con posterioridad al registro mediante un canal de denuncias de falsificación de edad. Pero como fácilmente pueden apreciar, la principal dificultad práctica que tenemos en relación con el cumplimiento del artículo 13 estriba precisamente en la inexistencia de instrumentos eficaces para verificar la edad real de los menores cuando prestan el consentimiento y se dan de alta en un servicio en Internet, sea una red social u otro servicio en Internet. No disponemos hasta el momento de instrumentos que nos permitan constatar con fiabilidad cuál es la edad de los menores cuando solicitan el acceso a uno de estos servicios. Y está comprobado que muchos menores mienten sobre su edad para tener acceso a los servicios de Internet, especialmente en las redes sociales.

Este es un fenómeno que no es un fenómeno español ni mucho menos, sino un fenómeno que tiene carácter universal. Y el proceso que actualmente se está llevando a cabo en Estados Unidos de revisión de la ley de privacidad de menores, la COPPA, se ha presentado un estudio según el cual el 85% de los niños norteamericanos entre 10 y 12 años tiene perfil en Facebook, cuando la edad mínima para darse de alta en Estados Unidos es 13 años. Es decir, que este es un problema de calado que necesariamente hay que reflexionar sobre él, sobre la barrera de la edad y sobre la posibilidad de establecer mecanismos más fiables, más eficaces para verificar cuál es la edad de los menores cuando dan su consentimiento e intervienen en Internet.

En la agencia, como una posible vía de solución para paliar esta carencia, hemos propuesto al Gobierno que en el DNI de los menores se incorpore el certificado de autenticación, el DNI electrónico, que se incorpore el certificado de autenticación que hasta ahora solo se habilita junto con el de firma a partir de la mayoría de edad o en los casos de

emancipación, lógicamente. Y esta propuesta ha sido muy bien acogida y se están dando los pasos necesarios. Hay que modificar el real decreto que regula el DNI electrónico, y según nuestras informaciones podría estar concluido antes de finalizar este año. Con ello tendremos un instrumento más, pero esto no soluciona toda la problemática del control de la edad. Obviamente, para que esta medida acabe siendo eficaz va a ser necesario además el compromiso de la industria en su implementación, que se establezcan mecanismos para verificar la edad a través de este medio. Es decir, tendremos un instrumento, pero con esto no hemos conseguido... Es un gran avance, por eso lo hemos propuesto, pero hay que ser conscientes de las limitaciones que también comporta este medio, y que en cualquier caso va a ser necesaria la colaboración, el compromiso de la industria en su implementación.

En este sentido sí tenemos que congratularnos también de que Tuenti, que está siguiendo de cerca este proceso con la agencia, haya establecido ya un nuevo sistema de verificación online de la edad a través del documento nacional de identidad electrónico. Por lo tanto, es posible, y ya tenemos la constatación de que esto se puede hacer en una empresa española. La dificultad es trasladar esto a las empresas de actuación global.

Bueno, junto a estas acciones que están dirigidas específicamente a supervisar la actuación de los proveedores de Internet y a velar por el respeto de la regulación de protección de datos, la agencia realiza también otras muchas actuaciones encaminadas a favorecer el cumplimiento de la normativa en relación con menores, entre las que quiero destacar la emisión de informes, informes jurídicos, contestando a consultas formuladas por responsables de tratamiento, en las que hemos hecho diversos pronunciamientos sobre el régimen de protección de datos de los menores de edad, tanto en entorno clásico como en entorno de Internet, y precisando y aclarando el contenido de la normativa vigente.

Se han emitido, por destacar algunos, informe jurídicos sobre aspectos tales como el mayor rigor que exige la información que se ha de facilitar a los menores, la limitación de los datos que se puedan recabar de los menores, la libertad que tiene el responsable del tratamiento para establecer el procedimiento de verificación de la edad, siempre que permita demostrar un nivel adecuado de diligencia. En este punto quiero hacer un inciso, y es que siempre tenemos que ser conscientes de que la normativa de protección de datos ha de ser tecnológicamente neutral.

Por lo tanto, desde la agencia no podemos decir, para cumplir la obligación legal, que hay que utilizar esta tecnología; nosotros podemos, como hemos hecho con el DNI electrónico, impulsar una que puede ser útil, favorecerla, pero necesitamos actuar con neutralidad desde el punto de vista de la tecnología, para no incidir en las leyes de mercado. Es decir, la normativa y la actuación de las autoridades de protección de datos ha de ser neutral en cuanto a los desarrollos tecnológicos, para no frenar ni avanzar determinados desarrollos, aunque obviamente nosotros siempre vamos a favorecer y avalar en este sentido aquellos que hemos constatado que permiten cumplir con la normativa de protección de datos. Pero por eso en este informe, como en otras manifestaciones que se hacen públicamente por parte de responsables de la agencia, conmigo a la cabeza, pues a veces se considera que somos demasiado neutros, demasiado cautos, y es que estamos vinculados por esta obligación de neutralidad tecnológica, no podemos decantarnos claramente por una tecnología en perjuicio de otra.

Por otra parte, aunque la mayoría de los supuestos de vulneración de derechos de los menores por su gravedad son constitutivos de delito, y en consecuencia la investigación y la eventual sanción no corresponden a la agencia, cuando se produce una infracción de la normativa de la protección de datos que no revista esa naturaleza de delito, la agencia ejerce también plenamente sus potestades de investigación y de sanción. Y en este sentido son varios los casos de vulneración de derechos de protección de datos de los menores en Internet que han sido investigados con la agencia y que han concluido con una sanción. Insisto, nosotros actuamos en lo que no tiene naturaleza de delito; cuando hay un delito, como saben, son las Fuerzas y Cuerpos de Seguridad del Estado y la Fiscalía los que tienen la competencia.

Pero por mencionar algunos ejemplos, la agencia sancionó a una entidad que ofrecía un servicio para adultos cuyo mecanismo de control era únicamente la fecha de nacimiento, y no se habían realizado las mínimas comprobaciones lógicas sobre el funcionamiento real de ese mecanismo. Ello permitió que un menor introdujera su fecha de nacimiento real y el sistema lo consideró mayor de edad porque introdujo solo «95» en lugar de «1995» como año de nacimiento, y el sistema consideró que tenía 1.911 años en este caso. Obviamente, este es un error grave en la configuración de la programación, pero la responsabilidad está por parte de quien pone en funcionamiento estos servicios, de no aplicar la diligencia

debida en la comprobación del funcionamiento real de este mecanismo de control.

Igualmente la agencia sancionó a una entidad que ofrecía productos y servicios para menores, en este caso sin articular procedimientos que garantizasen adecuadamente que había comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado. Además, la cláusula que obraba en la página web, aparte de tener una redacción en unos términos excesivamente legalistas, pro forma, sin tener en cuenta que iba dirigida a los menores, le trasladaba al menor toda la responsabilidad de haber solicitado el consentimiento paterno y de aceptar la política de privacidad de la empresa. Les cito brevemente un pasaje como ejemplo de mala práctica, que en este caso además vulnera la normativa española de protección de datos. Decía la cláusula informativa de esta empresa en la web: «En el supuesto de que el titular de los datos fuera menor de 14 años en el momento de la entrega de sus datos, con la aceptación de esta política de protección de datos manifiesta que ha entregado sus datos con el previo consentimiento de sus padres o representantes legales, y que en cualquier caso ha cumplimentado los formularios accesibles desde la página web en su presencia y bajo su supervisión». Y desgraciadamente, todavía existen estos tipos de cláusulas informativas dirigidas a menores, que con independencia de que en este caso además vulnera la exigencia de acreditar el consentimiento, en la medida en que le traslada responsabilidad al menor, está redactada en unos términos que son ininteligibles —por eso lo quería traer aquí a colación— para los menores. Y en esto estamos también trabajando, muchas veces con apercibimientos, con relaciones directas con los proveedores, que muchas veces, afortunadamente, vienen a consultar también cuando ponen en marcha un servicio para que elaboren cláusulas que tengan en cuenta, aparte de cumplir con la normativa, a quién van dirigidas.

También se sancionó por parte de la agencia a un portal de Internet que estaba orientado a favorecer el contacto personal entre usuarios, fundamentalmente adolescentes o jóvenes, porque las medidas adoptadas para verificar que los usuarios eran mayores de 14 años no mostraban en modo alguno ser eficaces.

Hay supuestos también en los que no son compañías, sino que son particulares los que vulneran la normativa de protección de datos. Y de ello también tenemos casos tratados y resueltos por la agencia. Como

el caso de la publicación en Facebook, en abierto, y por tanto accesible libremente para cualquier usuario de dicha red social, de un vídeo en el que aparecían varios escolares menores de edad que estaban de visita en un zoológico, y además resultaban plenamente identificables. En este caso la denuncia fue del director del colegio en el que estudiaban esos menores, y que les había llevado al zoológico, y hemos procedido a sancionar a quien había publicado estas imágenes en Facebook.

Hemos sancionado también otro caso por la grabación con cámara oculta de imágenes de la madre y de dos hijos menores de edad a la salida de un colegio por parte de un miembro de una asociación de damnificados por decisiones judiciales.

Y en este apartado hay que incluir también los casos en los que los menores son autores de los hechos infractores. En estos casos también tenemos algún ejemplo tratado y analizado en la agencia, como la publicación en un perfil de Facebook, un perfil de un menor, de fotografías y de datos de profesores en los que además se vertían insultos y alusiones de contenido sexual. En este caso la problemática está en la responsabilidad; en este caso había sido una menor de 11 años, por lo que en la agencia hemos optado por apercibir al titular de la línea (no una sanción económica, sino un apercibimiento) desde la que se había creado ese perfil y desde el que se estaban actualizando los datos de los profesores.

Una problemática especial nos plantean los casos de las denuncias de padres separados por el tratamiento de las imágenes, los datos personales en general, pero especialmente las imágenes de sus hijos en las redes sociales. Y aquí inicialmente en la agencia hemos intentado proteger los derechos de los menores, el superior interés de los menores, y durante un tiempo exigíamos el consentimiento de ambos progenitores para la publicación en redes sociales de los datos personales (fundamentalmente, insisto, imágenes) de los menores. Pero en la práctica nos hemos encontrado con que las situaciones jurídicas son muy complejas, que nos obligaban en algunos casos a entrar a analizar cuestiones de derecho civil, para lo que no somos competentes, y ver cómo estaba articulada la patria potestad. En algunos casos existen incluso capitulaciones sobre cuál va a ser el tratamiento de las imágenes de los hijos en las redes sociales. Por lo tanto, a nuestro pesar hemos tenido que cambiar el criterio e inhibirnos en favor de los tribunales, por carecer de competencia para interpretar las cuestiones civiles que son necesarias para dilucidar estos

conflictos entre padres separados. Pero este es un fenómeno creciente al que hemos intentado dar una solución, pero hemos llegado al límite de nuestra competencia y no podemos seguir por ese camino.

Aparte de todas estas actuaciones, de velar por el cumplimiento y de supervisar la actuación de los proveedores de servicios en Internet, consideramos que para lograr un nivel adecuado de protección de datos personales de los menores son imprescindibles las actuaciones de concienciación, las actuaciones de sensibilización, entre las que tiene que ocupar un lugar muy destacado la formación.

Es necesario educar, concienciar a los menores proporcionándoles conocimientos y la sensibilidad suficiente acerca de la protección de los datos personales, tanto de los propios como de los ajenos; porque muchas veces ponemos mucho el acento en la protección de los propios y se deja en un segundo lugar la actuación que los menores llevan a cabo con datos ajenos.

Y esta concienciación, educación es fundamental para que se puedan encontrar mejores condiciones de decidir las distintas situaciones en las que van a verse situados, colocados, que información personal dan, a quién la dan y para qué fines la dan. Y ahí no basta con la acción de control, la acción represiva; es imprescindible una acción preventiva en el sentido más amplio. La educación y la concienciación es, a nuestro juicio, la vía más eficaz para conseguir que los menores puedan usar y puedan disfrutar de Internet evitando estas situaciones de riesgo en la medida de lo posible y sin incurrir ellos en conductos que puedan resultar lesivas para otros, sean esos otros menores o sean adultos.

Y en la agencia venimos trabajando desde hace tiempo en esta línea, aunque no es una competencia propia en el sentido de autoridad de control y autoridad de supervisión. Pero estamos potenciando, no solo en este campo sino en todo lo que tiene que ver con la protección de datos, las acciones de concienciación y de sensibilización, la actuación preventiva como vía más eficaz para crear un nivel más alto, más adecuado de protección. Porque cuando hay que intervenir inspeccionando y sancionando, se ha producido ya la lesión. Por lo tanto es la constatación de la vulneración del derecho, y en esa medida, aunque es imprescindible continuar ejercitando estas potestades, no deja de ser siempre la constatación de un fracaso de la sociedad, cuando tiene que intervenir la potestad sancionadora, la potestad represora.

Y esto, en el contexto de la protección de los datos de los menores tiene muchísima más importancia si cabe. Y ahí estamos trabajando desde hace tiempo en esta línea. En nuestra página web, si la visitan, verán que tenemos dentro del canal del ciudadano una sección de menores con diversos recursos y materiales para facilitar la labor tanto a los padres como a los educadores en este campo. Ahí tenemos varios materiales elaborados directamente por la propia agencia. Les he traído aquí, para que puedan ver, algunos ejemplares: las recomendaciones a usuarios de Internet, que tiene un capítulo, el capítulo decimotercero, que versa expresamente sobre el uso de Internet por menores. Hemos editado también una guía, *Navega seguro. Derechos de los niños y deberes de los padres*, que contiene toda una serie de consejos y de recomendaciones dirigidos tanto a los menores como a los padres. Y hemos publicado también una guía educativa —solo les traigo la portada porque esta no está en formato papel, es solo digital— que es una adaptación, se llama *Registrarse, entrar, darse de baja*, que es una adaptación de un material que originariamente fue elaborado por la Oficina del Comisionado de Protección de Datos de Irlanda, y hemos adaptado al castellano en un proyecto conjunto, con las entonces cuatro agencias de protección de datos (la vasca, la catalana, la madrileña y la agencia española); está también disponible e la página web. He traído solo estos ejemplares, que son de los últimos que quedan en papel, y les voy a dejar los materiales también. Todos ellos son accesibles en la página web, pero ahí están compilados estos que les acabo de entregar, por si les pueden ser de utilidad y que lo tenga a disposición la ponencia de estudio. En cualquier caso, cualquier otro material que necesiten también estamos dispuestos a facilitarlo. Aparte de estos materiales, que son materiales elaborados por la propia agencia, en algún caso en colaboración con otras agencias, también se puede acceder a otros materiales y contenidos que están editados por otras autoridades de protección de datos, por otras instituciones, también a textos y a enlaces que puedan ser de interés que se han ido incorporando a lo largo del tiempo y que están a disposición de todos los que tengan responsabilidades en la educación y la protección de los menores, o que simplemente estén interesados en estas cuestiones.

Pero habida cuenta de la importancia que le damos a la adecuación de los menores para la protección de su privacidad, hemos decidido dar un paso más para colaborar, para poder apoyar en este proceso, aunque la agencia por sus propios medios no puede trabajar directamente con

los menores, solo podemos apoyar a quienes pueden contribuir a formar a los menores en estos aspectos, que son básicamente educadores y padres o tutores. Y hemos decidido potenciar esta línea de actuación, como anuncié ya en mi comparecencia en la Comisión Constitucional del Congreso el año pasado. Y después de analizar las necesidades actuales y las distintas alternativas, hemos optado por crear un nuevo *site*, una página dedicada en exclusiva a la protección de datos y a la privacidad de los menores en Internet. Y hemos estado trabajando a lo largo de este año en el proyecto, en el diseño y en la elaboración de unos contenidos que abarquen los principales aspectos a tener en cuenta en el uso de Internet por los menores, como pueden ser la importancia de la privacidad y el valor de los datos personales, los distintos contextos en los que se recaban datos y se tratan datos de los menores, el uso responsable de las redes sociales, y el uso responsable también de la mensajería instantánea, la identidad digital y los problemas de suplantación que se pueden producir en la red, y las diversas situaciones de riesgo, como el *cyberbullying*, el *grooming*, el *sexting*. Lo estamos analizando siempre desde la perspectiva de la protección de datos, aunque en algunas ocasiones se amplía el enfoque a otras cuestiones conexas. Y en todo caso se proporciona un catálogo de buenas prácticas, de consejos, de recursos para desenvolverse y para salir de situaciones comprometidas. Es decir, en muchos casos se intenta buscar situaciones reales, invitar al menor a dar la respuesta de cuál es la mejor salida y que luego pueda comprobar si esa es o no la mejor reacción en ese contexto, es decir, que está siempre contextualizado.

Actualmente, como ya saben, está concluida la primera fase del proyecto, que será presentado públicamente en un acto que tendrá lugar el próximo día 24 de octubre en la sede de la agencia. Les hemos cursado invitación, no sé si ha llegado; para nosotros sería un honor, aunque ya me han dicho que tienen dificultades. En cualquier caso, les daremos traslado de todos los contenidos cuando estén definitivamente cerrados. Es un proyecto en el que hemos puesto mucho empeño, dentro —insisto— de nuestras limitadas capacidades y recursos, porque la función central de la agencia y donde se están destinando la mayoría de los recursos es a tutelar los derechos de los ciudadanos cuando hay una denuncia, o investigar y sancionar cuando hay indicios de infracción. Tengan en cuenta que nosotros estamos ahora mismo resolviendo más de 60 asuntos diarios, y este volumen de actividad nos impide dedicar, como a mí

me gustaría, más recursos a la actividad preventiva y a esta tarea de elaboración de materiales o a discutir con quiénes están directamente en este ámbito en contacto con los menores.

Pero hemos diseñado un proyecto que tiene una vocación integral, que es escalable (por lo tanto va a permitir incorporar después materiales o recursos que se vayan elaborando y que se pueda actualizar periódicamente). En esta primera fase que vamos a presentar el día 24 contamos con dos bloques que les puedo avanzar sumariamente.

El primero se articula en torno a un cómic, con unos personajes que se busca que sean representativos (aquí no están tampoco los profesores, pero también aparecen, porque aparece el tutor), viven en estos entornos y se enfrentan a distintas situaciones, y se analizan las reacciones adecuadas, las erróneas, las más aconsejables y las menos aconsejables. Estos son materiales que están destinados a educadores, pero para ser usados directamente con los alumnos, y eventualmente, los padres pueden también utilizar estos materiales, estos distintos cómics y situaciones, donde digo que se analizan un poco todas las situaciones, incluso las situaciones de riesgo, de una manera amena con sus hijos, para ir introduciéndoles en estos aspectos. Este cómic está dirigido a la franja de entre 10, 12, y 14 y 15 años, por tanto pretende abarcar tanto a los que se acaban de iniciar o se están iniciando en el uso de Internet y las nuevas tecnologías como los que ya tienen cierta experiencia y tienen un uso intensivo, pero que tienen ciertas carencias respecto de la conciencia sobre el uso de los datos personales.

El segundo bloque tiene un enfoque más didáctico. Está configurado por unidades didácticas, fichas dedicadas a temas específicos. Les traigo aquí por ejemplo la que está dedicada al correo electrónico, los chats y la mensajería instantánea, donde se relaciones, diría que de una manera mucho más sistemática para que los docentes lo puedan utilizar en su propia preparación, en su propia concienciación, y luego extraer de aquí y aplicar lo que consideren oportuno en las clases, los glosarios, la terminología, la legislación aplicable, las definiciones, y luego las situaciones problemáticas que se pueden dar y las recomendaciones para el uso de cada uno de estos servicios de Internet. Tenemos también uno dedicado a situaciones de riesgo con este planteamiento.

Entonces, son dos bloques de materiales complementarios pero que tienen una filosofía distinta. Y como les decía, este es un proyecto esca-

lable que, en la medida de nuestras posibilidades, intentaremos ir complementando.

Es importante que contamos para este proyecto con la colaboración del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado, del Ministerio de Educación, por lo que el material, todos estos materiales a partir del día 24 no estarán disponibles solo en la página web de la agencia, sino también en la plataforma del INTEF. Por lo tanto, serán fácilmente accesibles para toda la comunidad educativa. Confiamos en contribuir con él a fomentar la cultura de la protección de datos entre padres y educadores, y a través de ellos también a los menores.

Y hay otras muchas cuestiones que merecerían también ser tratadas, que si lo consideran oportuno podemos abordar ahora a continuación. Y yo termino aquí, para no abusar más del tiempo que me han concedido y de su paciencia, esta intervención inicial, no sin antes desearles mucho éxito en el cometido de esta ponencia, que como les decía, por su planteamiento me parece el lugar ideal para analizar esta problemática que es tan poliédrica (nosotros aquí la vemos desde una perspectiva, pero los padres la ven desde otra, los educadores la ven desde otra); las empresas, las industria que están proporcionando estos servicios tienen también mucho que decir, creo que aquí hace falta continuar en la senda de la asunción de un compromiso real, la protección de la privacidad de los menores por parte de quienes prestan estos servicios, no hacer solo un enfoque generalizado basado en un modelo de negocio, de objetivos económicos rápidos y sin atender a la protección de la privacidad y de los datos personales, máxime cuando se trata de menores. En todo caso, estaremos muy atentos a las conclusiones, y receptivos en la medida en la que nos puedan hacer proposiciones o las sugerencias que sean realizables por parte de la agencia.

Sin más, agradeciéndoles de nuevo la atención, estoy a su disposición para contestar a las cuestiones.

COMPARECENCIA DEL DIRECTOR DEL CENTRO DE SEGURIDAD TIC ESCOLAR (CTiC), Y DIRECTOR EN LA FUNDACIÓN UNIR (UNIVERSIDAD INTERNACIONAL DE LA RIOJA) DEL ÁREA DE SEGURIDAD EN INTERNET Y PROTECCIÓN DE MENORES, D. CARLOS REPRESA ESTRADA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 24 DE OCTUBRE DE 2013.

El señor **DIRECTOR DEL CENTRO DE SEGURIDAD TIC ESCOLAR (CTiC)** (D. Carlos Represa Estrada): Buenos días. Es un placer para mí estar aquí. Y a la vista de la información que me acabáis de dar sobre cómo se ha generado esta ponencia, yo creo que también es importante que haga un poquito de historia de cómo es este proyecto, por qué estoy aquí.

Como pone ahí en la presentación, de formación soy jurista, soy abogado; y yo trabajaba ya hace tiempo como consultor de protección de datos especializado en centros educativos. Desde el primer momento, cuando yo trabajaba a nivel escolar prestando servicios, empecé a detectar que había una necesidad bastante acuciante de afrontar la entrada de las nuevas tecnologías en los colegios desde una perspectiva distinta del mero cumplimiento legal de una norma, que tiene muchas bondades pero que también suponía inconvenientes burocráticos importantes para los colegios, sobre todo a la hora de su aplicación en un entorno que tiene una serie de características propias; así se lo transmití al director de la Agencia de Protección de Datos, Artemi Rallo, y a todos los responsables que tenían competencias en la materia. Y a partir de ahí empecé a desarrollar un proyecto basado fundamentalmente en la educación como eje de la seguridad en Internet.

Este proyecto en un principio, como se inició en un momento complicado, en un momento en que tampoco se sabía hasta dónde iba a llegar la inmersión de los menores (estamos hablando de hace tres, cuatro años) ni la velocidad que iba a adquirir el desarrollo de nuevas tecnologías, pues en un principio, como todos los proyectos innovadores, tuvo una recepción tibia, por decirlo de alguna manera. A la vez que se ponían en marcha multitud de planes directores de seguridad por organismos competentes basados en charlas y acciones de concienciación por voluntarios

(yo fui uno de ellos) y por Fuerzas y Cuerpos de Seguridad del Estado, que precisamente no han sido positivos, o desde el punto de vista de los colegios no han causado el efecto deseado porque las Fuerzas y Cuerpos de Seguridad del Estado son eso, fuerzas y cuerpos de seguridad, no son educadores, no son profesionales de la educación, y porque el concepto de seguridad en Internet en principio se asimiló a seguridad informática o a delitos, y no tiene nada que ver desde luego, desde nuestro punto de vista.

A partir de ahí desarrollé un proyecto que presenté a un diputado, a Conrado Escobar, quien a la vez inició la creación de esa subcomisión parlamentaria. Y luego, posteriormente, ese proyecto lo fui presentando en diferentes entidades y universidades que han ido recepcionando el proyecto, adecuándolo, y hemos ido desarrollando nuevas ideas. Y es un poco lo que hoy vengo a exponer. Por tanto, para centrarnos, yo en estos momentos, aparte de esa labor como director de un centro de seguridad escolar, soy coordinador de la Escuela de Seguridad en la Red de Castilla-La Mancha (es un proyecto oficial de la Consejería de Educación), y luego soy responsable desde hace poco tiempo (empecé como profesor, pero me he incorporado como responsable), dentro de la Fundación UNIR, de una gran área que se ha denominado Seguridad en Internet y Protección de Menores. Al tiempo, también me llamaron de la Asociación de Tasadores y Peritos Judiciales Informáticos, que es una asociación que agrupa a los grandes *hackers*, como se suele decir, o cerebros de la seguridad informática, para montar también una sección de menores ante el incremento brutal que estaba existiendo de delitos de menores, y ante la demanda creciente de peritos especializados en menores por parte de los juzgados. Digamos que es un poco la labor que yo estoy realizando a nivel profesional.

Como introducción, simplemente unas fichas. Igual estos datos ya han salido aquí, supongo que son datos oficiales, pero a mí siempre me gusta enfocarlos desde el punto de vista... Toda mi ponencia, toda mi experiencia nace del mundo de los colegios, del mundo educativo. Por tanto, seguramente no va a ser ni la misma que pueda tener Protégeles ni la que pueda tener Borja Adsuara ni la que puedan tener Sebastián Muriel o muchos de los comparecientes que hayan podido pasar por aquí, porque yo me baso en las necesidades de los profesores, en lo que ellos me piden y en lo que nosotros observamos que está pasando en los colegios. Por tanto, a lo mejor algún tipo de aseveración o de premisa que yo pueda

establecer es distinta, pero ya digo que es todo fundamentado en la experiencia que tenemos en los colegios.

Estas estadísticas nos sitúan en un escenario de inmersión temprana, cada vez más temprana, cada vez más acelerada, y que aunque aquí pone 8 años, ya sabéis que hay internautas que tienen 3, 4, 5 años, cada vez estamos más cerca de que el nativo digital se convierta precisamente en eso que decimos, en una persona que según nace ya está en la red.

La cátedra UNIR, hace poco ha hecho un estudio muy interesante —que, por cierto, voy a entregar también a la ponencia porque no sé si lo tenéis—, es un estudio muy reciente que establece un nuevo concepto de seguridad, que es el que nosotros veníamos proponiendo en el campo de los colegios, que tiene mucho más que ver con la relación educativa, las normas de comunicación, es decir, como educación en valores, educación para la vida. Supera el concepto tradicional de seguridad y lo sitúa en un entorno de formación de la personalidad del menor. Y coincide plenamente con las experiencias que nosotros teníamos en los entornos educativos, y en función de eso estamos redirigiendo o reconduciendo el proyecto dentro de la universidad.

Por tanto, para nosotros la seguridad en Internet es un concepto nuevo completamente distinto de la seguridad informática, que no tiene nada que ver con lo que se ha estado transmitiendo en esas charlas que nosotros decimos, y que para nosotros es educación para la vida, educación ética y en valores.

¿Qué hacen nuestros menores? Pues hace poco el secretario de Estado de Seguridad lo dijo (esto son datos que cada día se actualizan): el 15% de los menores europeos entre 9 y 16 años que utilizan Internet ha enviado fotos o vídeos a alguna persona que no conoce. Ayer salió una noticia en la prensa: han hecho un estudio muy segmentado en Inglaterra a 450 adolescentes y les han hecho unas preguntas muy concretas. El 15% de los 450 adolescentes ha reconocido que ha hecho *sexting*, que ha enviado fotos comprometidas. Es un porcentaje brutal, o sea, las mismas personas que han hecho el estudio, que lo hicieron diciendo a ver qué está pasando realmente en un entorno socioeconómico medio algo, con gente que tiene *smartphone*, y la verdad es que la estadística es impresionante; está anticuada, pero está anticuada porque esta estadística es de hace tres meses, aquí todo lo que tenga más de tres o cuatro meses se nos queda obsoleto, porque todo lo que nosotros digamos ahora mismo,

todo lo que yo pueda decir a nivel de educación y de previsión en los colegios, tengan ustedes en cuenta que en dos meses se va a quedar obsoleto porque en dos meses el WhatsApp va a incorporar un sistema de edición de vídeo instantáneo. Lo que para la tecnología, lo que para los medios, lo que para los usuarios puede suponer un avance y puede ser muy importante, para mí va a suponer miles y miles de niños haciendo grabaciones de vídeo y compartiéndolas en WhatsApp o en Twitter en instantes, en segundos.

Para unos señores que son profesores, y que si prospera la enmienda transaccionada entre UPyD y el PP, van a ser autoridad pública por ley orgánica; es decir, hacer un vídeo y subirlo a Twitter de un señor que está dando clase es como si se hiciera de un policía en el desarrollo de sus funciones. Es muy grave, lo que pasa es que los menores no lo saben, no lo conocen, para ellos es algo natural, para ellos un juego, es la dignificación; para nosotros supone un reto, y supone un reto de educación. Eso no hay manera de pararlo. O sea, el que WhatsApp vaya a poner un editor de vídeo o que a WhatsApp se le considera a día de hoy un sistema de mensajería instantánea cuando no lo es a efectos de leyes, de utilización y de responsabilidad de los padres y de los menores, es un sistema que se puede comparar perfectamente a cualquier red social, porque para nosotros las herramientas en los entornos escolares no son herramientas sino que son funcionalidades. Un WhatsApp tiene funcionalidad de envío de paquetes de datos, de envío de imágenes, de envío de audio, y de envío de vídeo, por tanto es lo mismo que una red social, debería estar prohibido su acceso a menores de 14 años.

¿Qué hace el usuario medio español? Pues darle un WhatsApp con el teléfono, con el *smartphone*, al hijo de 14 años. ¿Quién es el responsable de la utilización del WhatsApp? El padre, porque el contrato está a nombre del titular de la línea, que tiene que tener 18 años. ¿Qué nos ha supuesto? Pues nos ha supuesto ya tener que aconsejar que se denuncie al padre en casos de *sexting* o de acoso en menores de 11 y 12 años, porque como no son responsables, hay que denunciar al padre. Es una situación complicada. Pero es una situación complicada, no por seguridad informática, sino por conocimiento social y por uso de las funcionalidades de este tipo de herramientas.

¿Qué pasará cuando lleguen las *Google glass*? Pues no lo sé, porque igual que las *Google glass* están ahí, ya hay gafas que son utilizadas por

los menores y que vienen graduadas. A ver a qué menor se le prohíbe utilizar unas gafas graduadas porque lleve una cámara al colegio. ¿Se va a poder prohibir, no se va a poder prohibir? A mí me da igual, el chisme me da igual. Si la gafa lleva incorporada una cámara, es una funcionalidad de recogida de imágenes personales regulada por la Ley Orgánica de Protección de Datos, y por lo tanto yo en un colegio lo puedo regular, puedo hacer que el niño esté educado y puedo controlar esa utilización; siempre y cuando la comunidad educativa se dé cuenta (que es una de las cosas que vamos a ver) de que el plan de convivencia se convierte en una herramienta fundamental para controlar y para educar, cosa que hasta ahora solo se ha hecho en la Consejería de Educación.

Todo esto que estoy diciendo está en la presentación que les voy a dejar a ustedes, pero voy dando pinceladas.

¿Qué se ha hecho hasta ahora? Pues hemos hecho mucho hincapié en realizar, en instalar controles parentales (el control parental es una herramienta de uso muy limitado). Si quieren, como este ordenador tiene conexión, luego puedo hacerles un pequeño taller de lo que es el control parental de Google para que vean ustedes cómo me lo salto y cómo entro en páginas de pornografía infantil y pederastia con el control parental activado, simplemente porque me lo han enseñado los niños, a mí, muchas de las cosas que he aprendido, me las enseñan los niños, cómo quitan el Canguro Net y cómo lo ponen, cómo se saltan los controles parentales o cómo utilizan los traductores para ir a páginas de pornografía cuando sus padres no les dejan y les ponen controles parentales; porque un traductor es una herramienta que por uso escolar el padre autoriza, y a través del traductor tú te puedes ir a cualquier página de pornografía china, por ejemplo. Entonces, al final la conclusión es que las prohibiciones limitan el uso de la red y limitan también las posibilidades de aprendizaje.

Esto es un poco lo que hemos hecho, y ahí me incluyo: yo también he dado muchas charlas de concienciación, he formado a policías. Pero, claro, cuando a un policía tú le preguntas en un entorno escolar, el profesor, oiga, ¿yo cómo tengo que hacer un blog educativo? Claro, se le van a poner las orejas a echar humo: ¡y yo qué sé! Pues es fundamental, esencial, que un profesor domine lo que es un blog como herramienta de comunicación, de información, qué derechos de propiedad intelectual se pueden ver afectados si yo subo un contenido de un menor, si comparto un contenido de un maestro, si cojo contenido de Internet y lo pongo.

¿Qué pasa con un blog si yo, aparte de la información mía, subo fotos de los profesores, subo fotos de los alumnos? ¿Quién tiene que tomar esa decisión?

Son tantas las interrogantes que se abren dentro del uso de las nuevas tecnologías que no son responsabilidad ni competencia de las fuerzas de seguridad y que son la base de la seguridad en Internet, que lógicamente estas acciones al final han ido decayendo. Y además crean un problema de percepción. Hay muchos colegios a los que nosotros vamos y nos dicen «si este colegio está seguro, ya vino el año pasado a dar una charla un voluntario». Y a veces he sido yo el que fue a dar la charla, hacía dos años y a 20 padres. Y ya con eso, el colegio piensa que está seguro.

Esto es lo que se ha hecho. Yo ni lo critico ni lo dejo de criticar, simplemente digo lo que es. ¿Es suficiente? Pues esto son estadísticas, que son absolutamente preocupantes. El diagrama es de la Guardia Civil, esto es de la Policía Nacional, los incrementos son tremendos. Y luego, nuestro famoso juez Calatayud, que ha estado un poco desaparecido por una enfermedad grave de su mujer, pero cada vez que aparece deja perlas como estas, esto es de hace dos días: «Este asunto nos tiene desbordados. El número de denuncias es mínimo respecto a lo que hay: los malos tratos, las vejaciones, el acoso a través de los móviles y las redes sociales va a más». Estamos metiéndonos ya en campos de permeabilidad de los problemas de los menores a malos tratos y a violencia de género. Antes de ayer salía un artículo muy interesante (esto es precisamente un extracto de ese artículo) que hace ya un análisis de los nuevos hábitos entre los adolescentes, como entregar tu clave de WhatsApp o de tu red social como prueba de amor, como prueba de fidelidad, dejar acceder a información que cada uno tiene en su *smartphone*. Y claro, cuando tú entregas tu clave de usuario, si a mí mañana cualquiera de ustedes me deja, o se descuida y accedo a su clave de usuario, puedo ser su pesadilla el resto de sus vidas, así de claro. Y no yo, compañeros de la asociación de peritos. Entonces, dar una clave de usuario y contraseña a un novio, por ejemplo, es absolutamente disparatado. Pues es un hábito que se está extendiendo entre los menores. Lo que dice el juez Calatayud con ese lenguaje que tiene directo, a veces puede chocar. Dice: «Nuestros chicos están llegando al autismo, ya no hablan, chatean. Y los padres no son conscientes, pero son responsables y a veces lo pagan». Ahí pone 5.000 y 10.000; hay padres ya a los que les han metido 30.000 y 50.000 euros,

en función del daño moral que han causado sus hijos de 11 y 12 años en Tuenti, por ejemplo. Pongo el ejemplo de Tuenti porque ya saben ustedes que es la red social que más colabora y que más ayuda a resolver sus casos. Porque lo de Twitter y Facebook... No sé si ustedes han tenido aquí la presencia de Marcelino Madrigal, ¿no ha venido aquí? En el Congreso está. Yo podría enseñarles. Marcelino denuncia 300 perfiles de pederastia todos los días en Twitter, perfiles que a lo mejor, después de múltiples denuncias, los cancelan y al día siguiente los vuelven a abrir, no hay ningún compromiso de comunicación ni obligación de Twitter de colaborar con las Fuerzas de Seguridad del Estado, con lo cual la pornografía y la pederastia que hay en Twitter es absolutamente intolerable, detrás de cada foto. Ayer subió Marcelino —y le dije: «bórralo y súbelo», porque él ya ha tenido varios toques de atención, incluso tenemos enfrentamientos a veces con las fuerzas de seguridad, más que nada porque no podemos hacer otra cosa que denunciar, no tenemos medios— una foto de una niña amordazada, atada, desnuda, en un perfil de Twitter, de estos que hay miles y miles y miles; y ahí está. Y mañana estará; hoy estaba todavía. Es algo tremendo.

¿Ahora qué nos preocupa? Nos preocupa muchísimo el cambio de política de publicidad de Facebook. Las noticias que salen a veces en los medios de comunicación, la gente lo ve y lo lee de una manera. Claro, nosotros cada vez que lo leemos tenemos que llevarlo al mundo del niño y al mundo del colegio. El que Facebook cambie la política de privacidad y abra el compartir contenidos a los menores, bueno, puede parecer bien o mal, pero al día siguiente sacan otra noticia y dicen: y ahora ponen el botón de *follower* y van a hacer un sistema similar a Twitter. ¿Por qué ha hecho eso Facebook? Porque Twitter le está comiendo el mercado de los menores, porque el menor busca la inmediatez, busca la satisfacción inmediata de la necesidad que tiene de comunicación, y en eso Twitter y WhatsApp se llevan la palma. Ahora Facebook, primero cambia la política de privacidad; segundo, abre el botón para hacer un sistema similar al *timeline* de Twitter. ¿Consecuencia? Pues si en Facebook había menos (que hay mucha pornografía infantil, mucha pederastia), ahora mismo va a abrir. ¿Por qué? ¿Qué sistema de denuncia tienen Facebook y Twitter ante la laxitud de las normas europeas? Quiera Dios que la iniciativa que ha prosperado antes de ayer, ha sido cuando se ha aprobado el nuevo proyecto de reglamento y cuando vaya al Parlamento Europeo, al final los Estados Unidos nos dejen conseguir un reglamento de protección de

datos adecuado. ¿Qué ocurre? Que Facebook tiene un sistema de denuncias basado en la subcontrata de una empresa que está en Marruecos y le pagan un euro por denuncia; cada vez que nosotros denunciamos un perfil, pagan un euro y lo borran. Pero es que con borrar un perfil de pornografía no se consigue nada, no hacemos nada. Lo que sería es detectar quién es la dirección, el titular de esa cuenta y perseguirlo, porque detrás de cada fotografía que sale en esos perfiles hay un niño abusado. Y es terrible, es un problema. Eso, el día que yo hago la clase de *sexting* y de pederastia, aviso a los profesores que se van a ver escenas que hieren la sensibilidad del docente, porque son terribles, es una cosa terrorífica. Y eso, todos los que estamos en Twitter lo tenemos al lado, por un lado y por otro, y nuestros niños también, y nuestros menores también.

Esto es Pantallas Amigas, no sé si ha estado aquí Jorge Flores; Jorge el otro día se pasó un poquito de frenada, pero bueno, estamos ya un poquito quemados también, esto lo dijo Jorge: «Estamos desprotegidos por el aumento bestial de casos entre menores». Y Jorge no es precisamente una persona que no conozca toda esta problemática. Digo que se pasó porque dijo «Las Fuerzas y Cuerpos de Seguridad del Estado tienen unidades especiales pero no dan abasto». Eso es verdad. Ellos dicen que no, pero es verdad, no dan abasto. Porque no tienen mecanismos y no tienen medios. Y porque además las fuerzas de seguridad intervienen cuando se denuncia, si no, no.

También tenemos problemas a veces de comprensión de lo que nos ocurre con los jueces porque no comprenden, no conocen, y porque hacen una aplicación estricta del Código Penal. Entonces, el artículo 401 del Código Penal, de usurpación de personalidad civil, aplicarlo para la suplantación de identidad digital, es algo absolutamente increíble. No sé si saben ustedes que los jueces solo solicitan la identificación de la dirección IP cuando el delito es un delito que se considera grave, es decir, que está penado con más de cinco años de cárcel; por debajo de cinco años de cárcel no solicita el juez la identificación de la dirección IP, con lo cual todo este tipo de acciones y delitos menores que afectan a pederastia y pornografía no los podemos perseguir porque no vamos a poder identificar la dirección IP. Si por un lado no tenemos colaboración del operador... Ahora mismo solo tenemos colaboración de Tuenti, total; de Twitter, cero; de Facebook, cero; y de Ask.fm, que es una red social peligrosísima, que es la que motivó que James Cameron dijera que iba a prohibir el acceso a pornografía por defecto a raíz de varios suicidios

que hubo en Inglaterra, es una red social letona que tiene ya más de 20 millones de usuarios, en España puede tener perfectamente un millón de usuarios, casi todos adolescentes, sin ningún tipo de medida de privacidad, de seguridad, de botón de denuncia, nada de nada de nada, y estamos indefensos, porque es una red social de contactos de pederastas y pornógrafos. Entonces, hay una total impunidad en las redes sociales legales, no impunidad para ellos, falta de responsabilidad y, por tanto, en el campo de la pederastia y la pornografía infantil, hay una total impunidad de los delincuentes en estos campos.

Volvamos a la parte mía, me he pasado de frenada porque la pederastia y la pornografía es uno de mis problemas, uno de los muchos.

Y aparte de esto, nosotros, como proponemos adquisición de habilidades, ¿qué hemos hecho? Pues lo primero —es lo que os decía—, presenté ese proyecto en el Congreso, y a través de eso la subcomisión, que luego amplió muchos objetivos, yo siempre me centraba en menores, desarrolló esta iniciativa mucho más amplia, pero que evidentemente está realizando un trabajo paralelo al que hacen ustedes en el Senado. Y luego, a partir de aquí yo lo empecé a presentar a organismos oficiales, colegios, y la situación de este proyecto educativo es la siguiente.

Por un lado, la Consejería de Educación de Castilla-La Mancha, que aceptó desarrollar la Escuela de Seguridad en la Red, que está en marcha, está funcionando. Pero era un proyecto de consejería, segmentado, y que tiene una gran paradoja y una gran virtud. Es un proyecto que se basa en la tecnología, a la vez. Y la Consejería de Educación desarrolló un centro de formación del profesorado basado en tecnología punta de Internet, lo mismo que ha hecho UNIR, pero esa tecnología punta desarrollada en el centro de formación, todavía está pendiente de desarrollar en otras consejerías, patronales, asociaciones. Diríamos que estamos hablando (Castilla-La Mancha tiene mil y pico colegios de los 20.000 o 22.000 colegios de España) de que ahora mismo se pueden beneficiar de ese centro de formación los mil y pico de Castilla-La Mancha. La universidad dijo: este proyecto no solo debe ser para una consejería, tiene que estar al alcance de cualquier colegio, y no solo de España, de cualquier lugar del mundo. Y aparte, la Universidad de Castilla-La Mancha, dentro del proyecto de la Consejería de Educación lo está metiendo en la formación de los futuros profesores, que es una pata fundamental, que el profesor que salga de la universidad ya salga preparado para enseñar seguridad a los niños, el objetivo final es el niño, lógicamente.

Y por último, la relación con el mundo de la seguridad informática, de la alta seguridad informática, que la tengo a través de la sección de menores de la Asociación de Tasadores y Peritos Judiciales.

¿En qué se basa nuestro proyecto educativo? En tres grandes iniciativas. Una es la escuela de privacidad y seguridad: ampliamos, por supuesto, el concepto a privacidad; no nos gusta nada el nombre de «seguridad», porque distorsiona, para nosotros el concepto de seguridad siempre nos lleva a seguridad informática y no lo es, pero hay que hacerlo; escuela de privacidad y seguridad en Internet para centros educativos.

Automáticamente empezamos en la universidad a hacer un curso, que estamos ya por la segunda edición, formando ya futuros directores de seguridad de centros educativos. No sé si saben ustedes que el nuevo reglamento trae la figura del DPO, el *data privacy officer*, como responsable de seguridad de las empresas; y nosotros dijimos: si un responsable de seguridad es importante en una empresa, ¿qué importancia va a tener en un colegio? Cuarenta veces mayor. ¿Qué vale más, un euro o un niño? Mil veces más un niño.

Y por supuesto —Raquel, por cierto, es la responsable— estamos ya creando el primer máster internacional que junte el ámbito jurídico con el ámbito de la seguridad informática para crear esos expertos en la seguridad en la red. Diríamos que son tres escalones de un mismo proyecto que empieza por los niños, que está arriba; el siguiente va a los directores, a los responsables educativos; y el más alto, todos aquellos que quieran dar ya un paso adelante en el concepto nuevo que proponemos de seguridad en Internet. No me he olvidado de las familias, que van en la escuela de seguridad en la red.

Este es el proyecto de la escuela de seguridad en la red de Castilla-La Mancha. Ahora mismo es un proyecto para ese colectivo. Esos son los alumnos, docentes, 1.700 centros educativos (en realidad son 1.200 o 1.300), pero que tiene una pata muy, muy importante, que es lo que decíamos al principio: el nuevo modelo de plan de convivencia; la escuela de seguridad, que es la parte más educativa; y luego, por último, creamos también, que eso viene de mi labor profesional, un centro de asistencia.

¿Por qué? Porque el profesor, ante la nueva adquisición de conocimientos, tiene dudas. Pero ya no solo que tenga dudas respecto de esos conocimientos nuevos que adquiere. Es que en esas dudas siempre va a

tener necesidades de asistencia por las novedades que se van ocurriendo. Yo a un profesor le puedo resolver los problemas a día de hoy, pero como mañana va a tener nuevos problemas (con el Google Glass, con el iWatch, con cualquier tipo de nueva tecnología que funcione a través de Internet), tengo que ser capaz de darle respuesta. Y no es lo mismo tener un acoso o tener un *bullying* en la red social Tuenti, que tiene veinte y tantas personas a disposición del colegio para solucionárselo, y aquí en el edificio de Telefónica en la Gran Vía, que tener un acoso, como tenemos miles de acosos en WhatsApp, que lo único que tiene es un FAQ, un nexo de preguntas, no hay nadie aquí en España, no tienen representante, y verdes las han segado y apáñate porque yo estoy en Estados Unidos y no quiero saber nada de si tus niños están pegando o están acosando o están difundiendo fotografías. Con lo cual, también entendimos que era necesario dar esa asistencia al profesor.

¿Cómo estamos haciendo el plan de convivencia? Pues con un equipo de trabajo colaborativo. Todos los representantes de la comunidad educativa (inspectores, directores) de la Consejería de Educación estamos desarrollando un nuevo modelo de plan de convivencia que tenga unas políticas o guías adonde el profesor pueda acudir en cualquier momento como herramienta de consulta, pero, lo más importante, que tenga unos protocolos claros de actuación docente. Es decir, que cuando yo tengo un caso de *cyberbullying*, si ya soy autoridad, tenga la capacidad para resolver ese conflicto. Y no hablo sólo de *cyberbullying*, último caso que tuvimos ayer: a un profesor le han suplantado la identidad en Twitter y están utilizando sus fotos y toda la información que le han sacado para acosar a alumnas, mandarles fotografías pornográficas y realizar comentarios obscenos del profesor con sus alumnas. Entonces, él lo primero que hizo cuando llamó a la policía fue: venga usted, denuncie y denuncie a Twitter. Nosotros le dijimos: No se te ocurra hacer eso porque te metes en un lío. Cuando vayas a la policía, abre un expediente, que el director del colegio firme todo lo que tú hagas, vamos a imprimir el timeline, vamos a analizar todo lo que está pasando, vamos a descubrir qué alumno (que es un alumno, que eso lo descubrimos siempre) está detrás de este acoso, y cuando lo tengas ya con la firma del director y un protocolo y un expediente, te vas a la policía, porque así no te lo van a archivar. Si tú vas ahora a la policía, el juez te lo va a archivar, precisamente porque no va a poder aplicar el 401 del Código Penal. Pero cuando tú presentas un documento firmado por el director como autoridad pública, tiene un

valor de prueba *iuris tantum*, con lo cual tiene la misma validez que la de un policía, a no ser que alguien desvirtúe esa prueba.

Entonces, a partir de ahí lo que hicimos fue trabajar en esta línea, crear esos protocolos. Y además ese protocolo permite dar respuesta a cualquier cosa, porque como el protocolo se mete en el plan de convivencia, hoy empiezo regulando (o regulaba, ya en la prehistoria) el teléfono móvil, y ahora el teléfono móvil me da igual, regulo sus usos, regulo la mensajería, regulo la red social, regulo mañana las Google Glass y lo que haga falta. Yo regulo conductas, regulo usos, que es lo que regula el reglamento de régimen interno y el plan de convivencia, no regulo chismes, no regulo máquinas, a mí la máquina me da igual. Tenemos muchos colegios que nos llaman porque les han dado a los niños tabletas, y lo primero que hacen los niños con la tableta que le dan es «a ver cómo funciona»; y están haciendo que funcione y ya han activado la doble cámara, sobre todo si es un iPad, y al tiempo que están diciendo cómo funciona está subiendo fotografías del profesor que les ha dado la tableta a Twitter. Y eso lo hemos visto en tiempo real desde una sala de dirección de un colegio, cómo lo hacían. Me da igual, eso es normal. Su curiosidad, el jugar, el intentar, el investigar les va a llevar a eso. Lo importante no es que lo hagan, lo importante es que sepan las consecuencias de ese acto y qué pasa si ellos en esa actuación cometen algún tipo de problema. Como no se les enseña, lo hacen pensando que es un juego. Cuando llegas y les aplicas la sanción se provoca un conflicto mucho mayor, y termina el padre, como ha pasado, denunciando al colegio a la Agencia Española de Protección de Datos por acceder al contenido de un teléfono. Por cierto, yo respeto la sentencia de la audiencia, pero entiendo que el Tribunal Supremo se la va a cargar, porque si la policía no puede acceder a un teléfono móvil, pues no sé cómo un director de un colegio puede acceder a un teléfono móvil. Nosotros seguimos recomendando que por favor cojan la firma del padre para acceder al contenido de un teléfono móvil, que lo hemos recomendado siempre, porque yo creo que ahí ha sido muy arriesgada la sentencia de la audiencia, y entendemos que el Tribunal Supremo se la va a cargar, no va a crear jurisprudencia.

Luego, en la escuela de seguridad, lo que hemos hecho ha sido dividirlo en tres grandes áreas. Y por supuesto, en primaria el objetivo es empezar a enseñar a los niños desde que tengan 5 años. Yo hago pruebas en educación infantil con mi mujer, que es maestra de educación infantil. Los resultados son muy bonitos. Por ahora nos vamos a conformar con

que sus profesores enseñen a los niños en las aulas, empiecen en conceptos básicos de seguridad, de privacidad, sobre todo de lo que nosotros llamamos de puesta en valor de su información, que un niño, desde que empieza a manejar la red, tenga conocimientos de lo importante que es la información que él va a poner, de su imagen, de su identidad, de sus textos, de sus fotos, de su familia, de su entorno, de su colegio y de su profesor. Ese es el objetivo. Y eso, el único que lo puede hacer, por supuesto, es el maestro.

No nos olvidamos; realmente el objetivo este, como ahora mismo no es materia curricular, lo que estamos haciendo es meterlo a través del plan de acción tutorial, que es una herramienta flexible que tienen los jefes de estudio para meter contenidos en las aulas con esos profesores. Diríamos que la estructura es: que tenemos a los profesores en la plataforma permanente de formación y tenemos a los jefes de estudio ya más avanzados introduciendo contenidos en las aulas a través del plan de acción tutorial.

Y por supuesto, la asignatura pendiente, que son los padres. Nosotros, al meterlo en itinerario en aula estamos teniendo buenos resultados; tenemos el privilegio de haber llenado dos veces un salón de actos, cosa que no se había conseguido nunca, normalmente van 20 padres; ahora ya parece que el tema está cambiando. Estamos haciendo talleres de navegación en Tuenti, en redes sociales con padres llenando aulas. Parece que el tema va cambiando, pero, bueno...

Y una herramienta, por supuesto: el aula virtual, que es lo que utilizamos en la universidad y es una herramienta mágica de formación porque nos permite calendarizar la formación, establecer un calendario de formación, y si un profesor quiere hacer un curso avanzado de *cyberbullying* o de prevención del *grooming* en las aulas, lo puede hacer adaptándose a sus necesidades y a sus posibilidades de horario, y sin límites de espacio-tiempo. O sea, cualquier profesor puede recibir la formación que quiera, y ya no estoy hablando solo sobre *cyberbullying*, puede recibir formación en LOPD o en cómo utilizar las herramientas de comunicación del colegio. Tenemos cientos de preguntas de si pueden utilizar Google Drive, Gmail, porque los profesores tienden mucho a decir a los niños de 11 años «abriros una cuenta de Gmail». Gmail es una herramienta de comunicación que exige la cesión de datos personales y está prohibido por la Ley de Protección de Datos. O sea, que los mismos

profesores, por desconocimiento o falta de asistencia, ya te meten a los niños y a los padres en dinámicas de incumplimiento legal. Pero no porque ellos lo quieran hacer, porque si tú a un profesor le dices «no, si creas un Google, tiene que ser en el Google Drive, en plataforma segura, sin publicidad, y que el padre sea el titular, o bien una plataforma educativa que tiene sus sistemas de correo internos y seguros», el resultado es el mismo; la funcionalidad es la misma, pero un niño de 11 años no puede tener una cuenta en Gmail, porque lo prohíbe la normativa europea, así de claro. No quiere decir que no la puede usar. Yo no quiero decir que un niño no pueda utilizar una red social con 11 años, todo lo contrario, si la utiliza con 11 años con seguridad, pues qué bien. Pero diríamos, que la edad de entrada en este tipo de herramienta es la edad de maduración, de conocimiento, los 14 años. En eso, nuestra apuesta es siempre el uso positivo, nunca la prohibición. Entonces, ese tipo de problemas se lo tienes que resolver, y el profesor lo tiene que tener también a su disposición. Si yo quiero conocimientos, por ejemplo, de la Ley de Servicios de la Sociedad de la Información, que es la que regula el uso de las *webs*, lo tengo que tener. Yo no puedo mandar a un niño un trabajo de búsqueda de información en Internet sin previamente haber visitado las páginas a las que les voy a mandar. Es lo que se llama —no sé si lo conocen ustedes— la metodología Web-Quest en educación: primero visito, analizo, y en función de esa visita y ese análisis es como mando los trabajos a mi alumno, porque a la vez me sirve para irle enseñando cuáles son las reglas. Yo ahora, en mi ordenador les podría enseñar una que es mía (tengo dos mías); yo llevo dos páginas falsas de Tuenti idénticas a Tuenti, hechas por nosotros, que utilizamos en talleres para los niños, les metemos, ellos ponen su contraseña y cuando le dan a «Intro» les mandamos a la buena y les robamos la contraseña. Entonces, de esas hay cientos de miles, páginas web falsas (*fake*), de bancos, de redes sociales, que evidentemente es lo que más nos preocupa a nosotros. Entonces, llevamos herramientas para que ellos se den cuenta: anda, ¿qué has hecho? ¿Cómo me has robado la contraseña? Pues te la he robado (porque les decimos que metan contraseñas falsas, es un juego) porque te has metido en una página que no es Tuenti. Y como esas hay miles. Entonces, es importantísimo que los profesores también conozcan cómo se distingue una página web legal de una no legal y una segura de una no segura.

Conclusión: la conclusión es que nosotros, a través de la escuela, del libro blanco y de la plataforma de asistencia al docente, hemos creado un

auténtico sistema de seguridad y de protección de menores en la red, en entorno educativo, desde las aulas, y contando con los profesores, dando respuesta a sus necesidades.

Cómo estamos ampliando esta formación, y un campo que es fundamental: nosotros estamos trabajando sobre una comunidad docente de 400.000 docentes; la mayoría inexpertos, la mayoría sin conocimientos, incluso los coordinadores TIC tienen muchos conocimientos técnicos de máquinas, pero desconocen lo que es el hábito social del menor. Para nosotros es fundamental que este conocimiento vaya a la formación universitaria.

El primer curso lo hicimos en prueba (que es este que veis arriba, que ya estamos en segunda edición, está siendo un exitazo). Pero lo normal es ir a este segundo que ya estamos preparando, para que todos aquellos que quieran ser responsables conforme a la nueva normativa comunitaria de la seguridad de los menores, que tengan su titulación y su reconocimiento para habilitarles en ese puesto de responsable, delegado, DPO, le llamaremos equis.

Raquel está preparando ya el primer máster universitario para *data privacy officer*, combinando conocimientos de seguridad informática con jurídicos y que permitan a todos aquellos profesionales que vienen de la protección de datos y que demandan este conocimiento avanzado de seguridad, que hasta ahora lo tenían vetado, realmente convertirse en las personas que a la vez sean los líderes de las empresas en cuanto a formación de los trabajadores en seguridad de la sociedad de la información, no seguridad de Internet.

Y luego, por último, dentro de ese proyecto educativo en Castilla-La Mancha, ya se ha incorporado, después de ver si funcionaba o no funcionaba, una universidad pública, que es la de Castilla-La Mancha; y su proyecto, evidentemente con su metodología, es integrar en 3º y 4º de grado una miniescuela de seguridad en la red, y en el proyecto, cuando vayan a hacer el *practicum* a los colegios, que empiecen ya a poner en práctica esos conocimientos que van a adquirir dentro de su formación universitaria. El objetivo es permeabilizar, que todo aquel docente que salga ya esté preparado para impartir clases en los colegios. Porque contenidos hay: INTECO tiene contenidos, PantallasAmigas, Protégeles tiene contenidos... Hay muchísimos contenidos. El problema es que el profesor no se atreve a dar esos contenidos precisamente porque desconoce

los fundamentos básicos. O sea, él no puede explicar cómo es una red porque no sabe lo que es una red social. Y para él, el sistema WhatsApp sigue siendo un sistema de envío de mensajes cuando no lo es. Ese es el problema real que se encuentran a la hora de utilizar las herramientas.

Entonces, nosotros definimos nuestro sistema de seguridad, o lo que proponemos, como preventivo, proactivo, tecnológico, permanente y sostenible. Es económico, era una de nuestras premisas. Yo empecé dando formación presencial; era inviable. La plataforma virtual, el aula virtual de la universidad nos permite que este sistema pueda llegar a cualquier rincón del mundo, a cualquier profesor, a cualquier docente, con independencia de su nivel económico, del sitio donde está y de cualquier tipo de condicionante. Lo único que necesitas es una conexión a Internet, con los problemas que puede tener ello también, pero es así.

Y por supuesto, dando cabida e integrando a todos los agentes públicos y privados implicados; y en esto voy a hacer una crítica, y lamento que sea así, pero yo digo las cosas muy claritas. Al tiempo que yo ponía en marcha este proyecto, mi colaboración con INTECO me llevó a ponerme en contacto y a tener una reunión con los responsables de Red.es, que a la vez pusieron en marcha otra comisión (en la que por cierto hasta ahora no he estado, ahora me han incluido, cosa curiosa) que todavía le sigue dando vueltas a la cabeza sobre cómo van a empezar a través de INTEF a poner en marcha un proyecto en el que no han hecho nada. Yo no dejo de sorprenderme: ahí hay infancia, hay no sé qué; vale, sí, a mí me parece muy bien, pero es que cuando queramos poner en marcha (estamos ahora, bueno, yo todavía no he estado, pero ayer me llamaron para asistir a mi primera reunión), yo no entiendo cómo estamos todavía ahí cuando esto es una realidad, esto está, esto se puede ver, la formación existe, los conocimientos existen, y además hay muchísima gente implicada; no se pueden ustedes imaginar la gente que quiere colaborar, que quiere participar. En el Congreso nos hicieron una pregunta, el diputado de Convergència i Unió hizo una pregunta, que estábamos allí Marcelino, Tuenti y tal; nosotros, dentro de este proyecto tenemos un proyecto segmentado con Tuenti muy bonito, que es relativo a redes sociales, dentro de este proyecto educativo, Tuenti nos está desarrollando una escuela de redes sociales, porque la implicación suya es total. Oiga, si está aquí fundación Alia2, si está aquí Protégeles, si está aquí el centro de seguridad, ¿por qué ustedes no trabajan juntos? Y yo le dije: yo lo he intentado pero ellos no, y ellos dieron su explicación. Es su chiringuito.

Protégeles recibe sus fondos de Safer Internet y solo responde ante la Comisión Europea —nos quedamos helados—, será que la Comisión Europea se financia no sé cómo, no sé cómo se financiará. Y fundación Alia2, como es una entidad que lo que hace es promover acciones institucionales y de márquetin en provecho propio, pues no colabora con nadie. Esa falta de conectividad, de colaboración, cuando ya hay universidades, cuando hay consejerías metidos en un proyecto educativo que necesita la participación de todos, no la entiendo, no la entendemos. Esa falta de participación, de colaboración en un proyecto que permitiría perfectamente integrar a jueces, magistrados, fiscales (yo conozco fiscales que saben muchísimo, que me dan clases a mí), es que ellos mismos dicen «si es que no conseguimos que haya una formación estable en menores, y al paso que vamos, vamos a tener más problemas con menores en delitos en la red que en adultos». Entonces, existe una especie de falta de sinergias y de comunicación y de colaboración preocupante, sobre todo porque yo creo que ya hay línea marcada y camino, que es el que tenemos que seguir, que es el que nosotros proponemos, que es el de educación en las aulas pero con un sistema que tenga una metodología clara; y a partir de ahí, desarrollar contenidos. Es lo que nos falta probablemente, contenidos. Y para los contenidos, hay gente muy capacitada, como puede ser el mismo PantallasAmigas, Jorge, o chavales, hay muchísima gente. Pero a la vez yo veo cómo hace Jorge Flores una iniciativa, chavales la misma iniciativa, hoy vamos a la Agencia de Española Protección de Datos y otra iniciativa, Fundación Telefónica a través de Generaciones Interactivas otra iniciativa, y cuando yo me pongo a ver los tres capítulos de dibujos animados, pues al final son lo mismo, tienen el mismo mensaje con diferentes personajes. Pues no lo entiendo, sinceramente.

Otras medidas, esto es simplemente la última diapositiva que nosotros demandamos: ¿una educación normativa? Por supuesto, el nuevo reglamento de protección de datos europeo, sacarlo adelante; la aplicación territorial, para nosotros es fundamental, por lo que vemos en las redes sociales: si tú facturas aquí, tú tienes que cumplir la normativa europea sí o sí. O sea, no puede ser que porque tú tengas tu sede social en Estados Unidos no cumplas las normas de privacidad y protección de datos europeas. Porque todo lo que ellos hablan en función del Tratado de Libre Comercio y de las consecuencias macroeconómicas que va a tener para Mountain View afecta a niños; todo lo que ellos hacen, todo lo que ellos dicen, todas las decisiones empresariales que toman, la decisión

empresarial que ha tomado Google de la publicidad social —no sé si la conocen ustedes—, que Google ha puesto ya en marcha un sistema de publicidad social, todos los que tengan Google+, que somos todos, porque para utilizar las herramientas de Google necesitamos estar en Google+, todo el que tenga Google+, automáticamente autoriza la utilización de su imagen y de su perfil para publicidad social. Ellos se curan en salud diciendo, y lo dicen en todos los medios de comunicación, que esa modificación de las condiciones no afecta a los menores. Claro, no afecta a los menores que hayan declarado al darse de alta que son menores. Creo que el 50% de la gente que hay en Google+ ha mentido sobre su edad, y eso lo saben ellos. Porque yo a Bárbara se lo digo muchas veces: «Bárbara, es que esto no es así». Ya, pero yo soy empresa, y ellos tienen una cátedra Google de privacidad, yo colaboro también, pero una cosa es la realidad institucional y de márquetin y otra cosa es lo que ellos hacen. Y esa decisión, por defecto... Hay una directiva comunitaria que establece que ese tipo de decisiones, la casilla debería ir por defecto marcada. Pues es al revés. Y encima, como a la Agencia de Protección de Datos le ha dado el varapalo que le ha dado Bruselas con el tema del derecho al olvido, pues ahora como que no están por la labor, y que nosotros denunciemos no tiene ninguna efectividad, es perder el tiempo para no conseguir nada, precisamente por la situación en la que estamos.

Este tipo de medidas que para la opinión pública tienen una repercusión, cualquier decisión que se tome a nivel de redes sociales en Internet afecta a los niños, porque esto es al final que Internet no fue creado para los niños, pero los niños están creando Internet. Y en función de eso, incluso las decisiones legislativas habría que pensarlas, analizarlas pensando las consecuencias que van a tener para niños de 5 y 6 años, y eso no lo hace nadie. Si no, no tendríamos un anuncio de Movistar del 4G con todos los niños explicando lo bueno que es el 4G, y es Movistar, Telefónica. Es que ese tipo de anuncios, también a veces son incomprensibles en el entorno tecnológico en el que nosotros nos movemos. Pero ya he dicho que lo que yo vivo en los colegios y lo que yo experimento no lo experimenta nadie.

Muchas gracias, y estoy a vuestra disposición para las preguntas que queráis hacer.

COMPARECENCIA DEL PRESIDENTE DE LA ASOCIACIÓN DE USUARIOS DE INTERNET (AUI), D. MIGUEL PÉREZ SUBÍAS, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 24 DE OCTUBRE DE 2013.

El señor **PRESIDENTE DE LA ASOCIACIÓN DE USUARIOS DE INTERNET (AUI)** (D. Miguel Pérez Subías): Muchas gracias. Lo primero, también, quiero reiterar mi agradecimiento, de mi persona y de la organización a la que represento, por tener la amabilidad de escuchar nuestra opinión en un tema que pensamos que es muy relevante. Porque al final, digamos, los cambios tecnológicos están metiendo un *timing* en el desarrollo de los niños que está influyendo en diferentes aspectos y creando situaciones que en algunos casos conviene, cuando menos, pensar y reflexionar; y yo creo que hacer este ejercicio de reflexión desde diferentes ópticas nos puede llegar a todos y nos puede ayudar a todos a entender qué es lo que está sucediendo.

Yo me he leído las ponencias de los intervinientes que estaban ya disponibles en la página web y por lo tanto voy a intentar no entrar en aquellos aspectos que ya se han comentado, y que algunos de ellos comparto y creo que están bien enfocados. Pero sí voy a intentar centrarme en otros que creo que no se han tocado de forma suficiente o de una forma distinta.

En primera instancia, quizá la primera reflexión es que cuando ponemos la palabra «riesgos» tendríamos que poner también «oportunidades». Porque si estamos en este barco es porque el cómputo parece que se decanta por la parte de oportunidades. Y siempre que aparece una nueva tecnología, por un lado nos genera un mar de oportunidades, y por otro lado, muchas veces la culpamos de todos los males, incluso de que los niños sean niños o de que los adolescentes sean adolescentes, cosa que la tecnología, ahí de momento no ha entrado.

He intentado hacer una pequeña... ¿dónde están estos riesgos, qué los causa? Yo creo que hay tres ámbitos. Uno es la potencia de la tecnología. Imaginemos, retrotraigámonos veinte años atrás, cuando éramos nosotros niños (o treinta, o cuarenta algunos), pero imaginemos que cuando salíamos del colegio nuestros padres nos ponían en nuestra cartera una máquina de fotos réflex, una cámara de vídeo, una máquina

de escribir, un teléfono, un geolocalizador... Todo eso está aquí. O sea, imaginemos a un niño de 8 años, de 10 años, de 12 años que sale de casa con todo ese bagaje potencial de herramientas. Es como si le damos un helicóptero, ya está. Pues esa es la situación que tenemos si analizamos la potencialidad de cambio que tiene la tecnología con respecto a lo que podíamos hacer nosotros en nuestra infancia. Lo cual, este aspecto que parece que ya damos por hecho es muy importante y genera una parte de los problemas a los que nos enfrentamos. Por lo tanto, la potencia de la tecnología en manos de personas de una que tienen una serie de criterios y una educación.

Por otra parte, están las nuevas situaciones. Es decir, el tener todas esas cosas en el bolsillo propicia nuevas situaciones. Que muchas veces no existían, por lo tanto no tenemos historia previa, es decir, no sabemos si el mucho uso de esto es una adicción o no es una adicción, porque no sabemos cuánto es el tiempo en que... Pero genera situaciones en las que hay geolocalización, en que lo audiovisual se potencia de una forma... Es decir, que hay nuevas situaciones propiciadas. ¿Cuáles son las nuevas situaciones que propicia esta tecnología, intentando hacer un poco de resumen?

Pues yo he intentado agruparlas en varios grupos: la facilidad con que lo privado pasa a ser público. Esta es una situación que antes estaba el boca a boca, pero tenía unas limitaciones, pero aquí no, aquí cualquier acción privada, un clic, muchas veces ni siquiera oímos ese clic y ya está subido en una red y todo el mundo tiene acceso. Es decir, la facilidad con que lo privado se torna público es una situación nueva.

Otra situación es la potencialidad de lo visual. Hasta no hace mucho lo audiovisual pertenecía, bien a los medios de comunicación, bien al ámbito de lo privado, había un *gap*. Ahora de repente no, nos encontramos con que todo lo audiovisual (foto y vídeos) forma parte de. Entonces, ahí empezamos a encontrar también otras situaciones que nos generan: por ejemplo, qué pasa con una fotografía, ¿quién es el dueño de la fotografía? ¿El que la publica o el que está en la fotografía? Cuando a mí me hacen una fotografía en una discoteca, no es lo mismo decir «Pepito ha estado en una discoteca» que ver una fotografía en la que se me ve potando o que se me ve en una situación que no me agradaría. Pero la fotografía, a lo mejor no la he hecho yo, la ha hecho mi amigo, mi amiguete, que ha dicho «mira qué gracia», y con el móvil lo ha subido a su red. Y

entonces nos encontramos que el material audiovisual no está suficientemente categorizado en cuanto a quién, cómo y qué derechos tengo con respecto a mi presencia como sujeto dentro de ese contexto, ese entorno, un entorno que cada vez es más público, cada vez es menos controlado. Con lo cual hay un *gap* generado por la presencia de lo audiovisual, que hasta ahora en el ámbito normativo, legislativo e incluso de práctica de usos y costumbres no existía.

Hay otro aspecto que es la geolocalización, con todo lo que eso implica. Es decir, el hecho de que se pueda asociar dónde estoy y todo lo que eso significa. Es decir, que yo en un momento dado... Hay cantidad de aplicaciones ahora, (ver a mis amigos o lo que sea); la gente puede saber. Todo esto tiene un potencial, sí, es que si una persona tiene alzheimer podemos localizarla, si un niño se pierde sabemos dónde está; bien, pero también tiene otra serie de connotaciones.

A su vez esto también nos está provocando que el ocio, la formación, la información, los riesgos y las posibilidades están en mi bolsillo en todo momento, y estamos con menores, con lo cual... Es decir, los cambios que provoca el cómo tengo que atraer su atención para que no se distraiga en aquello que yo no quiero que haga; porque se supone que yo, como padre o como educador, tengo la responsabilidad de educar. Pero él tiene un cacharro en el que, digamos, la tentación buena o mala está aquí. Esta situación antes no existía. Y eso está en el bolsillo. Antes salía de casa y la consola se quedaba en casa. Con lo cual tenemos ahí una serie de situaciones.

Tenemos otro aspecto que es el reconocimiento facial, una tecnología nueva. A partir de ahora casi todas las redes sociales permiten etiquetar la cara de una persona. Si esto lo sumamos a lo que he contado antes, nos encontramos con un abanico de situaciones en las cuales no solamente aparece mi foto, que a lo mejor, alguien me conoce, pero es que ahora ya, asociado a esa foto aparece mi nombre, asociado a mi nombre puedo asociar un buscador... Es decir, que hay tecnologías que están poniéndose encima de la mesa a disposición de las redes sociales, con lo cual tenemos nuevas situaciones a las que nos tenemos que enfrentar en este contexto de tecnología en el bolsillo, movilidad y disponibilidad de 24 horas.

Dejadme que os dé algunos datos muy rápidos. Hay algunos estudios (hay varios ya) que más o menos cifran el tiempo que está un adolescente

o un niño en contacto con una tecnología: en torno a las 7 horas y media del día útil; esa es la media. El 50% de los hogares (esto es un dato americano, en España no lo conozco) tienen la televisión enchufada todo el día, no se apaga. Niños menores de 8 años, el 30% sabe utilizar un *smartphone*. A lo mejor no lo tiene, pero déjamelo, cógelo, el niño que juega. No sé si esto es bueno o malo.

Entonces, esto nos lleva a que hay un cambio (y es donde yo voy a centrar un poco mi atención, aparte de los temas tecnológicos) que no somos capaces de valorar, porque hay un riesgo que es muy importante que es el desarrollo social y el cambio de las tecnologías que no somos capaces de visualizar porque la tecnología está avanzando a tal ritmo; los cambios sociológicos normalmente requieren de una, dos, tres o cuatro generaciones, y por lo tanto la influencia que tenemos en ese cambio generacional de ámbitos de usos y costumbres, no somos capaces de visualizarla, porque probablemente se producirán a la segunda generación, tercera generación, etc.; pero probablemente tendríamos que empezar a reflexionar sobre esas situaciones, porque las medidas que pongamos también tendrá influencia sobre los usos. Si nosotros nos retrotraemos a cuando éramos niños, el niño basaba su estimulación en el juego en contacto con una persona. Entonces, había una serie de desarrollos sensoriales que tenían que ver con tocarse, con jugar, con el movimiento. Si cogemos a este niño, que cuando es mayor, fundamentalmente es dependiendo de cómo ha sido su infancia y su niñez en cuanto a sus actividades, a sus relaciones y a su contexto, nos encontramos que las tecnologías lo que han provocado es un cambio brutal en cómo es la vida de ese niño, y por lo tanto va a tener una influencia brutal en cómo serán sus desarrollos posteriores. Y digo «brutal» por no decir si es bueno o malo, ahí podemos tener dudas. Yo voy a intentar poner en valor lo malo, los riesgos que hay y algunos que se han constatado.

Entonces, tenemos un niño que pasaba tres horas jugando con sus amigos, que se tocaban, que tenía contacto con la naturaleza; ahora nos encontramos con un niño que pasa 7 horas y media conectado a una pantalla, a un ordenador, donde tenemos sentidos que se están sobrestimulando (concretamente la visión y el oído) y hay otros que se están dejando de utilizar (todos los temas que tienen que tener con la movilidad, contacto, el tacto), otros que se están detrayendo del uso. Con lo cual nos encontramos con que la mayor parte del tiempo se sobrestimulan unos sentidos y hay otros que se dejan de usar. Y además, esa sobrestimula-

ción está producida, no por otros niños, sino por productos que en general hacemos los mayores, o que comercializamos o vendemos, es decir, que tienen un cierto... Mientras que en la etapa anterior ese déficit de tres, cuatro horas del niño que estaba jugando, su interacción era con otros niños, con lo cual la construcción mental en la que se desarrolla el cerebro de la persona (que es muy importante en esa época, no solo el desarrollo físico, que también hará un comentario, sino el desarrollo mental) tiene mucho que ver con ese tiempo, porque son muchísimas horas. El cambio es brutal. Con lo cual, aquí tenemos un eje al que no se le presta toda la atención porque el cambio no lo visualizamos, porque todavía no vemos ese efecto sobre la sociedad.

¿Qué es lo que está provocando este desarrollo? Pues básicamente hay falta de movilidad, por lo tanto empieza a haber trastornos de tipo de obesidad, diabetes... Nos encontramos que en las sociedades que nos llevan un poquito de delantera, pero ahora estamos entrando ahí, la vida es más sedentaria, se pasan más horas aislado, como he dicho, hay algunos sentidos que están sobrestimulados. Y todo esto genera problemas que tienen en el desarrollo, que pueden ser de tipo de salud, como puede ser la obesidad, como puede ser la diabetes, puede haber problemas en el desarrollo mental, puede haber problemas de autismo (de hecho los hay). Y esto provoca una serie de situaciones que pueden ser desde aislamiento, violencia, adicción... Esto nos lleva a trastornos que en el tiempo probablemente nos llevarán a un cambio. Algunos, los más catastrofistas nos dicen que nos moriremos antes. Es decir, que asumir biológicamente el cambio que la tecnología nos está introduciendo nos puede llevar a un cambio.

Este aspecto no se toca en general cuando se habla de los trastornos del niño, pero creo que merece la pena; y no he visto que se haya tocado. Entonces, estamos construyendo una persona cuya base de formación está basada en un pilar audiovisual, de visión celular, Internet, videojuegos, etc. Con lo cual, ¿cómo se construirá, cómo será esa persona, cómo reaccionará? Tenemos ahí un reto. Si me preguntan a mí: ¿esto hay que corregirlo o no? Pues tengo mis dudas, no lo sé; yo creo que sí. Creo que hay que compensar ese exceso de tiempo, hay que buscar los mecanismos. Si el padre no se lo puede dar porque el padre no está en casa, tenemos que buscar algún mecanismo para que en el conjunto del ámbito del niño el cambio no sea tan brusco. Esa es mi opinión. Es decir, no podemos pasar de 3 horas de juego a 7 horas de audiovisual, y las

horas de juego a media hora o veinte minutos, justo el recreo. Entonces, ahí tenemos un déficit.

Con lo cual, cuando analizamos este desequilibrio sensorial tenemos que volver un poco a la base anterior. Y la base anterior era que en el desarrollo del niño sus interacciones eran fundamentalmente con otros niños. Y esto genera una dinámica totalmente distinta a la que se genera cuando estamos interaccionando con una pantalla, con un juego, con lo que sea, donde continuamente hay un reto, donde continuamente hay alguien que nos quiere vender algo.

Y aquí entramos en la responsabilidad. Vale, eso es así: si tenemos que cambiar esto, ¿cómo lo podríamos hacer, cómo lo podríamos cambiar? Entonces, quiero dejar un poco este tema porque la responsabilidad es un elemento que no se ha tratado, digamos, en profundidad, pero nos tiene que hacer reflexionar sobre si deberíamos hacer algo en el ámbito, dado que cada vez son más tempranas las edades en las que se entra en contacto con esa tecnología, cada vez las pantallas se usan mucho antes, y cada vez ese tiempo va ocupando mucho más tiempo. Y no podemos dejarnos llevar solo por el mensaje positivista de que se estimula mucho la parte visual, y por tanto ese chaval cuando coge un fórmula uno es un fuera de serie, o cuando conduce. Que es verdad que hay sentidos que se desarrollan, pero hay otros que se pierden y se atrofian.

Con lo cual, nos encontramos con que la tecnología está provocando unos cambios de hábitos con esas implicaciones. Ahora, ¿todo esto dónde nos lleva? Pues nos lleva a que en ese futuro de ese niño que pronto estará en el mundo adulto, todo lo que hace va a tener influencia en su reputación, lo que llamamos identidad digital. Es decir, tú eres lo que eres por lo que eres y por cómo te ven los demás. Es decir, que hay un equilibrio entre lo que somos, hay una parte más íntima, la parte íntima cada vez pierde espacio frente a los que se dice de ti. Ahora (yo lo hago cuando voy a contratar a alguien), viene alguien, y lo primero que hago es mirar en Internet a ver qué se dice de él; y esto ya me condiciona prácticamente la primera criba de entrada. Hace un tiempo ya dije «esto no puede ser así, no puedo seguir en esta dinámica, porque no sé, esa reputación, cómo, por quién y por qué se ha construido». Es decir, prefiero volver a un sistema en el que yo primero entrevisto a la persona, me hago un criterio y luego ya empiezo a analizar. Me leo su currículum, pero me abstraigo, digamos, de lo que dicen que es. Sin embargo, durante un

tiempo yo he estado gestionando, dejando a gente fuera simplemente por lo que se decía. Entonces, eso que antes no te llegaba, porque antes lo que te llegaba es lo de «oye, que va a ir mi hijo a verte», «que va el amigo de», y había una pequeña influencia en el conocimiento cercano de la persona o de tal. Ahora eso lo hemos sustituido por lo que se dice en la red. Entonces, hay gente que hemos sido unos barrabases en nuestra... y ahora somos personas normales, a lo mejor no contamos todo lo que hemos hecho. Pero es verdad que la identidad digital, nuestra reputación nos condiciona, y por tanto todo esto se va a traducir.

Hay otro aspecto que también es importante, que es en qué medida esta dependencia de la tecnología, que detrás hay un interés fundamentalmente empresarial y no social, nos está también condicionando, en tanto que hay una manipulación para consumir determinados bienes, hacer las cosas de determinada forma, etc. Es decir, que de la manipulación que hace el grupo infantil a la manipulación que me hace una aplicación en cuanto a pautas de los retos que me pone, cómo se trata a la gente, etc., es radicalmente distinto. Y por tanto, hay una responsabilidad ahí que es de las propias empresas, que tenemos que ver cómo meterle mano, porque yo puedo poner un videojuego, vale, poner que en dos horas de estar jugando decir «esto ya es demasiado», o que sea el padre el que decida.

Entonces esto nos lleva a una situación, que es qué pasa con el padre o con el educador, es decir, cuando el padre o el educador quiere entrar en ese mundo. Nos encontramos, primero, que para interaccionar con ese mundo tienes que estar dentro de ese mundo, y el padre no está. Es decir, si tú tienes a tu hijo en Facebook y quieres protestar porque tu hijo ha hecho no sé qué, tú tienes que ser usuario de Facebook; no puedes decir nada, no puedes acceder, no hay forma, son puertas en las que solo los de la red, los de mi red pueden interaccionar, por la puerta que yo digo y tal, pero solo los de la red pueden interaccionar. Pero el padre, ¿yo por qué tengo que estar en Facebook para decirle a Facebook algo sobre mi hijo? Yo quiero hablar. Entonces, tenemos un déficit tremendo, tremendo, de la interacción entre el que no está en la red, en el juego, etc., y el que tiene la responsabilidad de educar. Y que no tendría por qué meterse. No, los padres que tienen que ser muy guay se tienen que meter en Facebook. O no, ¿por qué? ¿Por qué tenemos que exigir al padre que se meta? Yo lo pongo ahí. Quizá sería más sano que aquellos que tienen un nivel de uso tuvieran una puerta a la que se pueda llamar y se diga: oiga, tengo un problema. Quiero que a este niño que se llama Pálido Pato Donald no

le deje jugar más. Porque tiene 12 años, no sé; quiero que usted lo haga. Por ejemplo. Y eso se lo tengo que decir al Sony de turno o a tal. ¿Por qué? Pues porque, si no, si yo a mi hijo le corto la Play Station, se va a la casa del amigo, y si no, juega por el móvil. Entonces, la única forma útil, práctica... Es verdad, se podrá dar de alta de otra manera, pero... Hay mil vías, pero el padre se encuentra con que no sabe cómo interaccionar con ese mundo de redes sociales, de juegos, de videojuegos, o incluso de televisiones. Por lo tanto, hay un déficit en las personas que tenemos la responsabilidad de educar cuando tenemos que acceder a eso.

Dicho esto, dices: bueno, está claro que hay unos riesgos derivados de los usos, y hay otros riesgos de los malos; es decir, los malos saben que el niño tiene esa tecnología, tiene esos usos, y sabiendo que detrás hay un niño, aprovecha ese contexto para colarse y fomentar timos, abusos. De eso se ha hablado ya mucho, del papel de los malos, cómo entran, acosos, etc., pornografía infantil. Yo creo que eso está, digamos, más atado, ahí nos hemos preocupado más, preocuparnos de ver cómo a los males les metemos mano en este mundo.

Dicho esto, ¿qué se podría hacer?, desde mi punto de vista, qué cosas se pueden hacer. Yo dejo aquí algunas ideas que luego podemos debatir. Hay una que me parece importantísima, que es incluir la tecnología, tanto en sus beneficios como en sus riesgos, como material curricular. Es decir, esto cambia tan rápido (ahora estabais comentando cuando hemos salido si esto se llama *sexting*, si se llama como se llama); no sé cómo se llama, pero quizá deberíamos enseñarlo, y tendríamos que enseñar cómo se usan las opciones de privacidad, contar a un niño cuándo se detecta no sé cuántos, contarle algo; porque el padre, a lo mejor no lo sabe o lo desconoce, el cambio es tan rápido que yo no me entero. Si esto se introduce en materia curricular, probablemente tendrá un cierto *decalage*, pero habrá cosas que se seguirán manteniendo en el tiempo. Entonces, entiendo que esa tecnología no tiene que ser específicamente Internet, sino que tiene que ser lo que se lleve: puede ser el móvil o lo que sea. Pero que deberíamos, en las edades más tempranas introducir esto como materia curricular.

También deberíamos estudiar en los centros la compensación de los hábitos de los más pequeños y de los adolescentes para ver, entre la vida familiar y escolar, cómo compensar los déficits que se van creando. Sé que esto es complicadísimo, porque tú tienes que dar unas asignaturas.

No, vamos a dar más horas para que jueguen: no lo sé, pero yo creo que es importante, porque el cambio al que estamos sometiendo a los más pequeños es tremendo.

Hay un aspecto que creo que es importantísimo, que es el papel que juegan las herramientas. Tú puedes legislar lo que te dé la gana, pero un Facebook que cambie sus opciones de privacidad, el que las ventanas, las opciones de privacidad estén cerradas o estén abiertas, el impacto es brutal. Entonces, hasta ahora en general casi todas las aplicaciones o todas las que vienen de los mundos de Internet estaban orientadas para que todo fuera en abierto. ¿Por qué? Pues porque mi negocio estaba apalancado sobre publicidad. Por lo tanto, cuanto más contenido, cuanto más se pudiera indexar, etc., más posibilidades tenía yo de hacer negocio. Y esto se ha venido manteniendo con algunas excepciones.

Entonces, ¿qué es lo que sucede? Que al que entra ahí, a un niño le preocupa poco la intimidad, la privacidad, no está, está en otras cosas. Entonces, si tú le das una herramienta en la que todo está abierto, pues todo está abierto; y él nunca se ocupará de cerrar esas ventanas, y verá tan normal que estén todas las ventanas abiertas. Entonces, creo que sí se puede hacer una labor de regulación para que las aplicaciones que tengan un nivel de relevancia, a lo mejor no hace falta preocuparnos por todas y examinar todas, pero si usted tiene más de un 20% de cuota de mercado (un criterio, a lo mejor, de tamaño), usted tiene la obligación de tener. Dado que no hay forma humana de comprobar si el que se conecta es niño o no niño, ponga usted todas las ventanas cerradas, y quien quiera abrir y exponerse, que las tenga que abrir. Por lo tanto, ya tendrá que hacer el ejercicio de ir a un sitio, darle a una pestaña, tal. Ese es un criterio.

Hay otro criterio. Yo creo que ahí sí se puede hacer, y mucho: que a pesar de que Internet es global, los Estados son soberanos y tú puedes decir hoy sin ningún reparo que el uso de una aplicación exija estas condiciones de privacidad. Se ha hecho en protección de datos con las *cookies*, es decir, que se puede hacer. Luego, la aplicación, en la medida en que tiene un mercado importante, lo hará porque querrá ese mercado, y si no, lo aprovecharán otras. Por lo tanto, digamos que tenemos una labor muy importante en cuanto a las herramientas.

En cuanto a las puertas de acceso, lo mismo: vale, no hay forma humana de hablar con cualquiera de las aplicaciones, no hay ni un teléfono, no hay una dirección postal, pero usted podría decir: oiga, si usted tiene una

cuota de mercado en cuanto a usuarios en España, usted tiene obligación de; de forma que yo pueda, yo que todavía soy aficionado a mandar un certificado, que pueda mandar un certificado. Porque resulta que luego el correo electrónico, cuando voy a un ámbito jurisdiccional, a lo mejor no tiene la validez que pueda tener... Es decir, que desde el punto de vista regulatorio si nos centramos en poquitas cosas, pero muy concretas, de las grandes aplicaciones, también podemos avanzar mucho.

Hay otros aspectos que son más tecnológicos pero que también tienen mucha relevancia. Una de las claves, de los puntos más débiles de la seguridad de todas las aplicaciones está en la entrada, en cómo entro: clave y *password*, todos los sistemas clásicos. Entonces, la persona es una persona que te dice: yo tengo en todas las aplicaciones la misma clave. Y luego, al cabo del tiempo dice: voy a hacer dos, una para lo importante, importante, y otra para lo otro. Al cabo de mucho tiempo. Y aun así, ahora de vez en cuando digo: ¿esta cuál será, la buena, la mala? Y al final, acabas toda tu vida con la misma clave. De repente entra un *hacker*, coge los 3 millones de contraseñas de no sé quién, y está comprometida. Y además no solo eso, sino que todo el mundo utilizamos el perro de mi perro, Napoleón, tres o cuatro, nada. Entonces, es tan débil el sistema desde el punto de vista de control de acceso, que cualquiera que esté ahí mirando, tiquití, tiquití, ya está.

Hay una herramienta que ya la llevamos todos en el bolsillo que se llama teléfono móvil que puede generar un nivel de seguridad muy alto, simplemente que la clave sea dinámica y que te la mandan. Lo hacen los bancos. Es decir, que uno de los puntos más débiles del acceso a todas las aplicaciones y las que pueden comprometer nuestra seguridad y la de nuestros hijos está en... Entonces, podemos empezar a pensar, no sé si a regular, en que se puede subir enormemente, si estamos de acuerdo en que todos ya llevamos el móvil en la mano, en que esto puede aumentar el nivel de seguridad de una forma importante. Por lo tanto, seguramente ahí digamos: bueno, y el día que me lo deje, ¿qué pasa, que no puedo usar el Facebook? Pues sí, pero la seguridad tiene un contrapeso, ¿no? ¿Usted qué quiere? Si lo quiere tener fácil o... Pero creo que merece la pena echarle un vistazo al punto más débil.

Hay otros aspectos que tienen que ver con la interoperabilidad, que para mí son muy importantes. Se ha creado un mundo, el mundo de Internet que es terrible, porque no deja espacios. Es decir, el que acierta se

hace el rey del mambo. El que acierta en Facebook, funciona en Facebook, el que acierta en Twitter, el que acierta en el buscador, en Google; pero luego dices: ¿y cuántos Facebook hay? En España hay dos, el Facebook y el Tuenti. ¿Pero alguno más? No. Y en otros sitios, a lo mejor solo el Facebook. Es decir, no deja espacios. Entonces, ¿cuál es el problema que tiene el ciudadano? Que cuando yo me quiero ir no me puedo ir, porque mi contexto y mi entorno está ahí. Entonces, esto es un problema tanto para el ciudadano como para el desarrollo de nuevas oportunidades. Entonces, los que venimos del mundo de Internet, en que Internet resolvió un problema de intercomunicación de redes y que de repente todo el mundo dijo «podemos poner todas las redes en funcionamiento», ahora hemos empezado a poner otra vez vallas a los jardines, pero además con la diferencia de que ahora no solamente hay información, estamos las personas dentro. Es decir, antes estaban nuestros datos, pero ahora están las personas, mi relación con mi entorno. Entonces, si yo me quiero ir del WhatsApp al Line, pues o se pasan todos mis amigos o no hay forma de moverme; si me quiero ir del Facebook al Tuenti, pues no hay manera; si estoy en el Tuenti, que estás más seguro, pues resulta que mis amigos se van pasando al Facebook y yo no me puedo pasar al Facebook porque mis padres... O sí, y ya me paso. Entonces, hay un tema que merece la pena darle una pensada desde el punto de vista regulatorio que es la interoperabilidad: oiga, señores, está bien que ustedes tengan sus jardines, pero ustedes lo que no pueden hacer es arrogarse (entre comillas) la posesión de la persona. Es decir, tenemos que conseguir, esto también es complicado, porque la red dice «yo soy el que mando», si es el dominante, para qué se va a interconectar, que todo el mundo venga conmigo, ya está interconectado. Entonces nos encontramos con que, si queremos generar que pueda haber redes que den un valor añadido en la privacidad, en la publicidad, ¿cómo interconectar estas redes para que yo me pueda mover de una red a otra sin necesidad de que mis amigos se muevan y sin que yo pierda la posibilidad de interactuar? Porque, si os fijáis, todas se parecen. Lo que pueda hacer en el Tuenti se parece mucho a lo que se puede hacer en el Facebook; lo que se puede hacer en el WhatsApp se parece mucho a lo que se puede hacer en el Line. Pero hay monopolios de facto por áreas de actividad en los cuales, una vez que alguien agarra este monopolio, resulta terriblemente... Y en eso Internet es despiadado: entra en un sector, se erige un monopolio, todo lo demás lo destroza, y ya no hay manera. Con lo cual, digamos, ahí tenemos otra labor que hacer, que sería la interoperabilidad.

Hay otros aspectos que creo que se pueden tocar —los he comentado anteriormente—, que sería la responsabilidad de los fabricantes con respecto a los usos. Es decir, dotar a las aplicaciones de los elementos necesarios, sencillos, fáciles de utilizar, para que el educador pudiera de alguna forma interactuar sobre lo que llamamos control parental.

Aquí lo mismo, las dudas: las televisiones, casi todas tienen control parental. ¿Cuántos lo usamos? Pues casi nadie. Entonces, ¿dónde está el problema? No solamente está con que la herramienta tenga la posibilidad de, sino que para que eso se use, hay veces que el tenerlo no solamente es suficiente. Con lo cual hay todo un reto.

Y luego hay otro aspecto que también me preocupa, que es la simplificación, sobre todo en los entornos de redes sociales. En los entornos de redes sociales nosotros hemos reducido todo a los amigos o a amigos de mis amigos. Pero la vida real no es así. En la vida real tú tienes familiares, tienes gente de más confianza. Es decir, los círculos, ni son estancos ni son únicos. Con lo cual, digamos, cuando se establece un único nivel de acceso a la información, te encuentras con los problemas que tenemos en todas las rede sociales, que en el papel de amigos no están tus amigos; no quieres que estén los padres o los conocidos o las familias; entonces, cuesta establecer círculos que en la vida social sí que tenemos ya más... Quizás un esfuerzo que deberíamos hacer del lado de las aplicaciones, pero a lo mejor sí que se puede impulsar del lado del legislador o desde el punto de vista social, para que estas aplicaciones nos doten de las herramientas necesarias para decir «este es un familiar». No sé, criterios como «amigo», «conocido» (es lo mismo un amigo que un conocido), «del pueblo». No sé, hay un déficit en cuanto a la simplificación que se ha introducido en el sistema con respecto a las pautas de uso que tenemos en cuanto a la gestión de la información, a quién decimos, etc. Igual, las redes sociales nos han metido ahí en un tinglado en el que nos han querido digitalizar nuestras relaciones.

Ahí aparecen otras historias como son el derecho al olvido. Aquí las posiciones son también encontradas. Nosotros pensamos que al final esto es como las personas, es decir, yo no puedo obligar a nadie a que se olvide de mí, porque está en lo más íntimo. Pues en el Internet y en la red pasa igual. Si mi información está en una máquina, cuando esa máquina se muera... ¿Qué es lo que pasa? Que los ciclos, no sabemos cuánto duran. Antes sabíamos que los ciclos de una persona, más de cien años ya era

difícil, con lo cual, digamos, el derecho al olvido se iba; lo que se quedaba escrito tenía otra persistencia. Hay persistencias que ya están más contrastadas, pero lo digital, no sabemos la persistencia que tiene. Con lo cual, aquí nosotros no somos muy beligerantes, en tanto que pensamos que realmente si alguien lo hace público, es decir, si yo estoy diciendo «Fulanito ha hecho esto» y lo leo publicado en una página web, le tengo que decir «oiga...»; ahora, si en mi máquina hay una información ahí y está ahí dormida, ¿le tengo que obligar yo, cómo sé que usted la tiene ahí o no la tiene? Es decir, la responsabilidad está en cierta medida en aquel que haga público algo. Es decir, creo que esto está bastante asumido.

Y luego —y ya con esto termino— hay un aspecto que no se ha nombrado pero que yo sí quiero recalcar, que es la responsabilidad de la industria o de las empresas que están perdiendo en este cambio, y la influencia que tienen también en los menores. Cuando entra todo lo digital, esto hace tambalear todo un sector industrial, que es fundamentalmente el sector de los contenidos en sentido amplio (los periódicos, los libros, todo lo audiovisual). Entonces, se ha intentado traducir ese impacto, que es fundamentalmente económico, en un impacto de valores, se ha intentado que el compartir sea piratería (eso tiene una cierta influencia en cómo se asume desde el punto de vista de los más jóvenes), y se ha intentado que una pérdida de negocio que está, desde nuestro punto de vista, justificada por el cambio de modelo, es decir, aquello que vendías, que antes tu modelo era promocionar algo y vender copias de periódicos, de libros, ahora en Internet, como la copia, el precio del megabyte cada vez es más bajo y la facilidad de copiar cada vez es más alta, pues resulta que ya el contenido está por todos lados, porque el contenido en sí mismo no tiene un valor; por lo tanto, hacer negocio vendiendo copias del contenido ha dejado de tener sentido.

Pero alrededor de esto, y puedo hablar de los contenidos de otras industrias, hay toda una industria que se va, que se tiene que reconvertir a otra cosa. Pero no puede reconvertirse porque vive de vender libros, de vender periódicos, y no puede dejar de hacer lo que hace porque es lo que le da de comer. Y en el nuevo mundo los modelos de negocio son radicalmente distintos: son mucho más concentrados, globales, con lo cual los nuevos entrantes en esos negocios son gente que no tenía nada en el mundo anterior, son los tecnólogos, son los de los terminales, los de las aplicaciones. Y entonces hay una lucha ahí, que este sector que está perdiendo está intentando atar por la vía de la legislación el mantener

esa situación. Entonces el legislador se enfrenta a un problema en el que dices: vales, es verdad que estos señores generan mucho empleo, tenían una actividad, y por lo tanto si esto se destruye tenemos un problemón, porque es una reconversión. Pero se intenta abordar con una legislación diciendo que se prohíbe hacer lo que ya se está haciendo, y que además no se puede dejar de hacer. O sea, no hay mecanismos técnicos. Con lo cual hay una digresión entre el lenguaje que se utiliza y la legislación, ahora estamos en pleno... tenemos la Ley de Propiedad Intelectual, una modificación que se va... Y entonces tenemos que hay sectores que están intentando agarrarse al status quo que tenían, y lo que hacen de alguna forma es criminalizar al usuario. Con lo cual, la percepción del joven es que cuando él hace algo que él piensa que es natural, que es enviarte o pasarte un contenido, en la sociedad le estamos diciendo que eres un pirata, que estás contraviniendo los preceptos. Y él no entiende eso, dice: yo estoy haciendo algo que me parece bueno y saludable. Entonces, ahí tenemos una contradicción que me parece que también creo que deberíamos corregir. Entiendo que es complicadísimo y que los sectores del *lobby* son poderosísimos en el mundo del sector editorial, pero también tenemos que entender que el futuro lo tenemos que construir sobre la tecnología, no sobre lo que va a desaparecer, porque parece que eso nadie lo duda.

Entonces, quizá deberíamos hacer una reflexión, un esfuerzo desde el punto de vista de cómo nos dirigimos a los menores desde todos los ámbitos, incluidos estos ámbitos que están de alguna forma en un periodo de reconversión, y ahí habría que entender que al final ese niño, ese adolescente va a ser su cliente, y que hoy no le paga pero mañana sí si es capaz de encontrar un modelo de oferta, de negocio, de producto que sea atractivo. Por tanto, el lenguaje que empleamos, incluso la legislación que estamos haciendo, deberíamos cuidarla para no favorecer excesivamente, y deberíamos sensibilizar a estos sectores para que asuman su estado de reconversión, y no tanto el que de repente todos nos hemos convertido en piratas y en ladrones.

Entonces, a modo ya de resumen, yo creo que la tecnología ofrece un montón de posibilidades, que hay unos cambios que se visualizan en el corto plazo, que son más fáciles de ver, que hace falta introducir en el proceso educativo esto. Y a su vez (no he hablado, porque creo que se ha hablado mucho, de los malos), lo último que tengo que decir es que también tenemos que potenciar, sin ninguna duda, a aquellos que tienen

la labor, la responsabilidad de perseguir a aquellos que utilizan la tecnología para delinquir, y además en contra de un colectivo tan vulnerable.

Entonces, como resumen: se puede hacer mucho desde las aplicaciones, poco desde el ámbito legal hacia la ciudadanía; en el ámbito educativo, creo que se puede hacer bastante. Y en el ámbito pedagógico, de información... Yo creo que la clave, los que más nos pueden ayudar a generar buenas prácticas y a evitar los riesgos, sin ninguna duda son las aplicaciones que, para nuestra desgracia, la mayor parte no se desarrollan ni se implementan aquí, pero eso no nos debería llevar a renunciar a nuestra capacidad de pensar en qué queremos y en decir cómo habría que hacerlo.

Y ya está, con esto he terminado. Muchas gracias.

COMPARECENCIA DEL PRIMER DEFENSOR DEL MENOR DE LA COMUNIDAD DE MADRID, D. JAVIER URRA PORTILLO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 4 DE NOVIEMBRE DE 2013.

Nuevas tecnologias: riesgos y prevenciones

1. *La búsqueda de la innovación es un desafío constante en la evolución del ser humano.*

2. *La sociedad aumenta en complejidad, en incertidumbre.*
   La globalización añade diversidad, los avances tecnológicos precipitan el vértigo temporal y facilitan ¿el contacto? (si bien no «cara a cara» ni «piel con piel»).
   En todo caso facilitan la conectividad.

3. *Precisamos educar: En el silencio.*
   Para escuchar el eco de lo que nos dicen los otros y lo que emana de nuestro interior.
   En la utilización de un correcto lenguaje como imán pro-social y de las palabras como semillas de ideas.

El ordenador, el teléfono móvil, los videojuegos, la televisión, forman parte de nuestra cotidianidad, los usamos en el trabajo, en el tiempo de ocio y para relacionarnos con otras personas.

Se han hecho imprescindibles, y han generado cambios en nuestras vidas, en la forma de pensar, de aprender, de comunicarnos en la sociedad. Han modificado las formas de convivencia y de las relaciones personales y familiares.

Según un estudio realizado por el INJUVE en mayo de 2011 sobre los «Jóvenes y las nuevas tecnologías» se concluyó que los jóvenes están bastante interesados en los avances científicos y tecnológicos, sobre todo entre los 20 y 24 años. Así como en el tema de descargas y piratería en internet, y el desarrollo de la comunicación a través de la red. Creen que utilizando la tecnología se relacionan menos con su familia y se aíslan.

Usan internet varias veces al día, estando conectados alrededor de hora y media cada vez, se conectan en su casa, principalmente en su habitación, a través de un ordenador portátil o una tablet, seguidos del móvil. Utilizan la red principalmente para buscar información, descargas, y entablar relaciones e intercambiar fotos y videos en redes sociales, foros y comprobar su correo.

No piden ayuda a sus padres y si alguna vez lo hacen es por cuestiones «técnicas» (primordialmente económicas).

Ven menos la tele y la edad media en que comienzan a usar las nuevas tecnologías es sobre los 15 años.

Estamos ante verdaderos nativos digitales.

1. Riesgos

Ya en el 2009, el estudio INTECO, expone como riesgos a los que se enfrentan los menores en el uso de las TIC:

— Uso abusivo y desorden adictivo: excesivo tiempo de conexión que puede implicar dependencia o renuncia a la realización de otras actividades.
Los síntomas que podrían ser significativos son:

- Malestar, irritabilidad si no pueden utilizarse. Describen la sensación como «de agobio» sino tienen cerca el móvil por ejemplo.
- Alivio que genera el uso de los distintos dispositivos tecnológicos.
- Fracasos en el intento del control del uso.
- Dificultad para desconectarse.
- Mayor tiempo de dedicación del previsto.

La adicción aumenta según aumenta la edad del joven usuario. Si nos fijamos en su etiología encontramos el escape de la cotidianidad, es un refuerzo positivo de compensación, se busca contacto, genera distracción, evitando el dolor y el malestar emocional, genera confianza en uno mismo, evita nuevos retos.

Como factores de riesgo encontramos muchas veces problemas de personalidad como timidez excesiva, baja autoestima, rechazo de

la imagen corporal, dificultades de relación, no saber afrontar adecuadamente las dificultades cotidianas. Así como un fácil acceso a las TIC, el bajo costo…

Las tecnologías con riesgo de adicción son:

- Internet: Todo un fenómeno social que permite comunicarnos sin límites de espacio ni tiempo, ni de contenido en cuanto a información, entretenimiento…

  Fascina a los jóvenes por todas las posibilidades de aprendizaje, creatividad, relación, pertenencia a un grupo (redes sociales) que les facilita. Pero por el contrario pasan demasiado tiempo enganchados a la red.

- Móvil: lo utilizan para reforzar su identidad personal y colectiva y emanciparse de sus progenitores, pues garantizan la «seguridad» de su contenido. Muchos adolescentes lo consideran imprescindible para su vida, para sus relaciones sociales, para comunicarse de forma privada.

  Su principal forma de comunicación son los servicios de mensajería como el Whatssapp, el twitter y el tuenti. Estar pendiente de la respuesta al último mensaje enviado, de los seguidores que tienen,… les interfiere en tareas cotidianas como el estudio, las relaciones familiares e inclusive los momentos de ocio.

- Videojuegos: Son la forma de entretenimiento preferido por los niños y jóvenes que juegan en videoconsolas, consolas portátiles, móviles y en la red. Cuando juegan suelen olvidarse de realizar sus deberes, de compromisos adquiridos, incluso de sus amigos.

  Abuso de «videojuegos multijugador masivo en línea», con la problemática añadida de ser de pago algunos de ellos.

— Vulneración de derechos de propiedad industrial o intelectual (uso ilícito o descarga de imágenes, programas, contenido o software).

Quebrantan los Códigos Civil y Penal mediante la subida y descarga de archivos de las redes P2P («peer to peer», red de iguales).

Copian la información, o incluso descargan, los trabajos mandados en el colegio sin que haya ningún tipo de elaboración ni memorización de los contenidos (el «corta y pega» también en la Universidad).

— Acceso a contenidos inapropiados (sexual, xenófobo, terrorismo, anorexia y bulimia o contenido falso).

Las redes sociales son un punto de encuentro y a través de ellas existe el riesgo de anuncios de todo tipo (venta de armas de imitación, anabólicos y esteroides, páginas pornográficas, redes sociales de adultos, cultivo marihuana…).

En ocasiones internet es utilizado para la compra-venta de sustancias, en algunos casos de los que han pasado por Campus, hemos detectado que los chicos/as se han servido de internet para obtener información sobre sustancias tóxicas que burlen los controles de consumo habituales (Marihuana Sintética-SPICE), sirviéndose de esta herramienta para realizar la obtención de dicha sustancia, lo que permite que el adolescente realice un consumo de sustancias tóxicas y difícil de detectar por los adultos.

A la vez que contactan con personas que se dedican a esta venta, que en ocasiones deriva en que estos jóvenes son incluidos en la red de la compra-venta de sustancias.

Incitación a una maduración sexual temprana (dando lugar a parafilias: Desviación sexual como masoquismo, sadismo, vouyerismo, zoofilia, necrofilia). Uno de los riesgos más evidentes y peligrosos es la «educación sexual» que reciben los adolescentes a través de la red. Los adolescentes buscan información sexual, muchas veces, en portales pornográficos, asumiendo como normales prácticas, valores, actitudes y estética propias de la ficción, y que luego tratan de reproducir en sus relaciones.

Incitación y gusto por la violencia (en algún caso singular dando lugar a trastorno disocial).

Aprendizaje vicario de conductas de riesgo (por ejemplo «balconing»). Incitación de ideologías extremistas y sectaristas. Derivados del modelado y moldeamiento de conductas de los chicos a través de la gran cantidad de información que intercambian a través de las redes sociales.

Rotura de la barrera psicológica del suicidio, la bulimia, la anorexia…; motivando dichas conductas, inspirando, ensalzando, desmitificándolas y enseñando nuevas a su acervo.

Hemos detectado casos de jóvenes que recurren a internet para obtener programas de adelgazamiento. Estos programas no tienen por

qué haber sido elaborados por profesionales de la alimentación (nutricionistas, endocrinos, dietistas, médicos, etc.), pudiendo ser elaboradas incluso por personas afectadas por problemas relacionados con éste aspecto, por lo que no sólo no tendrán en cuenta muchos de los aspectos relevantes para la salud (física y mental) sino que darán valor, únicamente, a cuestiones superficiales como la imagen o la figura, Trastornos de la Conducta Alimentaria. Incluso llegando a exponer consejos para ocultar huellas. Dietas disparatadas.

— Interacción y acecho por otras personas y/o ciberbullying: acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños. Incluso llegando a ignorar a la víctima aislándola. Difusión, multiplicación del sufrimiento de la «víctima».

  Se realiza básicamente a través de internet en las redes sociales, e-mails, blogs, foros y los teléfonos móviles (empieza a hablarse de casos de acoso por Whatsapp).

  Especialmente los sufren los adolescentes entre 13 y 14 años.

  El compartir un espacio de privacidad con un gran número de «supuestos amigos» (sobre todo en redes sociales) implica que alguno de estos pueda compartir fotos o mensajes privados con un gran número de personas sin el permiso del propietario de ese contenido. Se publican dichas fotos, videos, mensajes comprometedores ridiculizando, amenazando y atentando contra la privacidad y la imagen del que va a ser víctima del acoso. En muchas ocasiones se chantajea con no realizar esta publicación a cambio de dinero, ropa, aparatos tecnológicos e incluso favores sexuales.

  Si las fotos enviadas son comprometidas, estaríamos hablando de sexting, se realiza tanto a través de la red como por Whatssapp con el móvil. Esta forma está aumentando ya que no es necesario conectarse a un ordenador para transferirlo, con una simple pulsación se graba y envía o se cuelga en la red.

  Puede llegar a ser tan traumático o más que el acoso escolar, ya que internet amplía su incidencia debido al anonimato e inmediatez con que se realiza, así como el gran alcance que tiene. Debido a la dificultad de eliminación de la información, puede perdurar el acoso aun después de que el agresor decida parar el acoso.

— Grooming y/o acoso sexual: «acoso ejercido por un adulto », se refiere a las acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor. Son situaciones de acoso con un contenido sexual explícito o implícito.

  Suele producirse a través de chat o servicio de mensajería instantánea y debe ser denunciado de forma inmediata (Se considera delito a partir de 2010).

  Hemos tenido alguna experiencia en la que personas mayores de edad han buscado chicas menores a través de las redes sociales, manteniendo durante un tiempo una relación virtual para posteriormente llevar esa relación al plano real, basada en una posición de poder, manipulación, amenazas, celotipias, etc., además de producirse abusos sexuales en esa pareja de forma habitual.

— Amenazas a la privacidad (robo, publicación y difusión de datos e imágenes personales).

  Exponen su vida en las diferentes redes sociales a través de escritos y de fotografías, usándolas a modo de diario, donde se pierde la intimidad personal y familiar con los consecuentes riesgos de acoso y de persecución por parte de terceros. Falta de discernimiento vida privada-vida pública.

— Control machista: ¿Quién te llama? ¿Quién te escribe? ¿Con quién te comunicas?

— Riesgo económico y/o fraude: conductas que tienen por objeto provocar un perjuicio económico al menor que se derivan de compras, subastas, apuestas, juegos de azar, etc.

  Acceden a través de la red o el móvil, con un bono gratuito inicial que puede llegar como publicidad no deseada (Observamos un problemático avance del juego de azar).

— Riesgos técnicos y/o malware (software malévolo): virus, troyanos y otras manifestaciones que pueden suponer un funcionamiento inadecuado del equipo, pérdida de información, etc. y/o un riesgo para la seguridad de quien lo usa.

  Esta infección puede revelar datos relevantes como contraseñas de correo, banco…e incluso puede activar la webcam.

2. Prevención

En ocasiones (las más) los adolescentes manejan la red mejor que sus progenitores, les ofrece más información de la que éstos les puedan dar, por lo que dejan de ser el referente, siendo sustituidos los adultos por Internet como fuente de información y de transmisión de valores.

Se genera un importante conflicto padres-hijos por la privacidad/supervisión del uso de las redes sociales. La sospecha por parte de los progenitores de un mal uso de la red por parte de sus hijos les lleva a intentar una supervisión/control que es vista por éstos como una violación de su intimidad, al acceder a las conversaciones íntimas que los hijos mantienen con su red de amigos.

Uno de los grandes miedos de los progenitores es la combinación existente entre los peligros de la red y el mejor control de la misma por parte de los hijos. Se sienten indefensos y en desventaja con sus hijos, pues estos muchas veces saben ocultar estas prácticas sin dejar rastro a los progenitores.

Es preciso encontrar un equilibrio con unos hábitos saludables. Para ello es indispensable la colaboración entre las familias y los centros educativos, apostando por unas buenas prácticas de las TIC, que integren comportamientos y pautas aplicables por los adolescentes dentro de su educación integral. Porque no es cuestión de la tecnología sino de educación.

— **Pautas para padres:**

- Transmitir que «en internet tu imagen es de todos».
- Adecuar la realidad jurídica a los avances tecnológicos.
- Alentemos la labor de las Fuerzas de Seguridad e impliquemos a las Empresas que se desempeñan en la red.
- Educar para ser saludable. Anticiparse y conocer los intereses y preferencias del ocio de los hijos y compartir con ellos momentos, espacios y actividades de tiempo libre. Esencial ofrecer otras alternativas de ocio como jugar con amigos; realizar actividades conjuntas en familia que faciliten el diálogo y la relación, leer, hacer deporte; escuchar música, estar en contacto con la naturaleza, realizar algún tipo de arte o actividad creativa, campamentos.

– Jugar a videojuegos o navegar por Internet con ellos a la vez que comentar y criticar los contenidos favoreciendo la comunicación familiar.

– Ubicar la consola, plataforma u ordenador en un lugar común de la casa (aunque ahora internet está en los bolsillos).

– Pactar con anterioridad desde el diálogo qué momentos de la semana o del día se dedicarán a Internet y a jugar.

– Supervisar el contenido y lenguaje de los chats y si son nocivos deberán plantearse censurarlos. Igualmente es preciso controlar que el hijo no sea víctima de acoso y generar con él una relación de confianza para que ante una situación de riesgo lo cuente de manera inmediata y así poder actuar.

– Conocer las cuentas de correo que manejan los adolescentes y controlar sus correos electrónicos puede ser de interés para los padres, pero siempre cara a cara, los hijos también tienen derecho a su intimidad y han de ser conocedores de la obligada supervisión que ejercen sus padres por su propio bien y del hogar.

– Deben tutelar (velar por) a los menores para que éstos se suscriban a redes sociales acordes a su edad y con cierto control sobre la edad de acceso.

– Deben aclararles el uso correcto del móvil, no compartir imágenes suyas ni de sus amigos con otras personas, si reciben imágenes pornográficas o con agresiones entregárselas a sus padres o a la policía…

– Existe una clasificación por contenidos en cada juego (código pegi), para que los padres puedan supervisarlos y que los orientará sobre qué pueden encontrar en él.

– Hacer respetar el tiempo de juego, previamente pactado, para no caer en la adicción (pautar los tiempos).

– Lo más importante es que los padres vigilen el contenido de lo que sus hijos ven en la tele, de dónde navegan en Internet, de los juegos con los que se divierten o los que les prestan sus amigos. La mejor manera es sentarse con ellos, observar y darles una explicación de lo que no entiendan, así como del uso que deben dar a la información que encuentren. Enseñarles a utilizar la

tecnología de forma crítica. Para ello se precisa un alto grado de confianza (que hemos de ganar, respetando su intimidad pero con supervisión), una responsabilidad compartida, una autonomía propiciada y ello debe conformarse desde los primeros estadíos de la evolución de nuestros hijos.

- Seamos pedagógicos con los niños desde su propia motivación audiovisual.
- Disponemos de poco tiempo pero debe ser de calidad. Y educar en la responsabilidad.
- Eduquemos más a los padres (de hoy y de mañana).

— **Pautas y dinámicas para educadores**

- Reflexionar sobre las características del uso de las TIC. A través de una encuesta para Internet (frecuencia de la conexión, duración, objetivo de la misma, lugar de la conexión...). Sobre el móvil (llamadas diarias, mensajes diarios, llamadas más frecuentes, motivos de la llamada). Sobre los videojuegos: frecuencia de la conexión, duración de la misma, lugar de juego, número de jugadores. Sobre los juegos de rol on-line: frecuencia de la conexión, duración, lugar de juego, con quién juegan.
- Descubrir la proporción de adolescentes que hacen un mal uso de las TIC. A través de una encuesta sobre el abuso a las TIC y hacer una reflexión grupal sobre sus usos o abusos.
- Escenificar situaciones cotidianas en relación al abuso de las TIC.
- O del chico que juega con la consola y no hace caso cuando su madre le llama.
- Hacer un debate sobre la intimidad on-line. Crear una discusión entre dos alumnos porque uno de ellos ha colgado fotos indiscretas del otro en el Facebook y toda la clase las ha visto.
- Estudiar las abreviaturas, emoticones, construcción de frases en tres modalidades escritas: mensajes de texto, Whatssapp y correo electrónico.
- Encuestar sobre cómo pasan el tiempo libre (en casa y fuera). Comparar.

– Clasificar los videojuegos.

– Analizar un caso. Por ejemplo decidir qué harían si un niño ha bajado sus notas y rendimientos desde que sus padres le han comprado el ordenador y la conexión a Internet.

– Elaborar un catálogo de buenas prácticas y riesgos en el uso del móvil y videojuegos. Analizar anuncios, noticias sobre esto. Hacer una campaña de sensibilización en el colegio. (Promover el consumo responsable).

– Facilitar experiencias que ayuden a realizar un buen uso de la red, por ejemplo incorporar su uso en las asignaturas que deben buscar información o realizar iniciativas desde la tutoría y/o asignaturas donde el grupo ponga en marcha su propia web o su propia Intranet y crear un espacio virtual de comunicación entre ellos y el profesor y/o tutor.

– Analizar las ventajas, inconvenientes y riesgos del juego online.

Testimonios de padres sobre sus hijos y las nuevas tecnologías.

— **Chico 18 años que ha estado en Recurra (programa de padres e hijos en conflicto) y ahora se encuentra de seguimiento**: «*Otro conflicto es que en casa está todo y digo todo el tiempo en su habitación con el ordenador. Ve películas porno y tonterías diversas pero nada instructivo. Encima, si voy a hablarle, le interrumpo y se enfada. No le puedo hablar, bueno últimamente ni entrar en la habitación, todo y digo todo le molesta. Está intratable. Sólo cuando quiere algo y en el último momento se dirige a mi. Hay veces que se va o viene de casa y no me dice ni adiós ni hola. Como si estuviese en una pensión».*

— **Chico 15 años que actualmente está en Campus:** *«Todo esto ha hecho que la situación en casa sea «un infierno», no se puede tratar con él, y la mayoría del tiempo la pasa o durmiendo o jugando al ordenador».*

— **Chico 17 años que actualmente está en Campus:** *«J siempre ha sido buen estudiante y buen deportista hasta que comenzó a sufrir el acoso escolar; a raíz de ahí fue abandonando su interés en todo*

y en este momento lo único que realmente le interesa es todo lo que tiene que ver con la tecnología: ordenador, teléfono móvil, etc. No se despega de la pantalla».

— **Testimonio de un padre que ha tenido visita de su hijo que está ingresado en Campus (refleja como leen y vulneran la intimidad de los chicos***): «Por Wassaps se que no ha consumido aparentemente. El nivel de lenguaje de sus wassaps son más tranquilos que en los de hace 6 meses. Mucha adulación a niñas, y pasa suavemente por encima en los temas de alcohol y droga-porros (casi sin mencionarlos)».*

PD. Las familias están y se sienten solas, y se requiere por tanto el compromiso de toda la sociedad.

En ese sentido mi agradecimiento al Senado por concitar la aportación de la industria, de la Justicia, de los educadores, de las Fuerzas de Seguridad.

Y hablando de Fuerzas de Seguridad y en estos días en que el espionaje es un tema recurrente y sabedor de que me meto en un «ciber-garden» reincidimos en la necesidad de introducir la figura del «AGENTE ENCUBIERTO» para temas de pornografía infantil en internet (como existe para otros delitos). Este es un tema que ustedes en su día debatieron y acordaron pero del que no hay reflejo real.

¡Defender a los niños lo exige! Los delincuentes se organizan ¿y nosotros?

Fuentes y datos consultados

— (2009) «Hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres». Informe realizado por INTECO (Instituto Nacional de Tecnologías de la Comunicación).

— (2011) «Jóvenes y nuevas tecnologías» Informe realizado por INJUVE (Instituto de Juventud de España). Ministerio de Sanidad, Servicios Sociales e Igualdad.

— (2011) «Cyberbulling. Guía de recursos para centros educativos en casos de ciberacoso». Defensor del Menor de la Comunidad de Madrid.

— Programa recURRA-GINSO para padres e hijos en conflicto. Datos obtenidos entre 2011-2013, tanto en el ámbito ambulatorio como en el Campus Residencial «Campus Unido».

— URRA, J. (2011). **Mi hijo y las nuevas tecnologías**. Madrid: Pirámide.

— URRA, J. (2013). **Respuestas practicas para padres agobiados. Disfrutar educando.** Barcelona: Espasa.

COMPARECENCIA DEL VOCAL DEL CONSEJO ASESOR DE LA FEDERACIÓN DE ASOCIACIONES DE CONSUMIDORES Y USUARIOS DE LOS MEDIOS (ICMEDIA), DON JUAN MARÍA MARTÍNEZ OTERO, EN LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, CELEBRADA EL DÍA 4 DE NOVIEMBRE DE 2013.

1. *Presentación*

Buenas tardes. En primer lugar quería agradecer la posibilidad que se ha brindado a iCmedia de participar en este foro de discusión en torno a los riesgos del uso de la Red por parte de los menores. Para iCmedia es un honor poder participar en este debate, tan importante y necesario, sobre la protección que merecen nuestros jóvenes y niños en el entorno de Internet.

iCmedia es la Federación de Asociaciones de Consumidores y usuarios de los medios, que aglutina a 17 asociaciones y decenas de miles de asociados, preocupados por la creación de un entorno audiovisual respetuoso con los derechos de los ciudadanos, también de los más pequeños. Entre sus objetivos primordiales, la Federación busca:

1. Representar y defender los derechos de los consumidores y usuarios de los medios, actuando como interlocutor válido y reconocido ante las administraciones públicas, los demás actores de la industria audiovisual, y la opinión pública;
2. Promover una sociedad civil activa en el mercado audiovisual, capaz de tomar decisiones informadas y con sentido crítico en el ámbito audiovisual; capaz de reclamar el respeto de sus derechos; y capaz de intervenir en los procesos de toma de decisiones en cuanto a la oferta audiovisual;
3. Defender y promover la tutela efectiva de los derechos de los niños y los jóvenes en el ámbito de los medios y contenidos audiovisuales. En este sentido, iCmedia ha sido recientemente admitida como miembro de la Comisión Mixta de Seguimiento del Código de Autorregulación de Contenidos Televisivos e Infancia.

Por mi parte, imparto clases de Derecho de la Comunicación en la Universidad CEU - Cardenal Herrera, de Valencia, y he centrado mi tesis doctoral y mi investigación en la protección jurídica de los menores en el entorno de las nuevas tecnologías. Junto con mi labor docente, participo regularmente en charlas de sensibilización en colegios de la Comunitat Valenciana, con la finalidad de orientar a adolescentes sobre la necesidad de hacer un uso sensato de Internet.

Durante estas semanas he leído detenidamente las distintas aportaciones a esta Comisión. De las diferentes ponencias, así como de la doctrina más acreditada en la materia, pueden separarse tres grupos de riesgos para los menores en Internet: los riesgos derivados de contenidos nocivos, como puede ser la pornografía en Internet o videojuegos particularmente violentos; los riesgos derivados de contenidos y conductas ilegales, como la pornografía infantil o la vulneración de los derechos de los menores; y los riesgos derivados de un mal uso de Internet por parte de los menores, como las adicciones o el sexting.

De acuerdo con la naturaleza y los fines de iCmedia, me gustaría centrar la primera parte de mi intervención en el ámbito de los contenidos audiovisuales nocivos, a los que los menores pueden acceder a través de las nuevas formas de televisión online. Hasta el momento, parece que hablar de riesgos frente a la televisión y riesgos en Internet eran cuestiones diferentes. No obstante, el fenómeno de convergencia mediática al que asistimos está colmando la brecha entre ambos medios, y cada vez son más los contenidos audiovisuales que, en formato digital, se ofrecen a la audiencia a través de Internet. Por ello, pienso que junto con fenómenos como el sexting, el ciberbullying, la pornografía infantil, o el grooming, es importante prestar atención a los riesgos que se derivan de contenidos audiovisuales. La difusión de contenidos audiovisuales potencialmente nocivos para los menores a través del cine, del video, o de la televisión, ha estado sujeta a ciertos límites y cautelas para proteger a los más pequeños. Resultaría preocupante que en este momento, en que comienzan a estar disponibles para los menores en Internet, los poderes públicos dejaran sin protección a los menores y sin asistencia a los padres y tutores, bajo la premisa de que Internet es un mar sin orillas al que no puede ponerse

coto. Como se ha afirmado aquí en relación con otros riesgos en Internet, esa afirmación ciberlibertaria de la web es incompatible con el Estado de Derecho y con la protección de los derechos de los colectivos más débiles.

En la segunda parte de mi intervención, me ocuparé de dos riesgos derivados de la conducta irresponsable del propio menor, como son los riesgos de adicción y distracción de las nuevas tecnologías; y el fenómeno del sexting.

Respecto de los contenidos ilegales que pueden perjudicar a los menores de edad —pornografía infantil, mensajes xenófobos, grooming, vulneración del derecho a la intimidad o a la propia imagen del menor, etc.—, no aportaré comentario alguno, habida cuenta de la atención que se les ha prestado en otras intervenciones.

2. *Riesgos derivados de contenidos nocivos*

Los contenidos nocivos a los que los menores se enfrentan en Internet son mensajes e imágenes que, estando protegidos por la libertad de expresión, pueden generar un perjuicio físico, mental o moral a los más pequeños —empleando la terminología tan repetida por las instituciones comunitarias. Se trata de contenidos, por ejemplo, relacionados con la pornografía, la violencia, el tabaco, el alcohol, las drogas, las paraciencias, las apuestas, etc. Respecto de estos contenidos, los usuarios nos debatimos entre dos grandes tendencias: los del grupo «protégeme» —aquellos que esperan que los proveedores no pongan o no puedan poner en la Red contenidos que sean percibidos como nocivos —y los del grupo «infórmame»— los que prefieren disponer de información adecuada y herramientas de control que les permitan ser ellos mismos quienes ejerzan el control.

A continuación, nos referiremos a dos grupos de contenidos nocivos, y a la respuesta que, desde nuestro punto de vista, deberían ofrecer los poderes públicos. En primer lugar, abordaremos los contenidos nocivos ofrecidos como actividad comercial por un programador que ofrece determinados contenidos audiovisuales a su audiencia. Estos servicios de contenido audiovisual —conformados por un catálogo de contenidos que

se ofrecen al espectador de forma más o menos ordenada, como contraprestación a una cantidad de dinero—, en ocasiones se prestan a través de Internet, por lo que no es extemporáneo referirnos a ellos aquí. Este tipo de servicios, llamados video a la carta, televisión en movilidad, etc., son asimilables a la televisión, y les resulta de aplicación la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual (LGCA). En segundo lugar, haremos unas reflexiones sobre la accesibilidad de pornografía en Internet, problema que ha preocupado y ocupado a diferentes Gobiernos, desde la administración Clinton en los albores de Internet, hasta la administración Cameron, en fechas mucho más recientes.

a. Contenidos audiovisuales - Nuevas modalidades de televisión a través de Internet

Dentro del universo de contenidos potencialmente nocivos en Internet —imágenes, videos caseros, páginas web— nos centraremos en primer lugar en los contenidos audiovisuales ofrecidos por un responsable de la línea editorial o programador. Estamos por lo tanto ante servicios muy similares a la televisión tradicional, siendo las principales diferencias que estos servicios se ofrecen a través de la Red y que el usuario tiene un mayor margen de decisión en cuanto al momento en el que ver el contenido.

Tres son los motivos que ponen esta cuestión en un primer plano:

En primer lugar, las principales estimaciones sobre consumo televisivo y convergencia mediática apuntan que en menos de un lustro la mayoría de los hogares estarán equipados con una televisión híbrida, que combinará contenidos lineales con contenidos a los que se accede a través de Internet. En este escenario, resulta imprescindible que los poderes públicos se planteen la forma en la que los menores de edad van a ser protegidos frente a este universo de contenidos que tendrán a su disposición en las pantallas de su hogar[1]. El modelo de protección de los me-

[1] Según datos recogidos en el Libro Verde de la Comisión Europea sobre la convergencia del mundo audiovisual (Prepararse para la convergencia plena del mundo audiovisual: crecimiento, creación y valores. Libro Verde. Bruselas, 24.04.2013 COM

nores frente a los contenidos audiovisuales en la televisión, como se ha venido entendiendo desde la década de los años 80, pronto va a quedarse obsoleto, y necesita una urgente reformulación, que incluya la regulación de los contenidos ofrecidos a través de Internet.

En segundo lugar, los datos de audiencia y consumo muestran que los contenidos audiovisuales siguen siendo los más demandados, utilizados y descargados por parte de los menores. Paulatinamente, dicho consumo abandona el soporte tradicional de la televisión y se sitúa en otras pantallas, fundamentalmente las de los teléfonos móviles. Pero gran parte de los contenidos son programas de televisión, series de entretenimiento y películas[2].

En tercer lugar, el sector de la regulación audiovisual en España atraviesa un momento delicado, lleno de asignaturas pendientes e incertidumbres. Por un lado, todavía no se ha terminado de desarrollar y aplicar la LGCA en materia de protección de menores: aún están pendientes la implantación de las guías electrónicas de programación, el desarrollo de los sistemas de control parental, y la revisión y unificación de los criterios de clasificación de contenidos. Por otro lado, en ausencia del CEMA, la SETSI ha sido sustituida por la reciente Comisión Nacional de los Mercados y la Competencia, y estamos a la espera de conocer su grado de compromiso con la causa de la protección de los menores. En este panorama surgen nuevas modalidades de acceso a contenidos audiovisuales a través de las pantallas del televisor (catch-up tv, tv over the top, y televisión híbrida o conectada), a las que la regulación nacional está llamada a dar respuesta. Esta encrucijada de la regulación audiovisual española exige de los poderes públicos una respuesta decidida

---

(2013) 231 final), se espera que la mayoría de los hogares europeos estén equipados con televisores conectables a internet de aquí a 2016. Para 2017, según previsiones de Informa Telecom & Media, el 31% de los hogares de todo el mundo contarán con televisión conectada.

[2] Entre otros, resultan interesantes los datos ofrecidos por: «Zero to Eight: Children's Media Use in America 2013», octubre de 2013. Disponible en: http://www.commonsensemedia.org/zero-to-eight-2013-infographic?utm_source=131029_infographic&utm_medium=email&utm_campaign=weekly

y creativa, que permita mantener en el nuevo contexto el respeto a los principios irrenunciables de nuestro entorno audiovisual: el pluralismo comunicativo, la diversidad cultural, y el respeto a los derechos de la audiencia, en particular los de los públicos más vulnerables: los niños.

¿Cómo vamos a proteger a los menores frente a los contenidos nocivos de estas nuevas formas de televisión? ¿Tiene sentido seguir hablando de la protección de los menores en la televisión y no referirse a los contenidos ofrecidos a través de Internet? ¿A qué servicios de Internet puede aplicarse la LGCA, y exigirles el respeto a los derechos de los menores? ¿A las TV en Internet? ¿A portales que ofrecen catálogos de vídeos previamente seleccionados por el editor? ¿Debe tener la CNMC competencia para sancionar a estos prestadores de servicios a través de Internet, en la medida en que ofrecen contenidos audiovisuales asimilables a la televisión tradicional? Desde iCmedia denunciamos que este debate, abierto tanto a nivel comunitario como en otros países, como Reino Unido o Francia, en nuestro país está siendo esquivado. La complejidad de la cuestión y la escasez de medios no eximen a los poderes públicos de una reflexión profunda, seguida de una toma de medidas adecuadas. Lo contrario, la pasividad que se observa hasta la fecha, sólo redunda en un entorno audiovisual anárquico, en el que prima la ley del mercado y el beneficio, muchas veces en perjuicio de los derechos de los más pequeños.

Desde iCmedia venimos insistiendo en la urgencia de desarrollar las previsiones de la LGCA en algunos aspectos, muchos de los cuales tienen también su aplicación respecto de los contenidos ofrecidos por la televisión en Internet:

– Reflexión sobre qué prestadores de contenidos audiovisuales online han de quedar sujetos a las LGCA. Empresas que comercializan series o películas; videoclubs online, televisión en Internet; portales de diarios que ofrecen vídeos previamente seleccionados sobre diferentes cuestiones. En los distintos países de la UE se están ensayando soluciones y respuestas a esta cuestión, mientras que en España hasta la fecha, como ya hemos subrayado, se viene orillando este debate.

– Clarificación y unificación de los criterios y procedimientos de calificación de los contenidos audiovisuales. A día de hoy, coexisten diferentes sistemas de clasificación. Sería interesante que la CNMC aprobara unas pautas de calificación que se aplicaran a todos los productos audiovisuales —también a los ofrecidos en línea—, con la finalidad de ayudar a los padres a tomar decisiones libres e informadas sobre la dieta audiovisual de los menores a su cargo.

– Definición y puesta en marcha de una política específica en materia de etiquetado digital de contenidos audiovisuales. Este etiquetado puede funcionar tanto para los filtros de la TDT como para los filtros de contenidos en Internet.

– Revisión del código de autorregulación sobre contenidos televisivos e infancia de 2004, y de los mecanismos de control de su aplicación. Como es sabido, el Código Autorregulador de 2004 es uno de los paradigmas de código cosmético e ineficaz. Si bien parece que en el último año se está relanzando su efectividad, todavía es preciso un compromiso más decidido para convertirlo en un verdadero instrumento de protección de los menores.

– Definición y puesta en marcha de normativa relativa a las obligaciones de información de los proveedores de servicios de comunicación audiovisual sobre los contenidos de la programación (Guías Electrónicas de Programación y servicios de información en internet).

– Exigencia, desarrollo y promoción de sistemas y dispositivos de control parental sobre los contenidos de los servicios de comunicación audiovisual. La brecha generacional y el analfabetismo audiovisual de algunos padres precisa de la creatividad de la industria para ir, progresivamente, educando a los padres en el uso de las herramientas de control parental.

Como puede colegirse, estas seis líneas de actuación son válidas para proteger a los menores frente a los contenidos nocivos en la televisión tradicional, pero también en los servicios homologables a la televisión

prestados a través de Internet. Para hacer efectiva esta protección, resulta fundamental que los prestadores de los servicios clasifiquen y etiqueten debida y uniformemente sus productos audiovisuales. Gracias a esta información, y ayudados por los filtros y otros sistemas de control parental, los padres podrán tomar las decisiones oportunas en relación con la dieta audiovisual de sus hijos. Se trata, así, de un sistema cuya responsabilidad es compartida: el responsable de los contenidos debe clasificarlos y etiquetarlos —control en origen—; y el padre o tutor debe decidir qué contenidos son accesibles desde los dispositivos de su hogar —control en destino—.

Al poder público corresponde esclarecer por vía legal y reglamentaria a quién se aplican las previsiones de la LGCA, establecer las condiciones básicas para la clasificación y señalización de los contenidos, y exigir el respeto de todo el aparato normativo por la vía administrativa y judicial.

Poderes públicos, industria y padres tienen así un papel determinante que desempeñar. Escudarse en la dificultad del paisaje mediático para no asumir las propias responsabilidades puede resultar cómodo, pero supone una traición omisiva al derecho de niños y jóvenes al correcto desarrollo de su personalidad.

b. La disponibilidad de pornografía online

Un segundo capítulo dentro de los contenidos nocivos es el de la pornografía en Internet y su enorme accesibilidad a los menores de edad. Esta cuestión ha sido puesta sobre la mesa este verano por el primer ministro británico Cameron, que ha planteado la posibilidad de restringir por defecto el acceso a contenidos pornográficos en los navegadores, y exigir a quien quiera consumir pornografía que haga una comunicación en este sentido a su proveedor de Internet. Gran parte de la opinión pública británica y mundial se ha apresurado a tachar a Cameron de censor e inquisidor, erigiéndose en defensores de la libertad de expresión en Internet.

Que la pornografía es un contenido puede perjudicar seriamente el correcto desarrollo de la personalidad de un menor no es una afirmación personal o gratuita, sino una premisa de la regulación europea y española

sobre los contenidos audiovisuales, como leemos literalmente en la Directiva de Servicios de Medios Audiovisuales de la Unión Europea o en nuestra LGCA (art. 12 y 7.2º respectivamente). En esta premisa —avalada por sentencias del TEDH y del TC— se asientan también numerosas medidas legales en relación con los contenidos televisivos, las películas X, los sex-shops, la publicidad de ciertos servicios, y un largo etcétera.

Resulta innegable que el acceso a la pornografía en Internet es enormemente fácil. Los datos de tráfico de estas páginas son enormes, sólo superados por servicios de correo electrónico y redes sociales. Estos contenidos pornográficos son consumidos de forma generalizada por adolescentes, principalmente varones.

¿No podemos hacer nada más para restringir el acceso a la pornografía online a los menores, como hacemos en otros medios de comunicación? Frente a esta pregunta, la administración Clinton, poco sospechosa de tabúes religiosos o morales, a la hora de regular Internet intentó por dos veces asemejar su régimen al de la televisión, para restringir los contenidos nocivos para los menores. Ambas normas fueron declaradas inconstitucionales por el Tribunal Supremo norteamericano, en base a dos motivos. En primer lugar, el TS sostuvo que la pornografía es un tipo de comunicación amparado por la libertad de expresión. Y, en segundo lugar, afirmó que Internet es un medio de comunicación más parecido a la prensa escrita que a la televisión, por lo que la intervención y regulación estatal en Internet debe reducirse a su mínima expresión. Esta asimilación de Internet a la prensa escrita se asentó en un doble argumento: en Internet no hay escasez de espectro; y en Internet los usuarios buscan activamente los contenidos, que no aparecen en su cuarto de estar, como sucede en el caso de la televisión.

Esta argumentación, que ha sido seguida por las regulaciones de los países europeos, resulta razonable, no hay duda. Pero desde el momento en que el acceso a Internet es casi omnipresente; desde que los menores llevan Internet en el móvil; desde que para hacer los deberes muchas veces tienen que estar conectados a Internet. desde que todo esto sucede, parece que es oportuno establecer algunas barreras a la pornografía online. Internet es el entorno en el que conviven y se mueven los menores.

Igual que en el entorno offline hemos prohibido la publicidad de películas X, la pornografía en abierto en televisión, el acceso de menores a determinados espectáculos o locales, o el ofrecimiento de pornografía a los menores, parece razonable que empecemos a implantar medidas similares en el entorno online.

Si estas medidas van en la línea señalada por Cameron —quien quiera pornografía que la autorice expresamente a su proveedor—, o en otra línea, no lo sé. Lo que sí que creo es que es preciso orquestar formas efectivas de restringir el acceso a estos contenidos, que, como dice la normativa europea, pueden resultar gravemente perjudiciales para el desarrollo físico, psíquico y moral de los jóvenes. Ignorar esta cuestión y permitir la oferta de pornografía a un solo click supone dejar a los menores desamparados ante unas solicitaciones y contenidos que no están preparados para resistir.

3. *Riesgos derivados de las conductas del menor*

Los riesgos a los que el menor de edad se enfrenta en su relación con Internet y las nuevas tecnologías no provienen tan sólo del exterior, de amenazas externas derivadas de contenidos nocivos o ilegales. Efectivamente, en ocasiones es el propio menor quien, debido a su inexperiencia, hace un uso inconsciente o poco maduro de las nuevas tecnologías, generando consecuencias que se vuelven contra él mismo. En este vasto campo, centraremos nuestra atención en dos riesgos: el riesgo de distracción permanente y de adicción a las nuevas tecnologías; y el fenómeno del sexting, de reciente aparición, que se está extendiendo de manera preocupante entre las capas jóvenes y adolescentes de nuestra sociedad.

a. Distracciones y adicciones

Quizá el primer riesgo al que los menores se enfrentan en el entorno de Internet —y que en ocasiones es poco subrayado— es el riesgo de la distracción permanente. Internet tiene una fuerza de atracción muy alta, y muchos menores viven totalmente pendientes de su vida online.

Esta atención desmedida a la Red puede generar verdaderas adicciones. Si repasamos algunos de los síntomas de una adicción, veremos que se producen también en Internet: «me siento mal cuando pasan horas sin poder conectarme», «discuto con mis padres y hermanos por conectarme a Internet», «me conecto durante horas sin haberlo previsto», «dejo de hacer otras cosas que me gustan por estar conectado». Internet, no es posible negarlo, puede llegar a ser adictivo, y es preciso alertar a los educadores sobre este particular. Sin adoptar tintes tan dramáticos, resulta evidente que un uso intemperante de Internet genera problemas en los menores y su entorno familiar: distracciones en el estudio, descenso del rendimiento escolar, faltas de educación en las relaciones, aislamiento, creación de identidades digitales falsas, maltrato del lenguaje, etc. En mi contacto en colegios con padres y adolescentes, pienso que esta es la cuestión que más preocupa a los educadores, ya que tiene una incidencia casi universal en la población adolescente. Otros problemas —bullying, sexting, etc.—, sin quitar un ápice a su gravedad, afectan a porcentajes pequeños de la sociedad. El riesgo de adicción, por el contrario, afecta a la inmensa mayoría de los adolescentes. Por lo que he podido consultar en la web del Senado, respecto de otras intervenciones en este foro, tan solo Salomé Adroher, directora general de servicios para la familia y la infancia, se detuvo a mencionar este riesgo para los más pequeños.

Frente a una visión algo adanista o ingenua de Internet —en la que en ocasiones personas adultas caen para no parecer anticuadas—, es preciso reivindicar que Internet no es bueno para todo. Por ejemplo, no es bueno para hacer deberes. No es bueno para fomentar en los chicos y chicas hábitos de reflexión. No es bueno para fomentar su capacidad de concentración o el pensamiento profundo. No es bueno para fomentar su hábito a la lectura. No es bueno para potenciar su memoria. En un estudio relativamente reciente, titulado: «Superficiales, ¿qué está haciendo Internet con nuestras mentes?», el periodista norteamericano Nicholas Carr, apoyado en estudios sociológicos y neurológicos, llega a una conclusión descorazonadora: Internet, por sus peculiaridades características, nos vuelve superficiales, o, en palabras de Carr, nos vuelve estúpidos. Como ejemplo de su discurso, es ilustradora la denominación que Carr le da a las nuevas tecnologías: «las nuevas tecnologías de la interrupción».

El discurso unidireccional de loa de Internet suele ignorar estos peligros, verdaderos riesgos para los menores de edad. McLuhan alertó hace décadas de que el medio es el mensaje, máxima que en Internet —con su hipertexto, su velocidad, su fragmentación— se hace particularmente cierta. Es preciso aprovechar sus ventajas, pero alertando a los educadores de los riesgos que la herramienta lleva consigo. La semana pasada la Asociación Americana de Pediatría ha hecho públicas unas recomendaciones para fomentar un uso saludable de las herramientas digitales por parte de los niños. En las mismas, se hace hincapié en la importancia de establecer normas claras de uso de las tecnologías, para garantizar aspectos como la capacidad de concentración del menor, su adecuada alimentación o el correcto desarrollo de sus ciclos de sueño[3]. En esta misma línea, el Departamento de Salud del gobierno británico publicó un informe en agosto de año en el que señalaba que los menores que dedican mucho tiempo a la televisión, los videojuegos e Internet son más proclives a tener una baja autoestima, y a padecer ansiedad y depresión[4]. Las advertencias frente a estos riesgos no provienen de ciberreaccionarios, nostálgicos del libro en papel y de la pizarra de tiza, sino de instituciones sanitarias y pediátricas de países altamente desarrollados.

Para afrontar este riesgo, a nivel internacional ya se están promoviendo iniciativas para fomentar un uso saludable y maduro de los avances digitales. Igual que se promueven hábitos alimenticios o educación vial, resultaría oportuno ir extendiendo en nuestro país los cursos de «defensa personal frente a las nuevas tecnologías», o las «dietas de adelgazamiento digital».

b. El sexting

El sexting consiste en el envío a través del teléfono móvil o el mail —casi siempre a través del whatsapp— de mensajes eróticos o pornográ-

[3] «Managing Media: We need a plan», octubre de 2013. Disponible en: http://www.aap.org/en-us/about-the-aap/aap-press-room/pages/Managing-Media-We-Need-a- Plan.aspx#sthash.gaWL2Ahg.dpuf

[4] «Sedentary lifestyles and too much screen time affect children's wellbeing», agosto de 2013. Disponible en: https://www.gov.uk/government/news/sedentary-lifestyles-and-too-much-screen-time-affect-childrens-wellbeing

ficos de producción casera, protagonizados por el emisor inicial. Aunque es pronto para hablar de su nivel de incidencia, los primeros estudios en Estados Unidos hablan de un 10% de menores de edad que lo han practicado. Un estudio británico publicado en octubre de 2013 afirma que más de la mitad de los menores británicos han sido invitados por sus compañeros o amigos a enviar este tipo de mensajes de carácter sexual y producción casera.

La aparición del sexting no debe causar extrañeza. En su propagación, inciden evidentemente varios factores ampliamente conocidos: la omnipresencia de dispositivos para captar imágenes; una cierta erotización de la adolescencia; la falta de cultura de la intimidad; y la necesidad de estar permanentemente conectados. Si estos factores se añaden ciertas dosis de gamberrismo y aburrimiento —tan propias del período adolescente—, la extensión del sexting está asegurada.

La práctica del sexting, tanto entre adultos como entre adolescentes, comporta unos riesgos evidentes. Quien lo practica pone en manos de un tercero material muy sensible, que puede copiarse y distribuirse sin ningún coste ni esfuerzo. Además, las relaciones en las que se enmarca el sexting, las de pareja, son por definición frágiles, y muchas veces concluyen en términos poco amistosos. Por ello, una vez concluida una relación, no resulta difícil que una de las partes, por despecho, venganza o aburrimiento, distribuya las imágenes entre amigos y conocidos. Es lo que en Estados Unidos se llama «porn revenge». Es entonces cuando surgen los problemas.

¿Qué debe hacer el Derecho frente al sexting?

En mi opinión, en el sexting entre adultos, castigar civilmente a quien difunda sexting ajeno sin permiso. Actualmente está en fase parlamentaria una reforma del Código Penal que incluye como delito la difusión de este tipo de mensajes sin permiso de su emisor primero y protagonista. Cabe preguntarse si la sede penal es la más oportuna para proteger el derecho a la intimidad de una persona que ha expuesto su intimidad de modo voluntario a un tercero. Quien practica sexting —siempre entre mayores de edad—, debe asumir los riesgos que libremente asume, máxime si se trata de riesgos perfectamente previsibles. El Derecho Penal no es el

medio más apropiado para proteger la inconsciencia de las personas. En mi opinión, más que dar soluciones paternalistas al problema del sexting, es preciso formar a la gente en una cultura de la responsabilidad online. La difusión de imágenes de sexting ajeno sin consentimiento del protagonista debería castigarse por la vía civil.

¿Qué sucede cuando el sexting está protagonizado por menores de edad? Las respuestas aquí resultan más complejas.

Su mera práctica, aunque las imágenes no sean difundidas más allá del ámbito consentido por su protagonista, ya plantea algunos problemas jurídicos. La persona que lo emite, si es la protagonista, está produciendo y emitiendo pornografía infantil conforme a las previsiones del Código Penal (art. 189). Quizá, al tratarse de un caso de autolesión, no quede vulnerado el bien jurídico protegido, la indemnidad sexual del menor. Pero. ¿y si hay un tercero en las imágenes? Además, quien envía ese contenido está difundiendo pornografía a otro menor, lo que también constituye un delito de ofrecimiento de pornografía a menores (art. 186 CP). No son pocos los adolescentes que han recibido, sin ninguna solicitud por su parte, imágenes pornográficas de otro compañero de clase. En tercer lugar, no debemos olvidar que la mera posesión de esas imágenes ya constituye un delito de mera posesión de pornografía infantil (art. 189 CP). Un elemento que ayudaría a esclarecer el panorama jurídico es la inclusión en algunos de estos tipos penales de una cláusula eximente en caso de simetría de edades entre los implicados, como ya viene interpretando la fiscalía de menores para los delitos de pornografía infantil. Cuando los implicados en el sexting son de edades similares, la reprochabilidad de la conducta es menor que cuando uno de ellos es mucho mayor que el otro, cuestión que daría entrada a un abuso de poder y nos permitiría hablar propiamente de pornografía infantil.

¿Qué responsabilidad tiene el menor que emite sexting? En la medida en que envía contenido pornográfico a otro menor, podríamos estar ante un delito de ofrecimiento de pornografía a menores (art. 186 CP). Si el menor receptor ha solicitado el contenido, en ese caso la responsabilidad debe quedar eliminada o atemperada. Cuando el receptor no lo ha solicitado, castigar penalmente el envío resulta exagerado. Quizá pueda

exigirse una pequeña indemnización por la vía civil, o exigirse al responsable determinados trabajos sociales o educativos. Se trataría de una medida educativa orientada a minimizar este tipo de conductas.

¿Y qué decir del menor que distribuye el mensaje sin permiso del emisor inicial, una vez lo ha recibido? ¿Podemos acusarle de difundir pornografía infantil (art. 189 CP)? ¿De distribución de sexting ajeno sin permiso (nuevo artículo 197.4º.bis CP)? ¿De un ilícito civil contra los derechos a la intimidad y a la propia imagen ajenas (art. 7 Ley Orgánica 1/1982)? Considero que habría que castigarle penalmente sólo en caso de que éste persiga de modo doloso una humillación grave del protagonista; en el resto de casos, motivados por la simple curiosidad o generados por la falta de cuidado, tan propios de la adolescencia, resultaría suficiente una sanción estrictamente civil. Y ello considerando que, en estos casos, gran parte de la responsabilidad del daño producido es culpa de la propia víctima, que difunde sus imágenes sin percibir el daño que las mismas le pueden causar. Cuando sea un mayor de edad quien difunde las imágenes —teniendo en mente la cuestión de la asimetría de edades—, sí que podrá incurrir en responsabilidad penal.

Por mi parte, es todo. Sé que he dejado muchas cuestiones sin abordar, como la protección de los derechos a la intimidad y la propia imagen de los menores en las redes sociales, la lucha contra la pornografía infantil, la cesión de datos personales de los menores, y un largo etcétera. Para centrar la exposición, he preferido centrar el discurso en cuatro puntos. Dos puntos relativos a los contenidos nocivos: la regulación de los contenidos audiovisuales en la televisión online, y la disponibilidad de pornografía en Internet; y dos puntos referentes a los riesgos derivados de la propia conducta del menor en Internet: la adicción a las nuevas tecnologías, y la compleja cuestión del sexting.

Muchas gracias por su atención, y quedo a su disposición para aquellas preguntas o reflexiones que tengan a bien plantearme.

COMPARECENCIA DEL SOCIO DIRECTOR DE S2 GRUPO, D. JOSÉ MIGUEL ROSELL TEJADA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 4 DE NOVIEMBRE DE 2013.

El señor **SOCIO DIRECTOR DE S2 GRUPO** (D. José Miguel Rosell Tejada): Mientras tanto, ante todo muchas gracias por invitarme a compartir con ustedes lo que sé sobre este tema, que seguro que con el tiempo que llevan ustedes ya estudiando todo esto, mucha más información e incluso muchos más datos van a tener ustedes en algunos sentidos.

Yo voy a cambiar un poco el tercio respecto al anterior ponente. Soy técnico, soy ingeniero, no soy abogado, y por tanto no voy a hablar de leyes, voy a darles un punto de vista técnico de una empresa, como verán, que se dedica a trabajar en los temas de seguridad y ciberseguridad. Para lo cual, como técnico que soy, voy a hacer uso de los medios que tengo, que me han puesto ustedes a mi disposición, y voy a utilizar una presentación que me va a permitir enseñarles incluso algunas cosas que yo creo que son interesantes y que pueden ser de su interés.

Para empezar, quiero empezar con una idea que voy a repetir varias veces a lo largo de la ponencia: y es que yo creo que el tema sobre el que estamos hablando, la situación de riesgo de los jóvenes no es el problema, para mí es una consecuencia. El problema en realidad somos nosotros. El problema es que falta una cultura en la sociedad sobre temas de ciberseguridad, digamos que falta una cultura mínima básica. Y el problema por tanto, como bien digo o como creo, somos nosotros y no los menores.

En cualquier caso, permítanme que les dé dos *flashes* de quién soy y a quién represento. Como les decía, soy director general de una empresa de seguridad, aparte de ser padre de dos niñas y de haberme, si me permiten la expresión, comido este problema durante los últimos seis o siete años en primera persona, y por tanto hablo como experto en la materia desde un punto de vista técnico y como padre de dos hijas que son usuarias intensivas de las redes sociales.

S2 Grupo es una empresa técnica especializada en temas de ciberseguridad; no tocamos la seguridad física, solo temas de seguridad desde

el punto de vista informático o tecnológico. Somos una empresa de unas 115 personas que actualmente estamos trabajando en distintas áreas para nuestros clientes, fundamentalmente en tres líneas de negocio, para que sepan ustedes de qué es de lo que puedo saber y de qué no. Trabajamos en proyectos de consultoría y auditoría para clientes, sobre todo para cuentas de tamaño medio y grande, que son las que en este momento están desarrollando mucho trabajo en materia de ciberseguridad. Tenemos un centro de servicios que presta servicio a nuestros clientes en formato 24 x 7, vigilando sus negocios y sus redes. Y además estamos desarrollando desde hace ya varios años productos de tecnología nacional para implantar en los clientes en los que estamos trabajando.

Evidentemente, no solo por eso creo que estamos aquí. Realmente nosotros estamos aquí porque desde hace ya algunos años (por ejemplo, la semana pasada nos dio el distintivo de igualdad la ministra de Sanidad), al margen de haber hecho determinado tipo de cosas internas en materia de responsabilidad social, llevamos mucho tiempo trabajando (por una historia que luego les contaré) en temas de seguridad y menores. Y en los temas, digamos, sociales hemos invertido mucho tiempo y mucha imaginación, como luego verán, en ver qué es lo que podíamos nosotros hacer para intentar poner nuestro granito de arena a la hora de resolver este problema.

Por este motivo pienso que el tema de la ponencia, estudio sobre los riesgos derivados del uso de la red por parte de menores, es un tema que a mí particularmente y a nuestra empresa nos es familiar; hemos trabajado mucho, como verán, en todo ello. Y me gustaría empezar con una frase del señor Churchill, de Winston Churchill, que siempre me ha llamado mucho la atención, que pronunció en un discurso en la Cámara de los Comunes en el año 1943, hablando de la reconstrucción de algunos edificios emblemáticos de Londres, y decía: «Nosotros damos forma a nuestros edificios y después nuestros edificios nos dan forma a nosotros». Es una frase que a la hora de hablar de la red y de lo que estamos viviendo ahora, de la sociedad en la que estamos viviendo ahora, es perfectamente válida. De hecho, nosotros en el año 1969 vimos el nacimiento de lo que fue en aquel momento ARPANET en unas universidades americanas, con la comunicación de cuatro ordenadores (estamos hablando del año 1969). Del año 1969 en adelante, la verdad es que la evolución fue muy lenta. Fueron pasando algunas cosas significativas; por ejemplo, William Gibson, en el año 1981 acuñó el término «ciberespacio» en una novela

que se llamaba *Johnny Mnemonic*, muy interesante sobre todo para entender la evolución de Internet o del ciberespacio fundamentalmente.

En el año 1983 vivimos el nacimiento de verdad de Internet, cuando se cambió de tecnología de comunicaciones antigua a lo que hoy es TCP, con lo cual en el año 1983, el 1 de enero de 1983 es cuando se data realmente el nacimiento de Internet tal y como lo conocemos.

A partir de ahí en el año 1984, otra vez el señor William Gibson, en una novela bastante famosa de ciencia ficción que se llama *Neuromante*, fue donde popularizó el término «ciberespacio». En la década de los noventa hubo una fiebre generalizada por subir todos los servicios, todo a la red, que acabó con el estallido de la burbuja de las .com en el año 2000. Evidentemente, en el camino quedaron muchas cosas, quedó mucha infraestructura instalada, mucha infraestructura para navegar a alta velocidad, y quedaron también empresas como Amazon, que no creo que necesiten ninguna presentación.

A partir de ahí, en el año 2004 se creó la primera gran red social, Facebook. Y a partir de 2004, yo creo que la historia ya la conocen ustedes: una locura de redes sociales, de medios, de contenidos en Internet, a través de LinkedIn, de Twitter, de YouTube, de Picasa, un montón de medios disponibles para todas las personas, incluidos los menores, que se han desarrollado en los últimos años.

Bien, al final de todo esto lo que tenemos es el concepto de ciberespacio que el señor Gibson acuñó de una forma, digamos, un poco etérea, que ha ido tomando forma con el nacimiento de Internet y con el desarrollo de las redes sociales. Hasta el punto de que en este momento, en el año 2013, lo hemos conectado todo a Internet, y cuando digo todo es todo, todo o casi todo; estamos en proceso de conexión de todo. En este momento hay quien dice también que si antaño la frontera de las redes eran las máquinas, en este momento hay quien dice que las personas somos el nuevo perímetro. Y el perímetro es lo más accesible, y por tanto lo más vulnerable en determinadas circunstancias.

Aquí quiero ponerles un pequeño ejemplo de un caso. Insisto, somos una empresa técnica, y como tal abordamos la auditoría de muchos equipos, de muchos elementos que tenemos en nuestras casas. Últimamente está de moda, con todos los temas de la eficiencia energética, poner unos cacharritos en casa que son unos cacharritos domóticos que se dedican a analizar el consumo energético y que nosotros desde un móvil podemos

acceder a él y podemos ver el consumo energético de nuestra casa, con el fin de apagar una lavadora o lo que sea. Estos cacharros, que aparentemente son inocuos, realmente cuando analizas un poco la seguridad de los dispositivos, te das cuenta de que realmente lo que son es un agujero de seguridad de cara al acceso a las propias redes. No se han preocupado en diseñar estos dispositivos teniendo en cuenta la seguridad de los mismos, con lo cual al final, claro, la gente te dice «¿y quién va a querer saber la información del consumo de mi casa?». Bueno, realmente la gente que piensa mal, el consumo de una casa yo lo puedo querer saber porque quiero saber cuando una persona está o no en casa, incluso patrones de salida de casa. O incluso, este aparatito que aparentemente es un aparato que me da información de mi consumo energético, realmente lo que acaba dándome es acceso a una red donde hay niños, donde hay personas, donde hay cámaras, donde hay dispositivos dentro de una red interna y mediante los cuales yo puedo obtener información de la familia, de la casa, etc.

Yo he analizado un poco toda la información que han tenido ustedes en las comparecencias anteriores, y me he quedado sobre todo (aparte de un montón de datos que no voy a repetir, y de hecho van a ver que no voy a entrar en estadísticas sobre el uso de la red por parte de menores, porque creo que ya tienen ustedes información suficiente) con dos datos: uno, una frase citada por el director general de la policía, Ignacio Cosidó, que dijo que básicamente ninguna tipología delictiva está creciendo al ritmo al que lo está haciendo la ciberdelincuencia, que además coincide con la introducción de la Estrategia Europea de Ciberseguridad, que viene a decir lo mismo. Y otro es el trabajo excepcional que está haciendo la policía (esto es capturado de hace un par de días) con 637.000 seguidores en el Twitter de la policía, y que incido no en el uso del canal (por lo menos en nuestra empresa tenemos varios canales de Twitter), sino en el cómo lo están haciendo. Es decir, cómo el uso de un canal como el que está utilizando la Policía Nacional, con poca inversión, con poco coste, puede tener la repercusión que está teniendo. Con lo cual incidiré después otra vez en el cómo más que en el qué, cómo vamos a hacer las cosas o cómo podemos hacer las cosas.

En definitiva, lo que en mi opinión es evidente es que tenemos un problema, un problema importante cuyo origen no está en los jóvenes, está en la sociedad. Y sobre esto, insisto, repetiré.

He dicho que no les voy a dar datos de los menores, y no lo voy a hacer. Lo que sí voy a darles es datos de la sociedad en general y algunos

—desde aquí, yo soy incapaz de leer, pero creo recordar más o menos lo que pone—, en algún caso, en el primero (esto es de la Estrategia Europea de Ciberseguridad) dice que hay aproximadamente un millón de víctimas diarias de ciberdelitos; el 12% de los usuarios de Internet ha tenido alguna experiencia de fraude *online*; si tenemos 2.000 millones de usuarios, estamos hablando de 240 millones de personas que han sufrido el fraude *online* en los últimos años; el 74% de los usuarios cree que se ha incrementado el riesgo de ser víctima de un ciberdelito. En España —muy importante— el 71% de los ciudadanos no se siente informado (por ejemplo, en Europa es el 59% los que dicen que creen que no tienen información). Importante desde el punto de vista empresarial, y doy fe de ello, el 56,8% de las empresas declara haber tenido algún incidente relacionado con temas de ciberseguridad. Los incidentes de ciberseguridad aumentan en frecuencia y magnitud, y son cada vez más complejos y no tienen fronteras, Cada día hay 150.000 virus en circulación y 148.000 ordenadores son infectados; y según el Foro Económico Mundial, hay entre un 10% y un 20% de probabilidad de que se interrumpan sistemas críticos de información en los próximos diez años, con pérdidas que yo ya no sé si son 250.000 millones de dólares o cuánto es. Lo que quiero decir con esto es que sí, hay muchas cifras sobre los problemas que tienen los menores, y otro montón de ellas sobre los problemas que tenemos como sociedad los adultos y la sociedad en general.

Con lo cual, ¿cuál es la situación? Pues en mi opinión, la situación es que las niñas y los niños, efectivamente, tienen muchos problemas. Las madres y los padres no se enteran de lo que está ocurriendo. Los adultos también tenemos muchos problemas. El cibecrimen mueve una cantidad de dinero alucinante. Un elevado número de niños ha sufrido acoso por Internet o ha tenido problemas con el uso de las redes sociales. Estamos incluso asistiendo a muertes en el mundo relacionadas con temas de ciberdelincuencia. El problema es que, encima, evoluciona a una velocidad de vértigo: no nos da tiempo a estar al día ni a los que nos dedicamos a esto, es que es casi imposible; y encima, hay una opinión generalizada de que el entorno legislativo no está a la altura de las necesidades, ni mucho menos. Y además tenemos muy pocas herramientas para luchar contra un problema cada vez mayor.

Y aquí quiero hacer mención de un problema, un ejemplo de tantos que podría poner, relacionado con nuestra empresa, que es de lo que puedo fundamentalmente hablar: nosotros somos una empresa de seguridad,

tenemos un centro 24 x 7, y vigilamos la infraestructura de seguridad de nuestros clientes; clientes, algunos de ellos importantes, grandes y con manejo de información sensible. Hace poco, el último incidente que hemos tenido (que fue hace, no sé, seis o siete meses) fue un incidente grave; nosotros, cuando tenemos un incidente declaramos una situación de emergencia, formamos un gabinete de crisis, todo en el ciberespacio; y evidentemente, nuestro objetivo en este caso es intentar impedir que los atacantes consigan entrar en nuestros sistemas, porque entonces ponemos en peligro nuestro negocio y el de nuestros clientes. Bien, en este caso tuvimos un incidente que duró tres días. Yo recuerdo uno de los días a las 5 de la mañana sentado en el gabinete de crisis, mirando a mis compañeros que saben de seguridad un montón, con las manos así sin poder hacer absolutamente nada; sabíamos de dónde venía el ataque, es más, sabíamos quién era, porque si quién es un dato y un dato es una dirección IP, sabíamos quién era el que nos estaba atacando; y no podíamos hacer absolutamente nada. ¿Qué pasó? Pues nada. No paso nada pues porque por suerte conseguimos impedir que estos señores entrasen en nuestros sistemas.

Lo que quiero decir con esto es que realmente no tenemos el equivalente a una ciberpatrulla. De hecho, esto lo denunciamos, sabemos quién es, y ha acabado en los juzgados y ha está siguiendo su proceso, cuatro meses más tarde del incidente. Pero realmente, ¿qué hubiese pasado si estos señores hubiesen conseguido entrar en mis sistemas? Pues hubiéramos tenido un problema, nosotros y nuestros clientes, muy gordo. Realmente estamos atados de pies y manos. No tenemos ni la capacidad de contrarrestar los ataques que nos están haciendo. Con lo cual lo único que podemos hacer es mirar. Y si entran, pues intentar responder.

Por lo tanto, ¿cómo definimos hoy la situación en que nos encontramos? Bueno, para empezar esta situación, desde nuestro punto de vista, y así lo dicen muchos estudios que hemos analizado, es una barrera para el desarrollo de la cibersociedad, es un problema importante con una frontera muy difusa. Yo no tengo claro que el problema sean los menores y que la solución esté en atacar, digamos, el problema que tienen los menores, sino el de la sociedad en su conjunto.

Es un problema que es cambiante, cambia a una velocidad alucinante. De hecho, en los últimos años la velocidad de cambio es cada vez mayor, y además puede llegar a limitar el desarrollo social, y limitarlo mucho;

porque el uso de Internet, el uso de las tecnologías es en tanto en cuanto genera confianza; si no hay confianza, al final, evidentemente, la opción será dejar de utilizarlo. Y eso, para la sociedad o para la sociedad en la que nos movemos, yo creo que es sinceramente malo. Con lo cual, en este momento lo que estamos analizando es un problema del que solo podemos ver la punta del iceberg.

Y además, insisto otra vez en la idea: yo creo que el problema somos nosotros. Y además, pensemos en algo que no se está analizando aún, que yo no lo estoy viendo, pero que no les quepa duda de que va a llegar, y es el utilizar a los jóvenes no solo como un fin, el problema del joven, sino como un medio. Es decir, si yo quiero obtener información sensible de una persona, posiblemente, si esta persona está suficientemente concienciada yo no podré atacar directamente a esa persona, pero sí a su familia, y utilizar a los niños en este caso como un medio y no como un fin en sí mismo.

Además, yo creo que deberíamos predicar con el ejemplo, y sinceramente no lo hacemos. En materia de educación vial, que luego volveré a tocar un poco el tema, a los niños les decimos «no se debe conducir hablando por el móvil, circular sin cinturón, cruzar con el semáforo en rojo, saltarnos un stop», etc. Pero nosotros permanentemente pirateamos la Wii de los niños para no pagar los juegos, descargamos todo tipo de contenidos sin saber su procedencia, usamos contraseñas débiles, compartimos las contraseñas con todo hijo de vecino, nos conectamos en cualquier sitio para descargar cualquier información sin un mínimo de precaución, y abrimos cualquier adjunto que nos informa de que hemos ganado el premio de una lotería a la que no hemos jugado siquiera. Entonces, ¿qué les vamos a decir a los niños, qué les podemos transmitir a los niños? Yo creo que el problema lo tenemos nosotros. Y somos nosotros los que tenemos que conseguir, digamos, arreglarlo.

Entonces, antes de entrar en lo que yo les voy a hablar, que es nuestra experiencia y la solución que yo creo que tiene todo esto, me gustaría comentar algunos errores, alguno de los cuales ha salido en la ponencia anterior y que me gustaría comentar.

Desde luego, en esta situación, lo que no es una solución es, como hacen muchos padres, meter la cabeza bajo el ala o debajo de la arena, esto no es la solución. Pero esta tampoco. Nosotros, en las conferencias que damos (que luego les contaré un poco cuál es nuestra experiencia en esa

materia), tenemos padres que se levantan de la silla directamente para ir a arrancar el ADSL de casa y decir «ya está». Esto no es la solución. Claro, esa no es la solución; esta tampoco. Yo pongo un control parental y ya está, un antivirus y ya está: vamos, ni de casualidad. Permítanme recordarles que en los móviles los controles parentales no existen. Y cada vez los niños usan más el móvil para acceder a Internet y a las redes sociales, con lo cual, por mucho que pongamos el control parental en el PC de casa, de poco nos va a servir, de muy poco.

Poner el ordenador en el salón tampoco es la solución. El ordenador es lo de menos; el avance, la evolución de todo esto... el ordenador es un dispositivo por el que los niños... es un cacharro antiguo que ven los niños como un electrodoméstico. Los chavales no utilizan el ordenador para acceder a un montón de información, utilizan los dispositivos móviles.

Prohibir, tampoco, en mi opinión; porque por mucho que prohibamos, se van a casa del vecino o se van a casa del amigo y ya tienen todo lo que tienen en sus manos. Ponerle puertas al campo, en mi opinión, es absolutamente inútil. Por mucho que intentemos regular muchas cosas en España, la red es global, lo queramos o no. Podemos romper la red, podemos quitarla entera. Pero no podemos limitarlo con actuaciones en el entorno de nuestro país. Porque yo les pregunto, yo puedo limitar el contenido de juegos, por ejemplo, que hace la publicidad de las televisiones de aquí, de España: ¿y la televisión mexicana que se ve a través de Internet, con un horario distinto? ¿Qué hacemos con ella? Es difícil. Yo creo que aunque hagamos cosas localmente, la solución tiene que ser global, no puede ser local jamás.

Dicen por ahí: los niños son más vulnerables porque son inocentes. Yo lo siento pero discrepo: no son más vulnerables porque son inocentes. Los mayores somos inocentes igual que los niños. El problema es que un problema en un niño tiene un mayor impacto, y cuando definimos la vulnerabilidad como la probabilidad de que una amenaza tenga éxito, el problema no es la probabilidad del suceso, es el impacto que sobre un joven tiene. En este caso las pruebas de ingeniería social (de hecho, nosotros hacemos auditorías con auditorías de ingeniería social que es el incidente más grave que tenemos en este momento en la sociedad); la ingeniería social funciona en el cien por cien de los casos, digo el cien por cien. O sea, si ustedes cogen una llave USB con un troyano y la dejan con

un cartelito que pone «confidencial» en el ascensor de una multinacional, les garantizo que en el cien por cien de los casos esa llave USB acaba pinchada en la red de la multinacional. Y no se lo estoy diciendo porque lo creo, se lo estoy diciendo porque lo sé. En el cien por cien de los casos, ¿vale? Con lo cual, lo de que los niños son más vulnerables porque son inocentes, yo creo que eso no es cierto.

También he oído, y lo han dicho aquí, que los jóvenes son nativos digitales y saben todo sobre la tecnología. Sí que es cierto que saben, pero por el número de horas que llevan. Realmente lo que pasa no es que ellos hayan nacido con un teclado en la mano y sepan mucho más que nosotros, qué va; es que le dedican muchísimo más tiempo. Y aquí lo que creo yo es que hay un problema de dejación de funciones de madres y padres, educadoras y educadores. Hay un problema de dejación de funciones porque es complicado. Yo estoy de acuerdo, es muy complicado. Pero realmente el problema, vuelvo otra vez al principio, no es de los niños, el problema es de la sociedad: es una sociedad distinta, completamente distinta, y ya podemos hacer lo que queramos, que va a seguir siendo una sociedad distinta. Lo que tenemos que hacer es adaptarnos a esa sociedad distinta. Su sociedad es una cibersociedad y va a seguir siéndolo. Con lo cual, tenemos que ayudar a nuestros colegas, a nuestros padres y madres y educadoras y educadores a que enseñen a los niños cómo usar esto en condiciones.

Bien, en este sentido, ¿qué es lo que podemos decirle, desde nuestro punto de vista, desde el punto de vista de una empresa que se dedica a trabajar en temas de seguridad? En el mundo empresarial todo esto, o buena parte de esto, está ya diseñado y existe. Hay modelos de gestión. Esto no es un proyecto, no podemos coger aquí y decir «vamos a hacer ahora un plan de choque para concienciar a niños o a jóvenes entre 13 y 16 años» y ya está. No es así. Porque mañana los riesgos van a ser diferentes, con lo cual esto es un proceso que, queramos o no, iniciamos el día que aceptamos meter en nuestras casas Internet, en los colegios Internet, en las empresas Internet; lo iniciamos y no tiene vuelta atrás, es muy difícil volver atrás. Con lo cual, lo que tenemos que diseñar es una solución que tenga en cuenta todo esto, que tenga en cuenta que tenemos que estar en un proceso continuo y que, si me permiten, desde un punto de vista ya técnico ingenieril, cuando nosotros nos enfrentamos a un problema de seguridad y decimos «vamos a diseñar un modelo de gestión de seguridad», ¿qué es lo que nos preguntamos? Primero, qué es

lo que quiero proteger y cuál es mi objetivo de protección; qué es lo que le puede pasar a mi objetivo de protección; cuál es la probabilidad de que le pase eso; y si le pasa, qué impacto tiene sobre su vida, sobre su bien, sobre su persona; qué es lo que yo puedo hacer para evitarlo. Y sobre todo, desde qué puntos de vista, en qué ámbitos, ¿un ámbito legal, un ámbito lógico, técnico, un ámbito físico, desde qué ámbitos? Esto para nosotros, desde el punto de vista técnico, es la definición del objetivo de protección, el TOP, cuál es mi objetivo de protección; el análisis de la taxonomía de amenazas, que si ustedes cogen una taxonomía de amenazas de adultos y de jóvenes, son idénticas, idénticas. El adulto dice «me han suplantado la identidad»; y el chaval dice «me han robado el Tuenti». Pero es lo mismo, ¿vale? Con lo cual, al final, aparte de la taxonomía de amenazas, que es igual, tenemos un problema de riesgo: los mecanismos de protección que tienen que cubrir el riesgo y los ámbitos de actuación (un ámbito legal, un ámbito técnico).

Voy a centrarme solo en dos, porque no tenemos más tiempo. Todos estos sistemas de gestión, la verdad es que están permanentemente orientados a la gestión del riesgo, hay veces que parece que compremos numeritos para tener más riesgo, como es el caso de este señor: esta foto, que la encontré por ahí, la verdad es que me dejó impactado. Pero es que en Internet, en el ciberespacio los menores y los mayores compramos numeritos para que nos toquen los problemas: navegamos por redes que no son seguras, descargamos contenidos que no sabemos de dónde vienen.

Claro, cuando hablamos de riesgo, como decía antes, tenemos que valorar por una parte el impacto y por otra parte la probabilidad. Y el riesgo es un producto de ambos. Nosotros podemos tener una amenaza sobre un adulto o sobre un menor. Posiblemente la probabilidad no sea muy distinta, la probabilidad de que algo ocurra no sea muy distinta; lo que cambia sustancialmente es el impacto. El impacto en un adulto puede ser una pérdida económica, un problema de reputación; en un niño, pues un problema físico, un problema de pornografía infantil. Con lo cual, el impacto es evidentemente distinto, y por tanto el riesgo también lo es. Pero la probabilidad prácticamente es igual. Incluso yo diría que como nosotros vamos, si me permiten la expresión, muchas veces muy de sobrados, a veces incluso es mayor la probabilidad de engañar a un adulto que de engañar a un niño. Depende en qué, ¿vale?

El otro punto que quería comentar es relativo a los mecanismos, qué es lo que nosotros podemos hacer para mitigar todo este riesgo. Tenemos

unos cuantos mecanismos. Uno, el de disuasión: «cuidado con el perro». Estos son extraordinariamente baratos y extraordinariamente eficientes. Es decir, una ley, por el mero hecho de promulgarse o de comunicarse, es un mecanismo de disuasión. Evidentemente, sino hay leyes que permitan determinado tipo de comportamientos, la disuasión no existe, ¿de acuerdo?

Después tenemos los mecanismos de protección. Es decir, un antivirus, un control parental: son mecanismos de protección. Pero los mecanismos de protección no siempre tienen que funcionar.

Cuando los mecanismos de protección no funcionan tenemos que tener mecanismos de detección, ¿que detecten qué? Que detecten que un niño tenga un problema, que detecten que se hayan saltado las barreras del antivirus y del control parental.

Evidentemente, cuando la detección funciona, tenemos que tener mecanismos de respuesta que nos sirven para ayudar al menor o al chaval a ver qué es lo que hace con ese problema.

Y después, mecanismos de recuperación, que a lo que nos llevan es a recuperar la posición inicial de partida.

En este sentido, los mecanismos de disuasión, fundamentalmente yo ahí veo mecanismos legales, de definir legislación que permita tanto a Fuerzas y Cuerpos de Seguridad del Estado como a las empresas que nos dedicamos a todo esto luchar contra estos incidentes.

Desde el punto de vista de protección (yo creo que es el punto además en el que hay que incidir), tenemos que incidir sobre la concienciación; concienciación, la autorregulación, la concienciación sobre la sociedad entera, no solo sobre los menores, sino sobre la sociedad.

Desde el punto de vista de detección: se ha trabajado muchísimo en problemas de protección, o mecanismos de protección de tipo de control parental, antivirus, pero en mecanismos de detección que identifiquen riesgos a los que está sometido un menor, hay muy pocas herramientas.

Y por último, mecanismos de respuesta y recuperación: el director general de INTECO, en la ponencia que he leído yo que tuvo con ustedes, les dijo que en una estadística que han hecho solo el 1% de los niños declara que acudiría a sus padres en caso de tener un problema con temas de ciberdelincuencia o con un problema en la red. Claro, si

no van a los padres, ¿adónde van? Pues en este momento están yendo a amigos, están pidiendo ayuda a amigos. Pero realmente creo que nosotros tenemos centros en España, hay CERT cualificados, tanto públicos como privados, que pueden prestar ese tipo de ayuda a los chavales. Lo que necesitan los chavales es saber dónde acudir. Igual que todos sabemos que hay un 112 que en el caso de ver un accidente podemos llamar al 112 y tenemos ayuda, no existe un ciber-112 o el equivalente al 112 en el ciberespacio. Igual que la sociedad física tiene una centro de emergencias, la sociedad virtual, la cibersociedad necesita también un centro de emergencias, un centro donde los chavales puedan pedir socorro, algo tan sencillo como eso.

En este sentido, ¿cuál es nuestra experiencia, qué es lo que hemos hecho nosotros? Pues como les decía, desde hace ya unos años (ya ahora les explicaré un poco la historia) hemos trabajado mucho, no en el qué, porque lo tenemos clarísimo desde hace mucho tiempo, a lo mejor estamos equivocados, pero el qué es que tenemos que concienciar en general a la sociedad, hemos trabajado mucho en el cómo, cómo hacerlo para que sea efectivo. Iniciativas de concienciación hay muchísimas; charlas, yo he ido a muchísimas, a dar muchísimas charlas (en mi opinión, hay muchas de ellas que no sirven absolutamente para nada), y además, dependiendo de quién sea el público objetivo, si son padres o son niños, el tipo de charla tiene que ser diferente, y en eso hemos trabajado.

Esto es un poco la línea de tiempo del trabajo de nuestra compañía en temas relacionados con el de la ponencia: empezamos en el año 2007 con la publicación de un blog que se llama Security Art Work en el ámbito técnico; es un ámbito técnico, que ahora les daré dos datos sobre el blog. En el año 2008 tuvimos un incidente en el que participamos como peritos de parte en un caso de pornografía infantil. En aquel momento eso nos marcó mucho, porque evidentemente no son casos agradables. A partir de ese momento decidimos que lo que íbamos a hacer nosotros en materia social es invertir en la formación a nuestros hijos y a los hijos de nuestros amigos, de nuestros clientes, de nuestros colegas, y empezamos con un proyecto que se llamó ProtegITs a finales de 2009 y principios de 2010. El proyecto tuvo tanto éxito que al final lo convertimos en una iniciativa en la que estamos trabajando y en la que estamos colaborando con empresas dando concienciación en materia de ciberseguridad a empleados y a familias, incluidos los hijos de los empleados. El proyecto

pasó a llamarse ProtegITs, y junto con Hijos Digitales, que es un blog que diseñamos para tener información asíncrona, no in situ, es en lo que estamos trabajando ahora. Algún informe que les contaré sobre el tema de los juegos, que además me ha hecho gracia que hagan antes esa apreciación, porque como consecuencia de las clases que nosotros hemos estado dando, uno de los problemas principales que detectamos fue precisamente el uso que los niños hacían de los juegos *online*. E hicimos un informe, y ahora comentaré un poquito sobre él.

Y ahora, en 2013, estamos pasando muchos de los contenidos, de la forma que les voy a contar ahora, que es una forma curiosa y un tanto original, los estamos pasando a una plataforma *online*.

Les decía que Security Art Work, que es una plataforma técnica que tiene solo dos datos, un millón de páginas vistas a lo largo de su historia, desde abril de 2007, pero en este momento tiene 5.218 seguidores. Es información fundamentalmente técnica, para compartir conocimiento de seguridad en ámbitos técnicos.

Hijos Digitales es un blog que se creó en mayo de 2011 orientado fundamentalmente a niños y padres. El lenguaje de este blog es nada técnico, es totalmente llano, para que lo entienda todo el mundo. Toca muchos temas relacionados con seguridad y temas relacionados con tecnología, con un enfoque de seguridad. Con mucho menos periodo de vida tiene casi 900.000 páginas vistas, y en este momento unos 1.500 seguidores en Twitter. Tiene mucho éxito, hasta el punto de que... Nos ha sorprendido, además, mucho, porque es un blog relativamente joven. Pero la gente tiene muchísima necesidad de este tipo de contenidos. Es un blog que publica una entrada diaria, como decía, en un lenguaje muy llano. Tuvo un día que fue el TOP, que fue el caso de una persona, un colaborador del blog que publicó el caso del ciberacoso a su hija. Lo curioso de este caso no fue el hecho, sino la solución que le dio; fue una solución imaginativa. Yo les invito a que lo lean porque es curiosísimo. O sea, la solución que le dio estaba basada... Esto fue un caso de acoso a través de WhatsApp, y en un momento determinado tenía muchos problemas, es muy largo, pero no voy a extenderme, y entonces se dio cuenta de que la solución no podía venir a través de las niñas que acosaban a su hija; la solución iba a venir de sus padres. Los propietarios de los números de teléfono móvil eran sus padres, y lo que hizo fue poner una denuncia a los propietarios de los teléfonos móviles. En una semana se acabó el problema.

Con lo cual, esto no es un problema de niños; esto es un problema de la sociedad, es un problema que nos muchísimo a los padres también. De hecho, tuvo 18.000 visitas en un solo día el caso este del ciberacoso. En este momento estamos en cerca de 100.000 visitas en Hijos Digitales, y yo creo que es una forma de comunicar muy útil, francamente útil. Porque además hay mucha colaboración, el crecimiento de 2013 respecto a 2012 está en torno al 400%, 700% y creciendo. Es un tipo de contenido muy demandado sobre todo por los padres, porque como decía antes, no saben dónde están sus hijos realmente.

El segundo proyecto, el proyecto, digamos, más grande que hemos desarrollado, se llama ProtegITs, con esta imagen un tanto curiosa: la I y la T es tecnologías de la información, y el paraguas representa seguridad, y sobre todo eso hemos montado, digamos, los elementos del proyecto.

Recuerden que antes les decía que para montar un proyecto de seguridad necesitamos diseñar mecanismos de cinco tipos. Este proyecto se diseñó técnicamente por un equipo de ingenieros, con un final que evidentemente tiene un final en instructores o en gente que ha dado clase a los niños; se diseñó un aula interactiva (que luego verán lo que es) con unos talleres prácticos, con una forma muy curiosa de dar los talleres, con unos pilotos que nos permitieron en un inicio conocer las amenazas a las que estaban expuestos los niños, con un guion, porque al final esto es prácticamente igual a una obra de teatro, con su guion perfectamente establecido, incluso con los ejemplos y todo, con un portal, un *kit* que lo que permitía era desplegar a través del portal mecanismos de protección con dos elementos, una barra y un hito que luego les presentaré (es la mascota del proyecto), un plan de comunicación, un centro de servicios y un club. Todo esto, que son medidas en torno a un proyecto, a una idea para echarles un cable a los chavales, tienen un grupo de medidas de disuasión (nosotros, evidentemente, no podemos legislar, con lo cual la parte legal no entra dentro de nuestras posibilidades), pero sí el comunicar la existencia de centros que se dedican a ayudar a los chavales en esta materia.

Hay un grupo de medidas que son medidas de protección. La concienciación, como decía antes, es una medida de protección fundamental. Hay un grupo de medidas que son de detección: intentan detectar situaciones de riesgo para los chavales. Y hay medidas que son de respuesta y recuperación: un sitio donde acudir, alguien a quien preguntar, alguien a quien decir «oye, necesito ayuda, por favor, ¿me puedes ayudar?».

Este proyecto: esta es el aula, es un aula muy controlada porque distribuimos troyanos y virus para que los chavales se den cuenta del riesgo, con lo cual todo lo montamos nosotros. De hecho, esta es una clase que damos en nuestras oficinas allí en Valencia, una clase donde tenemos una figura un tanto especial que es la de aquí del fondo, esta persona de aquí, es lo que nosotros llamamos «el malvado»; es una persona de nuestro equipo de *hacking*, y como ven, está detrás de un pequeño paraván (este paraván de aquí); esta persona es la instructora, en este caso es Eva, que es una instructora de chavales. El papel de la instructora es llevar el hilo conductor de la clase. El papel de nuestro amigo Javier, en este caso, del malvado, es darles unos cuantos sustos a los chavales. Y cuando digo «darles unos cuantos sustos» significa demostrarles lo que una persona con conocimiento podría hacer si fuese mala. Y lo que hacemos es demostrárselo en sus carnes. De hecho, diseñamos un guion con un montón de píldoras (que luego volveré sobre el concepto de las píldoras), que lo que son realmente son casos de incidentes anonimizados que hemos tratado con niños y con adultos, y que se los explicamos a los chavales de una forma muy sencilla. Utilizamos un concepto en este guion que llamamos «La bofetada digital». Claro, necesitamos que los chavales nos hagan caso y que se tomen en serio donde están. De hecho, cuando entran en un aula, que puede ser un aula parecida a esta, tienen todos sus portátiles, y nada más entrar en el aula, la mayoría de ellos entran en el Facebook o en el Tuenti, se «logan», se hacen usuario y contraseña y se meten; en ese momento, el malo ese que está ahí atrás, lo que les está haciendo es un *phishing*, y les está robando el usuario y la contraseña. Y el usuario y la contraseña lo publica. Y les dice «os acabamos de robar el usuario y la contraseña. Y además, estas contraseñas que estáis utilizando son malas». Y a partir de ahí empieza una dinámica en un aula donde lo que hacemos es distribuirles troyanos, robarles la cámara, para que se den cuenta ellos mismos en sus propias carnes qué es lo que podemos hacer sabiendo un poco de tecnología. Bien, este formato ha tenido un éxito increíble. De hecho, los chavales son los que nos van contando y los que nos van escribiendo el guion, y el guion se va adaptando a lo que nos piden. Una de las cosas que hicimos es meter un informe de seguridad de juegos *online*, porque nos dimos cuenta de que las niñas utilizan mucho las redes sociales; los niños juegan, juegan *online*. Entonces, alguno de ellos nos hablaba del dinero electrónico. Y entonces empezamos a estudiar qué era aquello del dinero electrónico,

y alucinamos, o sea, fue impresionante. Hicimos un informe, que está además en nuestra página web, *Seguridad de los juegos online en 2011*; descubrimos, por ejemplo, mafias, pero mafias organizadas; el dinero es un dinero virtual, es un dinero con el que se compran roles, son juegos de rol, y que yo tengo desde la posición 0 hasta la 99, soy más machote si estoy más alto en el rol. Y evidentemente, esto en la comunidad de los niños tiene mucho peso. Esto lo saben los niños y también lo saben los malos. Y en China, de hecho (hay alguna foto en el informe) hay cárceles donde los carceleros tienen a presos jugando a juegos de rol a los que juegan los chavales para conseguir dinero virtual, que luego se van a las páginas web de venta en Internet y las venden por dinero físico. Con lo cual, algo que aparentemente es un juego *online* que juegan con dinero virtual se convierte en un juego donde los niños están jugando con dinero físico, y donde estamos teniendo una cantidad de problemas, porque en teoría esos juegos no tienen dinero real, pero se está convirtiendo en una mafia, en un mercado negro impresionante.

Otro caso es el de un chaval que vino y que n os decía que lo primero que hacía él cuando llegaba a un sitio era robar la WiFi. ¿Cómo que robar la WiFi? Dice: «sí, mira». Y nos enseñaba los programas que utilizaba. Yo alucinaba. Estos chavales son *hackers* en potencia. Pero te enseñaban los programitas que utilizaban... Claro, este era un chaval de 15 años, a este tipo de chavales no les puedes decir que esto es un delito, porque es que yo creo que ni lo entienden, ellos necesitan estar conectados. Con lo cual dicen «¿cómo va a ser un delito?, si necesito conectarme, pues me conecto». Entonces, lo que hicimos fue darle un poco la vuelta: metimos una píldora en la clase lo que le contábamos qué es lo que una persona mala puede hacer, si yo soy malo y me roban mi WiFi, a partir de ese momento todo el tráfico que pasa por aquí lo veo, pero lo veo entero, con lo cual te robo tu usuario, tu contraseña, tus fotos, te lo robo todo. Eso sí que les hacía daño, ¿vale? Con lo cual buscamos la forma de intentar convencerles de que no hiciesen eso.

El proyecto tiene un portal. Tiene un *kit*, que nosotros intentamos diseñar herramientas que faltan. Evidentemente, filtros de control parental, herramientas antivirus hay un montón. Lo que pasa es que nosotros detectamos, digamos, dos agujeros, dos huecos en las herramientas que utilizan tanto hijos como padres.

Una es aquella que nos permite pedir ayuda. ¿Dónde piden ayuda y cómo? Los chavales, cuando están navegando están utilizando un nave-

gador, herramientas, y lo que necesitan es tener algo que mientras estén navegando les permita, por ejemplo como es el caso este, una pequeña barra cuyo único objetivo es tener un botón rojo que digas «necesito ayuda», y poner en contacto al chaval en este caso con un centro de servicios donde tiene a alguien que, con conocimiento tanto desde el punto de vista legal como desde el punto de vista técnico, es capaz de echarle un cable. Pero ese tipo de elementos de ayuda no existen en el mercado. O sea, filtros de control parental, sí; pero, ¿y cuando no funciona un filtro de control parental? Un filtro de control parental no sirve para cortar contenidos en una red social donde un niño está quedando con un adulto, no sirve para nada. Ahí necesitamos otro tipo de herramientas. Esta era una.

Y la otra es una que tuvo mucha polémica. Nosotros somos una empresa de seguridad, y como empresa de seguridad utilizamos herramientas que interceptan el tráfico, y lo hacemos en las redes de nuestras empresas para buscar tráfico anómalo, intentos de intrusión, intentos de ataque; estas herramientas son herramientas muy potentes, herramientas que nos permiten analizar el tráfico que funciona por una red. En este caso diseñamos una herramienta cuyo objetivo, a partir de una taxonomía de amenazas, por ejemplo, un diccionario de palabras con palabras como por ejemplo «anorexia», porque estamos hablando siempre de la pornografía infantil, pero nos olvidamos algunas veces de otro tipo de problemas que tienen los chavales en las redes, identificaban algunos tipos de palabras de forma que pudiesen disparar una alerta, decirle al padre «oye, mira a ver qué pasa, porque tu hijo está hablando de anorexia, de bulimia, de *sexting*, de sexo o de quedar». ¿Vale? Con eso, lo que hicimos fue diseñar una herramienta utilizando técnicas de las que nosotros utilizamos en la empresa para diseñar un cacharrito que se ponía en un ordenador y detectaba situaciones de riesgo. Ahora bien, evidentemente, esto es intercepción de comunicaciones. Y lo que hicimos es irnos a hablar con un grupo de fiscales, fiscales especializados en menores para pedirles su opinión. Nos dijeron: esto no se puede hacer. No se puede hacer. Por mucho que seas padre, tú no puedes interceptar las comunicaciones de un niño. Y nos propusieron que creásemos, así nació Ito, que es la mascota del proyecto, que es un elemento que lo que pretende es, primero, decirle al niño que existe, y decirle qué hace. Es decir, un elemento de análisis de comunicaciones le dice, Ito le dice al niño qué está utilizando —sobre todo para los niños más pequeños—, «estoy aquí y hago esto». Segundo, tiene que poderse desconectar. El niño tiene derecho a desconectarlo.

Claro, cuando te enfrentas a esto dices «vamos a ver, si desconecto Ito, la protección que intento montar sobre mi hijo o sobre mi familia ha desaparecido». No; no, porque la desconexión de la mascota, la desconexión de Ito es en sí mismo una alarma. Es decir, mira, yo te digo: «padre, tu hijo ha desconectado esto. Vete a hablar con él». Y así cumplíamos otra labor, que era el fomentar la comunicación entre los padres y los hijos para que todo esto funcionase un poco mejor.

Este es el aspecto de Ito. Ito, cuando estaba grabando decía que estaba grabando. Insisto que esto sobre todo está orientado a los chavales más pequeños. Cuando detectaba una amenaza se ponía en rojo y daba un montón de consejos, y el niño en este caso podía desconectarlo, y a partir de ese momento Ito dejaba de interceptar cualquier comunicación.

Como veis, este es un proyecto que tiene todas las piezas; tiene herramientas o mecanismos de protección, de detección, de disuasión y de respuesta y recuperación, con el centro de servicios.

A partir de ahí, esto tuvo tanto éxito que diseñamos, haciendo uso de la misma estrategia, un proyecto que se llamó ProtegITs y en el cual ya nos fuimos a hablar con empresas, no para hacer la concienciación típica en empresas en materia de seguridad, sino con departamentos de responsabilidad corporativa y con departamentos de tecnología, aunar esfuerzos y decirles «mira, vamos a hacer una labor social y además vamos a cumplir los requisitos que tienes tú en materia de seguridad dentro de tu compañía». Y empezamos a montar jornadas de seguridad familiares donde iban hijos de empleados y empleados, y jornadas orientadas al empleado. El éxito ha sido impresionante. Volvemos otra vez a lo mismo, es el cómo hacerlo. Está claro que lo que hay que hacer es concienciar, pero hay que buscar una forma de hacerlo que llegue a los niños, que llegue a los adultos y que nos sirva para realmente incrementar ese nivel de concienciación. Esto lo hemos hecho en organizaciones, entre otras, como Endesa, Red Eléctrica, que están apostando mucho por la concienciación de seguridad, no solo de sus compañías, sino también de las familias, de las personas que están trabajando en estas compañías.

Porque también tienen claro que el problema es un problema global. La seguridad de una empresa no se puede conseguir simplemente con la seguridad de los ordenadores de la empresa ni con la seguridad de los empleados; sino también necesitamos la seguridad de los entornos. Al final es un problema global, ¿de acuerdo?, como decíamos al principio.

Al final, en las jornadas familiares repartíamos una serie de decálogos. Aquí tienen algunas fotos, en este caso son David y Patxi, el bueno y el malo, en una preparación de una clase; algunas clases con chavales, de hecho hemos ido por toda España dando cursos de concienciación tanto a nivel empresarial como a nivel, digamos, social. En sitios donde nos lo han pedido también nos hemos ido a dar este tipo de charlas, que son las que entendemos que son francamente útiles.

¿Cosas que nos han pasado? Nos ha pasado de todo. Por ejemplo, una cosa que nos llama muchísimo la atención es que solo el 10% o el 15% de los asistentes suelen tener Facebook, y ninguno Tuenti. Lo primero que hice yo cuando mis hijas me dijeron que querían Facebook y Tuenti fue sacarme un perfil mío, con mi nombre y apellido, no un perfil falso, sino el mío, José Rosell. ¿Por qué? No se pueden imaginar el tiempo que tardó mi hija mayor en mejorar la seguridad de su perfil. Bueno, ya conseguí algo: que se preocupe por quién tiene que ver qué. Eso para mí, en ese momento fue suficiente. Ahí hay una labor inicial de saber qué es Facebook, qué es Tuenti. Por ejemplo, mi hija hace cuatro días vino con que en el colegio le habían pedido que se diese de alta en una red social que se llama Ask, que es «pregúntame y yo te respondo». De estas hay un montón. Y una de las cosas que necesitamos o que les transmitimos a la gente es que lo del parque de antaño, lo de llevar al hijo al parque y decirle «la tierra no se come», lo tenemos igual pero en formato digital. Y el parque, el recreo, el colegio es digital. Con lo cual, no tenemos más remedio que estar donde están nuestros hijos. Y no vale decir «es que ellos saben mucho». No saben mucho, se pasan más horas. Pero no saben más que nosotros, ¿vale?

Aquí hemos utilizado un concepto de píldora formativa donde exponemos casos, hacemos análisis de las consecuencias del caso y recomendamos prácticas para evitarlo. Esto lo copiamos de una cosa muy antigua en nuestro país, que son las campañas de la Dirección General de Tráfico. Las campañas de la Dirección General de Tráfico tuvieron mucho éxito, han tenido durante mucho tiempo mucho éxito porque mostraban los problemas derivados de no hacer un uso responsable, en este caso de la educación vial o de la conducción. En materia del ciberespacio pasa lo mismo: hay que enseñarle a la gente lo que pasa al no cumplir ciertas reglas.

Esto es una clase, digamos, de empleados, donde utilizamos también la píldora. Aquí tenemos, ya no vestidos de negro y blanco, porque esto no es

para niños, es ya para empleados, tenemos al instructor y a una persona de nuestro equipo de *hacking*; hacemos una representación de un día del buen empleado en una compañía, donde a lo que volvemos otra vez es a incidir en el cómo damos la concienciación y no en el qué; el cómo es enseñándoles con píldoras, con sucesos, con incidentes qué es lo que le puede pasar a una persona de una organización cuando hace un uso de una tecnología despistado. Ya no con mala fe, sino simplemente por no tener en cuenta determinado tipo de mecanismos. Todo esto lo estamos pasando ahora a *online*, y la verdad es que el resultado está siendo francamente bueno, lo que nos anima a seguir con todo este tipo de trabajo. Al margen de nuestro trabajo normal, que es trabajar en seguridad para las empresas, es que la gente está muy contenta, la gente nos pide más. De hecho, hay algunas cosas (les he puesto aquí y esto se lo pasaré completo), algunas respuestas de los chavales que son graciosísimas. Cuando les preguntas a los chavales «¿tú has tenido algún problema de estos que vemos aquí?». Casi ninguno, el 25% dice que sí, el resto que no. ¿Y conoces a alguien que haya tenido este problema? El 85% dice que sí, y el resto que no. Claro, es muy significativo. Cuando hablas con ellos te das cuenta de que los problemas de suplantación de identidades están a la orden del día, y es muy difícil pelear contra todo eso.

Hay un caso que a los padres sobre todo les causa mucha impresión, que es el del geoposicionamiento de las fotos. Y vuelvo a incidir sobre lo mismo: esto es una píldora que utilizamos. A los chavales se lo enseñamos y a los padres se lo contamos. Y hacemos la jornada paralela: los niños por una parte y los padres por otra. Cuando los padres le dan a un chaval (ahora con 9 o 10 años) un móvil de estos de última generación, un *smartphone*, una de las cosas que la mayoría no sabe es que el *smartphone* lleva de serie el geoposicionamiento de las fotos. Los chavales cogen la foto, las suben a Twitter, la suben a Tuenti, la suben a Facebook, e implícitamente están diciendo dónde están. Pero es que si sigues a algunos de ellos en Twitter, te dicen: «mira, me acabo de hacer una foto que estoy en el cumpleaños de fulanita», y suben la foto al Twitter. Y dicen «ya ahora me voy a casa». Y la casa la tengo yo grabada de dónde es. Con lo cual, si sé dónde está y sé dónde va, no tengo más que ponerme en medio para interceptarlos. Claro, a la gente... Hay programitas como este de aquí, aquí sale un mapa, que lo que hace es geoposicionar las fotos de una cuenta de Twitter en un mapa, y sabes conductas de desplazamiento, por dónde va, a qué horas va, te lo saca todo. Esto no es un problema de los niños. Al niño, a un chaval de 10 o de 11 años le das un móvil con el

geoposicionamiento conectado; y cuando sube fotos al Tuenti o al Twitter está diciendo dónde está, dónde voy, por dónde me suelo mover o por dónde vuelvo del cole a casa.

Bien, como conclusión yo quería poner un corto de un vídeo que dura tres minutos, que es muy significativo de lo que ocurre en términos generales.

> **[LOCUTOR VÍDEO]**: *Yo puedo comentaros un poco qué hay relacionado con la seguridad, relacionado con la ciberseguridad dentro de nuestra oferta formativa. Nosotros, en la escuela tenemos en este momento un grado en Informática...*

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): Esto es una conferencia de una persona que tiene un alto cargo en una escuela de informática en una universidad politécnica, en el ámbito de una conferencia de protección de infraestructuras críticas, algo que desde el punto de vista del riesgo, para un país como España o cualquiera de la Unión Europea es un riesgo muy elevado, evidentemente, es un problema muy importante.

> **[LOCUTOR VÍDEO]**: *Los nuevos grados son de cuatro años, son 240 créditos, y a fin y al cabo es equivalente a las antiguas ingenierías; de hecho el grado se llama en Ingeniería Informática. Y básicamente, puede pasar un alumno a hacer ese grado y no recibir específicamente ninguna formación en seguridad. Tenemos apenas 9 créditos de esos 240, es decir, algo menos de un 4%, de una formación optativa en algún aspecto relacionado con la seguridad.*

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): Ahora el segundo corte. Son cuatro cortes.

> **[LOCUTOR VÍDEO]**: *Y algo parecido sucede en nuestra oferta de másteres. Tenemos en este momento seis másteres alrededor del centro en temáticas de informática, y de esos seis másteres, pues cuatro no tienen nada de oferta de temas de seguridad; y los dos que lo tienen, pues también de nuevo tienen asignaturas con un carácter optativo.*

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): El tercero.

> **[LOCUTOR VÍDEO]**: *Nosotros nos encontramos en lo que es la enseñanza reglada un poco en una situación parecida a lo que co-*

mentaba Sebastián respecto a cuáles son los plazos; él hablaba de que en una normativa había que revisar cada cinco años, que en otra normativa había que revisar cada dos los planes. En nuestro caso nuestros planes de estudio se aprueban en un momento determinado y no tienen fecha de caducidad, aunque normalmente más pronto o más tarde se acaban renovando. Pero sí adolecemos en ocasiones de una cierta rigidez. Y a mí me ha preocupado especialmente el lugar que ha ocupado en esta mesa, porque no quiero, no me gustaría que la universidad, que la academia se encuentre un poco separada del resto de la sociedad, como me ha tocado en esta mesa. Entonces, realmente nosotros desde la academia, desde la escuela, aun siendo sensibles a esta problemática, consideramos que nos hemos centrado en ofrecer una formación generalista de ingeniería. Yo estoy convencido de que los estudiantes de ingeniería mecánica no necesariamente reciben una formación específica, no sé, en antirrobos de coches, ¿no? Lo cual no quiere decir que no sea una temática importante; lo cual no quiere decir que no pueda ser incluso una iniciativa empresarial de interés. Pero, claro, hay otras muchas cosas. Y a veces es difícil enfocar con precisión lo que es más adecuado en...

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): Y la última ya.

[LOCUTOR VÍDEO]: *...en cada momento. Y prácticamente, yo quería terminar un poco con la reflexión de que por ejemplo, cuando el señor Ford se plantea hacer el modelo T, pues posiblemente en lo último que esté preocupado es en a ver si se van a robar mucho los coches o no. Entonces, está claro, y creo que mis compañeros han hablado con mucha claridad respecto a la seriedad en particular de la protección de estas infraestructuras críticas, es decir, que no consideréis que no lo veo importante, sino más bien intento un poco disculpar en cierto modo el que nosotros, en lo que es la formación generalista, no tengamos una mayor abundancia de especialización. Yo puedo contaros un poco qué hay relacionado con la ciberseguridad dentro de nuestra oferta formativa...*

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): Ya está. En definitiva, yo creo que esto lo resume un poco todo: nosotros, en la sociedad en la que estamos, estamos trabajando todos los días en

materia de seguridad; ya habéis visto que con niños en una parte, con adultos, con empresas. La conciencia de la sociedad en general en materia de ciberseguridad es escasa o nula. Ni siquiera en las universidades, que deberían estar mucho más cerca de los problemas empresariales o de los problemas de Estado ligados directamente con los temas de seguridad (seguridad nacional, robo de patentes, etc.), ni siquiera ahí tenemos una conciencia clara de los temas de seguridad. Y en ese contexto, pues qué le vamos a pedir a los menores. Yo creo que tenemos un problema antes que resolver, y es un problema general de la sociedad.

Y en este sentido, simplemente para concluir, el problema que tenemos, en mi opinión, es muy grave; si queremos ayudar a los niños tenemos que resolver antes el problema que estábamos comentando, el de la cultura de la ciberseguridad en la sociedad, empezando por sus madres y padres y por sus profesoras y profesores, que no tienen ni idea, pero ni idea, es algo increíble, porque no han tenido la oportunidad tampoco.

Con esto, yo creo que resolveremos parte del problema, pero no todo; yo creo que ahí hay que ponerse manos a la obra con los temas de ciberseguridad en general. «Concienciación», para mí es la palabra clave; la clave es concienciación, no formación; estamos aún en la fase de concienciar, no formar; la formación es larga y cara; la concienciación no tanto. Y creo que nos tenemos que centran en cómo tratamos la concienciación y no tanto en que hay que hacer concienciación. Es decir, la concienciación tiene que ser efectiva. Yo he ido a conferencias, de hecho he leído incluso, en las ponencias que han tenido ustedes aquí, de la policía, algún policía que decía que en las conferencias que iban a dar a colegios, realmente no iban casi personas, y que incluso las personas que iban realmente no recibían el mensaje que ellos querían dar; con lo cual volvían a lo suyo: es que nosotros somos policías, no somos comunicadores ni formadores ni instructores. Yo creo que hay que trabajar muchísimo en cómo debemos dar esa concienciación más que en qué. Yo creo que una forma de hacerlo es las campañas parecidas a las Dirección General de Tráfico con las píldoras formativas o los casos de uso, como quieran llamarlo ustedes.

Y hasta aquí. Muchas gracias.

COMPARECENCIA DEL ASESOR DE COMUNICACIÓN Y ANALISTA DE LAS REDES SOCIALES, D. ANTONI GUTIÉRREZ-RUBÍ, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 27 DE NOVIEMBRE DE 2013.

Muchísimas gracias por la invitación. Gracias también a los senadores que me han escrito pidiéndome puntualmente que ampliara o que diera algún punto de vista adicional. Yo les escribí a todos ustedes para ponerme a su disposición, y agradezco a los que me han respondido.

Me gustaría iniciar mi intervención con un punto central, y es que quiero que desplacen ustedes mentalmente su atención del acceso a la conectividad. Este punto es básico para mi intervención y para comprender lo que les voy a decir. Si ustedes se preocupan por los riesgos de los menores en la Red pensando en el acceso, creo que cometerán un grave error. Si ustedes se preocupan por los riesgos de los menores en la Red pensando en la conectividad verán los problemas de otra manera y verán las soluciones también de otra manera.

Cuando uno ve solo problema de acceso piensa que con impedirlo (el acceso) se resuelve el problema, y, por tanto, su mentalidad es cerrar, impedir, dificultar de alguna manera, legalizar, ilegalizar, controlar y/o limitar el acceso. Pero lo nuevo, el dato nuevo que les quiero trasladar, es que esa opción, cuando se ve desde la conectividad, hace que se vean otro tipo de problemas y otro tipo de soluciones que ahora voy a explicar.

Primer punto, la penetración de dispositivos móviles entre los menores y adolescentes es imparable; tienen acceso a Internet y desde muchos dispositivos (tabletas y *smartphones*); España es el primer país europeo con mayor tasa de penetración de teléfonos inteligentes. De todo esto les voy a dar datos. Por lo tanto, Internet no se encuentra en el ordenador, Internet se encuentra en cualquier dispositivo móvil. Y donde empiezan o donde se pueden resolver los riesgos y los problemas para los menores no es en el acceso a Internet sino en la conectividad digital; es aquí donde cambia toda la perspectiva.

Además, el acceso desde las pantallas de proximidad (es decir, móviles y tabletas) va a ser el acceso preferente de Internet, ya lo es hoy en

España. Otro estudio, el quinto estudio anual del *Mobile Marketing* sitúa el acceso a Internet desde las tabletas y desde los *smartphones* muy por encima del acceso desde los ordenadores, tanto de mesa como portátiles. Y, además, las aplicaciones, el conjunto de las aplicaciones, se llevan el 80 % del tráfico de Internet actualmente (un ejemplo de estas aplicaciones que se es WhatsApp).

Por lo tanto, no vean páginas web, vean conectividad en Internet. Si ven conectividad en Internet, los problemas son de otra tipología.

Además, el *smartphone* y la pantalla de proximidad se convierten en los elementos centrales de la itinerancia. La mayoría de nuestros niños y menores se están desplazando continuamente (cuando van a la escuela, cuando van a las actividades extraescolares, cuando están esperando a que sus padres les recojan…), se mueven. El 75 % de los viajeros de cualquier edad utiliza *smartphones* y tabletas cuando viaja y, por lo tanto, tiene acceso a la conectividad, si tiene banda ancha o tiene ese servicio.

El incremento de la «empresa tableta» lleva además a la posibilidad de la «escuela tableta», de una manera extraordinaria (la venta de tabletas en España ya es muy superior a la de cualquier otro dispositivo digital). Y todos los datos son extraordinariamente abrumadores respecto a la importancia del *smartphone* y de la tableta como elementos centrales de la configuración de la conectividad de nuestras sociedades.

Datos muy importantes: 8 de cada 10 padres dejan sus tabletas a sus hijos menores de 11 años. Son datos del ámbito de la Unión Europea y de Estados Unidos; en España, las cifras son muy parecidas. Y el 70 % de los escolares en Estados Unidos querría ya sustituir todos sus libros de texto por dispositivos móviles o servicios móviles o propuestas móviles para el estudio. En estos momentos, hay un debate en el Senado norteamericano muy importante sobre la centralidad de la tableta y del móvil en el sistema educativo.

Por lo tanto, vamos a un escenario donde el acceso se produce en unos entornos de conectividad de extraordinaria proximidad (tabletas y *smartphones*) que cambian las ecuaciones y las relaciones.

Las redes sociales y móviles ya están en el centro del aprendizaje en las escuelas de Estados Unidos. Hablamos de dispositivos con acceso a Internet. Y se está produciendo un proceso inverso por el cual profesores, pedagogos, enseñantes, etcétera, están aprendiendo de sus alumnos en el itinerario y el conocimiento digital.

Con esto lo que les quería decir es dónde hay que poner el foco y dónde hay que empezar a reflexionar.

Segunda idea: la conectividad es una oportunidad extraordinaria del adolescente. Los adolescentes ven en la conectividad una manera natural de ser adolescentes, donde el riesgo se vive con gran inhibición y con una falsa sensación de seguridad. Cuando un adolescente tenía que entrar en un lugar arriesgado para él, la exposición presencial (acceder, llamar a la puerta, entrar, por ejemplo en una farmacia y pedir un preservativo…) suponía una inhibición muy fuerte. Estar en la cama, bajo tus sábanas, conectado a Internet es una inhibición muy débil. Por lo tanto, esta extrema conectividad de los dispositivos móviles hace que los adolescentes vean una oportunidad para vivir su momento vital con una fuerte inhibición al riesgo, dato muy importante.

Las conductas típicas de la preadolescencia y de la adolescencia (centradas en uno mismo, las pasiones y las empatías, las conductas de riesgo, como decía) se facilitan de una manera muy natural en la conectividad, con acceso o no a Internet; la conectividad entendida en un sentido muy amplio de la palabra. Evidentemente, estamos hablando de una manera natural de vivir el impulso, la pasión, las filias, las fobias, etcétera. Para entendernos, un adolescente y un menor pueden vivir con una sensación falsa de control de esa situación, ya que el entorno físico no es determinante para esa sensación. Es un cambio muy importante, por ejemplo, de mi edad o de la suya.

Esto, además, produce otro tipo de cambios, y es que la mayoría de las relaciones de nuestros menores y de nuestros adolescentes tendrá como elemento de relación central la pantalla. La pantalla será el *hall* de entrada a las relaciones humanas. Se socializarán, no solamente conocerán, aprenderán, sino que su inicio a la socialización estará mediado por una pantalla de proximidad. Muy diferente a los inicios de socialización analógicos, en donde el tiempo y el espacio, coincidir en un lugar y en una hora, es fundamental para ello. Aquí no: la ruptura del tiempo y del espacio para la socialización modifica las reglas del juego, las maneras en las que voy a conocer a mis amigos y mis amigas, las maneras en las que voy a sentir su cercanía, conocimientos, afectos, etcétera.

Por lo tanto, hay un desplazamiento —también muy importante— del conocimiento relacional mediado por una pantalla al conocimiento relacional mediado por unas circunstancias, un contexto, el tiempo y el

espacio. Los menores y los adolescentes sienten que su oportunidad relacional aumenta a través de la pantalla, y se reduce en lo presencial. En consecuencia, sienten que tienen más posibilidades de tener más amigos y amigas; sienten que tienen más posibilidades de tener más experiencias, vivirlas más intensamente sin moverse. El atractivo, para la vida adolescente, de la conectividad es muy alto. Es una manera de vivir la adolescencia que tiene estas condiciones.

En este sentido, una vez que les he planteado este escenario, me gustaría sacarles un poco del foco del riesgo convencional, tradicional, asociado a lo ilegal. Y me gustaría situarles el riesgo en lo nocivo, que es otra cosa, y hablar de lo nocivo y de lo ilegal. Hablemos de otro tipo de riesgos.

Por ejemplo, el machismo digital. Es uno de los riesgos, el machismo, la misoginia digital, más severos, más duros que la conectividad puede favorecer. Se reproducen patrones patriarcales, estereotipos de género que pensábamos que estaban en fase de superación y que anidan, se reproducen, crecen con un efecto, digamos, muy distorsionador en estos mundos de conectividad. Es más, no quisiera alarmarles, pero desde mi punto de vista, estamos ante un peligroso retroceso en términos de políticas de igualdad, políticas de respeto. El entorno digital, el ecosistema digital, este entorno de conectividad, permite el uso vigilante, el uso inquisidor, el uso protector, el uso propietario de las relaciones humanas: como te puedo vigilar porque sé cuándo has leído este mensaje, sé a qué hora lo has leído, puedo exigirte que me respondas; y si no me respondes, es que estás haciendo algo que no me quieres decir. La incorporación de una tecnología tan envolvente que deja tan en abierto las conectividades hace que los espacios de intimidad queden expuestos y se reproducen conductas que pensábamos que estaban retrocediendo en nuestra sociedad.

Las posibilidades del machismo digital o del sexismo a golpe de WhatsApp son reales. Y, por lo tanto, no estamos todavía, no hemos llegado todavía, a ninguna página pornográfica ni a una página de delitos sexuales contra los menores, pero estamos en otro tipo de riesgos que, a mi juicio, tienen una gran trascendencia en la creación de estas preocupaciones.

Otro aspecto de riesgos: el *bullying* digital. El *bullying* digital es muy fuerte. Las posibilidades de hacer *bullying* digital son muy fáciles: desde grabarte una conversación a hacerte una fotografía inadecuada, hacerte *pressing*…Presionar y extorsionar, a través de la conectividad, resulta

muy fácil. Y, por lo tanto, es un espacio también donde el *bullying* pasa del entorno presencial al entorno digital con graves consecuencias. La mayoría de los datos que les pueden dar las Fuerzas y Cuerpos de Seguridad, en relación con las agresiones, con los suicidios juveniles, etcétera, tienen un fuerte componente vinculado al *bullying* digital.

Otro riesgo, el *sexting* y la *sextortion*, que son dos conceptos diferentes. El *sexting*: producir imágenes de contenido sexual explícito, difundirlas o provocarlas, comercializándolas o no, o utilizándolas para la extorsión. Otra posibilidad. El último dato que les puedo presentar, de hace solo un mes, donde la policía detuvo a menores porque habían difundido un vídeo de *sexting* de dos niñas de 13 años que, jugando, se habían hecho unas fotografías en sus domicilios, y que esos menores, mayores de 13 años pero menores, habían divulgado, es un dato asociado a esa realidad. *Sexting* y *sextortion* en menores y en adolescentes, son, pues, una posibilidad.

Y, evidentemente, el *grooming*, que es otra palabra un poco difícil, y que es la posibilidad, la facilidad con la que un adulto puede crear, a través de la suplantación de identidad, a través de la proximidad, a través de técnicas que puedan estar vinculadas a la «gamificación», al juego, a la propuesta, etcétera, elementos de confianza con menores en un entorno digital. Es muy fácil generar un entorno de confianza entre un adulto y un menor, si el adulto conoce cómo funcionan las reglas de construcción de reputación y de confianza en un entorno digital. A eso se llama *grooming*. En muchos casos, el *grooming* es la antesala de un abuso sexual o de una conducta inapropiada o ilícita.

Con esto, lo que les quería hacer notar es que, demasiado preocupados por el acceso a las páginas, hemos perdido de vista las posibilidades (las ventajas y los riesgos también) que puede tener para nuestros menores y nuestros adolescentes una alta densidad y conectividad, que, además, permita acceso a Internet, gracias a tabletas y dispositivos móviles.

Acabo con este —digamos— rosario de riesgos con las tecnoadicciones. Las tecnoadicciones, además, son un problema creciente; no tenemos todavía datos entre menores y adolescentes, pero la tecnoadicción es un problema real de nuestra sociedad. Para que ustedes se hagan una idea, el tiempo de exposición a una pantalla de proximidad (una pantalla que no es televisión, que no es cine, sino pantallas de proximidad entre nuestros adolescentes) está rozando las cuatro horas, es decir, muy por

encima del tiempo dedicado a la televisión. Estamos hablando de posibilidades de altas exposiciones que puedan generar tecnoadicciones.

Es en este contexto donde se sitúa la parte de las propuestas que me gustaría plantearles.

Primero, es muy importante la reacción de los principales buscadores que se ha conocido esta semana: Google y Bing, Google y Microsoft han anunciado un acuerdo para limitar 100.000 búsquedas relacionadas con pederastia, fotografías explícitas sexuales, etcétera. 100.000 palabras. Es un dato del 21 de noviembre, un dato muy relevante, juntos contra la pornografía infantil. Es decir, han encontrado 100.000 combinaciones de palabras y de preguntas que pueden llevar previsiblemente a una red oculta o a una red explícita de pornografía o de contenido explícito. Y, por lo tanto, lo que va a hacer el buscador es que cuando hayas escrito estas palabras y quieras llegar, no te dejará; te impide el acceso y te avisa de que, probablemente, estarás entrando en una zona de riesgo, desde el punto de vista de legalidad e ilegalidad. Es un dato relevante. Todo lo que puedan hacer en esta dirección, para conseguir grandes acuerdos con los principales *players*, con los principales operadores de Internet para que el acceso sea, digamos, alertado, severamente impedido o facilitado, háganlo. Incluso a costa de cualquier tipo de compensación, para el buscador o para el servidor, hagan cualquier tipo de acción; impedir el acceso último sigue siendo importante.

Segunda recomendación: la reacción de los medios de comunicación es vital para este combate. La iniciativa que está desarrollando, por ejemplo, *The Guardian*, o las informaciones recientes que hemos recibido en los medios de comunicación sobre sexismo digital, etcétera, contribuyen de manera extraordinaria a crear una cultura de prevención, de alerta, de atención. En este sentido, el ejemplo de *The Guardian* es un ejemplo magnífico. Ha recibido apoyo institucional, apoyo además privado y público para crear contenidos de valor alrededor de la protección de los derechos de los menores. Es una de las cosas de las que les voy también a advertir en una de mis próximas recomendaciones. Faltan recursos, faltan pistas, faltan documentos, faltan buenas prácticas para nuestros profesores, educadores… para nuestras familias. Por lo tanto, si hay un medio de comunicación que toma esa decisión de crear repositorios, contenidos, vídeos, etcétera, hay que apoyarle. Y desde las administraciones hay que hacer todo tipo de esfuerzo para que los medios de comunicación *online* y *offline*, públicos y privados, dispongan de muchos contenidos a favor de la educación y de la cultura digital. Esa es una buena iniciativa. El acuer-

do de *The Guardian* está hecho con Naciones Unidas y con el Gobierno británico, y es un ejemplo extraordinario. Se ha convertido en la principal fuente de información para el mundo anglosajón y, en particular, el mundo británico. Deben ustedes saber también que la iniciativa del Gobierno británico en la regulación y en la defensa de los derechos de los menores es la que ha provocado que Google y Microsoft hayan reaccionado. Por lo tanto, ustedes tienen muchas posibilidades todavía en sus manos. Es decir, cuando fuerzan, apoyan y promocionan, las empresas pueden reaccionar. Y la segunda recomendación es: apoyen a aquellos medios de comunicación públicos y privados que hacen de la información, en relación con estos temas, un centro de su interés.

Tercera recomendación: hay que introducir en la oferta educativa reglada el concepto de que en la vida de las personas será tan importante el currículum vítae como el *digital vitae*. Nuestros jóvenes, cuando estén en condiciones de buscar un máster o ir a la universidad o buscar trabajo, sus empleadores les van a medir por el *digital vitae*. Nuestros niños y nuestros menores y nuestros adolescentes tienen que saber que educarse y formarse y pasar y conseguir unas determinadas matriculaciones, notas y superar determinadas cotas en el sistema educativo tiene que estar asociado también al *digital vitae*. Si uno descuida su *digital vitae*, lo más probable es que tenga problemas de empleabilidad muy serios. En el 70 % de las decisiones de contratación de un empleado en los Estados Unidos, el principal dosier, la principal carpeta es el *digital vitae*. Por lo tanto, no podemos educar a nuestros menores sin la conciencia de que su *digital vitae* tendrá consecuencias para ellos en la vida. De la misma manera que si abandonan los estudios, suspenden o incumplen, digamos, su programación educativa, pues eso tiene consecuencias también para ellos y para sus relaciones familiares.

El *digital vitae* es el centro, y eso, lamentablemente, tengo que decirles que ni en la nueva Ley de Educación ni en las últimas leyes está en el epicentro de nuestro sistema de formación. Si no introducen esta variable, va a ser muy difícil. Los niños y los adolescentes tienen que saber que lo que dejan no es su pasado, es su futuro, que esto es arqueología al revés, que lo que van a encontrarse en el futuro es lo que dejaron, y que eso puede tener consecuencias para ellos en términos de proyección, relaciones, etcétera.

Cuarta recomendación: nuestro mundo avanza imparablemente a una altísima conectividad, en donde la identidad segura se convierte en un

elemento central de la conectividad; saber quién soy, saber con quién voy a hablar, saber qué operación, transacción de información, de dato, de compra, de lo que sea, la identidad segura es un elemento central. De la misma manera que educamos a nuestros menores en que hay un momento en la vida en que necesitan un documento nacional de identidad que es imprescindible para una serie de transacciones, de operaciones y de relaciones en el mundo adulto, tienen que saber que su identidad digital jugará el mismo papel. Y, por lo tanto, hay que educar a nuestros menores en el concepto de identidad digital, que tiene mucho que ver con el *digital vitae*, aunque que es otra cosa.

Quinta recomendación: he visto en sus documentos que hablan ustedes de profesores y de educantes, etcétera; pero donde tenemos el vacío es en las AMPA, las Asociaciones de Padres y Madres de Alumnos, que se sienten desbordadas, desesperanzadas y angustiadas por lo que no comprenden. Y, en consecuencia, hay que tranquilizar a los padres y a las madres, a nuestros adultos, de que es posible enseñar a ser digital de la misma manera que se enseña a andar. Con el siguiente proceso: cuando enseñamos a nuestros niños y niñas a andar, les damos la mano, les ayudamos en esos primeros pasos, les ponemos un andador cuando todavía no se pueden sostener, les damos la mano y después les damos el dedito; y, cuando les soltamos, apartando ese dedito, estamos cerca para que no se caigan. Lo mismo que hacemos para enseñarles a andar hay que hacerlo en lo digital. Con unos padres que no sepan dar la mano digital, es muy probable que ese niño se pegue un trompazo, muy probable. Por lo tanto, la mano digital es fundamental.

Primer concepto, la mano. Segundo, las normas: cuando nuestros menores saben andar les enseñamos el semáforo rojo, el paso de cebra, la acera y la calle; les decimos que para caminar por la calle no pueden ir por la vía, tienen que ir por la acera, y que cuando hay un semáforo en rojo o ámbar deben pararse o no deben cruzar. Por lo tanto, segunda parte: las normas, qué cosas pueden ser nocivas, qué cosas pueden ser ilegales. Y eso me parece que es muy importante.

Y tercero, el acompañamiento: cuando les dejamos ir solos al colegio, nos preocupamos de qué línea de metro van a coger, si llevan la tarjeta o no para coger el metro, a qué hora salen y a qué hora van a llegar, y por qué ruta van a ir. Van solos, pero estamos pendientes. Entonces, o somos capaces de introducir en la sociedad española, que dada la brutal disrupción de lo digital en la vida familiar, los padres tienen que estar en

condiciones de dar la mano, mostrar las normas y hacer acompañamiento, como cuando les enseñamos a andar, o vamos hacia un problema muy serio de autoridad, digamos, no solamente familiar, sino de autoridad en la sociedad, muy importante.

Sexta idea: a nuestros menores y a nuestros adolescentes les acabamos preguntando quiénes son sus amigos y cómo se llaman, y cuáles son las familias de sus amigos; nos preocupan sus relaciones presenciales. Si a las familias y a los educadores no les preocupan las relaciones digitales, que van a ser el centro de la socialización, no les vamos a poder dar la mano. Por lo tanto, este es un esfuerzo que solo se puede hacer si comprendes cómo se construyen las relaciones humanas en un entorno digital. Pero conocer las relaciones es muy importante.

Y acabo con la última cosa, y después dos recomendaciones muy pequeñas con las que me voy a atrever.

Lo nocivo y lo ilegal no son lo mismo. El aprendizaje y el conocimiento de lo nocivo puede ser la mejor manera de impedir lo ilegal o una práctica ilegal o un uso ilegal. Si ustedes solo se conforman, o nos conformamos, con impedir lo ilegal, es decir, controlar el acceso, y no trabajamos sobre las posibilidades, los riesgos y las ventajas, lo nocivo y lo positivo de una alta conectividad en nuestros entornos, yo creo que cometeremos un gran error; no es lo mismo. A nuestros hijos, cuando les educamos, cuando les decimos lo que está bien y lo que está mal, lo que está mal se lo mostramos, cada uno a su manera, cada uno con sus valores, cada uno con sus principios, pero la opción de elegir lo positivo y lo negativo, el bien y el mal, lo conveniente o lo inconveniente, se establece basándose en una elección. Y, por lo tanto, lo nocivo no puede ser evitado en este proceso de educación: hay que mostrar lo nocivo, acompañar para que se pueda escoger, para que progresivamente menores, adolescentes y jóvenes puedan controlar su *digital vitae*.

Las últimas recomendaciones: creo que ustedes deben impulsar coaliciones amplias público-privadas, instituciones-sociedad civil en este combate; Ciberalerta, Generaciones Interactivas, PantallasAmigas, Enfoque Seguro son organizaciones a las que hay que animar, potenciar, estimular, proteger, favorecer…; están haciendo un trabajo extraordinario. Hay que liberarlas de cargas, es decir, hay que estimular, hay que hacer una ofensiva muy proactiva en favor de coaliciones amplias sociedad-instituciones.

Segunda recomendación: ustedes deben compartir la información. Entiendo que esto es una ponencia y, por lo tanto, se produce en un escenario, digamos, reservado. Pero uno de los grandes problemas que tiene la sociedad española es que hay mucha información disgregada. Por ejemplo, la Policía Nacional, que estuvo aquí, entiendo, con una de las ponencias, pues no sé si conoce suficientemente bien las prácticas de los Mossos d'Esquadra, por poner un ejemplo, u otras, sobre datos, buenas prácticas, etcétera. Lo mismo pasa entre el Senado y el Congreso, en relación a que hay una Comisión sobre redes; lo mismo pasa entre esta ponencia y los ponentes; yo me atreví a hacer una página web que se llama Red Segura con las ponencias que ustedes publican; soy un ciudadano, ustedes publican una información, tengo derecho a hacerlo, me interesa el tema, lo publicado, y es una página de referencia. Es decir, no hay documentación compartida y, por tanto, tenemos que hacer un alzamiento de documentación compartida lo más rápidamente posible para que todos aquellos que quieran ser partícipes de este combate puedan participar.

Y con esto acabo. Ustedes me han llamado para hablar de los riesgos, y quería ser honesto con esta petición y hablarles de los riesgos. Pero el principal riesgo es el desconocimiento: si la sociedad española no conoce el potencial, no de riesgo, sino de beneficio de la alta conectividad, van a faltar leyes y policías, y jueces…van a faltar, pero muchísimos. Y, por ello, lo que hay que introducir es una nueva cultura de educación que tenga que ver con el *digital vitae* y con el enorme potencial que esto puede tener en la escuela y en las familias, y con la necesidad que tenemos de apoyar a nuestros padres, a las familias en este proceso. El ejemplo de la mano es muy ilustrativo: les damos la mano a nuestros hijos, se la soltamos, pero les enseñamos las normas y después les acompañamos, aunque no vayamos con ellos. Es lo mismo que hay que hacer. Si dejamos solos a nuestros menores y a nuestros adolescentes en este entorno de alta conectividad, la incapacidad que van a tener los educadores y los padres para hacer este proceso educativo será extraordinaria; y podemos perder, no sé si una generación, pero sin tener unos niveles de influencia positiva en términos de autoridad, en términos de trazabilidad social, en términos de valores compartidos, a una nueva generación que —en muy poco tiempo— va a considerar que sus amigos son un *link*, no una persona.

Espero que les haya sido útil. Les facilitaré esta información y los datos en un documento. Gracias.

COMPARECENCIA DEL PROFESOR TITULAR DE LA FACULTAD DE PSICOLOGÍA DE LA UNIVERSIDAD DE VALENCIA, D. MARIANO CHÓLIZ MONTAÑÉS, EN LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 27 DE NOVIEMBRE DE 2013.

El señor **PROFESOR TITULAR DE LA FACULTAD DE PSICOLOGÍA DE LA UNIVERSIDAD DE VALENCIA** (D. Mariano Chóliz Montañés): Muchas gracias, presidente. Lo primero de todo, quiero agradecer muy sinceramente la oportunidad de estar aquí con sus señorías; para mí es un orgullo y un honor que podamos debatir sobre cosas en que estamos trabajando en el día a día. Entiendo, además, que la soberanía del pueblo reside en sus representantes, y tener la oportunidad de dialogar con ustedes para mí es una satisfacción enorme. Además tengo amistad personal con una de sus señorías; yo vivo en La Eliana, y entonces fue una casualidad cuando me llamó a la Universidad de Valencia, y como yo estaba trabajando en esto, pues satisfacción triple.

Me llamo Mariano Chóliz; soy profesor titular de universidad, estoy acreditado a catedrático, pero corren tiempos difíciles, ¿verdad?, y está la plaza que no sale. Pero ahí estamos. Mi área de investigación son las adicciones, las adicciones comportamentales, es decir, las que no tienen sustancia; y dentro de las adicciones, la adicción al juego y las adicciones tecnológicas. Y esa es el área en la que llevo trabajando varios años.

Yo había pensado en hacer una breve introducción de los riesgos que puede tener Internet, y en concreto más las redes sociales también, en menores; y después abordar dos temas que tienen que ver con lo que son las adicciones, que son la adicción a Internet y la adicción provocada por Internet, que puede ser de otro tipo. Y en cualquier momento, si al hilo de lo que estoy hablando sus señorías quieren comentar alguna cosa, pues podemos hablarlo, como ustedes deseen.

Más que de menores voy a hablar de adolescentes, en el sentido de que es el término psicológico, si quieren, «menor» es el término jurídico; la importancia a nivel psicológico es el desarrollo evolutivo, principalmente en la adolescencia, aunque también en la última parte de la infancia, primera de la juventud, etcétera.

En principio habría dos preguntas que hacernos: por qué son tan relevantes Internet y las nuevas tecnologías en los adolescentes y por qué provocan esta alarma social. He puesto entre comillas «nuevas tecnologías» porque para los menores no son nuevas, existen de toda la vida. Ya les habrán hablado de que son nativos digitales, nosotros somos inmigrantes digitales que hemos llegado a esa tierra ignota.

De cualquier manera, eso también es un arma de doble filo, en el sentido de que se lo decimos tantas veces que ellos llegan a pensar que son unos *hackers* y son unos auténticos expertos; son unos superusuarios (ya habrán tenido la oportunidad), con los riesgos que eso tiene. Son unos usuarios extraordinarios de las tecnologías pero no las han fabricado ellos. Y ese es uno de los problemas que pueden llegar a tener en ese exceso de confianza muchas veces.

¿Por qué son tan relevantes las tecnologías para los adolescentes? Pues provocan fascinación; para ellos no hay nada mejor que les regalen una tableta, en función de la edad será una tecnología u otra, pero es el regalo estrella. Aprenden rápidamente el manejo. Todo tiene una similitud en el manejo, y el aprendizaje se generaliza. Las utilizan, las herramientas tecnológicas las aprovechan más de lo que podemos aprovecharlas los más mayores, es una forma de ocio atractiva, y principalmente lo que a nosotros nos ocupa es que son un instrumento extraordinario para favorecer las relaciones interpersonales. Puede parecer un poco paradójico porque muchas veces se critica «están en Internet y no están en la calle». Están en Internet y después están en la calle o no. Pero de hecho, lo que se dicen por Internet, cara a cara no se lo llegarían a decir. Es decir, de alguna manera es un modelo de relación interpersonal que es cambiante, que está cambiando y que los adolescentes lo utilizan muchísimo. Prácticamente todos los adolescentes tienen un teléfono móvil en la actualidad. Y además, ya en la actualidad, conectado a Internet, y los videojuegos es probablemente la forma de ocio más generalizada, al menos en nuestra sociedad.

Entonces, ¿por qué provocan alarma social, si las tecnologías son tan extraordinarias y para ellos tan fascinantes? Pues por varios problemas, entre ellos dos: el ciberacoso (del que en esta ponencia han tenido oportunidad de discutir varias veces) y otro, el tema de la adicción, que es en el que yo me quería centrar un poco más. Aparte de que muchas veces los adultos tienen reticencia por esas nuevas tecnologías. Cada vez me-

nos, porque como también somos usuarios, cada vez las vamos teniendo menos, pero en principio que si el libro contra el ordenador, que si la red social y no estás en la calle, etcétera. Había, digamos, cierto recelo por estos temas, sobre todo cuando vemos que los niños son tan diestros, mucho más que los propios adultos. Entonces, eso genera una especie de alarma. Pero principalmente por los riesgos que tiene, que es el objeto de esta ponencia.

Esto lo voy a pasar un poco más rápido, pero serían los criterios del diagnóstico para un trastorno adictivo. El uso excesivo o compulsivo de las tecnologías puede llevar a tener un problema de adicción. Y en la adicción, a mí me gustaría que hicieran el parangón con lo que puede ser cualquier otra drogodependencia, pero en lugar de sustancia es el uso, en este caso de las tecnologías. Manifiestan tolerancia, es decir, cada vez necesitan utilizar más las tecnologías, se encuentran mal cuando no pueden realizarlas, digamos, o cuando se interrumpe Internet, no pueden dejar de utilizarlo aunque lo pretendan, emplean excesivo tiempo, es decir, muestran un patrón que clínicamente es muy parecido a lo que es un trastorno adictivo.

Hablamos de menores y hablamos de adicciones en la adolescencia porque los adolescentes son especialmente vulnerables a cualquier adicción, no solamente a las tecnológicas sino a cualquier drogodependencia o a cualquier adicción, por cuestiones de desarrollo. La adolescencia es un periodo crítico para la prevención de las adicciones en este sentido. Todavía no están desarrolladas las áreas del córtex prefrontal que son responsables del control del comportamiento, de la planificación, etcétera, y eso les hace especialmente vulnerables; aparte de que ellos necesitan actividades que les activen extraordinariamente o que les provoquen mucho placer, cuando son poco resistentes a la frustración, y manejan mal sus impulsos, digamos de alguna manera (esto es una cuestión de desarrollo, todos hemos sido adolescentes). Es decir, la adolescencia es un periodo especialmente crítico para cualquier adicción. Si además estamos en que los adolescentes utilizan universalmente las tecnologías, podemos llegar a tener un problema en ese sentido de adicción a las tecnologías, iniciada en la adolescencia.

Esta sería un poco la introducción y la contextualización. Yo quería centrarme en dos tipos de problemas adictivos que están relacionados con los adolescentes y las tecnologías. En un primer lugar la adicción a

Internet, y más en concreto a lo que son las redes sociales, que se reflejaría por una dependencia de la red social (hasta hace poco Tuenti, ahora Facebook) por parte de menores; y otro tipo de adicciones que son provocadas por la propia Internet. En ese caso, por el área de investigación en la que yo me encuentro, es la adicción al juego de azar. La adicción al juego es una patología grave. Y en la medida en que el juego también se hace *online*, Internet tiene una serie de aspectos que agravan, digamos, el riesgo de cualquier juego de azar. Y ahí me iba a centrar un poco.

En lo que se refiere a las adicciones tecnológicas, en la Universidad de Valencia hemos desarrollado un programa de prevención, que hemos pasado a más de 6.000 adolescentes, principalmente en la comunidad valenciana pero también en otras comunidades autónomas y también en otros países, básicamente basándonos en varios principios.

En primer lugar, que la prevención debe ser universal en el sentido de que todos los adolescentes utilizan las tecnologías; por lo tanto, debe haber en el ámbito escolar, y además ahora que ya hay especialidades de Magisterio de nuevas tecnologías, especial precaución en la prevención de este tipo de adicciones en el ámbito escolar, que además es donde los tenemos recluidos (bueno, identificados); todos los menores están escolarizados en ese sentido hasta los 16 años; entonces, debe ser universal en ese sentido.

La prevención debe ocurrir antes de que aparezca la conducta problemática, si no, ya después tenemos que ir a tratamientos. Y la información es necesaria, eso se ha visto en cualquier tipo de prevención, pero no es suficiente. Además de informar, que hay que informar, por supuestísimo, hay que sensibilizar y hay que enseñar a la gente qué es lo que tiene que hacer. Entonces, nosotros desarrollamos un programa de prevención que, si a alguna de sus señorías le interesa, se lo puedo hacer llegar, que nos lo va a editar TEA (TEA es una editorial de test psicológicos) y que se lo voy a presentar ahora.

No sé el tiempo que llevo. ¿Quince minutos ya? Entonces se lo voy a presentar simplemente así para que lo vean, y si a alguna de sus señorías le interesa, se lo paso con mucho gusto.

Es un programa de prevención que va en un DVD y que pretende utilizarse en el ámbito escolar, en lo que son las clases de tutorías; hay un módulo de móvil, otro de Internet y otro de videojuegos, con tres sesiones. La primera sesión es puramente informativa, en la que a los chavales

se les dice cuáles son las ventajas, ya de una manera didáctica, interaccionando con ellos: ¿qué ventajas tiene Internet? Pues las ventajas que puede tener Internet. ¿Qué inconvenientes puede llegar a tener Internet? Y después se les pasa una serie de cuestionarios (en psicología tenemos que medir), y se les enseñan actividades. Esto está pensado para el ámbito escolar, pues vamos a hacer tres tareas: ponte un horario semanal para conectarte a Internet, procura no conectarte todos los días, no conectarte más de una hora los días que te conectes; y antes de conectarte, por ejemplo, decide qué es lo que vas a hacer. Se llega a una negociación. Un ejemplo: me voy a conectar los martes de 7 a 8, los jueves de 8 a 9 y los sábados en este horario, y cada uno el horario que le convenga. Y después, a la semana siguiente, se revisa.

Si hay tiempo, se le explica lo que son los criterios de adicción a Internet, y si no hay tiempo ya se pasa a la siguiente sesión, en la que se intenta ver qué tal les ha ido el trabajo durante la semana, si recuerdan los criterios de la adicción a Internet. Y ya, para sensibilizar, utilizamos dos tipos de estrategias: o bien el humor (mediante cómics), o bien los testimonios de chavales que han tenido ese problema con adicción a Internet. Entonces, aquí tenemos un vídeo de un chaval que tenía problemas de adicción a Internet (si quieren las señorías, después lo vemos). Y se debate qué problemas ha tenido. Si queda más tiempo, se va con el humor: «querido Miguel, ¿cómo te va? Por aquí bien pero te echamos de menos; por favor, apaga el ordenador y baja a comer algo. Con cariño, tus papás». Y a los chavales se les dice; esto se lo podemos decir, pero igual que se lo dice su maestro, igual que se lo dicen sus padres. Con el humor, digamos que de alguna manera rompemos las barreras que tienen. ¿Qué le pasa, qué le ocurre? Y los chavales debaten qué es lo que le ocurre: que se aísla de su familia por utilizar demasiado Internet, está demasiado tiempo, no puede dejar de conectarse, etcétera.

Y después, qué es lo que se puede hacer: utilizar Internet en una zona común, etcétera. Es decir, buscar estrategias que sean ellos mismos los que las propongan, porque cuando uno propone las estrategias es más fácil que después las cumplan. Hay decenas de cómics, hay varios testimonios también para que los tutores, los profesores puedan utilizarlo en la medida en que consideren.

Después habría otra sesión también igual, para reforzar, y lo mismo para móvil o videojuegos. Nosotros recomendamos que se haga una cada

año: tres sesiones de Internet un año, tres de móvil otro, tres de videojuegos. Ya digo, esto lo hemos pasado a más de 6.000 adolescentes, es un programa que está acreditado por la Generalitat Valenciana como oficial para prevención de adicciones tecnológicas; es el único que hay, y que pongo a su disposición por si a alguien le interesa, por supuesto. De aquí han salido dos tesis doctorales, tenemos varios trabajos científicos; puede ser interesante. Y aparte, también hemos creado una unidad para tratamiento, que sería el libro que les he presentado.

Disculpen ustedes por la rapidez, pero quería centrarme ahora en el siguiente tema, que es el juego *online*, la adicción al juego *online*. Hemos hablado un poco de la vulnerabilidad de los adolescentes a las tecnologías, a las adicciones tecnológicas; hemos visto quizás una de las socialmente más visibles, que es el tiempo que pasan los chavales en Internet y todo el problema que eso tiene.

Pero Internet es también una herramienta extraordinariamente útil, qué voy a decir, Internet es la seña de identidad de nuestras sociedades, pero que en el caso del juego puede llegar a ser un problema. En DSM-V, que es el manual de clasificación de los trastornos psiquiátricos, en mayo de este año lo que antiguamente se llamaba ludopatía y después juego patológico se ha categorizado en el mismo paquete que las drogodependencias; ahora están drogodependencias, alcoholismo, tabaquismo y juego como trastornos adictivos, puesto que ha habido un incremento de evidencias –leo textualmente de la APA– consistente en que el juego activa el sistema cerebral de recompensa de forma similar a como lo hacen las drogas de abuso, ya que los síntomas clínicos de los trastornos provocados por el juego son similares a los que provocan las drogas. Es decir, cuando estamos hablando del juego patológico no estamos hablando ni de un vicio ni de alguien que juega porque quiere y tal, sino de una verdadera enfermedad mental, similar en este caso a las drogodependencias.

Hay una serie de síntomas clínicos que me voy a pasar.

A modo de perspectiva social sí quería poner un par de datos. El juego, aparte de ser un problema, la adicción al juego, es una de las actividades económicas más relevantes, supone más del 2% del PIB en España en la actualidad. Esta sería la evolución de lo que los españoles nos hemos gastado en juego desde 1996 hasta 2011 en miles de millones de euros (en 2008, 32.000 millones de euros), en juegos legales (loterías, casinos, bingos, tragaperras). A partir de 2008 y por efecto directo de la crisis, fue

disminuyendo la cantidad de juego que se jugaba; actualmente estaremos en 23.000 millones de euros en ese tipo de juegos.

En 2011 ocurre otro fenómeno, que es la ley de regulación del juego. Hasta 2011 el juego *online* en España era ilegal; no estaba legalizado y en ese momento todo el juego que no estaba expresamente permitido estaba prohibido. Sin embargo, se venían patrocinando equipos de fútbol (Bwin el Real Madrid, etcétera, Unibet al Valencia y tal). Era alegal, pero, bueno... En 2011 se legaliza y esta sería la gráfica. Es decir, introduciendo, incorporando los juegos legales de azar al *online*, tendríamos que en 2011 (esto sería en el gasto: casinos, bingos, lotería nacional, esto es sorprendente, las tragaperras, las máquinas tragaperras), y el juego *online* en 2011 era sobre 3.000 millones de euros, ya, en el momento de la aparición de la ley. En 2012 todos los juegos bajan, excepto el *online*, que sube. Y por estimaciones, porque no son datos totalmente... fiables sí son, pero no son al euro, digamos, estaríamos hablando de 5.000 millones de euros.

Además yo participo en una asociación de jugadores como asesor, en FEJAR, que es una federación nacional, y actualmente el juego *online* ya es el segundo juego en gravedad para provocar adicción al juego, solamente detrás de las tragaperras, que por supuesto son las reinas del mambo todavía, en este caso. Pero en juego *online* ya estamos hablando de que habrá 1.400.000 personas que están identificadas para jugar y se han gastado 5.000 millones de euros; es decir, 4.000 euros por persona de media al año; hay gente que puede estar perdiendo fortunas, como de hecho creo que está pasando.

¿Y por qué en una ponencia de menores esto? Pues porque arranca ya aquí. Es decir, el juego *online* es un juego que se lleva a cabo en Internet, que hay dos tipos de juegos que son especialmente atractivos, más para jóvenes; vamos a ver, los menores no pueden jugar, pero tampoco pueden beber alcohol, ¿no? De hecho, juegan. En la capacidad que tienen y con los subterfugios que tengan, pero sobre todo están aprendiendo a jugar. Porque, a mi juicio, estamos llevando una deriva a que el juego *online* se ve como una oportunidad de negocio, como efectivamente lo es para algunas personas o algunas empresas, pero tiene sus riesgos, tiene riesgos importantes. El juego *online* tiene una serie de características que estructuralmente lo hacen muy peligroso: es muy accesible, ya se puede jugar técnicamente con teléfonos móviles, se puede jugar en cualquier cone-

xión a Internet. El premio es inmediato: esa es una de las características por las cuales las tragaperras son tan adictivas, porque el premio te lo dan inmediatamente, es atractivo. Y aprovechan todos los recursos de las nuevas tecnologías: te dan bonos de bienvenida. Esos bonos de bienvenida, en psicología se llama «muestra de reforzamiento», es una estrategia que se utiliza cuando una conducta es muy raro que se lleve a cabo y la tienes que reforzar antes, le tienes que dar el premio antes. Claro, aquí te dan equis euros para jugar, de otra manera nadie se pondría a jugar.

Pero sobre todo es que es un nuevo nicho de mercado: quiero decir, todos los juegos que estaban legales, digamos, anteriormente, eran principalmente personas adultas, a partir de 40 años, principalmente. La mayor parte de personas que están accediendo por primera vez al juego, y al juego *online*, son jóvenes. Aquí tenía un anuncio de Rafa Nadal jugando al póquer.

Esto es una página de *20 Minutos*, que es un periódico gratuito, de tirada, en la que esto se habla de tres veinteañeros que se han forrado por llevarse un montón de millones jugando al póquer. Esto en realidad es un anuncio; parece una noticia, pero es publicidad de una casa de apuestas. Hay un interés en promocionar el póquer *online*, y además venderlo como si fuera una forma profesional. A ver si tengo la oportunidad de que se vea... Son dos minutos y medio o una cosa así.

[VÍDEO]

El tema es cómo se está vendiendo esta actividad, ¿no? Una actividad que de hecho ha movido en España 5.000 millones de euros este año, que realmente mueve mucho dinero. Y aquí el dinero, si me permiten, ni se crea ni se destruye, solo cambia de bolsillo; quiero decir que las ganancias de todos estos chavales son fruto de las pérdidas de otros. Porque en el póquer, unos ganan y otros pierden. Yo no digo que se vaya a prohibir, pero que habrá que regular de alguna manera, porque si no después, ¿cómo hacemos prevención nosotros? ¿Y qué valores les estamos transmitiendo cuando están viendo esto?, a los chavales, me refiero. Cuando hacemos nuestro programa de prevención como el que hemos hecho de redes sociales y decimos «el valor del esfuerzo» y tal, dicen «¿pero para qué?». Les estamos vendiendo otra cosa.

Y algo que todavía no está, pero que sería a mi juicio bastante peligroso es una noticia relativamente reciente, de 888, que es una de las casas de apuestas más fuertes del mundo; 888 ha reconocido el potencial de los juegos sociales. Nuestra oferta de Facebook Freemium, en juego por diversión, han encontrado una importante audiencia y estamos muy entusiasmados con la oportunidad de los juegos de dinero real en Facebook; estamos trabajando codo a codo con Facebook en este lanzamiento asegurando que introducimos lo mejor de ambos mundos, de dinero real y los juegos sociales. Con lo cual, si no solamente en Internet, si se meten en Facebook, que tiene, ¿cuántos usuarios?, mil y pico millones en el mundo, pues podemos tener un problema. Aquí esto no es tan sencillo puesto que hay barreras internacionales y todas esas cosas, cada país tiene su legislación. Pero puede ser un problema.

Y por último, ya para dejarlo un poco más... Digamos que la reflexión que a mí me gustaría hacer aquí es eso, el tema de cómo vamos a prevenir a los menores la adicción al juego *online* diciéndoles lo importante que es el esfuerzo, que el dinero no es todo, en fin, cuando te vienen con historias de este otro tipo. Es muy difícil.

Y si quieren sus señorías... Esto es un anuncio muy antiguo.

[VÍDEO]

Quiero decir, ¿qué valores les estamos transmitiendo? Quiero decir que es un tema que a mí como docente y como profesor, que estás viendo a los chavales y que los ves ahí, pues me preocupa.

Y de nuevo les agradezco la atención que me han prestado, y a su disposición para lo que deseen.

COMPARECENCIA DEL DECANO-PRESIDENTE DEL COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN (COIT) D. EUGENIO FONTÁN OÑATE, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 30 ENERO DE 2014.

Buenos días. Agradezco en mi nombre y en el del Colegio Oficial de Ingenieros de Telecomunicación la invitación a comparecer ante sus señorías para trasladarles nuestra visión sobre este tema que consideramos fundamental para conseguir un correcto desarrollo de los servicios de la Sociedad de la Información: dotar a los mismos de las garantías suficientes de uso por parte de los usuarios, especialmente los menores, los llamados nativos digitales.

Como ustedes saben, las redes sociales, de las que los jóvenes son usuarios intensivos, son servicios basados en plataformas que operan sobre internet y que, resumidamente, constituyen una nueva forma de comunicación, todavía en expansión. Los ingenieros de telecomunicación, aplicando nuestro conocimiento científico y técnico, hemos contribuido a diseñar y construir las redes de telecomunicaciones necesarias para el desarrollo de este y otros paradigmas tecnológicos que están convirtiendo a Internet en la herramienta de la pancomunicación.

Lo que inicialmente se llamó «web 2.0» a mediados de la década pasada (o lo que es lo mismo, las primeras experiencias de interactividad entre los emisores de información y los receptores de la misma) ha derivado hacia un nuevo escenario donde prácticamente todos los usuarios somos creadores de contenido y lo compartimos a través de herramientas como estas que hoy nos ocupan. Desde cualquier punto del planeta y desde cualquiera que sea el terminal (fijo, móvil, televisión, ...) podemos conseguir una repercusión a nuestros mensajes impensable hace una década, proceso que viene acentuándose con la democratización del acceso a las redes de telecomunicación, que en el caso concreto de nuestro país llega a índices muy elevados de penetración. Según el informe anual presentado este mismo mes por la Fundación Telefónica, en la franja de 16 a

24 años, un 86% de los usuarios de Internet son intensivos, esto es, viven conectados y consultan el móvil unas 150 veces al día.

Hoy en día cada dos minutos se publican en Facebook tantas fotos como se hicieron en todo el siglo XIX. En 48 horas se genera la misma información que la humanidad había creado desde el inicio de los tiempos hasta el año 2003 *(Eric Schmidt)*. 48 horas de video se suben cada minuto a Youtube. 200 millones de tuits se lanzan diariamente en Twitter… y todo esto es posible porque las telecomunicaciones siguen avanzando a un ritmo imparable. La evolución de la banda ancha y la fibra hasta el hogar y la evolución de las redes móviles que han incrementado la capacidad de datos con UMTS y LTE (3ª y 4ª generación respectivamente), unido a la irrupción de nuevos dispositivos (fundamentalmente tablets y smartphones) ha permitido ubicuidad del acceso a las redes sociales, y otros servicios de internet, por parte de un amplio espectro de la población.

El siguiente estadio, llamado «Internet de las cosas», permitirá conectar los objetos a Internet, y a los mismos, recopilar información sobre las costumbres y pautas de comportamiento de los usuarios y consumidores. Se calcula que en 2020 habrá 50.000 millones de dispositivos conectados a la red. Éstos captarán cantidades ingentes de información que, almacenada y procesada, estará disponible para la toma de decisiones en todos los ámbitos. Lo que hemos dado en llamar la era del Big Data es uno de los campos de estudio más pujantes actualmente de la ingeniería. Las principales empresas se están posicionando en materia de análisis y procesamiento de esta inmensa cantidad de información que vamos a manejar. Este nuevo entorno de los macrodatos, ya en puertas, nos va a plantear retos apasionantes a los ingenieros y sociólogos, pero también a las autoridades que deben anticipar los riesgos derivados y ofrecer garantías al ciudadano sobre la custodia de sus datos.

Es por ello que, dado que otros expertos más cualificados que yo desgranarán ante ustedes las prácticas abiertamente delictivas que se producen en la Red y que afectan a los menores, y también desde otras ramas se les expondrá la necesidad de formar a nuestros jóvenes para el correcto uso de estas herramientas, me van a permitir centrarme en este aspecto concreto que trato de introducir: estos avances revolucionarios que he mencionado, que sin duda facilitarán la vida de las personas,

tienen implicaciones muy importantes en cuanto al manejo de lo que denominamos «identidad digital» y también sobre el propio concepto de privacidad y su protección. Existe y existirá cada vez más y más información nuestra en el mundo virtual, las herramientas para procesar esa información e inferir conclusiones sobre nuestras pautas de comportamiento o de consumo se están perfeccionando y debemos adelantarnos a estos cambios para que se produzcan con todas las garantías.

Sin embargo, se da la paradoja de que este nuevo medio de comunicación, Internet, el más poderoso de los inventados hasta la fecha, está sometido a instrumentos regulatorios tradicionales, que en muchos casos no están adaptados a esta realidad totalmente nueva. Las telecomunicaciones se regulan internacionalmente a través de organismos como la Unión Internacional de Telecomunicaciones (dependiente de la ONU) lo que, entre otras cosas, garantiza que podamos realizar una llamada a otro país, o usar el mismo terminal móvil cuando vamos al extranjero, por ejemplo. Aspectos como estos son coordinados internacionalmente.

Es cierto además que en el entorno de Internet existen organismos internacionales como la Internet Engineering Task Force (IETF) que coordina los nuevos protocolos de comunicación entre servidores de internet o ICANN (Internet Corporation for Assigned Names and Numbers) que coordina la administración de los elementos técnicos del DNS para garantizar la resolución unívoca de los nombres, una organización que, por cierto, fue creada por mandato del gobierno estadounidense y responde únicamente al mismo, aunque regule la asignación de dominios en Internet en todo el mundo, pero esta coordinación internacional en el ámbito de Internet es principalmente técnica. De hecho, ICANN, integrado por expertos representantes de instituciones y empresas, es el organismo que más se aproxima a encarnar hoy por hoy la gobernanza en Internet. Sobre esto existe un debate muy interesante, poco conocido por el gran público, que demuestra que estamos ante una disyuntiva que marcará el destino de la red: ¿debe ser regulada a través de los mecanismos convencionales regulatorios que se aplican a los asuntos supranacionales o vamos hacia un modelo de autorregulación acordada por los agentes implicados, cercanos a las continuas novedades tecnológicas y de negocio?

Es notorio que la práctica totalidad de las redes sociales de mayor éxito son estadounidenses, por lo que al usuario de a pie español o europeo, nadie le informa ni le garantiza si se están cumpliendo o no los derechos que tiene en su respectivo país respecto a sus datos o si, permítanme el comentario, en su actividad en la red pesa más la primera enmienda[1] de la Constitución americana. ¿Dónde se almacenan nuestros datos?¿qué se hace con ellos?¿Se manejan con las debidas garantías de seguridad? El usuario de a pie no tiene respuesta a estas preguntas.

A mediados de diciembre pasado los grandes gigantes de Internet (Google, Microsoft, Yahoo, Facebook, Twitter, Netflix, LinkedIn, Comcast, AT&T) se reunían con el presidente Obama para reclamar transparencia sobre las operaciones de las agencias de inteligencia estadounidense sobre los datos de la Red. Es curioso que muchas de estas empresas soliciten transparencia y apertura tanto al gobierno como a los ciudadanos y a su vez oculten los modelos predictivos que han desarrollado sobre los datos de sus usuarios.

El debate sobre la privacidad ha puesto en el otro brazo de la balanza la seguridad (siendo supuestamente la primera de más peso para los europeos y la segunda para los estadounidenses). Jaron Lanier, uno de los gurús más influyentes del mundo de Internet, afirmaba recientemente en un artículo publicado por «Investigación y Ciencia» que *«Cuando se habla del gran compromiso entre privacidad y seguridad, o entre privacidad y servicios, se da a entender que éste resulta inevitable. Es como si hubiéramos olvidado lo más esencial de los ordenadores: que son programables*» Los programas son los que deben garantizarnos qué se puede y qué no se puede hacer.

Europa debe pugnar por proteger nuestro derecho a poseer los datos que nos conciernen. Alex Pentland, Profesor del MIT y asesor del World Economic Forum en esta materia afirma que «*para lograr una sociedad*

---

[1] Primera Enmienda: *El Congreso no hará ley alguna con respecto a la adopción de una religión o prohibiendo el libre ejercicio de dichas actividades; o que coarte la libertad de expresión o de la prensa, o el derecho del pueblo para reunirse pacíficamente, y para solicitar al gobierno la reparación de agravios.*

justa en la era de los datos, debemos alcanzar un Nuevo Acuerdo sobre Datos, cuya clave es tratar los datos personales como un activo, sobre el que los individuos tienen derecho de propiedad» Propone Pentland tres puntos irrenunciables:

— *Usted tiene derecho a poseer los datos que le conciernen, sea cual sea la entidad que recoge los datos, le pertenecen y puede acceder a ellos en cualquier momento*. Los entes que recopilan datos cumplen una función parecida a la de un banco que gestiona el patrimonio de sus clientes.

— *Usted tiene derecho al pleno control sobre el uso de sus datos.* Las condiciones de uso deben ser autorizadas y estar claramente explicadas en lenguaje llano. Si no está satisfecho sobre el uso de esos datos puede retirar la custodia de los mismos en cualquier momento (igual que procedería a cerrar una cuenta bancaria).

— *Usted tiene derecho a disponer de sus datos y a distribuirlos*. Está facultado para destruir o redistribuir los datos que le conciernen en cualquier momento.

Debe propiciarse un debate internacional de calado que tenga esta consideración sobre los datos. Solo así se conseguirá una correcta protección de los derechos de los ciudadanos, de los internautas y por supuesto, de los menores. La huella digital de los que hoy tienen 30 años, o lo que es lo mismo, su historial completo en la web, según AVG se remonta ya a 10 o 15 años atrás. La mayoría de los bebés están en internet antes de los dos años. Cuando cumplan 30 llevarán más de dos décadas de vida digital.

La oportunidad que le brinda a Europa la puesta en marcha de manera coordinada de su Agenda Digital, no debe dejar al margen asuntos tan prioritarios para la ciudadanía como estos. Pensemos que una de las líneas estratégicas de la Agenda Digital es la protección de los menores en la Red.

La propia Comisión Europea, realizó en 2011 un informe basado en 25.000 encuestas a jóvenes de Europa, del que se extraían conclusiones para la reflexión. El 77% de los menores de edad, con edades

comprendidas entre los 13 y los 16 años utilizaba entonces las redes sociales (ahora serán más) y también un 38% de los menores con edades comprendidas entre los 9 y los 12 años. De las redes sociales evaluadas entonces, solo dos (Bebo y MySpace) tenían establecida una configuración por defecto que garantizaba que la información de los menores solo era vista por sus contactos aprobados. Esto es, las redes sociales más utilizadas dejaban por defecto accesibles los perfiles de los menores a cualquiera que quisiera consultarlos en la red. La seguridad de los menores en la red, que están indisolublemente concernidos al ser éstos usuarios intensivos de las redes sociales debe ser promovida entre todos y, por supuesto, desde la Administración, y las medidas que se adopten deben acompasarse con la necesaria «alfabetización digital» que no debe restringirse al uso de las propias herramientas, sino a la correcta gestión por parte del usuario (máxime si hablamos de menores) de su información personal en la red.

En España el 39% de los adolescentes pasan más de dos horas al día en las redes sociales y lo hacen al margen de que se encuentren en el colegio o en otras actividades (la media europea es del 23%). Tuenti es la red social más empleada por los adolescentes (de entre 10 y 16 años) Casi el 60% están presentes en este servicio, mientras que el 56% tiene perfil en Facebook, el 12% en Google+ y el 3% en Myspace.

Nuestros niños y jóvenes no son conscientes de que ya cuentan con un historial completo, con una biografía detallada, que incluye sus gustos, sus actividades, sus amigos, sus opiniones, sus recuerdos, etc. accesible en la red. Existen métodos para conseguir, por trazabilidad de datos, un perfil muy concreto de millones de usuarios de redes sociales menores de edad en el mundo y no existe una conciencia en los mismos de proteger esa privacidad para que esta información no pueda ser utilizada a la larga de manera maliciosa. Pensemos que aproximadamente el 30% de los contactos que tienen los adolescentes en las redes sociales son desconocidos o «amigos virtuales» según un reciente informe de la OCU.

Entre los menores de 10 a 13 años, el 44% tiene un perfil en Facebook. Se dan de alta simplemente simulando una edad que no tienen, ya que las más populares redes sociales están restringidas para menores de

16 años (14 en las redes sociales específicas para adolescentes). Estamos ante una tendencia imparable en la que, por supuesto, debemos formar desde muy pequeños a los niños para que vigilen su privacidad y su seguridad, pero en el que no debemos descuidar las exigencias a las empresas que operan estas grandes plataformas.

En nuestro país hasta la más pequeña de las PYMES debe cumplir con la Ley Orgánica de Protección de Datos. ¿Se exige ese cumplimiento estricto a Facebook y otras plataformas, que han revelado recientemente las solicitudes de acceso a datos de sus usuarios por parte de los diversos gobiernos del mundo? ¿A quién y de qué manera debe reclamar un usuario al que le han suplantado su identidad en una red social?¿Puede un usuario solicitar su «portabilidad» de una a otra red social, como se exige a las compañías telefonía móvil, sin perder toda su información personal? ¿Se le ofrecen garantías de borrado de sus contenidos al darse de baja? El cierre del servicio de Megaupload, independientemente de las causas, provocó que muchos usuarios perdiesen archivos personales que habían depositado en ese servicio. ¿Qué pasaría si el día de mañana Facebook o Twitter, que constituyen para muchas personas su diario personal cierran o cambian las condiciones del servicio? Es un escenario improbable pero técnicamente posible. Pensemos que a nivel técnico, estas plataformas son aplicaciones hospedadas en servidores alojados en centros de datos. Probablemente con máximas garantías de seguridad en cuanto a redundancia y disponibilidad, porque de ello depende el negocio. Pero en definitiva, aplicaciones que pueden desactivarse o modificarse de forma muy rápida sin el consentimiento de los usuarios.

El modelo de Internet que hemos construido, está basado en la gratuidad, que ya es entendida por los propios internautas como un derecho. Este modelo tiene obvias virtudes, porque permite que las bondades de la Sociedad de la Información se extiendan rápidamente, pero también importantes inconvenientes, ya que en muchos casos el prestador de servicios se escuda en que los ofrece de forma gratuita para no garantizar que los ofrece con unos parámetros de calidad adecuada. Y además, plantea importantes interrogantes sobre la adecuada

retribución de los generadores de contenidos y sobre la sostenibilidad del ecosistema de Internet.

En este contexto ¿Quién va a garantizar nuestro derecho al secreto constitucional de las comunicaciones? Hasta ahora teníamos una compañía operadora registrada en la CMT (Ahora CNMC) y con unas obligaciones concretas y estrictas en este campo, pero ¿Cómo podemos garantizar la seguridad de la información si ni siquiera tenemos opción de exigir responsabilidades a estas empresas cuando este derecho es vulnerado o cuando los datos quedan al descubierto por algún agujero de seguridad? Estas empresas, en muchos casos, no tienen oficinas ni personal en nuestro país, pero sin embargo cuentan con millones de usuarios españoles (un 93% de los internautas españoles tiene al menos una cuenta activa en redes sociales)

En definitiva, hay múltiples aspectos que deberían ser abordados urgentemente relativos a los derechos fundamentales de los usuarios a los que debemos garantizar su intimidad, su reputación e incluso aspectos tan sensibles como el derecho al olvido digital, o cómo operar con toda la información volcada por un usuario en las redes sociales una vez que éste haya fallecido.

Además, debemos categorizar las «infracciones» que se cometan en el entorno digital porque, si bien hay algunas que son un mero reflejo de las ya reguladas en el mundo físico, como obviamente, muchas de las abiertamente delictivas (pensemos por ejemplo en el acoso a menores o en la apología del terrorismo) existen otras que nacen de la utilización de estas nuevas herramientas y no están previstas en el ordenamiento (por ejemplo la suplantación de identidad virtual, o la publicación en abierto de información etiquetada como privada por el usuario) y ante las que, hoy por hoy, el internauta se encuentra desprotegido.

Derivar algunas de estas infracciones al ámbito policial o judicial, además de ser una medida posiblemente desproporcionada, podría colapsar el sistema. Por ello, parece lógico contemplar también la resolución de estos conflictos desde el ámbito administrativo, como ya ocurre con otras actividades relacionadas con las propias telecomunicaciones.

Pensemos en un caso de ciberbullyng sobre un menor, ¿a qué instancias debe dirigirse un padre para solicitar a una red social la desactivación de una imagen o video que denigra al menor? Hoy por hoy esos cauces no están debidamente articulados y debemos poder exigir que se articulen para una correcta y sobre todo rápida respuesta por parte de los prestadores de los servicios.

Ofrecer a los internautas la posibilidad de denunciar ante el órgano administrativo competente aquellas acciones que vulneren los derechos citados en esta intervención obligaría a los responsables de estas plataformas a atenerse a unas exigencias concretas de calidad del servicio, lo que, sin duda, redundaría en la puesta en marcha mecanismos ágiles para la resolución de estos problemas.

Por supuesto, los telecos y técnicos que trabajan día a día en la puesta en marcha de estos servicios trataremos de aportar en soluciones a los problemas de seguridad pero entendemos que para conseguir una efectiva protección de los menores y de todos los usuarios de Internet es preciso acometer medidas valientes que sitúen a estos agentes que operan y que, no lo olvidemos, basan sus potentísimos negocios en la red, a cumplir con unos baremos básicos de calidad del servicio, que incluyen la rápida respuesta a estos conflictos.

Como ya se ha expuesto, consideramos que al igual que las telecomunicaciones están coordinadas internacionalmente, parece razonable que las aplicaciones, y en concreto las redes sociales, en la medida en que utilizan datos y contenidos personales de los usuarios, también lo estén. Y estas iniciativas deben cobrar fuerza en el marco europeo, desde donde debe darse un impulso para que todo ciudadano usuario de redes sociales esté puntualmente informado de si la compañía a la que confía sus datos y a través de la que se comunica, cumple unos determinados requisitos de seguridad y garantiza sus derechos fundamentales. Máxime cuando estos usuarios son menores y es obligación de todos que estén especialmente protegidos.

Desde el Colegio Oficial de Ingenieros de Telecomunicación, a través de nuestros grupos de trabajo, que implican a expertos en todas las temá-

ticas ligadas a nuestra ingeniería, estamos trabajando ya en propuestas concretas en el entorno de las redes sociales, que esperamos sean de utilidad para la reflexión en profundidad sobre este asunto que afecta a la práctica totalidad de nuestros jóvenes y a un amplísimo porcentaje de población española.

Quedo a su disposición para cualquier cuestión que quieran formularme. Muchas gracias.

COMPARECENCIA DE LA PSICÓLOGA SOCIAL EXPERTA EN SOCIEDAD-RED Y RESPONSABLE DEL ESPACIO EL CAPARAZÓN, DÑA. DOLORS REIG HERNÁNDEZ, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 30 DE ENERO DE 2014.

La señora **PSICÓLOGA SOCIAL EXPERTA EN SOCIEDAD-RED Y RESPONSABLE DEL ESPACIO EL CAPARAZÓN** (Dña. Dolors Reig Hernández): Yo he entrado un poco antes, y no puedo evitar matizar o hacer un comentario genérico sobre algunas de las cosas que he escuchado, sobre todo de una de las cosas.

Parto de un punto de vista distinto. Os confieso que plantear el tema de Internet y jóvenes en cuanto a los riesgos, para mí (y quien conoce mi trayectoria y mi discurso habitual lo sabe) ha sido un problema. O sea, realmente suelo mirar más a las oportunidades, me dedico al tema de educación, me dedico al tema del empoderamiento, me dedico a toda esta serie de temas que miran más la parte positiva. Aun así, he intentado enfocarlo, y creo que lo he conseguido.

Pero quería comentar con respecto a la ponencia anterior un matiz que creo que no he hecho en mi intervención pero que creo que está muy bien para empezar. Yo creo que muchas veces planteamos Internet como algo sobrenatural o como algo, una capa que ha venido como a cambiarlo todo. No es eso Internet; Hablamos ya de la sociedad posdigital, concepto que significa un Internet y una realidad que están entremezcladas, que no tiene sentido separar. El interviniente anterior hablaba de etiquetar determinados contenidos, de forma que si yo los comparto con él y él los comparte con otra persona variando algo, él pueda tener algún tipo de responsabilidad. Es bueno no separar ambos ámbitos y acudir a la metáfora de la calle: ¿podría yo ir a una plaza, decirle a este señor algo y culparle después si él se lo dice a otra persona? Yo creo que eso entra en el ámbito de las normas informales y no tiene demasiado sentido regularlo en Internet. Sería lo mismo que regular el cotilleo, no sé si se me entiende. De alguna forma, en esta sociedad nos pasa a los adultos, nos pasa a los no nativos digitales, que tendemos a sobrerregular cosas que en el mundo real, en la plaza del pueblo, que yo creo que es la gran metáfora de las redes sociales (yo siempre digo que son como plazas del

pueblo ampliadas, son las nuevas plazas, los nuevos bares, los nuevos espacios públicos) no regulamos, dejando a las costumbres o el ámbito de lo informal. Es bueno platearse los temas de internet siempre buscando analogías en el mundo offline. Tengo una hija de 15 años y me di cuenta de estas cosas hace mucho tiempo. Cuando le decía «te he enviado un mensaje en Facebook diciéndote no sé qué», decía: mamá, ¿por qué mencionas la marca del mensaje cuando me envías un mensaje? Un mensaje es un mensaje, por debajo de la puerta, en Facebook en WhatsApp, en Twitter, para ellos de alguna forma es algo natural, no tiene marca ni diferencias en lo on y lo offline... es como la luz, el agua, la electricidad. Para los adultos que no hemos crecido con esto, evidentemente, es distinto. Hay una frase que lo resume muy bien, yo creo, que es la que dice que la tecnología solo es tecnología para aquel que ha nacido antes que ella. O sea, que cuando nosotros lo vemos como algo impuesto, que ha irrumpido en nuestras vidas, para ellos es algo natural. A mi hija le cuesta incluso saber a qué me dedico, para ella no tiene sentido, es como si le dijera me dedico a la vida, me dedico al mundo, me dedico a las relaciones. Y no entiende nada. ¿Internet?, ¿cómo te dedicas a esas cosas? No lo distinguen como un ámbito distinto de su realidad.

Dicho esto, vamos a empezar por la presentación; creo que lo que estamos viviendo con el tema de Internet es un tema simplemente evolutivo: ni cualquier época pasada fue mejor ni siempre lo será. Tendemos a pensar que cualquier época pasada fue mejor y que cualquier cambio evolutivo en el ser humano es negativo. Le pasaba incluso a Sócrates cuando le decía a Platón, en relación con los libros, la escritura, ¿qué va a pasar con la memoria? Si escribimos todo, vamos a perder capacidades mnésicas. Y en definitiva no ha sido así, o sí ha sido así pero hemos ganado, por contra, el libro como instrumento de cultura y de transmisión cultural y social, o sea hemos ganado muchísimo más de lo que hemos perdido.

Nos pasa muchas veces con Internet algo parecido. Parece que valoramos más lo negativo que lo positivo. Ya todo está digitalizado, ya todos somos personas permanentemente conectadas a la red. Y eso, evidentemente, nos cambia. Os he traído un libro, después os lo dejaré, está apuntado al final, en el que yo y un psicólogo de aquí, de Madrid, analizamos un poco este tipo de cambios, cómo nos cambia Internet, cómo nos cambia la experiencia de conectividad: cambios cognitivos, cambios sociales, y también cambios en valores.

Desde este punto de vista, ya os digo que voy a intentar centrarme en los riesgos pero sin dejar de lado las oportunidades. Creo que, como todo en la vida, la eclosión social que supone Internet genera muchísimas oportunidades y también genera muchísimos riesgos, o sea que estamos hablando tranquilamente de la misma cosa.

Pero sobre todo estamos hablando de estos tres cambios que creo que es importante destacar desde el principio: en primer lugar ya no hablamos en público, hablamos en red. Esto es diferente, el cambio en la comunicación es absolutamente espectacular. Yo siempre digo que en Twitter soy mucho más precavida de lo que soy en una sala de conferencias, en una sala de conferencias se acota el mensaje, es difícil descontextualizarlo, y en el caso de que alguien lo lance a redes, siempre puede haber alguien en la sala que me defienda y diga «oye, esto no lo dijo Dolors». Un mensaje en Twitter, según cómo lo expreses, según cómo... si puede ser descontextualizado y puede hacerte la vida imposible, te lo puede llegar a afectar seriamente a tu reputación. O sea, yo creo que uno de los peligros es esta nueva forma de comunicación que, digamos, descontextualiza los mensajes absolutamente. No es lo mismo el mensaje que yo lanzo a gente conocida, que sé más o menos por dónde me va a responder, que el mensaje que lanzo a la red, donde puede ser descontextualizado y llegar a cualquier tipo de público.

Esto, en determinadas escuelas, normalmente privadas o concertadas, como muy implicadas en todo esto de la red, lo están trabajando ya. Cuando se habla de educación y de educación en Internet, muchas veces nos fijamos solo en temas de netiqueta, lo de no gritar en los foros, no poner mayúsculas, todas estas cosas ya un poco de otra época. En otros casos se empieza a trabajar en este «hablar en red»: no digas según qué frase, lo que decíamos: «si dices no sé qué, después se puede modificar»; cuando hablas en red es difícil modificar nada de lo que dices, no digas cosas demasiado genéricas, intenta concretar, una serie de cosas que hacen que un mensaje sea más difícil de desvirtuar, no solo para los jóvenes, yo creo que cualquiera de nosotros, cuando hablamos en red tendríamos que tener en cuenta esta posibilidad de descontextualización.

Yo lo llamo psicología del individuo conectado y lo destaco porque, repito, somos diferentes desde que vivimos en las redes sociales. Esta frase es de Castells y la dijo en motivo de las revoluciones de los países árabes. La experiencia de conectividad nos cambia, cognitiva, social-

mente y en valores, posibilitando la aparición de jóvenes superhéroes o supervillanos.

Utilizo la metáfora del superhéroe o supervillano al hablar de jóvenes y redes. Porque cuidado…, estamos ante algo muy poderoso, los riesgos de la red, yo creo que estamos empezando a verlos ahora, son tremendos. Los riesgos de la red llegan hasta el punto de la impresión de pistolas 3D. Dentro de nada estaremos hablando de todas estas cosas. El debate sobre las armas en Estados Unidos será absurdo en poco tiempo: ya no hará falta comprar armas, te podrás descargar en portales legales o ilegales de forma incontrolable, el software para imprimir, en impresoras 3D domésticas, cualquier pistola capaz de matar a gente. Realmente el escenario de los riesgos de la red, creo que lo estamos minusvalorando, infravalorando. A la vez también es un instrumento para hacer grandes cosas: se están imprimiendo riñones artificiales, cosas maravillosas. O sea, creo que las tecnologías en este sentido nos hacen muy poderosos y por eso os explicaba este constructo teórico, que me parece bastante interesante de ir más allá del concepto de TIC, tecnologías de la información y de la comunicación, al concepto de TAC, dentro de la vertiente que tiene en cuento a posibilidades de aprendizaje y conocimiento, Educación 2.0, Escuela 2.0, todo el tema este de tecnologías como potenciadoras del aprendizaje, universidades de todo el mundo que están lanzando cursos gratuitos, cualquier persona en cualquier lugar del mundo puede obtener un diploma de Harvard, de Stanford, están democratizando de alguna forma el acceso a la información y al conocimiento, más que en cualquier otro momento en la historia. Pero sobre todo creo que debe ocuparnos el concepto de tecnologías como instrumentos de empoderamiento y de participación, lo que yo misma denominaba TEP hace un tiempo.

Uno de los temas sobre los que me centraré al hablar de oportunidades y riesgos va a ser esta participación; facilitar esta participación de los jóvenes en la vida pública; estamos en un momento de descubrimiento, y de necesidad de que los jóvenes se impliquen y participen. Tenemos la oportunidad, con estas tecnologías, de implicarles más en la vida política, en la vida política, en la vida pública, etc.

Nuestros jóvenes están saliendo a las calles pidiendo participar. Se han acostumbrado a participar en redes, la experiencia de decir diez mil veces al día «me gusta», «no me gusta», «esto lo difundo», «esto no lo difundo», «este me cae bien», «este me cae mal»... Es decir, esta influen-

cia constante en sus propias vidas va a acabar trasladándose a una necesidad imperiosa de participar en todos los ámbitos, también en la vida pública. Necesitamos democracias más directas.

¿En qué sentido? La participación, como os decía, puede ser muy interesante, muy productiva, muy positiva o muy negativa. Yo siempre pongo el ejemplo de las *riots* británicas versus 15-M; Los movimientos asociados al 15-M nos pueden gustar más o menos, pero en general eran pacíficos, en general fueron movilizaciones más o menos pacíficas, de jóvenes, simplemente participando. Los jóvenes en las *riots* británicas también eran jóvenes participando, pero acabaron quemando supermercados, matando a comerciantes, etc.

¿De qué va a depender que estas TEP, estos instrumentos de participación (en este caso las redes que permiten organizarse más fácilmente) generen un diálogo pacífico o acaben como las *riots* británicas? Aquí voy al centro de mi discurso, que es que ante el escenario actual de potencia de las tecnologías sólo tenemos dos salvaciones: cultura y valores, y no hay más. Intentaré desglosarlos, pero cultura, una base cultural sólida, sin la cual los valores, creo que es difícil adquirirlos. Volviendo al tema de los superhéroes, tenemos jóvenes que con estas tecnologías pueden hacer supercosas o pueden hacer *riots* británicas; *riots* británicas, u organizarse todos, llegar a un supermercado y entrar todos de golpe. Os hablaba de las impresoras 3D, pero uno de los grandes cambios de Internet es el poder de la organización sin organizaciones, es decir, el ciudadano puede más que nunca organizar cosas para las que antes necesitaba el sindicato, organizaciones, ONG... Ahora cualquier ciudadano con una idea bien elaborada y potente puede llegar, o no, o una mala idea en el caso de la participación que no queremos, una participación más negativa, pero cualquier persona puede llegar a organizarte cualquier tipo de tinglado —si me dejáis utilizar la expresión.

Buenas noticias: yo estoy convencida, y de hecho lo dije en el 15-M, de que en ese sentido nuestros jóvenes no van mal; no tenemos malos jóvenes, sino todo lo contrario. Para demostrar esto os voy a explicar un poco qué está pasando en el ámbito de las redes sociales a día de hoy. Los jóvenes se están yendo de Facebook, se están yendo de Facebook por lo que todos deberíamos irnos de Facebook, porque es una red que no respeta su privacidad, eso de que la madre les pida amistad, eso de que ellos saben que su privacidad no está del todo preservada y que todo

lo que suben a Facebook puede ser compartido, todo esto les molesta y están migrando a entornos mucho más privados.

Fijaos que muchas veces sufrimos por la privacidad de los jóvenes y somos los adultos los que no sabemos ni proteger demasiado nuestra privacidad. Mi madre de 70, yo creo que es incapaz de configurar su perfil de Facebook para preservar aquellos datos que le interesa preservar; y mi hija desde los 14, os aseguro que es absolutamente capaz de preservarlo todo. Un ejemplo es aquello de que tiene mucho amigos, o tenía muchos amigos cuando era una red masiva, tenía muchos amigos; pero hablando en privado solo hablan los amigos de verdad. Una de las cosas, vamos a cualquier perfil de adolescente en Facebook y decimos, ¡uy, este se hace amigo de cualquiera! Es que queda bien tener muchos amigos en Facebook, con lo cual quizá sí tienen 2.000 amigos en Facebook, porque sí es una sociedad más exhibicionista y sí queda bien tener 5.000 amigos en Facebook. Pero a la hora de verdad, y comprobado por muchísimos estudios, la relación de verdad la establece con sus cercanos, no la establece con el señor de Kentucky que le ha pedido amistad y no sabe muy bien quién es; todo lo contrario, precisamente porque es su medio, son conscientes de que pueden tener problemas y muchas veces son más conscientes que los adultos con ciertas conductas en la red.

Cualquier estudio con adolescentes acaba mostrando eso. Realmente les hacemos menos cuidadosos de la privacidad de lo que realmente son. Y lo son tanto que han migrado a WhatsApp, han migrado a entornos mucho más privados. Cuidado, que no son del todo seguros, ni mucho menos, y tienen muchísimos agujeros de seguridad, no estoy diciendo que sean más seguros. Pero sí que muestran cómo la idea esta de publicar sus vidas que tanto miedo nos da a los adultos, a ellos también se lo ha dado. Es algo que tampoco quieren...

También han migrado instagram o entornos peculiares como *snapchat*, que no sé si lo conocéis, pero es uno de los escenarios de futuro peligrosos, ya es una realidad a día de hoy en España. En Instagram comparten fotos, son muy visuales, es un entorno más rápido que Facebook... lo que buscan allí es conseguir muchos «me gusta», reforzando en el fondo esta sociedad del ego. Estoy totalmente de acuerdo en que es así pero a la vez buscan entrornos más seguros. Snapchat es un lugar en el que envías una foto que se autodestruye en pocos segundos. Tampoco tienen esta idea de la permanencia que tenemos los adultos. Esto está

provocando que se use para ciertas cosas extrañas o de alto contenido sexual, lo cual es peligroso. No estoy diciendo que sea seguro, también hay formas de capturar imágenes de forma permanente allí, pero sí muestra que su actitud es la de preservar la privacidad.

Y en tercer lugar, y más positivo hoy, están los entornos vinculados a intereses, como Tumblr o Twitter. Los primeros antropólogos que estudiaron el tema de las redes sociales y jóvenes, hablaban de que en Internet los jóvenes hacían básicamente tres cosas: la primera, el tonto. ¿Qué hacía yo a los 15 años cuando salía de casa y le decía a mamá «me quiero ir a dar una vuelta»?, y me decía «pero, ¿para qué vas a quedar con las amigas?». Y yo le decía: «Pues no sé». —«Pero, ¿qué vais a hacer?». —«Nada, pues quedar.» Esto en inglés se llama *hanging out*, y evidentemente es algo que se hace en redes sociales. Ese es el primer uso de las redes sociales por parte de los jóvenes que, vuelvo a lo de antes, como en la vida real, se hace en Internet y se hace fuera de Internet. De hecho, el hecho de que queden en Internet, no quita que queden fuera de Internet, que era uno de los mitos al principio, que desde que hay redes sociales los jóvenes se relacionan, no se miran a la cara. Pues yo no sé qué jóvenes conocéis, pero los que yo conozco, desafortunadamente no se quedan más en casa. Las relaciones sociales en internet complementan y no sustituyen las de la vida real.

El segundo uso es empezar a explorar intereses. Fijaos en las blogueras de moda; me gusta la moda, empiezo a visitar blogs de moda y puedo abrir, más pronto que nunca, mi propio blog que me puede reportar un futuro profesional más o menos brillante, de moda, de promoción, de fútbol, de cualquier interés, eso es lo que empiezan a hacer, se llama así, *Geeking around.* Se trata del uso de internet orientado a intereses profesionalizables, o que en todo caso les están enseñando competencias para ser profesionales en el futuro.

Y en tercer lugar ya, profesionalizarse de verdad, que sería el caso de estas blogueras de moda. Pero para que veáis que realmente desde los 13, 14 años nuestros jóvenes tienen más posibilidades que nunca de tener una orientación vocacional. Si a mí antes a los 13 años me hubiera interesado la moda lo hubiera tenido complicado, en mi pueblo, en los ámbitos limitados de lo físico. En Internet podemos acceder desde muy jóvenes a muchísimos tipos de recurso de la comunidad profesional que nos interese.

Esto es una oportunidad también para padres y profesores, para acompañar y apoyar todos estos intereses.

Superpoderes, para resumirlos: son más inteligentes, eso ni dudarlo. Los indicadores en general, el denominado efecto Flynn, aseguran que aumentamos tres puntos el coeficiente intelectual cada diez años, la humanidad, la población de las sociedades occidentales, de las sociedades más evolucionadas. Esto no ha cambiado desde que existe. O sea, es indudable que son más inteligentes. Y si no queréis llamarlo así, es indudable que tienen más información y que existe aquello de la inteligencia colectiva, que significa que donde no llego yo, llega el grupo. Lo de la plaza del pueblo, yo no sabía muy bien si la información que me había llegado era cierta o no, me iba a la plaza del pueblo y preguntaba (oye, ¿esto qué tal?); ellos van a las redes sociales y preguntan. Con lo cual son menos manipulables que antes.

Tienen nuevos valores: yo siempre digo que el *bicing*, esto de compartir las bicicletas y que además se está llevando ya compartir los coches y de todo, en el fondo lo hemos heredado de Internet. Yo lo llamo la filosofía Spotify. Spotify s un servicio en el que tú puedes escuchar música todo el día y no tienes ninguna necesidad de poseer cds ni ninguna otra cosa físicamente, elimina el concepto de propiedad clásico, y añade el concepto de compartir. Simplemente lo que valoras es tener acceso a esas cosas, no necesariamente tienes que tenerlas físicamente. Ese es uno de los nuevos valores que nace, yo me acostumbro a compartir en Internet, y después se va trasladando a ámbitos de la vida real.

El tema genera problemas (para el negocio turístico cuando por ejemplo se comparten viviendas), pero no deja de significar que hay nuevos valores. En una sociedad como la española en la que nos costaba alquilar hasta hace relativamente poco tiempo, pues todos estos nuevos valores de no poseer y sí acceder al servicio se van trasladando.

Los valores orientaran lo importante: ¿Qué participación tenemos? Estamos de acuerdo en que es una tecnología empoderadora, que permite participar, pero nos gustaría que esa participación fuese más responsable, que fuera más crítica, más culta. Para ser alguien en Internet, como para todo en esta vida, es cada vez más importante tener una sólida base de cultura.

Crítica, culta, responsable, basada en valores y creativa. Me voy a detener un poquito más en estas cosas, porque entramos en el campo de los riesgos. ¿Qué va a pasar si no tenemos una participación crítica?

Pues que en Internet nos vamos a dejar llevar, como en la vida real, pero quizás hasta más, por una serie de sesgos, de problemas, de fallos en el fondo del funcionamiento del cerebro humano. ¿Qué puede pasar si nuestros jóvenes no son críticos? Que el conocido efecto contagio haga que se dejen llevar por cualquier tipo de movilización. El tema es especialmente grave en cuanto al *cyberbullying*, ¿por qué le acosáis? Les preguntamos… «porque toda la clase lo hace», nos responden. Cuando sabemos de la gravedad de los nuevos tipos de Bullying 24 horas al día y 7 días a la semana, pudiendo quedar escrito de forma permanente, es importante recordar la importancia de educar en un sentido crítico que disminuya los sesgos.

Yo os he puesto aquí un ejemplo que me parece muy gráfico, y es el tema de la polarización, al tema se le llama también homofilia. El tema de que tendemos en el fondo a relacionarnos en esta vida con gente que se nos parece. Esto es algo natural, es algo psicológicamente conocido, es algo que todos hacemos, pero que en Internet puede suponer quizás un riesgo todavía mayor.

Este gráfico es curioso, son los libros; está hecho a partir de un análisis de los libros que leen los conservadores estadounidenses versus los que leen los progresistas estadounidenses. Podéis consultar si queréis luego el título de los libros, pero lo curioso es que no leen nada, nada, ni un conservador lee un libro de un progresista, ni un progresista lee un libro de un conservador. Eso en el fondo es malísimo, más en internet cuando podemos seleccionar en mayor medida las fuentes que escuchamos. A este que dice cosas que no me gustan dejo de seguirle en Twitter, ya no escucho nada más que no me guste. Contra esto, el riesgo de polarización podemos educarlo con pensamiento crítico, como siempre. Es un ejemplo de sesgo. Hay muchos otros sesgos, de dejarse llevar emocionalmente por el grupo, en fin, muchísimos más.

Segundo riesgo, desinformación: la viñeta, yo creo que es muy ilustrativa. Una chica no sabía algo y le preguntó a papá, ¿qué pasa, papá, que no había Google o qué? En el fondo esto es así, y en el fondo está demostrado que esto es así y que los jóvenes preguntan en Google tres veces antes que preguntar... vamos, a papá es el último al que le preguntan, normalmente. Cuidado, que esto es lo que tenemos que evitar; cuidado, que lo que tenemos que hacer es educar —lo tenéis abajo— como enseñanza de filtraje. Volvemos a lo de antes: en Internet hay muchísima in-

formación, pero no toda, evidentemente, es relevante, no toda, evidentemente, es correcta, no toda, evidentemente, es positiva. Yo siempre digo que cuanta más información haya, es como el grano de la paja, habrá más paja pero también habrá más grano. Mejor que haya mucha información, pero desde luego la gran competencia del ciudadano del siglo XXI va a ser filtrar, van a ser esas capacidades de filtrar de toda esta amalgama informativa lo que vale y lo que no vale. Eso es competencia de los padres, eso es competencia de la escuela, eso es competencia de los ámbitos culturales en general. Volvemos a la cultura de los valores como hábitos básicos: seleccionar fuentes de información, saber seleccionar, ya no solo fuentes de información, seleccionar también contactos.

Dejadme que os ponga un ejemplo antes de seguir. Hubo un estudio hace unos años que pretendía demostrar cómo de manipulables éramos en cuanto a la información de Internet. Para demostrar que éramos manipulables, lo que hicieron es construir un sitio web, en Wiki en este caso, con diseño de Wiki, que es lo más creíble, con tipografías, colores de Wikipedia, donde recopilaban un montón de datos, un montón de estudios que demostraban que había nacido una nueva especie de pulpo, que era el pulpo arbóreo, que era capaz de nacer, vivir, reproducirse, morir en los árboles. Yo doy muchísimas charlas para educadores, para maestros, y este ejemplo me va muy bien porque allí siempre hay algún biólogo, y siempre pregunto «¿hay en la sala algún biólogo?», y siempre hay cuatro o cinco. Os lo digo porque el estudio demostró que sí, que somos tremendamente manipulables por la información en Internet. Todo el mundo se cree el estudio, el 90% de los 10.000 estudiantes norteamericanos de muchas especialidades a los que se les pasó el sitio web, se lo creyeron sin ponerlo en duda en ningún punto.

Volvemos a lo de antes. Yo siempre pregunto si hay biólogos en la sala. ¿Demuestra el estudio que somos manipulables en Internet? Si esto no hubiera sido Wiki y hubiera sido una enciclopedia en papel, un documental en televisión, no nos lo hubiéramos creído? ¿O también se lo hubieran creído? ¿Qué es lo que falla? Es la base biológica, lo que falla es una buena base cultural en biología. Ninguno de los biólogos se cree que un pulpo pueda ser capaz de nacer, de vivir y reproducirse en los árboles, más que nada porque no puede comer insectos, hay una serie de cosas biológicas que yo no domino tampoco, pero que cualquiera que tenga una buena base de biología no se creería.

Volvemos a lo de antes: no se trata de decirles a los chavales «cuidado, que lo que pone en los blogs no es cierto, cuidado, que lo que pone en la Wikipedia no es cierto, cuidado». Todo este tipo de consejos sobre formatos, en el fondo no tiene sentido. ¿Cuál es el criterio que sí tiene sentido? La buena base cultural que les permita filtrar. Por eso digo que, lo destaco siempre muchísimo porque se contrapone, porque parece que se contrapongan tecnología y cultura. Y creo que es todo lo contrario, la verdad; la mejor arma que tenemos va a ser esa base cultural, esa base cultural en el ámbito del conocimiento.

En el ámbito de la emotividad, de la sexualidad, de la educación emocional está pasando exactamente lo mismo. Dice la viñeta «Pedrito, es hora de tener una charla sobre sexo, y dice Pedrito: ¿qué te gustaría saber, papá? Cuidado, porque este mismo filtrado de la información, y estamos hablando de que es importante en la biología en la política, en cualquier ámbito, es importante tener una buena base, cuidado, porque en el ámbito íntimo también lo es. Hay un riesgo, que no sé si os lo han explicado ya, creo que sí por lo que he visto de las ponencias anteriores, que es el riesgo de la exposición a la sexualidad en la red que está generando problemas muy graves, por ejemplo en cuanto a desigualdades de género, está generando que los niños ven de todo y por lo tanto quieren de todo; y las niñas enamoradizas de 14 están dispuestas a darlo todo. Emocionalmente una niña de 14 es muy vulnerable. Un niño, no tanto, todos lo sabemos. Por lo tanto, esa sobrexposición sexual a los primeros resultados en las búsquedas de google, dominadas por industrias de la pornografía sin demasiada sensibilidad hacia los efectos emocionales en las chicas, está causando problemas de respeto a la emocionalidad y a la sexualidad de la mujer. Es un ejemplo más de cómo este padre no debería decirle al niño «sí, sí, en Internet hay de todo, pero de todo esto, que sepas que a las niñas les vas a hacer daño si les pides esto, si...»; en fin, esa charla necesaria, ese filtrado necesario también en el ámbito íntimo.

Riesgo, *cyberbullying*: evidentemente, es un riesgo. He cambiado mucho de opinión desde que estoy estudiando Internet y antes decía que el *cyberbullying* no era peor que el *bullying*, no era peor que el *bullying* que me pudieran hacer a mí con 14 años en la plaza del pueblo. Ahora veo que sí es peor. Y es peor porque es 24 horas al día en todos los ámbitos, en todo momento, es imposible escapar de él. Sabéis que están todo el día whatsappeando, todo el día conectados, con lo cual en cualquier

contexto; antes te encerrabas en casa, en la habitación llorabas un poco, y allí ya tenías un ámbito de aislamiento. Ahora es muy difícil aislarse, con lo cual es muy duro. Aun así, desde los noventa parece que están disminuyendo los índices de suicidio. Yo creo que es un dato que también debemos tener en cuenta para no alarmar excesivamente. Son muy mediáticos los casos de suicidio provocado por *cyberbullying*; de hecho, son tan mediáticos porque hay casos de niñas grabándose que al día siguiente se suicidan, es como muy exhibicionista también todo el tema del suicidio en el caso de la red. Pero realmente están bajando los índices de suicidio adolescente.

Os he dicho lo de la sexualidad, y también debo destacar que también está bajando el porcentaje de relaciones sexuales entre adolescentes más jóvenes. O sea, contra lo que pueda parecer, no se están hipersexualizando. Cuidado, porque los datos después contradicen en cierta forma los miedos que tenemos los adultos. No es cierto que tengan más relaciones sexuales que antes o más frecuentemente, no, hay datos que demuestran que no es cierto.

Y en el caso del *cyberbullying* y el suicidio, lo mismo. Aun así, lo tenemos que tener en cuenta por la gravedad. Yo creo que en este caso, en el de suicidio, sea poco o sea mucho, hay que estar ahí. Hay que estar ahí y tener en cuenta estas cosas de aquí.

Difama, que algo queda: la difamación fuera de Internet podía ser más o menos volátil. En este caso, en Internet todo lo que queda escrito es mucho más permanente en el tiempo. Además, el ser humano tiende a esto, tiende al «difama, que algo queda». O sea, creo que debemos enseñarles también, que la educación que debemos darles es hacerles conscientes de eso, de que cualquier tipo de difamación... Yo creo que el tema de difamación sí habría que regularlo muy bien en Internet, porque también en la calle está regulado. El hecho de difamar puede ser muy peligroso, y más teniendo en cuenta que si antes quedaba algo cerebralmente, ahora además queda por escrito.

Responsabilidad y sentido crítico: yo siempre pongo como ejemplo de esto Gossip, una herramienta que no sé si ya está prohibida, pero debería estarlo, que como bien podéis traducir, es una herramienta que se titula Rumor; esto es apología del *cyberbullying* claramente. Uno de los elementos en sociología, clarísimos, del acoso es el rumor; o sea, se empieza a decir que la niña en cuestión es no sé qué, y aquello acaba en aco-

so, eso se sabe desde siempre. Por lo tanto, una aplicación que se lance al mercado llamándose Gossip, te está diciendo directamente «rumorea todo lo que quieras» (significa «rumor» en inglés). Os lo digo porque hay una aplicación aprobada en la APP Store y aprobada en muchos lugares, y que yo no entiendo cómo se ha aprobado, porque está haciendo apología directamente del acoso.

Aun así, la pongo de ejemplo de que el punto de vista prohibitivo en este caso estaría bien, yo la prohibiría directamente en este caso, pero aun así no vamos a poder aliviar el hecho de que abran una página en Facebook y rumoreen. Eso podemos prohibirlo porque tiene un mal nombre, pero una página en Facebook puede servir de tablón de rumores varios. De hecho, el fenómeno de los *informers*, que fue bastante potente hace un tiempo, consistía en eso, un tablón que llevaba una personas anónima y a la que yo podía enviar comentarios malignos de cualquier profesor del instituto; y pongo el ejemplo porque allí hubo denuncias en Cataluña precisamente, donde intervinieron los Mossos d'Esquadra para cerrar páginas de *informers*. O sea, yo creo que eso no vamos a poder regularlo.

Con lo cual, yo creo que la estrategia es la que, evidentemente, a mí me surgió de Gossip. Yo descubro Gossip casualmente muchísimo antes de que fuera mediático, también por mi hija de 14 años, que entra en casa y de golpe —por si no sabéis lo que es— me dice: mama (tocando el Smartphone)—, el vecino del tercero se ha liado con la vecina del primero. Digo: a ver, niña, ¿quién te está diciendo esto? Esto es una tontería. ¿Quién te lo está diciendo? Y dice: no, mama, es que hay una aplicación geolocalizada que tú la das de alta, pones qué está pasando en este edificio y ahí todos podemos colgar rumores de todos. Evidentemente, ¿qué hice en ese momento? Creo que es evidente lo que habría que hacer en educación en ese momento: sentar a la niña al lado y decirle «¡ah, qué bonita la aplicación!». Y dice: no, mamá si es muy divertido. Digo: a mí me parece fatal esto, niña. ¿Por qué, mama, si es muy divertido? Pues mira, ven aquí: todos esos secretos que tú me has contado y que tú siempre me cuentas de los niños que te gustan y de todo esto, como es tan divertido, lo vamos a poner en el Gossip de tu instituto para que lo sepa todo el mundo, como es tan divertido. Ay, no, mama, eso no. Empatía, al final, además de prohibir, también formar, y también introducir estas herramientas como excusas para trabajar el tema de la empatía, creo que es fundamental.

O sea, no vamos a poder prohibirlo todo. Si no existe Gossip, van a abrir una página de Facebook. Con lo cual, volvemos a lo de antes: edu-

cación emocional, empatía, no hagas a los demás lo que no quieras que te hagan a ti mismo, etc. Todas estas cosas son cada vez más importantes.

Conciencia de estar hablando en red: esta idea de la permanencia del rumor 2.0 sería lo mismo.

Esto lo he destacado antes, pero para profundizar un poco más. Otro de los riesgos, si hiciéramos una encuesta en la calle también saldría esto, saldría Internet, desde que tenemos Internet la gente está tonta. De hecho, hubo un libro incluso, de un tal Nicholas Carr, que se vendió bastante y creo que se ha vendido más que cualquier libro que hable bien de Internet, que se llamaba precisamente *Google nos vuelve estúpidos*. Y esto en librería se vendió muchísimo. Demuestra el miedo que tenemos ante cualquier avance tecnológico.

¿Internet realmente nos vuelve estúpidos? A ver, lo que está claro es que Internet nos cambia. Y los conceptos de inteligencia, por ejemplo, cambian. La inteligencia tradicional consistente en memorizar nombres de ríos, capitales de países, etc., empieza, o una de las facetas de esa inteligencia empieza a ser absurda. Esto es como el debate de la calculadora: ¿era necesario saberse todas las fórmulas cuando podías calcularlo con calculadora? Quizás en algún momento, la lógica sí. Pero en el fondo, cambian las tecnologías, con lo cual cambian los tipos de inteligencia necesarios. Está demostrado que les cuesta muchísimo a los jóvenes de hoy ya memorizar este tipo de datos. Tú les haces memorizar la lista de los reyes godos y para ellos es una tortura infinita, les cuesta muchísimo. ¿Por qué? Porque a la altura de tres clics lo van a tener.

¿Qué es lo que aumenta?, y a cambio, lo que veíamos antes de la memoria versus no memoria: el libro, seguro que acabó un poco con la memoria, pero a la vez nos dio más recursos para buscar información. En este caso está aumentando muchísimo esta inteligencia fluida también. No tanto la inteligencia cristalizada, que es esta que memoriza, la cultura de memorizar cosas básicas, sino esta inteligencia fluida que consiste en saber buscar información de forma fácil, saber procesar varias ideas a la vez, todas estas cosas. O sea, cambia el tipo de inteligencia que usa el ser humano.

Si queréis una metáfora que sirve mucho, es esta de la memoria de trabajo: los ordenadores tienen el disco duro donde se almacena la información; nuestro disco duro, nuestra memoria actualmente está en nosotros pero también está fuera de nosotros, en el *smartphone* mismo llevamos

datos, llevamos informaciones que a veces consultamos, de hecho nuestro disco duro es infinito desde que está Internet, con una buena base cultural buscamos cualquier cosa y tenemos información; la memoria de trabajo, el procesador, es lo que ahora cambia y evoluciona. Nuestros hijos tienen mejor procesador que nosotros. Y el tema de la multitarea, por ejemplo, creo que demuestra eso. No existe en sí la multitarea, o se no saben ver y enterarse de una película por primera vez y leer un libro a la vez, eso sería absurdo, eso cognitivamente todavía (y digo todavía porque parece ser que ya hay primeros indicios de que el cerebro humano está evolucionando y va hacia allá), todavía no es posible, pero sí que saben, por ejemplo, cambiar de actividad muy rápido. Esto, cuando los adultos nos quejamos de que nos dispersa, que tanta información nos da una sensación de dispersión, en el fondo lo que nos pasa es que no sabemos cambiar de tarea rápido: estamos escribiéndole a alguien, y de golpe no podemos consultar lo que nos está diciendo un amigo. Ellos sí, ellos hacen *switch*, que se dice, muy, muy rápidamente. O sea, el procesamiento de información se optimiza. Lo que es procesar múltiples fuentes de información a la vez se está optimizando sí o sí, eso es algo que realmente está ocurriendo, el ser humano se adapta al medio, por eso os ponía el gráfico de la evolución. Todo esto... antes vivíamos en los árboles, con lo cual teníamos que tener las garras más prensiles de alguna forma; ahora vivimos en un entorno informativo complejo, con lo cual procesamos de forma mejor la información.

Vivimos en la era del hemisferio derecho, una participación creativa. Creo que no está tanto en vuestra tarea, o sea que no voy a ir tanto por ahí, pero sí que quiero destacar cómo Internet está generando también opciones creativas de hacer las cosas. De hecho, muchas de las cosas que están surgiendo en torno a esto de los coches compartidos, los *spotify*, son ideas, son *start-ups*, son empresas iniciadas por jóvenes que son capaces, porque no tienen el sustrato cultural que nosotros tenemos, la estructura hecha ya de las cosas que debe ser de determinada forma, gracias a Internet y a que consultan ideas de otros lugares y a que son mucho más abiertos, pueden generar esa creatividad. Pero no voy por ahí, porque creo que ahí sí que salgo un poco de la temática.

Otro riesgo, adicción: a ver, la frase, creo que es la que siempre digo y repetiré hasta la saciedad; como psicóloga, sé bastante de adicciones y os puedo asegurar que no existe la adicción a Internet; de hecho, el DSM-V, el último tratado de clasificación de enfermedades mentales

en el mundo, no se ha atrevido a incluirlo, pero sí existe la adicción a cosas que se pueden hacer en Internet. Sí existe la ludopatía en Internet, sí existe la adicción al juego en Internet (y fuera de Internet), sí existe la adicción a las redes sociales de Internet, sí existe la adicción a la sociabilidad, sí existe la gente que ya no sabe estar sola. Pero cuidado con eso, porque eso es un cambio sociocultural: ¿no saben estar solos, tendrán que estar solos alguna vez más en su vida, o siempre tendrán WhatsApp que les conecte el mundo, a sus pares de alguna forma? Cuidado, porque ahí el límite entre considerarlo adicción o normalidad social es complejo. Cuando tienes al niño al lado que no te mira a la cara y está «whatsappeando», piensas que ese niño es adicto a Internet. Pero en el fondo, en su mundo eso va a ser habitual, y en el fondo esa capacidad de mantener las dos relaciones a la vez también puede ser o es un cambio social que estamos viviendo.

Desde luego, si algo está haciendo Internet es cambiar las relaciones sociales. Yo publiqué un libro que se llamaba *Socionomía* (tenéis al final la referencia,) pero a mí me hubiera gustado mucho más el título de «Sociedad aumentada»); creo que lo que está pasando, o el gran cambio de paradigma se produce precisamente por esta hiperrelacionabilidad que vivimos. Estamos todo el día relacionándonos con muchísima más gente que nunca antes, participamos de muchísimas más comunidades que nunca antes (nos implicamos menos en todas ellas, eso es cierto también), pero digamos que el universo relacional se expande de una forma infinita desde que existen estas redes sociales. Volviendo a la metáfora de la plaza del pueblo, pues si en el pueblo no había gente que hablara de botánica y mi interés era botánico, me tenía que ir a otro pueblo o, como ocurría habitualmente, no aprendía nada de botánica en mi vida. Hoy en día puedo explorar cualquier posible interés o puedo formar parte de cualquier comunidad alrededor del mundo.

De hecho, si os fijáis, a nivel de conocimientos se está produciendo algo muy curioso, que es la emergencia de perfiles generalistas; eso de Leonardo Da Vinci, que sabía un poco de todo (posiblemente mucho de todo), pero eso de saber mucho de todo y nada de nada está ocurriendo mucho desde que tenemos Internet, porque tenemos tantísimas fuentes de información disponible, tantísimos intereses, podemos explotarlos todos, con lo cual el joven de hoy sabe mucho de muchas cosas y quizás no demasiado de nada; quizá sí que se superficializa un poco el conocimiento de todo ello. Pero tampoco es malo ese perfil generalista en momento

de cambio en los que es importante ver el árbol y no tanto las ramas; o sea, realmente está empezando a emerger un perfil de ese tipo.

También en las relaciones, también cuesta muchísimo más implicarles, o las afiliaciones son mucho más débiles de lo que eran antes; la familia, la comunidad del pueblo te ataba de una forma que ahora es imposible que ate a cualquiera de nuestros jóvenes. Ellos están acostumbrados a participar de muchas comunidades, de forma muy electiva; vienen, se van, tienen un grupo de WhatsApp, lo cierran, abren otro, cambian de amigos muy fácilmente (creo que incluso las relaciones de pareja van a ser mucho menos estables, y ya se está demostrando que tienden a ser menos estables que antes, etc.).

Pero de todas formas estamos hablando, si os fijáis en la pirámide de Maslow, lo que está cambiando Internet, por eso es un cambio de paradigma, y por eso es tan importante, está cambiando al ser humano en tanto en cuanto está afectando a su necesidad de afiliación, a su necesidad de reconocimiento social (cuando cuelgan una foto en Instagram lo que quieren es tener 82 *likes* y tener más que el vecino, o tener más amigos que el vecino); y esa necesidad de autorrealización a través de tus intereses (por eso pongo un poco el icono de los blogs arriba) que también proporciona Internet.

Pero para que veáis que las redes sociales, en el fondo están cubriendo necesidades humanas básicas. Con lo cual, uno, están aquí para quedarse; y dos, van a suponer un cambio de paradigma, están cambiando al ser humano, con lo cual van a acabar cambiando muchísimos aspectos de la sociedad también.

Acabo ya: uno de los problemas de esta adicción a la sociabilidad en Internet, que estoy de acuerdo en que sí existe o en que sí tenemos que contrarrestarla, es el problema de que no queda tiempo para la reflexión, eso de «estarán siempre acompañados a lo largo de su vida»; sí, ¿pero cuándo van a estar solos? Estar solo, de alguna forma, tiene ciertas funciones de autoconocimiento, de reflexión, de introspección, necesarias para la creatividad, para escribir un texto de más de tres párrafos, para muchas cosas en esta vida hay que enseñar a estar solos.

Por eso siempre hablo de educar la desconexión. Estas escuelas que os decía más avanzadas que están trabajando absolutamente inmersas en tecnología, es muy curioso porque están trabajando sistemas de desconexión tan aparentemente extraños como incluso meditación. Una es-

cuela de la que no voy a decir el nombre, pero hace poco en una charla me sorprendieron muchísimo, ellos mismos me dijeron «no, no, si aquí estamos educando en la desconexión, nos ponemos a meditar tres veces por semana». Digo: esto de la meditación que me sonaba a mí ya un poco paranormal, parece ser que está funcionando bien (no ciertas meditaciones), pero está funcionando bien para educar la desconexión. No estoy diciendo que enseñemos a meditar, pero sí que... Esto es como cualquier sistema de comunicación que afecte a una necesidad básica del ser humano, como es la sociabilidad, es normal que cause adicción. Cuando nació el telégrafo, las madres enviaban —como anécdota— 50 telegramas diarios al niño que vivía no sé dónde (tu papá se ha levantado y ha desayunado huevos fritos; tu papá se encuentra mal esta tarde; a ver cuándo vienes para Navidad). O sea, lo que hacemos ahora en WhatsApp, lo que hacemos ahora en Facebook se hacía con los primeros telégrafos, con los primeros telegramas. Evidentemente, esto bajó con el tiempo, pero creo que también es importante enseñar a moderarlo y enseñar a desconectar de vez en cuando, o a que hay que aprender a estar solos en esta vida para muchas cosas.

En fin, yo creo que ya está. Solo quiero incidir en que las noticias son buenas, yo creo que estamos ante una de las generaciones más prometedoras de la historia. De hecho, el otro día pensando me hizo gracia, porque generación X, generación Y, generación Z, hemos llegado al final de algo, simbólicamente coincide, yo creo que sí hemos llegado a un cambio importante en el ser humano que nos hace mejores. Esta es una imagen de una serie norteamericana de éxito entre jóvenes (se llama Glee en este caso, por si tenéis curiosidad), que por ejemplo está mostrando lo que yo digo, si antes en educación y en el mundo en general triunfaba más quien era como los demás, quien asumía las normas del grupo, hoy en día la ética esta de explotar la diferencia, de explotar el talento individual, que tan importante es y que pienso que nos puede hacer muy felices y que puede cambiar cosas bastante disfuncionales de nuestra sociedad, pues está emergiendo con fuerza. El hecho de que no todos ven los mismos programas de televisión, no todos acceden a las mismas fuentes de información, este hecho lo que hace es generar diversidad, generar tolerancia a la diversidad y diversidad personal, lo cual en el fondo creo que es un valor bastante positivo para el futuro que nos viene.

Diversos, creativos, inteligentes, responsables socialmente: hay estudios muy curiosos que muestran cómo uno de los ámbitos emergentes,

o sea, yo asesoro muchísimas veces para emprender, para nuevos filones de ocupación, y asesoro en temas de responsabilidad social, si la gente de cierta edad en el supermercado ve huevos ecológicos y huevos normales y le cuestan un euro más, compra los normales, seguro, los jóvenes son capaces, incluso en tiempos de crisis, de gastarse un euro más en los huevos ecológicos; falta producto ecológico, de hecho, falta producto responsable, si hubiera más opciones responsables, los estudios indican que los jóvenes optarían por ellos, etc.

Realmente estamos ante una generación que, si os fijáis... Yo leía hace poco muy curioso, decía: tienen muchísimas herramientas, y además fijaos en que tienen algo que no hemos tenido antes también, y es ese acceso a toda la información, que les hace conscientes de los problemas del mundo, no viven tan engañados como hemos vivido. Ya no os digo que demasiado, son incluso pragmáticos, son incluso demasiado realistas. Antes vivíamos un poco en la nube de la desinformación, de solo lo que nos mostraba la televisión y podíamos incluso ser más felices. Ahora lo ven absolutamente todo. Eso los hace más pragmáticos, más realistas. Si tenemos en cuenta que tienen instrumentos muy interesantes y esos valores, ya os digo, yo creo que la generación es prometedora en sí.

En fin, yo lo dejaría aquí. Os dejo un par de referencias. Os he traído un libro, este de aquí. Si queréis más copias, no tendría problema, si necesitaseis más copias, de este de aquí tengo varias, es un libro descargable libremente desde la web, si ponéis el título lo podéis descargar, y es un estudio de campo hecho en institutos de secundaria de aquí de Madrid precisamente, por el doctor Vílchez, Luis Fernando Vílchez, que es de la Autónoma de Madrid, y por mí, hablando un poco de todos estos cambios en valores, en cognición, cambios sociales de los jóvenes en la era de la hiperconectividad.

Y este es mi otro libro, *Socionomía*, que se publicó hace un año, este ya es de pago, o sea que no os digo tanto, pero sí que el primero además yo creo que es más acorde con lo que estáis trabajando, os he traído una copia y ningún problema porque ya digo que es gratuito y descargable.

COMPARECENCIA DEL INGENIERO INFORMÁTICO E INGENIERO EN ORGANIZACIÓN INDUSTRIAL, D. FÉLIX BREZO FERNÁNDEZ, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 30 DE ENERO DE 2014.

El señor **INGENIERO INFORMÁTICO E INGENIERO EN ORGANIZACIÓN INDUSTRIAL** (D. Félix Brezo Fernández): Lo primero de todo es agradecer la invitación y la posibilidad de exponer cuáles son los puntos de vista de una persona que trabaja en el día a día en el ámbito de la seguridad en la red en general y en el de los riesgos derivados de su uso en particular. Quiero agradecer también la preocupación de las instituciones acerca de un campo y de un ámbito que está cada vez más presente en la vida diaria de todos los españoles, de la sociedad europea en general y, particularmente, del sector de la ciudadanía que conforman los menores en un número cada vez mayor.

A continuación, les voy indicar cuáles van a ser los contenidos de mi intervención. En primer lugar, procederé a identificar algunas de las facilidades que ofrece la tecnología (lo voy a hacer también desde un punto de vista bastante práctico, bastante visual). Se hace necesario ver hasta qué punto las tecnologías, de las que otros ponentes también se habrán hecho eco, están a disposición de cualquier individuo que opere en las redes. Seguidamente, hablaré de las redes sociales y de qué tipo de información se puede obtener a través de ellas y del juego online y de las implicaciones que estas plataformas pueden tener para los menores. También me acercaré a otro tipo de divisas de fácil acceso, no solo bitcoin, tema bastante recurrente últimamente pero no necesariamente reciente, sino también en videojuegos y en plataformas de juego online, como Diablo II, World of Warcraft y similares, en los que existen auténticas economías sumergidas en las que se pueden comprar y vender productos virtuales para luego extraer el dinero hacia el mundo real. Precisamente por esto último, estas plataformas han pasado a ser también nicho de otro tipo de actividades ilícitas que seguramente no vienen tan relacionadas con el tema concreto de la ponencia de hoy pero que no podemos dejar de tener en mente.

Como ya hemos avanzado, vamos a empezar por repasar algunas de las facilidades que ofrece la tecnología. No es extraño representar esta

realidad comparando dos sucesos similares que han ocurrido en momentos diferentes pero relativamente cercanos. Algunos emplean la imagen de la investidura del Papa Francisco en 2013 para compararla con la imagen de la investidura de Benedicto XVI en 2005, apenas ocho años antes, pero lo cierto es que se podrían utilizar eventos deportivos o acontecimientos culturales para comprobar la penetración de los smartphones de un año a otro. ¿Qué subyace? El acceso a la tecnología y a los smartphones se ha democratizado a pasos agigantados. Hace nada era prácticamente impensable que un menor pudiera tener acceso a un dispositivo en el que pudiera sacarse fotos, compartirlas en la red y comunicarse con terceros sin prácticamente ningún tipo de control parental. La tecnología —afortunadamente, casi siempre para bien— nos amplía horizontes, pero si no tomamos las precauciones necesarias, si no educamos a nuestra gente sobre las implicaciones de su uso, estas nuevas funcionalidades inconscientemente utilizadas pueden ser explotadas por terceros.

Además, en el caso de la tecnología, de las redes y de Internet se da otra circunstancia que se convierte en un problema recurrente: las condiciones legales en unos países y en otros son diferentes. Si ya lo que en España es delito, podría no estar tipificado como tal en países culturalmente similares como Estados Unidos o Europa, la problemática se acrecienta cuando entran en juego estructuras legislativas similares de países menos cercanos de otros continentes más alejados de nuestras costumbres y con otras problemáticas más acuciantes.

Pero, ¿hasta qué punto somos conscientes de lo sencillo que es conectarse desde otro país? Quería aprovechar para exponer a sus señorías en directo lo fácil que es utilizar, por ejemplo, la red TOR. Sin entrar en demasiado detalles, la red TOR es una plataforma que, a partir de una aplicación libre descargable y mediante apenas un par de clics, permite a los usuarios conectarse a la red empleando una dirección IP diferente a la propia, empleando un nodo de esta red como puente entre el destino final y ellos mismos. En esta demostración, para utilizar una nueva identidad bastaría con pincha en «Utilizar una nueva identidad» para conectarnos a través de otra dirección. Al intentar localizarla en este ejemplo, los servicios de localización aproximada indican que estamos intentando realizar una conexión desde Rumania. Lo que acabamos de ver pone de manifiesto que, en apenas dos clics y sin que sea necesario tener ningún tipo de conocimiento avanzado en materia de seguridad, sin ser un hacker o un gran experto se puede conseguir enmascarar la procedencia de una

conexión. Estamos hablando de tareas que puede realizar cualquiera sin problemas y con unas herramientas que están a disposición de cualquiera, gratuitas, y accesibles y de una sencillez como la que se ha querido mostrar en esta pequeña demostración. De hecho, si estos mecanismos y otros similares fueran utilizados de una forma profesional, podrían hacer que el rastreo de un teórico delito llegara a ser extremadamente complicado, sobre todo si su seguimiento dependiera de países como los que hemos comentado anteriormente, países que no tienen desarrollada ningún tipo de legislación en temas de ciberseguridad.

De ahí el interés de realizar esta prueba en vivo: para ver con nuestros ojos que tenemos en el rastreo de los problemas de la red un problema serio y que su solución no pasa solamente por el desarrollo de una sólida legislación española, sino por la formalización de acuerdos cada vez más estrechos a nivel europeo y a nivel internacional.

Esta problemática se han puesto de manifiesto en otros ámbitos. Los programas de espionaje masivo y de recolección indiscriminada de información en cantidades ingentes también han copado numerosos titulares recientemente. Lo que es cierto es que existen aplicaciones y scripts con licencia de software libre y, por tanto, de uso, copia, modificación y distribución completamente gratuita que con 2.000 líneas de código Python que puede editar y configurar a su discreción cualquier programador para recabar de forma masiva la información pública sobre una entidad que opera en la red. Es el caso de Facebook Stalker (facebookstalker.py), que permite la conexión con Facebook para descargar y almacenar absolutamente toda la información a la que tenga acceso la cuenta de un usuario. Estas herramientas permiten, por ejemplo, recolectar desde fuera qué información pública tiene un determinado perfil. Huelga decir que entre la información que los usuarios facilitan gratuitamente hay datos de un carácter tan sensible como las afiliaciones políticas, las simpatías, los grupos favoritos, los eventos deportivos o musicales a los que va a acceder o ha accedido un contacto, los patrones de conexión a la red social en función de las horas en las que actualiza su muro o introduce comentarios en las fotos de conocidos, etc.

Sin embargo, la funcionalidad de estas herramientas no es lo sorprendente. Almacenar y obtener tus estadísticas de cara a construir un perfil virtual de una persona real es fácil y está al acceso de cualquiera. Se trata de miles de líneas de código que utilizadas de forma malintencionada

pueden automatizar la obtención de información sobre cualquiera y que, por tanto, sobreexponen de una manera especial a nuestros menores.

Asimismo, de la globalización de los servicios web emanan otros problemas. ¿Qué ocurre si, estando en vía pública, es el satélite del buscador de turno el que saca una fotografía? Esa información, ese derecho a la intimidad, ese derecho de acceso y rectificación, ¿lo podemos ejercer siempre desde España o dependemos de la ubicación de estos servidores pese a que la fotografía se obtiene sobre territorio español? ¿Existen mecanismos suficientes como para que los organismos públicos puedan presionar de forma efectiva cuando se atente contra la privacidad o se pongan en jaque cuestiones de seguridad? Estas problemáticas derivadas en parte del derecho a la intimidad y que se aplican a la totalidad de las personas son particularmente sensibles, como ya se pueden hacer una idea, en el caso de los menores.

El caso que comentaba la anterior ponente acerca de las Google glasses: pensar en un dispositivo como las Google glasses que permita un procesamiento de las imágenes en tiempo real para aplicar máscaras de reconocimiento facial y cotejar esa información con la disponible públicamente a través de las redes sociales. Las tecnologías, algunas más maduras que otras, para realizar este tipo de búsquedas no son ciencia ficción. Sin ir más lejos, y a modo de prueba, Google en su servicio de Google Images hace tiempo que cuenta con un buscador que permite identificar imágenes similares empleando como criterio de búsqueda el contenido de las mismas. sus colores y formas. Si se combinaran la información proveniente de diferentes herramientas se puede construir un perfil público (remarco esto) con información detallada sobre personas completamente anónimas como nunca antes se había pensado.

Estamos en un mundo en el que los ciberdelincuentes han encontrado más motivos que nunca para dedicarse a la ciberdelincuencia. La relativa facilidad de monetizar cualquier infección gracias a la masificación del uso de plataformas de pago, ha convertido en la sustracción en un negocio muy rentable. De hecho, diariamente se publican ofertas de compraventa de números de tarjeta de crédito con CVV, fecha de caducidad y demás datos personales. Esta información se vende en el mercado negro a precios variables a partir de los 3 USD. De la misma forma que se producen robos en las calles y en los bancos, y de la misma forma que hay gente que defrauda de una manera o de otra, existen delincuentes que

robando credenciales bancarias y poniéndolas a disposición de terceros están haciendo negocio.

Para recuperar el tema de las redes sociales quería poner sobre la mesa una analogía que ilustra lo paradójico de la situación cuando a los menores, a niños de 6, 7 u 8 años les hablamos sin tapujos de los reyes magos y les recordamos que no queremos que hablen con extraños o que no abran la puerta a nadie mientras ponemos en sus manos dispositivos que les permiten conectarse a todo tipo de contenidos, contar información sobre ellos y conectarles con completos desconocidos sin que los adultos muchas veces sepan qué pueden hacer para protegerlos.

Lo cierto es que en España tenemos mecanismos para empezar a hacer esto realidad. Y en el caso de las plataformas de juego online, que son plataformas para mayores de 18 años, se obliga a la identificación con nombre, apellidos y DNI entre otros datos personales. Si se quisiera implantarlos, hay tecnología para llevarlo a cabo. Ocurre lo de siempre: los mecanismos son más engorrosos: lleva más tiempo tener configurar un lector de tarjetas para poderte identificar ante una empresa y que esta pueda contrastar los datos. Pero mecanismos, existen. No podemos enrrocarnos en el: «no, es que no tenemos tecnología que nos permita garantizar la seguridad de los menores» porque esa tecnología existe.

Además, se dan otros problemas que también son inherentes a las redes sociales. Hace apenas unos días se detenía en Estados Unidos al administrador de una serie de páginas de contenido pornográfico en las que se difundían vídeos de contenido sexual. Pese a que los vídeos eran grabados de forma consentida por los propias parejas, eran colgados a en internet a posteriori por uno de los dos miembros de la misma en el momento en que la pareja se rompía. Además de ser un evidente atentado contra la intimidad pareja, esta situación adquiere unos tintes más graves si los que protagonizan dichos contenidos son menores. La masificación del uso de la tecnología deja aún más expuestos a los menores lo que debería derivarse en una sensibilización especial que no se ve reflejada en la realidad. De hecho, en abril de 2013 tuvo lugar la difusión masiva a través de Twitter de enlaces a un vídeo de contenido sexual entre los que aparecían diferentes menores. Como bien avisaba el CNP, la mera posesión (habría que revisar en este punto el concepto posesión, dado que si se visualiza online, técnicamente el vídeo también es descargado temporalmente al equipo del usuario) o distribución del vídeo es delito. Pese a

ello, el vídeo alcanzó rápidamente un gran número de visitas y fue dado a conocer en dicha red social siendo tema del momento durante varias horas. El principal problema que subyace es que ni los usuarios son conscientes de que la distribución de dicho vídeo es pornografía infantil ni se han dispuesto elementos disuasorios aplicables al fenómeno de las redes sociales. ¿Es suficiente con perseguir a los productores y distribuidores originales del vídeo para concienciar a la sociedad de que lo que estamos haciendo es algo tan grave o se hace necesario desplegar iniciativas y/o normativas que adviertan de que la difusión de ese tipo de contenidos es un delito particularmente grave cuando los protagonistas son menores? Desde luego, la naturaleza y cantidad de comentarios llevados a cabo no ponía de manifiesto la conciencia social en estas cuestiones.

Las redes sociales tienen también muchas ventajas. Evidentemente podemos conocer un montón de cosas sobre un montón de gente y adoptar nuevas ideas y jugar y perder el tiempo. Ese cambio de hábitos, ha dado paso también a nuevos modelos de negocio como el que explotan algunas compañías de desarrollo de videojuegos que han encontrado en los micropagos un nuevo filón. Por un lado, los juegos de 60 euros de antaño mantienen su mercado, pero van dando paso poco a poco a otro tipo de soluciones de entretenimiento a las que se puede acceder por menos de tres o cuatro euros. Por otro, cada vez aparecen más aplicaciones gratuitas que, a través de sencillos micropagos, permiten ampliar la experiencia de los jugadores. La ventaja es que estos créditos adicionales son más sencillos de pagar, incluso a través del teléfono móvil a la vez que, al tener un coste menor, se acercan también a públicos (como el infantil) con menos capacidades para realizar desembolsos superiores.

Además, existen entornos de realidad aumentada que no tienen por qué ser necesariamente juegos. El caso de Second Life es un caso muy claro. Se trata de una plataforma de realidad aumentada en la que el usuario ya no se crea un perfil sino un personaje con identidad propia que luego puede interactuar en 3D en un mundo tridimensional. Está destinado principalmente a las relaciones interpersonales y a conocer gente. La cuestión es que han emergido por debajo economías en las que se puede adquirir gorros, chaquetas y adornos para tu personaje, incluso de carácter sexual. Para ello, la plataforma cuenta con mecanismos que te permiten adquirir créditos de Second Life (*linden dollars*) que a posteriori también se pueden retirar y que, por tanto, podrían derivar en otro tipo de prácticas que también deberían ser investigadas en otro tipo de ponencias.

El juego *online* es un ámbito que hasta mayo de 2012 no disponía de una normativa legal específica en nuestro país. Por aquel entonces, las principales salas de juego online del momento operaban en España pese a estar afincadas en territorios de ultramar como Guernsey, la Isla de Man, Gibraltar o similares. De hecho, este era el caso de Full Tilt Poker sala de juego afincada en Guernsey, territorio de ultramar británico dependiente de la Corona de 78 kilómetros cuadrados y 1.900 habitantes y en el que estaba alojada la segunda mayor sala de póquer del mundo.

En este sentido, el 15 de abril de 2011 tuvo lugar el conocido como *black friday.* Se suspendió la actividad en Full Tilt Poker a raíz de una serie de problemáticas con las licencias y el bloqueo de las cuentas de juego y de dinero virtual de centenares de miles de jugadores a nivel mundial. Gracias precisamente a la legislación española hoy se dispone de garantías adicionales de transparencia y de mecanismos para perseguir en España aquellos sitios que, por ejemplo, no cumplan con los estándares de prevención de la ludopatía o no eviten que los menores puedan jugar en sitios de juego *online*, por ejemplo.

Sin embargo, aún habiendo desarrollado esta normativa los usuarios pueden seguir encontrando plataformas no están afincadas en España en las que registrarse es tan sencillo como rellenar una serie de campos de datos, insertar tu nombre y usuario y empezar a jugar. En casi todas ellas se ofrecen además reclamos en forma de bonos de primer depósito o bonos de fidelidad para atraer un mayor número de jugadores.

Es decir, independientemente de que sea fácil o difícil después extraer el dinero obtenido en esas cuentas, el problema es que nuestros menores están más expuestos a ellas por la publicidad y este tipo de salas no tienen la obligación de cumplir nuestra legislación. La solución es complicada: por un lado, se podría proponer el bloqueo del acceso a todas las páginas externas no reguladas en España en un ejercicio que podría ser entendido como una medida para coartar la libertad de expresión. Se podría sostener el argumento de la protección de los menores, pero habría que establecer claramente en qué casos está justificado y en qué casos no lo estaría. Seguramente, eso es cuestión para que el Pleno y el Senado y el conjunto de la ciudadanía en general lo consideren.

A este escenario hay que añadir otra derivada: la de la persecución de los delitos relacionados con el blanqueo de capitales. Una legislación estricta pone a disposición de las FyCSE herramientas que obligan a

las empresas y a las plataformas a ofrecer información cuando nuestros estamentos consideren que puede existir algún tipo de delito pero.. ¿qué potestad tiene España para exigirle a un sitio web afincado en las Antillas Holandesas para que le dé información de las transacciones que están realizando sus jugadores? Acuerdos bilaterales aparte, no tiene ninguna potestad.

Lo cierto es que el sector del juego *online* ha experimentado un crecimiento sin parangón. Antes de la regulación existían aproximadamente 170.000 jugadores en España; seis meses después de la regulación, los expertos situaban la cifra en torno al millón de jugadores (997.000). Se ha acercado la publicidad y el hecho de que sea abiertamente legal seguramente ha alimentado este crecimiento. Pero las apuestas y los juegos han pasado a formar parte también de nuestro día a día. Si un usuario navegara por los principales sitios de noticias deportivas, se encontrará con que se habla de partidos de fútbol y coeficientes de apuestas prácticamente incrustados en las propias noticias, se habla de bonos gratis para apostar y se habla de jugar al póquer *online* gratis. A modo de demostración, si accedemos ahora mismo a los principales sitios deportivos de este país encontraremos por todos los lados *pop-ups* y ventanas («bet» no sé cuánto, «apuesta» no sé cómo, el Madrid se paga más barato o más caro). Estos ganchos son también percibidos por los menores, público especialmente sensible porque a menudo incluyen entre sus páginas de consulta diaria este tipo de plataformas no permaneciendo ajenos a las señales que les recuerdan que el tema de las apuestas sigue ahí.

Sin embargo, si vamos a la televisión los contenidos considerados para adultos se difunden a partir de una determinada hora como las líneas de contacto telefónico o la pornografía. De igual manera, se ponen avisos de contenidos no recomendados para menores de 18 años, de 13 años o de 7 años. Esa cultura de concienciación no la estamos viendo en los sitios *online* ni tan siquiera en los que operan en y desde España.

De la misma forma que ocurre en la red, ocurre en la radio. Al sintonizar cualquier emisora en horario de deportes de fin de semana se promocionan continuamente los sitios de apuestas, sin protección de ningún tipo hacia menor y con práctica impunidad en lo que respecta a los horarios. Este es un ámbito en el que creo sinceramente que se podría actuar de una forma prácticamente inmediata en términos legislativos que ya se mostró eficaz en el pasado. En el caso de la Fórmula 1, hasta hace 8 o

10 años la publicidad del tabaco era predominante y copaba gran parte de los espacios publicitarios de los grandes premios. Sin embargo, llegó un momento en que los diferentes países empezaron a retirar el tabaco de todos estos espacios desarrollando iniciativas legislativas locales, desapareciendo también los contenidos de bebidas alcohólicas. En los casos del alcohol y del tabaco se pusieron los mecanismos que se estimó conveniente.

En otro orden de cosas, *bitcoin* es una emergente criptodivisa que necesita de la red para transferirse empleando ficheros. La complejidad de efectuar transferencias con *bitcoins* para gente que sabe manejarlo es trivial. Se trata de una economía plenamente especulativa que da cobertura a todo tipo de productos. La difusión de los *bitcoins* necesita de dos elementos para que tenga lugar. Por un lado, está la conexión a internet necesaria para que el resto de la red distribuida que gestiona la economía valide la transacción y, por otro lado, un ligero retardo que permita a esta verificar que el *bitcoin* pertenece a quien die hacerlo a partir de una serie de procesos matemáticos relacionados con la criptografía de clave pública.

Las características distribuidas de la red obligan a que las transacciones sean públicas para que cualquier nodo de la misma pueda realizar las verificaciones pertinentes. De hecho, el seguimiento de las transacciones se puede realizar a partir de diferentes páginas que almacenan la cadena de bloques (nombre con el que se hace referencia al histórico de transacciones de bitcoins) comprobando así de qué cuenta a qué cuenta se han ido transfiriendo estos *bitcoins*. Pero, ¿tiene sentido que sean transacciones públicas y doten de una capa adicional de anonimato? Por un lado, se puede saber en todo momento cuántos *bitcoins* tiene cada cuenta mientras que, por otro, a diferencia de lo que ocurre en el mundo real, en *bitcoin* en cuestión de segundos se pueden crear decenas de miles de cuentas con un mismo propietario. Así, se facilita el camuflaje de las operaciones a partir de transferencias entre cuentas que en realidad son gestionadas por la misma identidad terminando por difuminar completamente cuál es el origen de las transacciones.

Esta realidad lleva consigo implícitos cuestiones de fiscalidad de fiscalidad de difícil solución dada que las transferencias económicas se realizan a través de *entidades* fuera del control de los estatales y ajenas a toda norma. Estamos hablando de una moneda cuyo curso no está oficia-

lizado por parte de ningún estamento, porque no se considera una divisa funcional. Pero la realidad nos demuestra que la gente está realizando pagos, está comprando servicios, está adquiriendo libros y películas y está contratando programadores. Aún así, sigue siendo muy difícil establecer criterios de fiscalidad robustos con divisas gestionadas de forma ajena a los bancos nacionales porque ni existe un mercado cambiario oficial ni tampoco es posible forzar el cumplimiento de las normativas fiscales nacionales.

Sabiendo esto, ¿por qué hablamos de los *bitcoins*? En noviembre de 2013 se producía un fenómeno que disparaba el *bitcoin* a prácticamente 250 dólares despegando desde los 2 dólares. Sin embargo, en un momento dado se dieron una serie de circunstancias que propiciaron su caída como la inesperada paralización (forzosa o premeditada) de la cotización en algunos de los principales mercados de intercambio. El resultado fue una bajada que alcanzó un mínimo de 83 dólares poniendo de manifiesto que se trata de una economía globalizada sobre la que determinadas entidades podrían ejercer una influencia tal que cambiara el curso de la economía.

Las características que la configuran son los movimientos especulativos especialmente agresivos al margen de todo control europeo o nacional y la desprotección de los usuarios frente a las injerencias de poderes económicos asimétricos como, por ejemplo, las ventas masivas planificadas a precios más bajos de lo normal para lanzar el mercado a la baja y volverlos a comprar a continuación. Se trata por tanto de un producto volátil y complejo de gestionar con una penetración cada vez mayor.

La cuestión es: ¿estamos hablando de una economía que crece? Pues sí. En noviembre de 2013 el *bitcoin* se cambiaba a 246, como hemos visto; hoy se cotiza en torno a 1.000 dólares el *bitcoin* cuando hace apenas dos años se cotizaba a 2 dólares y hace cinco lo hacía a poco más de 0,06 dólares. Es decir, el que tenía un *bitcoin* hace dos años, ahora tiene quinientas veces más; y el que tenía un *bitcoin* hace cinco habría multiplicado su inversión por 15.000. Si a todo esto se suma la dudosa procedencia de algunas transacciones y el anonimato que proporcionaría una gestión efectiva, estamos hablando de economías en auge al margen de los esfuerzos que propone nuestra legislación.

Lo cierto es que *bitcoin* es solamente la punta del iceberg. Existen también otro tipo de criptodivisas y otro tipo de mercados cambiarios

con los que puede interactuar el ciudadano. Criptodivisas y movimientos como los que van apareciendo en SecondLife o los que ya han aparecido en World of Warcraft. Precisamente ayer, en una conferencia de Iñaki Bernal del BBVA facilitaba el dato de que el mercado interno de Diablo II tenía una capitalización, solamente en China, mayor incluso que los *bitcoins*.

Esto que estamos contando no es nuevo ni necesariamente reciente, porque aunque son muchos los países que están empezando iniciativas legislativas para contener estas divisas, es cada vez el mayor número de servicios que las aceptan. No se escapa a los investigadores la existencia de mercados en los que se permite la compraventa de todo tipo de productos como drogas o medicamentos prohibidos (uno de los casos es Silk Road) y en los que incluso se han llegado a ofrecer ataques de denegación de servicio contra terceros o campañas publicitarias. Esta información está en la red a través de redes como TOR y es de acceso es trivial.

Se da además otra particularidad: precisamente para garantizar el anonimato de estas transacciones, los delincuentes utilizan herramientas de anonimización como las que hemos visto anteriormente para enmascarar actividades de tráfico de drogas, venta de armas y otros elementos que escapan al control estatal. Cualquiera, incluso los menores, podrían acceder a sitios de juego *online* y utilizar *bitcoins* con diversos fines. Registrarse en este tipo de sitios es incluso más fácil que en los sitios que utilizan transacciones tradicionales porque aquí lo único que necesitas es un nombre, un usuario, la contraseña, y repetir la contraseña. y con eso ya es suficiente para realizar las cuentas.

E insisto, lo más importante de esta cuestión es que no se trata de conceptos a desarrollar en la mente de alguien sino que son ya realidades que quedan hoy patentes. Hay casos de algunas salas de apuestas afincadas en las Antillas Holandesas que utilizan software que luego permite la interacción con cuentas de PayPal y de bancos europeos que aceptan también los *bitcoins*, y para cuyo registro no es necesario prácticamente suministrar ningún tipo de información.

Para ir terminando, quería extraer un par de conclusiones con respecto a estas temáticas. Por un lado, mis perspectivas para el futuro, no son en absoluto satisfactorias. La principal problemática de la persecución de este tipo de delitos, tanto relacionados con pornografía infantil, como con el abuso de menores o los relacionados con el juego, va a depender

mucho de cuáles sean las relaciones entre Estados y la convicción de estos a la hora de perseguirlos. Incluso desarrollando en España una legislación robusta aquí, al ser internet una red global, el establecimiento de protocolos de intercambio de información rápidos y eficaces con el resto de países de la Unión Europea, con Estados Unidos o con Rusia va a ser fundamental a la hora de perseguir con garantías a los ciberdelincuentes.

Por otro lado, no quería dejar pasar la burbuja de lo social, de estar disponible en todas las redes sociales el mayor tiempo posible. Una situación que ya de por sí deja expuestos a los adultos, expone sobremanera a menores que no tienen por qué necesariamente comprender cuál es el sentido de la información que están suministrando ni los modelos de negocio que emanan de ellos, no deberían tener que preocuparse por el hecho de que los datos e su perfil están siendo utilizados para mostrarles publicidad a medida orientada a explotar sus intereses y a canalizar sus hábitos hacia determinados tipos de contenidos que son más susceptibles de consumir.

Y además, recuperar la existencia de nuevos escenarios. Los robos virtuales están a la orden del día como lo está la sustracción de credenciales bancarias o de credenciales de cuentas de correo y de activos tecnológicos corporativos. Nuevamente volvemos a exigir a los menores que comprendan aspectos que los mayores de edad no llegamos siquiera a dimensionar con garantías. Pese a que los menores pueden interactuar con completos desconocidos que pueden sacarle partido de muchísimas formas, lo cierto es que la red muchas veces no se concibe como algo externo seguramente porque el menor se mantiene dentro de nuestros hogares.

Para que nos hagamos a la idea, hace unos años una de las contratistas de los Estados Unidos recibía una oferta por parte del Gobierno de los Estados Unidos para la generación de un software que permitiera el control de apenas una decena de identidades *online* diferentes. Se quedaron cortos, porque hace apenas unas semanas, la prensa hacía público que una de las personas detenidas en una operación contra la pornografía infantil podía haber mantenido contacto con hasta 500 menores. La gestión de diferentes identidades digitales ficticias es mucho más sencilla de llevar a cabo a través de la red y es una situación que no pasa desapercibida.

Por último, quería aprovechar para insistir en que se trata de competencias que no solamente pueden quedarse en el debate, que, por otro

lado, es muy gratificante comprobar que se está manteniendo a nivel nacional, sino que deben ir muchísimo más allá para poder iniciar los mecanismos que establezcan un marco conjunto de colaboración a nivel internacional en el que se permita una persecución eficaz de los delitos y de quienes los cometen en pos de la preservación de los derechos y libertades de todos en general y de nuestros menores en particular.

Por mi parte, estoy a su disposición para cualquier tipo de pregunta que quieran formular.

COMPARECENCIA DEL MÁNAGER DE RESPONSABILIDAD SOCIAL CORPORATIVA DE ORANGE, D. JESÚS GUIJARRO VALLADOLID, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 10 DE FEBRERO DE 2014.

I. *Introducción*

Orange, perteneciente al Grupo Orange, es un operador alternativo de referencia del mercado español y uno de los principales inversores en la industria de telecomunicaciones, con más de 15.000 millones de euros de inversión acumulada en España. Con un claro enfoque hacia la innovación, Orange sitúa al cliente en el centro de toda su actividad, cuyo fin es poner a su disposición productos sencillos, útiles y de última generación con las máximas garantías de calidad y servicio. Gracias a todo ello, Orange es un actor fundamental del sector de las telecomunicaciones en nuestro país, donde presta servicio a más de 14 millones de clientes.

La Responsabilidad Social Corporativa forma parte de su estrategia como empresa y la hoja de ruta en esta materia viene marcada por nuestro plan «Conquistas 2015», que se traduce en la adopción de una estrategia empresarial innovadora, basada en la colaboración y la corresponsabilidad.

En otras palabras, Orange tiene como objetivo fundamental cooperar con todos sus grupos de interés para establecer las condiciones que favorezcan un desarrollo sostenible, al mismo tiempo que se da respuesta a los desafíos que plantea un mundo tan dinámico como el actual, también en materia de uso responsable de las nuevas tecnologías como el caso que hoy nos ocupa.

En este sentido, Orange reconoce y tiene muy presente la importancia que tiene hoy la protección de los menores, con las tecnologías de la información en constante y veloz evolución. Por ello, impulsa todas aquellas iniciativas que permitan a sus clientes afrontar con éxito el desafío que supone garantizar que los menores puedan utilizar de forma segura todas las posibilidades que ofrecen las TIC.

El Grupo Orange firmó en febrero de 2007, junto a los principales operadores móviles europeos, el Acuerdo de Autorregulación denomina-

do «Marco europeo para un uso más seguro del móvil por niños y adolescentes». Uno de los compromisos de dicho Acuerdo era el desarrollo de Códigos de Conducta similares en los diferentes estados miembros de la Unión Europea.

En aplicación de este compromiso, Orange España firmó en diciembre de 2007, junto con otras operadoras españolas, el «**Código de Conducta de los Operadores Móviles para el Fomento del Uso Responsable por parte de menores de edad en el acceso a los Servicios de Contenidos de Comunicaciones Electrónicas Móviles en España**». Mediante la firma de este Código, Orange España se compromete a:

- etiquetar los contenidos que hayan sido clasificados como no adecuados para menores de 18 años conforme a los estándares sociales europeos.
- facilitar mecanismos de control de acceso que eviten el acceso por parte de los menores de edad a contenidos clasificados para adultos.
- promover campañas de sensibilización relativas al uso responsable de los servicios móviles.
- luchar contra la difusión de contenidos ilícitos.

En el marco de estos compromisos, hace ahora un año y con motivo del Día Internacional de la Internet Segura, presentamos la web Navega Seguro repleta de consejos para padres y tutores en el uso responsable de las TIC entre los más pequeños.

El objetivo del portal, al que podemos calificar de «centro on-line de orientación familiar», es ofrecer recomendaciones, consejos y recursos de interés para la formación y orientación de los menores sobre la importancia de una navegación segura.

Queremos dar respuestas a preguntas como qué hacer si los pequeños de la casa son víctimas de un caso de sexting (difusión de contenidos de carácter sexual) o ciberbullyng (acoso a través de Internet), cuáles son los dispositivos más indicados para los más pequeños, cómo instalar un sistema de control parental o cómo deben acceder los menores a las redes sociales de forma segura.

Nuestra vocación, no solo es informar sino también fomentar la participación, ofreciendo a los usuarios la oportunidad de realizar comentarios, aportar sus opiniones o proponer nuevas ideas.

Igualmente, Orange colabora con la Asociación Protégeles impartiendo charlas en colegios sobre navegación segura en Internet así como facilitando el acceso desde sus páginas a la línea de denuncia sobre pornografía infantil. Este acuerdo refuerza el compromiso de Orange en la protección de los menores frente al uso indebido de las nuevas tecnologías, dando cumplimiento a las obligaciones asumidas por la compañía en la firma del código antes citado.

II. *Contexto actual*

La extensión de la telefonía móvil ha alcanzado a todos los sectores de la población, incluidos los más jóvenes. Es frecuente que niños y adolescentes dispongan de teléfono móvil de uso particular, y que cada vez lo hagan a edades más tempranas.

Niños y adolescentes españoles son consumidores habituales de tecnología, y así lo confirman una vez más los datos de Octubre de 2013 del Instituto Nacional de Estadística referidos a la Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares. La evolución de los resultados según la edad sugiere que el uso de Internet y, sobre todo, del ordenador, es una práctica mayoritaria en edades anteriores a los 10 años. Por su parte, la disposición de teléfono móvil se incrementa significativamente a partir de los 10 años, 26.1% hasta alcanzar el 90.2% en la población de 15 años.

Por otro lado, los dispositivos móviles han evolucionado hasta tal punto que, con la tecnología actual, un smartphone presenta prácticamente las funcionalidades de un ordenador personal.

El contexto, por tanto, se define en primer lugar por un colectivo, el de niños y adolescentes, que está accediendo a edades cada vez más tempranas a dispositivos móviles que convergen, en cuanto a prestaciones, con pequeños ordenadores personales.

El desarrollo de las pantallas táctiles han hecho de los smartphones y tabletas digitales elementos muy atractivos para los más pequeños, que aprenden a usarlos pero que carecen todavía de las habilidades necesarias para que los utilicen con máxima seguridad.

Una primera conclusión a tener en cuenta: **los niños empiezan a usar Internet a edades cada vez más tempranas, cuando carecen de las**

habilidades técnicas, críticas y sociales necesarias, lo que les sitúa en una posición más vulnerable.

No obstante, los beneficios derivados de la utilización del teléfono móvil por parte de los menores son también conocidos: a los padres les ofrece la sensación de seguridad y control sobre los hijos (el 88% de los padres se siente más seguro si puede localizar a su hijo a través del móvil[1]), y a los niños les proporciona una sensación de libertad y autonomía además de contribuir a desarrollar competencias como autonomía y responsabilidad (además de destrezas motoras y cognitivas).

Así las cosas, **el reto consiste en encontrar el equilibrio entre el aprovechamiento del potencial que ofrecen los smartphones y la prevención ante posibles riesgos.**

III. Situación actual del uso de smartphones por los niños y adolescentes españoles

En este contexto, se hace necesario elaborar un diagnóstico de los usos del Smartphone y hábitos seguros por parte de adolescentes y, asimismo, conocer la percepción que de dichos usos y hábitos seguros tienen sus madres y padres. Es importante, además, conocer su conciencia de los riesgos, su reacción ante los mismos y las medidas de seguridad que adoptan.

Cómo de frecuentes son estos riesgos, cuántos de estos riesgos se traducen en auténticos daños para el menor, cómo reaccionan los niños, si algunos niños son especialmente vulnerables o cómo pueden o deben actuar los padres —éstas y más preguntas deben contestarse de manera fiable.

Es importante evitar los temores basados en consideraciones morales o preocupaciones exageradas, sobre todo porque éstas pueden desembocar en intentos por restringir las libertades de los niños o limitar sus oportunidades online.

Para dar respuesta a estas cuestiones INTECO y Orange llevamos a cabo el «Estudio sobre hábitos seguros en el uso de smartphones por los

---

[1] INTECOy Orange (2010). *Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles.* Informe disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_moviles_menores

niños y adolescentes españoles», un sondeo de opinión consistente en la realización de 800 encuestas personales en hogares españoles, realizándose en cada familia dos entrevistas: al menor y a su padre, madre o tutor legal.

Los resultados del estudio se completan con las aportaciones de 32 expertos (profesionales e instituciones) pertenecientes a diversas áreas de conocimiento, que han aportado una visión cualitativa y multidisciplinar a este proyecto de investigación.

Las conclusiones de este análisis son:

En primer lugar, para los adultos, la oferta de aplicaciones es el principal motivo para comprar un teléfono inteligente y a través de ellas, buscan contenidos relacionados con el tiempo libre, consultan el correo electrónico o acceden al perfil en redes sociales.

En segundo lugar, al igual que los adultos, los menores eligen el dispositivo por las aplicaciones que incorpora, aunque se dejan influenciar por las tendencias de moda o por sus amigos.

Al utilizar el smartphone, los menores son usuarios más intensivos que sus padres en servicios de uso generalizado (llamadas de voz o mensajes de texto) y específicamente de servicios «avanzados» (acceso a redes sociales, chat y mensajería instantánea, navegación web, etc.).

En general, los padres conocen estas prácticas, aunque (**y esto es importante**) tienden a subestimar el uso que hacen los chavales de ciertos servicios, en especial aquellos que implican un acceso a Internet.

Asimismo, **se observa una brecha en los relativos a la generación y difusión de contenidos**. Los terminales actuales disponen de cámaras de alta resolución y posibilidades audiovisuales elevadas, que los chicos utilizan para tomar imágenes o vídeos y también enviarlos o subirlos a Internet. Esta costumbre puede constituir una amenaza a la privacidad, en cuanto a que esas imágenes constituyen datos personales de los menores (los identifican) y, una vez enviados, se pierde el control sobre ellos.

También constatamos que los smartphones ofrecen una movilidad plena, que chicos y chicas aprovechan para chatear, buscar información en la Red, etc., mientras se desplazan o acuden a lugares de ocio. A su vez, los momentos de mayor tiempo libre (fines de semana, vacaciones) coinciden con los de mayor intensidad en el uso, sin olvidar que son

ciudadanos digitales, por lo que cabe esperar que cada vez más, esta actividad sea diaria.

En tercer lugar, los riesgos más habituales son: Uso excesivo, Adicción, Amenazas a la privacidad, Acceso a contenidos inapropiados, Grooming, Sexting, Ciberbullying, Riesgo económico y/o fraude, Riesgos de carácter técnico, …

Los niños y adolescentes que disponen de un smartphone para su uso particular, conocen en general los distintos riesgos y sus conductas.

Por su parte, los padres demuestran ser conscientes de la incidencia de riesgos que les ocurren a sus hijos, aunque se observan en general un conocimiento inferior al manifestado por sus hijos. **Esta diferencia viene a resaltar la importancia de que el adulto se implique en el aprendizaje y la convivencia de las nuevas tecnologías en familia, educando a los menores en la responsabilidad y no en la restricción, para favorecer un clima de confianza en el hogar, que permita a los menores acudir a sus padres o adultos de referencia en caso de incidencia.**

Esto debe conducir a la reflexión en cuanto al papel que tienen los padres en la educación de sus hijos en el uso de los smartphones. En primer lugar, es aconsejable fomentar un clima de confianza y protección que permita a los hijos dialogar con sus padres sobre las situaciones inadecuadas que pueden encontrarse en esta utilización y acudir a ellos en caso necesario. En segundo lugar, aplicar unas medidas y hábitos de seguridad en familia permite evitar o minimizar los impactos de las situaciones de riesgo.

En cuarto lugar, los niños necesitan aprender cómo utilizar el smartphone de un modo seguro. Su opinión sobre el control o supervisión paterna es positiva en general, sobre todo entre los más pequeños.

En las familias españolas existen normas de uso o limitaciones que parecen ser conocidas y comprendidas por los chavales, relativas al límite del gasto mensual, la prohibición de utilizarlo en clase, el tiempo de uso o lo que pueden hacer o ver.

En todo caso, el teléfono móvil parece instalarse en las familias como una herramienta que aporta confianza y protección a los padres, al permitirles estar en contacto constante con sus hijos. Además, la mayoría considera que la información proporcionada es suficiente para que el menor utilice el smartphone de forma segura.

Por último, los adultos se reconocen como principales responsables de informar sobre la seguridad en el uso del smartphone, apoyándose en los operadores, los centros escolares, la Administración y los fabricantes de terminales.

IV. *Como proteger a los menores*

Una vez radiografiada la realidad, analicemos como proteger a los menores, para lo cual podemos considerar distintas alternativas tecnológicas y/o normativas.

A. Las tecnologías como solución

La primera de las vías a considerar son las herramientas tecnológicas.

Existen productos disponibles que cuando son instalados tienen la capacidad de bloquear información no deseada como pornografía, obscenidades, violencia. Otros programas proveen acceso a Internet sólo durante horas específicas durante el día, proveen un historial de las páginas visitadas por sus hijos y previenen el acceso a servicios como «chat». Existen también otros programas que pueden utilizarse para bloquear información personal que identifique a sus hijos, como nombre, dirección y números telefónicos

El objetivo principal de este tipo de programas de «control parental», es bloquear el acceso a contenidos y/o espiar el uso realizado.

No obstante hemos de ser conscientes que:

Primero Los niños o jóvenes con habilidades informáticas pueden «hackear» este tipo de programas. Para aprender más sobre este tipo de prácticas, solo se ha de realizar una búsqueda con las palabras «parental control software» en un buscador.

Segundo Suelen ofrecer respuestas de manera reactiva a la realidad y temáticas sociales con lo que disminuyen su efectividad.

Tercero Ninguno de estos programas ha sido totalmente efectivo una vez a prueba. La realidad, es que estos productos no pueden bloquear todo contenido dañino. Podemos afirmar que estos programas bloquean demasiado y a la vez muy poco.

Algunas pruebas de estos productos han dado a conocer que estos programas pueden bloquear sitios que no contienen

obscenidades, por ejemplo, la palabra «seno» puede encontrarse en la página de la Asociación Española Contra el Cáncer y se refiere al cáncer del seno.

Quienes apoyan el uso obligatorio de filtros en las escuelas y bibliotecas buscan prevenir que los niños tengan acceso a información dañina en Internet. Los críticos de estos filtros están preocupados de que eso signifique una censura con base al criterio de las personas que desarrollan estos programas. Asimismo, algunos críticos creen que la gente joven también tiene derecho a la privacidad, especialmente aquellos en la segunda mitad de su adolescencia.

El niño también tiene un derecho a la vida privada en el contexto familiar. La monitorización de su ordenador, el uso de videovigilancia o la geolocalización mediante el móvil son soluciones extremas. Deben usarse sólo cuando resulte imprescindible y teniendo en cuenta la proporcionalidad de la medida en función de su finalidad y de la edad del menor

En cualquier caso, debemos de considerar que la utilización de los programas de control parental debe estar adaptada a cada situación (hogar, centro educativo) y al desarrollo del menor, pero en ningún caso como substitutos de la supervisión paterna.

B. Regulación jurídica respecto al delito

La segunda de las vías a considerar podría ser la regulación jurídica.

Sin embargo, en España existe diversa normativa que protege los derechos de los menores a nivel general, y en particular, a aquellos que puedan verse afectados por el uso de las nuevas tecnologías por parte de dichos menores.

El rango normativo a este respecto es amplio ya que comprende desde la Constitución Española, como norma superior, hasta un conjunto de normas de menor rango como veremos a continuación. A esta normativa habría que añadir la doctrina tanto del Tribunal Constitucional como la de otros tribunales inferiores.

Cabe destacar, entre otras, las siguientes normas:

1. La Constitución Española mereciendo especial mención el artículo 18 en sus distintos apartados.

2. Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor.
3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
4. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
5. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

Al amparo del este marco normativo se tratan de proteger, entre otros, dos derechos fundamentales tales como:

- el derecho al honor, la intimidad y la propia imagen así como
- el derecho a la protección de datos de carácter personal de los menores que con motivo del creciente uso de las nuevas tecnologías por los menores, se ven afectados cada vez con mayor frecuencia.

En primer lugar y con respecto los *Derechos al honor, la intimidad y la propia imagen*, cada vez nos encontramos con mayor frecuencia con vulneraciones de los citados derechos por parte de los propios menores, que dentro de su ámbito escolar, familiar o de ocio, realizan actos que infringen los citados derechos en relación a otros menores y adultos normalmente de su entorno más cercano. *Niños y adolescentes no son únicamente víctimas sino que también son participantes activos y necesarios en muchas situaciones donde otros sufren*.

Este tipo de conductas colocan al menor tanto como víctima de abusos, como de autor de los mismos y dentro del ámbito de Internet comienzan a surgir nuevos tipos delictivos específicos, derivados de los actos o actividades ilícitas realizadas a través de las nuevas tecnologías, como

1. ciberbullying (acoso a menores por sus iguales),
2. grooming (acoso sexual a un menor por parte de un adulto),
3. sexting (difusión de contenidos de tipo sexual producidos por menores) o incluso la extorsión entre menores.

que en la mayoría de los casos coinciden con conductas ya tipificadas en nuestro código penal:

- Delitos contra el derecho a la intimidad, el derecho a la propia imagen (Art. 197 C. Penal)

- Calumnias e injurias (Arts. 205, 206 y 208 del C. Penal)
- Amenazas (Art. 169 C. Penal)
- Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor. (Arts. 270-272 C. Penal)
- Pornografía infantil (Art. 189 C. Penal)

En segundo lugar y con relación al *derecho a la protección de datos de carácter personal* tal y como afirma la Agencia Española de Protección de Datos, todos tenemos el derecho a la protección de nuestros datos. Este derecho consiste en nuestra capacidad de controlar el uso que pueda hacer de nuestros datos cualquier tercero, entendiendo por dato de carácter personal, aquella información que nos identifica o nos puede hacer identificables, como el nombre, el NIF, una fotografía o incluso una grabación de nuestra voz.

En el mundo de Internet es donde los menores se encuentran particularmente expuestos al uso no autorizado de sus datos de carácter personal. Esto viene originado tanto por la inclusión indiscriminada y excesiva que el propio menor pueda realizar de sus datos en la red, como por el abuso que determinados terceros, y sobre todo, compañías dedicadas al ocio, a la publicidad y a las relaciones sociales en la red llevan a cabo, utilizando los datos recabados de sus usuarios con fines puramente comerciales, por el alto valor económico que tiene esta información para muchos sectores, excediendo dicho uso del ámbito de lo necesario para los servicios prestados.

Las empresas del sector dedicadas a los servicios de mensajería, redes sociales, aplicaciones, etc. suelen llevar a cabo conductas que bien o no son conforme a derecho o bien rozan el ilícito, tales como:

a) No informar suficientemente a los usuarios sobre el uso que van a hacer de sus datos en el momento en que el usuario se da de alta en el servicio. Las políticas de privacidad no son claras, ni, de forma frecuente, permiten al usuario configurar su perfil de forma que se garantice la seguridad de sus datos. Esta circunstancia incide especialmente en los menores quienes, como ya hemos dicho antes, carecen de la capacidad y madurez cognitiva suficiente para comprender los términos de dichas políticas de privacidad y valorar los riesgos y consecuencias derivadas de la inclusión de sus datos.

b) Ceder los datos de carácter personal de sus usuarios sin el consentimiento requerido legalmente para ello y en muchas ocasiones, sin ni siquiera informar de dicha cesión a los interesados.

c) Incumplir de manera sistemática las obligaciones y plazos legales en cuanto a la cancelación de los datos de carácter personal de sus usuarios.

A modo de ejemplo, la aplicación Whatasap registra automáticamente los listados de contacto de los terminales de cada uno de sus miles de usuarios en un servidor externo, sin que la gran mayoría de sus usuarios hayan aceptado dicha inclusión de manera consciente.

La propia Agencia de Protección de datos, en previsión de lo anterior, ha puesto en su página Web a disposición de todo los usuarios información de interés para cuya finalidad es servir de guía a la hora de configurar las opciones de privacidad de los navegadores, redes sociales y sistemas operativos móviles más comunes. Ante este tipo de situaciones, la Agencia de Protección de datos interviene, y en aplicación de la Ley de Protección de datos, enmarcada dentro de la Directiva Comunitaria 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, investiga conductas que exceden el ámbito de lo permitido y que suponen un uso ilícito de los datos de carácter personal de los usuarios, imponiendo importantes sanciones, que pueden ir desde 900 hasta los 600.000 Euros.

Pero más allá de esto, la pérdida de control general que existe al introducir información y contenidos de carácter personal e íntimo en la red se hace extensible y agrava en los menores de edad, que tienden a incluir de manera descontrolada todo tipo de información personal sin medir las consecuencias de ello, pudiendo dicha información ser objeto de uso no autorizado por terceros tanto adultos como otros menores y puede atraer la atención de personas con perfil delictivo relacionado, entre otros, con los abusos a menores y a la pornografía infantil.

En la actualidad, los menores perciben como algo natural el hecho de subir a la red a través de los distintos dispositivos y servicios que nos ofrecen las nuevas tecnologías fotografías, videos e información tanto propias como relativas a su familia, amigos y resto de su entorno educativo. La inclusión de dichos contenidos se realiza en la mayoría de

los casos sin autorización de las personas que aparecen en los videos o fotografías o a las que van referidos dichos contenidos.

En este punto es importante resaltar que la imagen está considerada como un dato de carácter personal y por tanto le es de aplicación el límite de edad de los 14 años para que el menor pueda prestar por sí mismo su consentimiento al acceso y uso de su propia imagen.

Por lo tanto, un menor de 14 años desde el punto de vista jurídico no puede introducir su imagen en la red sin autorización de sus padres o tutores. Asimismo, cuando un menor quiera subir imágenes de otros menores a la red, deberá contar con el consentimiento de dichos menores de edad y en los casos en que éstos no hubieran cumplido los 14 años, será necesario el consentimiento de sus padres o tutores.

En cualquier caso debemos poner de manifiesto que la velocidad del avance tecnológico y social a día de hoy puede favorecer que el marco normativo actual no pueda dar respuesta a nuevas situaciones que se puedan plantear como consecuencia del uso de los menores de las nuevas tecnologías lo que puede llevar a un desamparo legal.

V. *Conclusiones*

A la vista de todo lo anteriormente expuesto podemos afirmar que, desde nuestro punto de vista, hay dos focos/retos principales de actuación para garantizar un uso seguro de las tecnologías por parte de los menores.

- La necesidad de incluir de forma sistematizada la formación en el uso seguro de Internet en los centros escolares. La educación para un uso seguro de Internet es imprescindible y no puede ser solo el resultado de una formación autodidacta o aprendizaje fuera de la escuela.
- Encontrar un equilibrio entre los beneficios de la recogida y utilización de la información y el derecho a la privacidad.

En España, desde hace varios años y con fuerza creciente, se viene trabajando a través de colaboraciones publico privadas para la información, la sensibilización y la formación en el uso seguro y responsable de las TICs.

Orange España desde hace ya algunos años viene desarrollando acciones dirigidas a concienciar al mayor número de personas, sobre la

importancia de hacer un uso responsable y seguro de la red por parte de los más jóvenes.

Pero aun cuando el esfuerzo de Orange y otras compañías junto a organizaciones y administraciones está siendo ímprobo, este es a todas luces insuficiente. Desde nuestro punto de vista, solo si el sistema educativo español contara con una asignatura para enseñar a los jóvenes a navegar por Internet con Seguridad estaríamos en disposición de abordar la problemática con plenas garantías de éxito.

En segundo lugar, hemos de poner en valor la privacidad de las personas en general y de los menores en particular. Internet, las redes sociales, los buscadores y los dispositivos móviles han cambiado de una forma radical y para siempre el valor de la información personal. Empresas, gobiernos, delincuentes, periodistas y curiosos se nutren de la información que encuentran sobre nosotros en Internet.

En este nuevo mundo de Internet se necesita concienciar que los datos tienen valor y que las personas tienen el derecho a decidir si los difunden o no. Este nuevo modelo de propiedad podría reforzar la privacidad de las personas porque, para autorizar la utilización de los datos, deben asegurarse primeramente de no ir *regalándolos* por ahí.

En este sentido parece aconsejable que los desarrolladores revelen de una manera muy sencilla cómo sus aplicaciones utilizan los datos personales de los usuarios, similar a como el etiquetado de los productos da a conocer su información fundamental.

Solo si los consumidores saben lo que está pasando, puedan tomar decisiones informadas y elegir las aplicaciones que se adapten a sus preferencias.

Para finalizar mi exposición, y más allá de estas recomendaciones, consideramos (y esta comisión es todo un ejemplo) que el papel fundamental de la Administración es el de impulsar las colaboraciones público-privadas, para buscar soluciones y respuestas en este debate.

COMPARECENCIA DEL DIRECTOR DE TECNOLOGÍA DE MICROSOFT IBÉRICA, D. HÉCTOR SÁNCHEZ MONTENEGRO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 24 DE FEBRERO DE 2014.

El señor **DIRECTOR DE TECNOLOGÍA DE MICROSOFT IBÉRICA** (D. Héctor Sánchez Montenegro): Muy bien, muy amable, muchas gracias. Yo creo que es de buena educación, primero, presentarse. Soy el director de Tecnología de Microsoft Ibérica; he sido anteriormente el director de Seguridad, de Microsoft también, llevo —ayer hice— 14 años en la compañía; anteriormente he estado trabajando en empresas españolas como DINSA, Banesto, Level Data, incluso en el INI; soy licenciado en Físicas por la Universidad Autónoma de Madrid. Y este tema, yo creo que nos toca, además ya no solo a nivel profesional; soy padre de tres menores, con lo cual, muchas veces andamos poniéndonos y quitándonos los gorros según corresponda.

Entonces, yo quisiera empezar esta exposición agradeciendo sinceramente la invitación que desde esta comisión conjunta del Senado han cursado a la compañía que represento, Microsoft Ibérica; es para nosotros un gran honor ser convocados en este foro, y para mí en particular, siempre lo es, es la cuarta ocasión en la que tengo el privilegio de exponer ante señorías de algunas de las cámaras sobre temáticas de diferentes ámbitos. Y en esta ocasión, sobre un terreno muy específico de la ciberseguridad como es la seguridad de los menores en Internet.

Y creo que es un acierto la preocupación y la ocupación de sus señorías por este asunto. Creo que es oportuno, es necesario, es importante, y es un asunto sobre el que sin lugar a dudas hay que reflexionar porque es y seguirá siendo de importancia durante mucho tiempo.

La ciberseguridad resulta más importante que nunca y plantea un campo de batalla del que todos formamos parte de forma activa o pasiva, incluidos nuestros menores; y es necesario conocer cuál es ese marco en el cual todo esto ocurre. No en vano acabamos de publicar como país la Estrategia de Ciberseguridad Nacional, posicionando al nivel de importancia que corresponde el ámbito de la tecnología y la seguridad en Internet, hasta el punto de incluso considerarlo en el ámbito militar como

un mando más, Mando de Ciberseguridad, que se une a los tradicionales de Tierra, Mar y Aire. O en el ámbito civil, la ciberseguridad es también un área prioritaria respecto a la protección ciudadana, protección de empresas, protección de infraestructuras críticas.

De hecho, los centros de respuesta a incidentes en Internet en España, los denominados CERT, parecen tener últimamente más protagonismo del que han tenido hasta la fecha, tanto los CERT de ámbito público como el CCN-CERT, el organismo adscrito al CNI y dirigido a la protección de las infraestructuras tecnológicas de la Administración Central del Estado, pasando por INTECO-CERT, dirigido a empresas, CNPIC-CERT, dirigido a infraestructuras críticas desde el Ministerio del Interior, Red Iris, el próximo CERT que están montando desde el Mando de Ciberseguridad, etc.; así como un largo etcétera de CERT autonómicos, incluso CERT de grandes empresas en el sector privado. Actualmente, yo creo que no me equivocaría si dijera que en España podemos llegar, a lo mejor, a 10, 12, 14 CERT.

Lo cual forma parte realmente de nuestro panorama en materia de seguridad a nivel público; no sé si a veces puede ser un problema la coordinación de estos centros, duplicidad de esfuerzos, pero puede ser otro ámbito de discusión, ¿no?

Quería aproximarme paulatinamente al ámbito de estudio de la ponencia sobre la que ustedes trabajan comenzando por la absoluta disrupción tecnológica, en primer lugar, que nos rodea. Es por ello por lo que he decidido estructurar esta exposición en dos partes claramente diferenciables pero muy relacionadas entre sí. Un primer apartado dedicado a la importancia de la tecnología, la innovación, los contenidos, los servicios a través de la red, incluyendo nuevas realidades que afectan a este escenario, como es el *cloud computing* (computación en la nube), que aunque no es el objeto específico de esta ponencia, lo sería sin duda de otra, tenemos que considerar que la computación en la nube forma parte protagonista de la revolución tecnológica que nuestra sociedad y sus menores experimentan a su alrededor.

A continuación incidiré en el ámbito de la ciberseguridad como nueva circunstancias, hasta llegar al paso particular de la seguridad en menores, cuya problemática no es sencilla de visualizar en profundidad sin entender el escenario global que como sociedad, incluyendo a esos menores, estamos construyendo y al que nos estamos dirigiendo.

A estas alturas, creo que queda claro que la tecnología no es una moda, no es un capricho, no es un esnobismo. Es más, creo que todo contrario, me atrevería a decir que, a diferencia de la realidad de hace unos diez o quince años, cualquier actitud personal o corporativa que en la realidad se resistiera a la tecnología, paradójicamente tendría más posibilidades de ser calificado de esnob; o sea, realmente forma parte de nuestro día a día.

Llevamos tanto tiempo hablando también en Internet en el capítulo de nuevas tecnologías, que realmente nos preguntamos cuál es el periodo de caducidad ya del adjetivo «nuevas»; esto ya no es nuevo.

Por tanto, no es mi propósito compartir con sus señorías obviedades sobre lo importante que es la red de redes, la importancia de su existencia, de su libertad, de su crecimiento, de las oportunidades que de forma democrática se ofrecen a cualquiera de sus usuarios, el acceso a la información, los servicios, y un largo etcétera de beneficios tan evidentes como importantes, que no en vano en algunos países como Finlandia el acceso a la red se ha llegado a convertir en un derecho constitucional.

Pero es cierto que nuestras expectativas sobre el uso inteligente de la tecnología crecen, y de hecho pedimos con frecuencia que las políticas públicas sean favorables a un proceso de innovación tecnológica que:

uno, mejore la inclusión ciudadana, transparencia y confianza y colaboración en la administración como parte de un gobierno más abierto;

dos, estimule la competitividad, la creación de empleo cualificado y el crecimiento sostenible a través de *clusters* económicos que den fundamento a esas grandes apuestas que como nación decidamos como prioritarias;

tres, incremente los usos y alcances de los servicios de la administración electrónica fortaleciendo adicionalmente requisitos esenciales como aquellos relacionados con la sanidad, la educación o la seguridad pública;

cuatro, mejore la colaboración entre las administraciones públicas redundando en un mejor servicio al ciudadano, desde la interoperabilidad, seguridad y privacidad de datos y sistemas;

y cinco, incluso proteja el medio ambiente mediante un crecimiento sostenible.

Las inversiones tecnológicas resultan imprescindibles para tales cometidos. Y muy especialmente en un momento en el que adicionalmente queremos reequilibrar nuestro modelo productivo a favor de propuestas basadas en la innovación y en la tecnología. En efecto, la tecnología debe ser el vehículo principal que impulse dicho cambio.

Dicho esto, me gustaría compartir el siguiente contenido. Existen determinadas compañías que en un momento dado de la historia tienen la capacidad, por su predominancia, por su prevalencia, de visualizar, de visionar cuál puede ser el futuro más inmediato en base a las experimentaciones propias y ajenas que pueden estar percibiendo a su alrededor. Es el caso, por ejemplo, en los años noventa, de una de esas compañías, que era AT&T. AT&T era una compañía con esa capacidad de visionado. Hicieron público un vídeo —que les voy a poner a continuación, muy cortito, AT&T Vídeo pongo por aquí—, que realmente lo que intentaban hacernos en el año 1993 es aventurar lo que en aquel entonces sería ciencia ficción de lo que iba a ser el mundo de la tecnología tan solo diez años después.

Vamos a verlo, y no sé si compartirán el sentimiento que yo tengo cuando veo esto, que me resulta hasta entrañable, de lo que en aquel entonces era ciencia ficción, en qué estado está ahora cuando lo vemos unos cuantos años después.

[VÍDEO]

Por lo menos resulta un poquito chocante lo que en aquel entonces... y cómo somos capaces de ir incorporando tecnologías sin apenas darnos cuenta, y visiones futuristas como esa, ahora resultan hasta entrañables en ese sentido.

Voy a poner un minuto de... en este momento vamos a asomarnos, es decir, una de las compañías, de las muchas compañías, no es la única, pero de las compañías que tienen ahora mismo esa capacidad de poder visionar qué puede ser ese mismo futuro dentro de los próximos diez años, pues es Microsoft. Hay otras, pero una de ellas es Microsoft. Y no solo en base a la tecnología que desarrolle Microsoft, sino a lo que Microsoft ve que se está haciendo en universidades, que están haciendo nuestros competidores; cuál puede ser el mundo de la tecnología y el mundo de la sociedad dentro de diez años. Es como que abramos una

ventana al futuro, una ventana al futuro que a lo mejor dentro de cinco años visionamos este vídeo y nos parece igual de entrañable que nos ha parecido el de AT&T. Con lo cual, creo que es interesante simplemente para ver cuál es el mundo al que vamos y los riesgos que realmente podemos estar experimentando también.

[VÍDEO]

Dispositivos inteligentes, hasta el cristal del taxi es un dispositivo inteligente que me está dando información de contexto. No se visualiza, pero aquí hay una computación en la nube brutal; cualquier dispositivo, una mesa de cristal, está leyendo datos de otro sitio; es decir, cuando se habla de *cloud computing*, es el futuro, y no se trata solo de acceder a cuatro servidores en la red, es que realmente estamos hablando de la computación que es ubicua, realmente en cualquier sitio eres susceptible de acceder, eres tú además el dueño de esa computación que se produce a tu alrededor. En tu contexto. El vídeo dura seis minutos, lo tienen en la presentación. No es mi intención... Quiero llevarles cuando antes a la temática que nos ocupa, pero sí me parecía imprescindible saber el porqué de las cosas que ocurren ahora en cuanto a una tecnificación absoluta, porque es que esto es lo que estamos visionando, estamos visualizando cómo va a ser nuestra sociedad dentro de no demasiados años.

Si les parece, lo voy a dejar aquí. Pero espero haber despertado su curiosidad para que puedan verlo completo, porque es un ejercicio que yo creo interesante.

Bien, esa es la realidad —lo que les comentaba— que debemos visualizar, esa ventana por la que nos hemos asomado nos muestra un futuro muy inmediato, absolutamente basado en tecnología, en tecnología implícita o embebida en la situación, pero que cimentará la forma de vivir en los próximos diez años. Y debemos preparar a nuestra sociedad, y en especial a nuestros hoy menores, para que no solo saquen partido de esa revolución, sino para que además la entiendan y la lideren.

Ojalá la regulación necesaria en todos los aspectos avance a la velocidad que la innovación exige y consigamos disminuir ese permanente *gap* que observamos en diferentes ámbitos, y que en ocasiones resulta ser un terreno abonado para actuaciones improvisadas o inseguras.

Son cinco las tendencias tecnológicas que definirán nuestra sociedad en los próximos años, y que tienen que ver:

uno, con *social media*;

dos, interfaces naturales de interacción con la tecnología (ahí no aparecido ni un solo PC, es una forma nueva de interaccionar con la tecnología);

tres, *big data*, acceso masivo a información, datos, sacar conclusiones de parámetros realmente no relacionados, desestructurados, esa es la palabra que más recoge el fenómeno del *big data*;

cuatro, *cloud computing*, lo hemos visto en cada paso;

cinco, movilidad.

Entonces, de los cinco, cuatro confluyen directamente en la problemática que esta comisión examina. De ahí incidir en lo realmente importante y acertado, que de verdad considero, de la constitución de la comisión, y además voy a ir luego a hablar al final más en detalle de este tema.

Llegado a este punto, y si ya intuimos el mundo al que nos dirigimos, y es muy probable que en nuestros propios domicilios familiares (hijos, hermanos, nietos, sobrinos) podamos chequear por nosotros mismos, sin necesidad de recurrir a eruditos estudios, que algo nuevo está pasando cuando menores desde los 9 o 10 años comienzan a manifestar su interés por el acceso a Internet desde dispositivos móviles, traspasando una barrera que es la que más les define. Mientras que generaciones anteriores hacen un uso intensivo de Internet pero como opción de *switch on*, *switch off*, es decir, lo utilizamos para algo concreto y específico, nuestros menores lo manejas desde un concepto diferente, desde la perspectiva del *always on*, viven o pretenden vivir en Internet. Por pura estadística son, en consecuencia, aquellos colectivos que más tiempo de exposición puede tener, tanto a lo bueno como a lo malo de la red.

Los adolescentes a partir de 14 años, definen con una palabra contundente y cargada de emotividad su sentimiento en el caso de haberse visto privados de su *smartphone* durante un periodo prolongado de tiempo, semanas o meses. Y esa palabra es «aislamiento». No tienen ni que pensarlo un segundo: aislamiento, es el sentimiento que tienen cuando se sienten privados. Si bien las relaciones de verdad, obviamente, se producen en el mundo físico, el llamado mundo virtual les sirve de medio

facilitador o mecanismo para favorecer la comunicación en el mundo real, no son mundos diferentes.

La ciberseguridad se ha convertido, en consecuencia, en un elemento de vital importancia, en la medida en que aumenta el uso que hacemos de Internet, y especialmente en lo que respecta a los usuarios más desprotegidos por falta de conocimientos, experiencia, derivados, lógicamente, de su corta edad, como es el caso de los menores.

Algunos han llegado incluso a establecer la relación entre la famosa jerarquía de necesidades de Marlow y los diferentes estados de ciberseguridad de una persona, obviamente en el primer mundo. Es decir, solo puedo llegar a obtener un beneficio productivo de la tecnología cuando tengo garantizadas una serie de necesidades previas, entre las que está la seguridad. Es una aproximación, como poco, curiosa, y que pongo igualmente a disposición de sus señorías si tuvieran interés en examinar ese documento; es decir, un *matching* entre toda la teoría de Marlow y la ciberseguridad. Resulta sorprendente, pero tampoco era cuestión de contarlo aquí en detalle.

Y la ciberseguridad es importante, no solo por el uso que de la red hacemos las personas y la criticidad de las interacciones y transacciones que a través de Internet se realizan; también aumenta su protagonismo en la medida en que cada vez más dispositivos no humanos se conectan a Internet. Hablo del Internet de las cosas, de las ciudades inteligentes, de las redes inteligentes, de los sensores en entornos de *smartcities*, hasta el punto de que existen ya más dispositivos inteligentes conectados a Internet que personas, y en muchos casos manejando infraestructuras críticas.

Las enormes ventajas para la vida de los ciudadanos derivadas de vivir en un entorno de los llamados inteligentes, presentes en la evolución de nuestras ciudades (los llamados CityNext) presentan igualmente riesgos, y tenemos una enorme literatura de casos reales: algunos conocerán lo que ha ocurrido en los canales de Ámsterdam hace tres o cuatro meses, Ámsterdam es una ciudad construida por debajo del nivel del mar, la criticidad del manejo correcto de los canales es que es vital para la ciudad. Bueno, pues verse sometido realmente a la incidencia de *hackers* que realmente hicieron... es como si aquí se hubiera hackeado la fábrica de la moneda y los certificados que emite, vulnerando toda la confianza establecida en los mecanismos de seguridad y control de elementos físicos; eso ocurrió en la ciudad de Ámsterdam.

Los enriquecedores de uranio de Irán, esos ataques que se hicieron vía ciberseguridad, vía ataque cibernético, para acelerar y que no pudieran producir como era deseado por ellos. Posibilidades: alterar las mezclas en potabilizadoras de agua, que puedan realmente afectar al consumo de una población.

Había traído aquí un ejemplo un poco también muy particular, sobre el manejo de infraestructuras críticas a través de Internet

[VÍDEO]

Está en un atasco; ha conectado con el sistema de control de señales de tráfico en tiempo real, con mensajes en las autopistas.

Él se lo está pasando muy bien, ¿no? Pero, obviamente, sí que la vulnerabilidad de nuestros sistemas puede ser preocupante.

Al final esto no ha tenido demasiada consecuencia, pero muchas infraestructuras críticas pueden tener un grado de vulnerabilidad similar, por eso es tan importante, efectivamente, la creación dentro del Ministerio del Interior de un CNPIC que trabaje en este ámbito.

Es decir, las cosas en materia de ciberseguridad han cambiado por cuatro o cinco factores fundamentalmente:

uno, los ataques que se reciben permanentemente que se detectan proviene de cualquier sitio, no hay que buscar lejanos lugares de Oriente,... no, no, miremos con más atención al vecino, que igual nos podríamos llevar sorpresas; pero es que además,

dos, se dirigen a cualquier objetivo, no hace falta ser un banco para ser objeto de un ataque. Son muchos los ataques dirigidos, por ejemplo, a robar la intimidad de una persona, de un menor, para posterior chantaje; o ataques dirigidos a capturar la propiedad intelectual de una industria, que sufre un ataque, que,

tres, es dirigido solo a ella, para conseguir una información determinada y no otra; son lo que se llaman los ataques persistentes avanzados, y realmente preocupan mucho a todas las fuerzas de seguridad;

cuatro, ya no se trata de *script kids*, ya no se trata de chavales detrás de un programita haciendo cualquier acción escondida detrás de una dirección IP; la ingeniería inversa sobre estos ataques demuestra la existencia

de auténticos equipos profesionales de desarrollo, lo que indica la profesionalización y negocio detrás de estas actividades;

cinco, la tecnología es vulnerable, *full stop*; no existe la invulnerabilidad cien por cien, por eso es muy importante que cuando tomemos decisiones en materia tecnológica, la seguridad sea considerada en su aspecto más amplio y nos hagamos preguntas del estilo de cuáles son los criterios de desarrollo seguro del fabricante, cómo de ágiles son sus mecanismos de respuesta a incidentes de seguridad, ¿mantienen espacios de colaboración con el sector, clientes y usuarios en materia de seguridad?, ¿mantienen una voluntad clara de ayudarme a cumplir con mis obligaciones legales en ámbitos como la seguridad y la privacidad?, etc.

Igualmente, son tres las acciones que en ciberseguridad se plantean, que son prevención, detección y respuesta. Cada una de ellas necesita de sus acciones, herramientas, inversiones, y no siempre de la mano de la tecnología.

Bien, Microsoft, y en particular Microsoft Ibérica en este caso, somos una de las compañías tradicionalmente más comprometidas con la seguridad y la protección de los menores, y que posicionaré con una sola frase: somos la única compañía tecnológica en España que luce con tremendo orgullo el haber sido condecorada por tres fuerzas policiales, como son los Mossos d'Esquadra, la Policía Nacional y la Guardia Civil, con medallas al mérito policial con distintivo blanco, y créanme sus señorías que tales distinciones son resultado de muchos años de trabajo conjunto, eficaz, de relación de socios, de alta sensibilidad mutua ante la persecución de delitos en la red. He puesto aquí algunas...

Mantenemos igualmente acuerdos de seguridad con muchos de los organismos de nuestras administraciones relacionados con la ciberseguridad, como INTECO, con el que tenemos firmados dos acuerdos, uno de los cuales es pionero en este momento a nivel internacional (es el que aparece aquí firmado por el secretario de Estado Víctor Calvo-Sotelo, este junio de 2013); con el Centro Criptológico Nacional del CNI, con quien compartimos los bienes más preciados de Microsoft como es el código fuente de los productos más importantes que desarrollamos (es más, creo que en esta imagen aparecen los últimos tres secretarios de Estado del CNI,...); CESICAT, hemos trabajado y publicado manuales conjuntamente con la Agencia Española de Protección de Datos, hasta cien empleados voluntarios de Microsoft Ibérica han colaborado codo

con codo con Policía Nacional para recorrernos más de cien colegios por toda España dando charlas a padres y alumnos; hemos colaborado con ONG como Protégeles formando a monitores y grupos *scouts* de toda España, desarrollando materiales formativos sobre seguridad infantil, y un largo etcétera.

Pero también somos conscientes de que este es un proceso que no puede detenerse, ni hay demasiado tiempo para la autosatisfacción; los riesgos evolucionan, y nuestra respuesta ha de hacerlo en la misma medida.

Visualizamos los riesgos como el de las cuatro C: riesgo en el contenido, riesgo inherente al contacto, riesgo en la conducta, riesgo en el comercio. Nuestra aproximación a esos riesgos se hace desde una triple perspectiva, tres pilares a cuál más importante y que con mayor o menor pericia hay que contemplar de forma global: educación y guías, herramientas tecnológicas, y *partnership* o colaboración.

Con respecto al primero, con respecto a la educación y guías, tenemos que tener en cuenta que el conocimiento es cambiante. En Internet es simplemente una realidad que no puede ignorarse, lo que hoy es útil, en tres meses deja de tener sentido por la aparición de nuevas herramientas, moda, aplicación, etc. Y los destinatarios de la información no solo son los menores, lo son los padres y educadores, que en muchas ocasiones están a años luz del conocimiento de sus hijos y alumnos respectivamente.

Pero existe una constante que debemos potenciar, y no es otra que la comunicación, la conversación con los menores. Es fundamental que les ayudemos a identificar aquellos parámetros sospechosos o aquellas acciones frente a las cuales siempre han de ponerse alerta. Debemos entender que, independientemente de lo que hagamos como padres, como educadores, como sociedad, llegará el momento en el que el menor se enfrente a una decisión él solo. Igual que ocurre en otros muchos ámbitos de la vida, como el consumo de drogas, alcohol, etc. Y llegado ese momento, que llegará más pronto que tarde, será muy importante haber mantenido conversaciones abiertas y transparentes, no culpabilizadoras con el menor, y sobre todo haber conseguido crear un lazo de confianza tal que el menor no tenga reparos en consultarnos o pedirnos consejo ante una situación como esa. No es en absoluto sencillo, pero es probablemente más eficaz que otras alternativas más obstaculizadoras como la restricción de acceso. Los menores encontrarán la forma de saltarse,

en un alto porcentaje, cualquier tipo de barrera, mediante dispositivos prestados, WiFi públicas, amigos, etc.

Herramientas tecnológicas: existen muchas tecnologías de control parental. Desde Microsoft proveemos herramientas de este estilo, claro que sí. Pueden llegar a ser muy útiles. También es cierto que bajo la categoría de «menor» caben actitudes, comportamientos y niveles de madurez que nada tienen que ver unos con otros: para menores hasta 10, 12 años, puede resultar útil el uso de herramientas de control parental que filtren contenidos o información; en adelante, resulta bastante más difícil implementar herramientas de esas características sin abrir debates en la familia sobre la intimidad del menor o la confianza depositada en él.

A nivel de proveedor, Microsoft ha desarrollado tecnología denominada PhotoDNA, por ejemplo, tremendamente eficaz en la persecución de delitos de pornografía infantil, y donada a todo organismo, empresa, fuerza de seguridad que quiera utilizarla. Sin ir más lejos, ahora mismo Facebook o Google hacen uso de esa tecnología en sus sistemas centrales. Esta tecnología se ha donado también a una empresa para que lo integre dentro de sus soluciones de ámbito más amplio en materia de soporte a las fuerzas de seguridad, pero con la condición de que cuando la fuerza de seguridad vaya a utilizar esa tecnología PhotoDNA, se le dé la licencia de forma gratuita con respecto a esa funcionalidad concreta.

Y *partnership* y colaboración, como tercer pilar. Probablemente sea uno de los puntos más importantes: colaboración en todos los ámbitos, educativos, judiciales, políticos, policiales, administrativos, tecnológicos... Los reconocimientos recibidos por Microsoft de las medallas al mérito policial con distintivo blanco, que fueron otorgadas en 2010 y 2011 respectivamente, tienen que ver especialmente con este pilar. Microsoft da respuesta, al mes, a del orden de 200 peticiones judiciales de información, al mes, en España, a Ertzaina, Mossos d'Esquadra, Guardia Civil, Policía Nacional fundamentalmente, y resto de policías, pero fundamentalmente con las que más trabajamos son estas cuatros. Es nuestra obligación, obviamente, pero a nadie se le premia por cumplir con su obligación. La implicación de Microsoft en la persecución de este tipo de delitos es lo suficientemente ágil y responsable como para que las investigaciones de nuestras fuerzas de seguridad aumenten sus posibilidades de llegar a buen puerto. Les invitaré además a sus señorías que lo

contrastaran por ustedes mismos, al contacto con diferentes fuerzas de policía, cuando hablan de proveedores internacionales y les pregunten, por ejemplo, a quién les gustaría que se pareciera el comportamiento de multinacionales al respecto, en lo que respecta al trabajo de persecución de delitos,. Apostaría que les dirían directamente que Microsoft es el ejemplo a seguir, Microsoft Ibérica, que aquí también lo hemos estado persiguiendo de forma especial, incluso enseñando al resto de nuestra corporación cómo se pueden hacer las cosas en esta materia.

Eso sí, hay que invertir, obviamente; tenemos personas dedicadas 24x7, que solo se dedican a esto, nada más; y es una inversión que hace Microsoft, pero que necesitamos sentirnos, obviamente, a gusto, reconocidos e integrados en la sociedad en la cual estamos viviendo, que es la de aquí y no es otra.

A nivel internacional, algunas actuaciones de Microsoft son especialmente relevantes, como colaboración con organismos como el ICMEC, el International Center for Missing and Exploited Children

Y llegados a este punto, y dado el carácter multinacional de la compañía a la que pertenezco, quería compartir con sus señorías alguna información relativa a estado del arte de esta problemática en relación con otros países de nuestro entorno. Hemos elaborado un estudio reciente al respecto de diversas problemáticas relacionadas con la protección de menores, y en concreto en materia tan delicada como el ciberacoso o *cyberbullying*, es decir el abuso entre iguales.

El análisis se ha hecho en 25 países (Australia, Argentina, Brasil, Canadá, China, República Checa, Egipto, Francia, Alemania, India, Italia, Japón, Malasia, Marruecos, Noruega, Pakistán, Polonia, Qatar, Rusia, Singapur, España, Turquía, Reino Unido y Estados Unidos) entre niños y niñas entre 8 y 17 años.

Algunos datos interesantes obtenidos: pues el 37% reportan haber sufrido algún tipo de acoso *online*, como media, el 37%; adelanto que esa es la media, además, de España, en España estamos justo con ese valor, justo en la media. El 24% reconoce haber acosado a alguien; estar más de 10 horas por semana *online* aumenta las probabilidades de sufrir acoso, que pasan de un 29% a un 46%; el 86% reconoce haber sido acosado *online* u *offline*; el acoso *offline* se da el doble que el *online*, un 73% versus un 37%; el 42% dice no saber nada sobre *bullying*; el *bullying online* es

más frecuente entre los 13 y los 17 años, y sin embargo entre los 8 y los 12 sufren más el *bullying offline*.

Algunos datos geográficos interesantes son: España se mantiene en valores intermedios en el estudio de esos 25 países; solo destaca especialmente por ser el segundo país cuyos menores expresan mayor preocupación sobre el *bullying online* (a continuación Brasil). Los países con mayores índices de *bullying online*, de forma muy destacada, el primero China, con un 70%, seguido de India, Argentina, Rusia, Turquía. España se encuentra justo en la media, con el 37%, y luego los países con menor índice de *bullying* son Japón, Francia, Italia (con un 28%), Estados Unidos (con un 29%), Noruega, Pakistán, Egipto, Qatar, Malasia... Es *bullying online*. Muchos de estos países, luego resulta que son lo *top* en los *bullying offline*, por ejemplo Estados Unidos, es uno de los países con mayor incidencia. El país donde más *bullying offline* existe es Marruecos, Canadá, Reino Unido, Estados Unidos, Australia.

El informe es muchísimo más amplio, y lo pongo en su totalidad a disposición de sus señorías, si quieren examinarlo. De hecho, lo tengo puesto como anexo en esta *slide*, con lo cual ya lo tienen.

En resumen, y para concluir esta exposición, queda mucho por hacer en el ámbito de la ciberseguridad en general, y en el de la protección de menores en la red en particular. Identificar las palancas de acción es un excelente primer paso, y sinceramente —y además subrayo la palabra «sinceramente», porque he vivido situaciones en ese sentido—, creo que sus señorías en el transcurso de esta ponencia, comprendiendo a los comparecientes que han ido compartiendo su conocimiento y preocupaciones ante ustedes, les pone en una situación privilegiada, y créanme que única, para identificar y facilitar la acción de esas palancas. No resulta muy habitual, aunque puedan pensar lo contrario, reunir tanto conocimiento experto como el que ustedes han conseguido en el desarrollo de esta ponencia, no es habitual; ni piensen, en mi opinión, que existe un diálogo permanente y fácil entre muchos de los comparecientes que han pasado durante todo el año pasado y este en esta ponencia, no es habitual.

Es por ello por lo que la foto global que ustedes manejan puede ser única. Es probable que igualmente hayan observado el enorme interés que los comparecientes habrán puesto en compartir sus preocupaciones, exponer sugerencias desde la realidad de los hechos; y es que al final del día, aunque vengamos aquí con la etiqueta que nos toca, en mi caso la

de Microsoft, todos tenemos otra etiqueta personal que nos motiva especialmente, y es la de miembros de una sociedad, ya sea como padres de familia (en mi caso), educadores, etc., que a su conocimiento profesional suman el interés adicional de proteger hijos, alumnos, etc., inmersos en un mundo digital tan apasionante como complejo.

Nada más; muchas gracias de nuevo por la atención, y quedo a disposición para cualquier pregunta. Muchas gracias.

COMPARECENCIA DEL DIRECTOR GENERAL DE OPERACIONES DE TUENTI, D. SEBASTIÁN MURIEL HERRERO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 24 DE FEBRERO DE 2014.

Tuenti. Plataforma de comunicación social y móvil española

Tuenti es una compañía tecnológica 100% española, con cerca de 200 empleados de alta cualificación, con una media de edad 28 años y oficinas en Madrid y Barcelona. Somos a día de hoy una de las principales empresas tecnológicas en Europa, apostando fuertemente por la innovación y el desarrollo de productos de alto valor añadido con el móvil siempre en el centro de nuestra estrategia.

Somos una plataforma social y móvil para comunicarse de manera muy simple y segura con las personas que más importan, con los amigos de verdad, y que en la actualidad cuenta con 16 millones de usuarios registrados de los cuales el 75% son mayores de edad.

Tuenti. Compromiso con la protección de los menores en Internet

Tuenti está comprometida con la protección de los menores en su plataforma y nuestra motivación principal es ofrecer una experiencia segura a todos nuestros usuarios. Nuestros objetivos principales son 3:

1. **Dotar** a los menores, padres y educadores de las herramientas y mecanismos adecuados para que puedan reportar cualquier contenido inapropiado, perfil sospechoso o falso, suplantación de identidad o cualquier otro material o conducta ilegal.
2. **Proteger** a los menores a través de colaboraciones con los cuerpos y fuerzas de seguridad y organizaciones de protección al menor.
3. **Informar y educar** a los menores, padres y educadores de todas las herramientas que ponemos a su disposición para mantener su seguridad y proteger su privacidad en Tuenti.

Tuenti. Estrategia de privacidad y seguridad

Tuenti ha diseñado su propia estrategia de privacidad y seguridad a través de una serie de medidas únicas en el mercado, entre las que cabe señalar:

- No indexación de los datos e información personal de los usuarios en buscadores. Es decir, ni siquiera Google entra en lo que se comparte en Tuenti. Lo que pasa en Tuenti se queda en Tuenti.
- Verificación de los usuarios por email y /o teléfono.
- Sólo se permiten identidades reales.
- Encriptación y cifrado de las conversaciones de chat (protocolo SSL).
- Modelo único de privacidad en redes sociales: Distinción entre amigos y contactos. El usuario puede optar por agregar a un usuario como:
  - Contacto: Sólo para chatear
  - Amigo: Chatear y compartir su información, contenidos, tablón, etc.
- Máximo nivel de privacidad por defecto para todos los usuarios, con independencia de su edad y sin permitir el acceso a su información a terceros.
- Nueva Política de Privacidad: Más clara, transparente, sencilla y comprensible.
- Nuevo Panel de Privacidad más intuitivo, sencillo y fácil de manejar, con el que el usuario puede configurar el grado de privacidad con el que quiere relacionarse en la red social.
- Nuevo Centro de Ayuda y Seguridad tuenti.com/privacidad, con nuevos recursos de ayuda, informativos y formativos, incluyendo espacios audiovisuales y recomendaciones de uso responsable para padres, educadores y usuarios.

Tuenti. Pilares fundamentales de nuestra política de privacidad y seguridad: transparencia, información, control y seguridad.

Frente al contexto general de internet y de otras redes sociales, en Tuenti tenemos el marco de actuación más claro y comprometido a este respecto, hasta el punto de poder afirmar que Tuenti es una de las redes sociales más seguras (no sólo en España, sino en el mundo entero) y la que cuenta con la Política de Privacidad y Seguridad más estricta y rigu-

rosa basada en cuatro pilares fundamentales: transparencia, información, control y seguridad.

Tuenti. Conclusiones generales.

- Internet es, cada vez, más social, más móvil y más global.
- El fenómeno de la movilidad y los smartphones han cambiado el concepto de redes sociales tal y como las conocíamos hasta ahora.
- Cualquier aplicación que permita la comunicación entre los usuarios y el intercambio de información y contenidos entre los mismos puede ya ser considerada una red social (Whatsapp, Line, We Chat, Geek, Tellit, etc.). Y esto es importante de cara a cómo la regulación y la autorregulación van a abordar este fenómeno. Es decir, tener claro el objeto de la misma, quienes son sus destinatarios y los nuevos actores de este nuevo ecosistema de las aplicaciones móviles.
- Según datos de la Comisión Europea, cada día se lanzan al mercado mundial 1.600 nuevas aplicaciones móviles y de media cada usuario se descarga 37 en su smartphone, lo que da clara cuenta de la dimensión de este fenómeno global que rompe con las concepciones territoriales tradicionales. Así, una empresa japonesa puede lanzar una aplicación a nivel global, y en pocos días ser descargada en España por 20 millones de usuarios.
- Los usuarios, nativos digitales, ya están en Internet. Cada vez tiene menos sentido poner el foco en el registro y la verificación de su edad, especialmente en entornos de movilidad, sino en la propia utilización segura y responsable de las TIC por los menores.
- Se debería incorporar las TIC en general y las redes sociales en particular como asignatura obligatoria desde los primeros niveles de la enseñanza.
- Todo va muy rápido en Internet, y la regulación siempre va un paso por detrás. Por eso tiene sentido fomentar y promover la autorregulación, e incluso plantear esquemas extrajudiciales de resolución de controversias online en temas de menores e Internet.

- Si hablamos de regulación, es necesario que todas las empresas, nacionales e internacionales, que ofrecen sus servicios a ciudadanos españoles tengan las mismas reglas de juego, para no perjudicar a los actores nacionales que competimos en un entorno global y que hemos demostrado nuestro compromiso real con la privacidad y la seguridad.
- En un escenario dominado por la tecnología, el objetivo es desarrollar un marco jurídico:
  - Que sea adecuado para los entornos globales en los que se mueven empresas de distintos países y jurisdicciones.
  - Que favorezca la actual revolución digital que estamos viviendo y no ponga barreras innecesarias a la innovación.
  - Que permita el desarrollo de negocios digitales y sea un factor de estímulo de la economía digital y la creación de empleo.
  - Que sea sencillo, flexible y abierto, genere confianza, seguridad y certidumbre a ciudadanos y empresas, sin poner excesivas cargas administrativas a éstas y favoreciendo la inversión, protegiendo la privacidad y la seguridad de los ciudadanos en internet.
- Cuestiones como la verificación de la edad de los menores pueden tener un impacto no sólo ya en las empresas que tenemos que cumplir con esta obligación sino en el uso los menores hagan de los servicios de Internet.

  A pesar de nuestro protocolo de verificación y borrado de perfiles de menores de 14 años (único entre las redes sociales que operan en España), que incluso incorpora el DNIe como mecanismo de verificación de la identidad, la realidad de las restricciones de edad a día de hoy es que están provocando situaciones contrarias a las que preveían evitar:
  - Las denuncias de usuarios por motivos de edad (no tener la edad mínima de 14) es ya la primera causa de acoso entre usuarios, generando situaciones de vacío y exclusión social.
  - Nos encontramos con quejas de padres por expulsar a sus hijos de Tuenti.

– Nuestro equipo de soporte explica a los padres que la Ley les permite prestar su consentimiento para que sus hijos menores de 14 estén en Tuenti, pero también son muchos los padres que se oponen a facilitar su DNI y Libro de Familia para autorizar su registro, cuando esto no es necesario en ninguna otra red social de Internet.

Tuenti. Propuestas concretas.

– *Exigir el cumplimiento de la legalidad vigente a las empresas extranjeras* que dirigen sus servicios al territorio nacional y *prohibir que se publiciten en los medios y soportes españoles (especialmente TV)* mientras no cumplan los requisitos de privacidad y seguridad de conformidad con la normativa española y europea.

– *Eliminar la obligación de la verificación de la edad* de los usuarios en el momento de registro en los servicios de redes sociales.

– *Incorporar como asignatura obligatoria* desde los primeros niveles de la enseñanza las *Tecnologías de la Información y la Comunicación* y su uso seguro y responsable.

– Fomentar la cultura de la privacidad y la seguridad en Internet mediante *iniciativas y campañas de divulgación y concienciación sociales*.

COMPARECENCIA DEL DIRECTOR GENERAL DE LA FEDERACIÓN PARA LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL (FAP), D. JOSÉ MANUEL TOURNÉ ALEGRE, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 10 DE MARZO DE 2014.

El señor **DIRECTOR GENERAL DE LA FEDERACIÓN PARA LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL (FAP)** (D. José Manuel Tourné Alegre): Muchas gracias. Es un honor comparecer en una de las cámaras legislativas de nuestro Estado y poder informar desde la humilde experiencia de quien les habla acerca de esto de Internet, sus peligros para los menores, y conectarlo con el sector del que yo vengo, que es el de la protección de la propiedad intelectual; es la federación a la que sirvo desde hace treinta años, y por otro lado presido igualmente la Unión Videográfica Española, que es la asociación que integra a los distribuidores de vídeo y de derechos digitales para Internet.

Y es que buscar contenidos, especialmente audiovisuales en Internet, sí trae peligros para los menores de edad. Pero antes de empezar por ahí, a mí me gustaría dejar claro que Internet es visto por el sector como una enorme oportunidad. Internet es, digamos, lo que más podría desear un realizador de contenidos, puesto que es una red que te permite transmitir con enorme agilidad y con una reducción de costes importante tus contenidos a un universo amplísimo, no solo nacional, sino que va incluso mucho más allá. Poder estrenar una película directamente en Internet y que accedan a ella personas que de otra manera no irían a una sala de cine o que no la alquilarían en un videoclub, o no les gusta esperar a que la emitan en televisión, es una magnífica oportunidad.

Sin embargo, como verán, no son quienes hacen contenidos quienes se están beneficiando de esa oportunidad. Y las cosas han llegado a un límite en el que va a costar sacar beneficio y ventaja de esas oportunidades. Yo siempre creo que estamos a tiempo, pero mucho depende de cómo evolucionen las leyes que se están precisamente tramitando en el Congreso en estos días, y que pasarán por esta casa en breve. Dicho eso, para el sector y para los que realizan contenidos es una gran oportunidad.

¿Qué es Internet para un pirata? Y esto es lo que yo he tratado de traerles aquí en esta presentación que les muestro a continuación. Pues

ese señor que está ahí en medio con el cuchillo entre los dientes es el que se aprovecha de Internet. ¿Y por qué se aprovecha? Bueno, pues Internet, para él, como para mucha gente, tiene cosas muy interesantes. Esto son diálogos reales, recogidos de una página, de un foro de películas: «cuando saldrá al cine se ve bien»... Ya no es que la construcción gramatical sea muy acertada, es que reconocen que las películas en Internet tienen algunos fallos. A mí me llama la atención el «ebolucionando» ese, y claro, no es por acortar las frases, es que poner una j o una g, o «save» con v en vez de con b, en fin, todo esto es habitual, esta es la cultura de los foros de Internet. Está lleno, no hay más que entrar en cualquier página de descargas ilícitas y verán ustedes que esto es real.

Pero en Internet, además, para el pirata hay muchas cosas. Y además, mira tú por dónde, son gratis: tenemos películas y series de televisión, y además nadie nos dice si son para mayores de 18, de 15, de 14; las calificaciones de las películas, aquí no parecen obligatorias. Saben ustedes que para editar una película y sacarla hay que solicitar al Ministerio de Educación, Cultura y Deporte un certificado de calificación; se califica la película y hay una recomendación que orienta a los padres, que por lo menos quieren o queremos recurrir a esa información, sobre si es adecuado o no el contenido para nuestros hijos.

Lo mismo respecto a los videojuegos, saben ustedes, el código PEGI que todos los videojuegos llevan indicando cuál es el tipo de contenido; pues de esto, en esas páginas no aparece ningún tipo de información.

Pero tenemos aquí a Pablito; Pablito es un chaval, es un nativo digital, como se dice hoy en día. Pablito maneja las nuevas tecnologías con enorme habilidad y no sabe que en una revista hay que pasar páginas para verlas, sino que directamente hace así, que es como demuestra su habilidad. Y le gusta Bob Esponja. Y decide: para ver a Bob Esponja, lo único que tengo que hacer es ponerlo en Internet Y entonces, se va al buscador, Google es el más habitual, y teclea: «series Bob Esponja». La tercera opción que le aparece, como ven ustedes —esto es real, son capturas de la pantalla real—, la tercera opción entre 5 millones de opciones sobre Bob Esponja que hay en Google es «series Pepito». Y dice: ¡Ah, pues mira qué bien! Yo voy a entrar aquí, en «series Pepito». Y entonces, Pablito se va a «series Pepito» y efectivamente, encuentra la temporada uno de Bob Esponja, la dos, la tres... Y aquí, en esta página de repente ve, oye, ¿qué pone aquí de adultos, +18? Esto está en esta página como

está en otras muchas; por si quieren, hablamos de series yonquis, que recientemente ha sido noticia en los medios. Esas pestañas no se las he querido poner más gráficamente, imagino que con lo que ven ya intuyen suficientemente cuál es el contenido de esas pestañas.

Pero no es solo eso, es que mientras se está entrando le van a saltar *pop-ups*, o sea, *banners*, publicidad de apuestas en red y de multitud de situaciones. Algunas, incluso para estafarle. Esto es: empezará Bob Esponja, empezará cualquier serie, y si quieres continuar viendo la película, aparece una ventana que te obliga a incluir tu número de teléfono. Esto es real, esto es un pantallazo concreto de esta página. Colocas ese número de teléfono, y no solo no ves la película, sino que además lo que te empieza es a caer un montón de *spam* en tu número de teléfono móvil y de publicidad y de información que no es la más adecuada, desde luego, para un niño de 8 años, pero probablemente tampoco deseada ni por su padre ni por su madre: juego, apuestas en red...

Y ¿qué más tiene Internet para nuestro amigo el pirata? Pues es un sitio donde puedo hablar con mis amigos. Lo que pasa es que a mí, les aseguro que me sorprende un poco el nivel de diálogos que hay en Internet: «aprende a escribir, analfabeto, que sois más catetos y más brutos, puto retrasado»...»...estoy hablando con el dueño del circo, no con el mono, así que haz el favor de no meterte payaso. Lo que sobran en este mundo son los putos fachas de mierda...» Lo pueden ustedes leer; no es, desde mi punto de vista, lo más constructivo para nuestra sociedad. Quizá tenga algo que ver porque lo que manejan y lo que ven en esas páginas es similar a estas imágenes, son de una película de las que ofrecen estas páginas.

Así que, ¿qué le pasa a este señor? ¿Que es eso lo que quiere? No, le da igual. Él hace mucho dinero con lo que está viendo cada día. Porque este señor no lo hace gratuitamente. Este señor que vive de su página de Internet y que se encarga de subir, con algún otro tipo de identidad, las películas que graba en una sala de cine con una cámara, saca mucho dinero de esto. Según los informes policiales que obran en autos de algunos de los procedimientos judiciales en marcha contra estas páginas, desde 175.000 euros anuales hasta 410.000 euros anuales: ingreso por publicidad, por facilitar los datos, por vender los datos que van captando, por los clics.

Pero además, es que este mensaje, no se les está advirtiendo —como antes de empezar esta presentación hablaba con alguno de ustedes— no

se les está transmitiendo a los niños cómo evitarlo. Los nativos digitales, que estarán entre los 0 y los 20 años en la actualidad, no han recibido de sus padres un mensaje previniéndoles de qué es Internet o cómo se maneja, probablemente porque incluso sus padres saben menos de Internet que ellos mismos; salvo algunos casos que hemos tenido el privilegio de dedicarnos a esto y profundizar en lo que Internet ofrece, la mayoría de los padres, cuando su hijo está en Facebook cree que está hablando con sus compañeros de colegio y nada más, y no es siempre así, como seguramente han tenido ustedes ocasión de percibir en otras presentaciones que me han precedido y en otras que continuarán.

Yo les he querido conectar esto con el mundo de las descargas de contenidos, del que tanto se habla, las páginas de enlaces y demás.

Este mensaje no se les ha hecho llegar tampoco en el colegio. Es más, a veces lo que se les ha hecho llegar es justo todo lo contrario. La noticia que tienen ustedes ahí en la parte inferior izquierda es real: una profesora de una guardería de niños tenía que salir un momento y les dejó con una película que ella misma había descargado de Internet; resultó que la película era pornográfica, y cuando volvió se encontró con el pastel. Como pueden ver ustedes, he sacado algunas noticias de hace unos años, de 2009, de 2008. ¿Qué es lo que ofrecen? Pues «instálate un ADSL para bajarte lo que quieras», «el 4G, que está por llegar, te permitirá descargar películas de 800 megas». Hay bastante irresponsabilidad en Internet, no es un barrio responsable; no es el barrio de una ciudad en el que la farmacia te ofrece las medicinas adecuadas, el banco no te estafa con *phishing* o el videoclub está lleno de piratería. En Internet, desgraciadamente, hay muchas tiendas como las que digo.

Porque, entre otras cosas, para abrir una tienda en Internet, teóricamente te tienes que identificar (artículo 10 de la Ley de Servicios de la Sociedad de la Información), pero los piratas no lo cumplen. Y si se incumple, no pasa nada. La Secretaría de Estado de Telecomunicaciones tiene no menos de 250 denuncias en su mesa contra páginas que no cumplen ese requisito del artículo 10; solo ha abierto un expediente sancionador, de entre 250. Y tiene obligación de abrirlo, en cada caso que le pasa la Sección Segunda de la Comisión de Propiedad Intelectual. Ha abierto uno de esos; del resto, doscientas y pico denuncias, ni una sola ha iniciado un expediente sancionador. Y es algo tan simple como si mañana un frutero quiere abrir una frutería en una ciudad de este país, pues

llegará, pedirá las autorizaciones pertinentes, y está sometido a cualquier tipo de inspección para garantizar que lo que ofrece al público esté en condiciones.

El sector legítimo intenta por todos los medios posibles adaptarse a estas nuevas tecnologías. Como ya les he dicho, para ellos es una oportunidad, y hay multitud de páginas —las pueden ustedes consultar en esa página que se llama mesientodecine—, que ofrecen contenidos perfectamente legítimos, regulados y que cumplen con las normas que el Estado dicta en cuanto a calificación por edades de las películas, en cuanto a garantizar que el acceso es supervisado por adultos. Entre otras cosas porque son de pago; aunque haya que pagar, a lo mejor un euro, dos euros, tres euros por descargarte una película, pero ya estás pasando por una tarjeta de crédito y un conocimiento de quién está usando eso.

Es lamentable que algunas páginas que fueron pioneras, como Media Express o PixBox de Telefónica, hayan tenido que desaparecer porque la competencia desleal que sufren de las páginas piratas no les ha dejado evolucionar. Y esa es una competencia —como bien decía, hay comportamientos irresponsables— en la que se ha crecido a costa del «descárgate lo que quieras, que son 20 megas» —se acordarán ustedes de ese anuncio— o de permitir que tu publicidad comparta espacio con verdaderas estafas. Ahí tienen ustedes un ejemplo de una página de descarga de películas: *El lobo de Wall Street* es una película de reciente estreno cinematográfico, está disponible sin que el titular lo haya autorizado; pero además, es que esa página ingresa dinero; ingresa dinero de esas marcas que tienen ustedes ahí expuestas (Movistar, Privalia), que comparten espacio con otra oferta, que es justo la que aparece ahí abajo, en la que te están pidiendo tu número de teléfono móvil para estafarte. Yo creo que les debería importar, pero... Y este es otro caso similar: Génesis Seguros con Orange, compartiendo espacio con otro sitio singular.

Para ir terminando, además del daño psicológico, moral o incluso, a veces físico, que pueda causar a los menores de edad el acceso a estas páginas por esos otros contenidos, está también el daño que supone que dos generaciones hayan crecido sin saber que la propiedad intelectual es un bien digno de ser respetado, que la propiedad intelectual genera riqueza y empleo. Y al contrario, lo que se les ha transmitido es «gratis total». Y es gratis total a medias, porque el ordenador, la línea telefónica, todo eso se paga.

¿Y quién paga la factura al final? Eso son los datos del sector cinematográfico. Es verdad que el incremento del precio de la entrada ha hecho que la recaudación mantenga ahí un cierto abombamiento, pero la gráfica que ven ustedes, la línea naranja, es la línea de espectadores, que ha ido cayendo desde el año 2006 hasta el actual de forma continuada. Qué decir del consumo de vídeo: en este país se editaba una película como *Titanic*, que era la más taquillera del momento, y se vendían 3,5 millones de DVD y de VHS. Lo lógico, digamos, adaptado a algo que ha tenido mucho éxito entre el público. Cuando llega «Avatar», del mismo director, y también la más taquillera de su momento, vendió 300.000. Tres millones y medio frente a 300.000; un sector de 430 millones de euros al año, generación de empleo (25.000 puestos de trabajo y demás), a un sector que no ha llegado a los 80 millones en el último año.

¿Y el problema? Pues que hay víctimas, pero parece que estas víctimas son invisibles. O son muy ricos, ¿no?, Maribel Verdú, Sergi López. ¿Qué es esa lista? Pues esa es la lista de los títulos de crédito de una película —he buscado una muy normalita—, *El laberinto del fauno*, que es una película con una participación española en la producción muy importante, se rueda en nuestro país, y ustedes seguro que conocen a los cuatro o cinco primeros nombres que ahí aparecen, incluso a lo mejor hasta al sexto; pero si ya vamos más abajo, ¿quién es Milo Taboada, quién es Pedro Marzo, quién es José Luis Torrijo? Son artistas, protagonistas de la película, no son ningún tipo de millonarios. Pero si seguimos avanzando, pues ese escultor, Nicolás Villar o Luciano Romero, que trabajan en atrezo, son imprescindibles para que la película se haga. Una película es un proyecto a largo plazo, son seis, ocho años hasta que se realiza; es una empresa que va a funcionar durante todo ese tiempo dando empleo (en el caso de esta, 640 personas a lo largo del tiempo); hay contables, hay abogados, hay... Se hace posible, y se tienen que especializar: el carpintero que se trajo Guillermo del Toro para hacer la película se lo trajo de fuera. Y yo no creo que sea porque no haya carpinteros en El Espinar, que es donde se rodó gran parte de ella, que seguro que los hay y muy buenos, pero difícilmente un carpintero español se puede especializar en darle texturas al trabajo que realice si no interviene en más de una película cada dos o tres años. Y esto es una realidad como consecuencia de la piratería.

A mí me parece que el valor de la propiedad intelectual en las generaciones de gente joven es importante, sobre todo porque como no tenemos

otros recursos naturales, ni tampoco en investigación, estamos a la par que otras economías del mundo, pues me parece que es una buena competencia defender la creatividad y el talento del ser humano. Hace unos días se publicaban los datos de patentes del mundo, y resulta que Europa sigue a la cabeza en el registro de patentes, no sé por cuánto tiempo, pero creo que merece la pena protegerlas.

Y con esto acabo mi exposición y estoy a su disposición.

COMPARECENCIA DE LA EXPERTA EN INNOVACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN, DÑA. SALUD MARTÍNEZ MONREAL, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 10 DE MARZO DE 2014.

La señora **EXPERTA EN INNOVACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN** (Dña. Salud Martínez Monreal): Buenas tardes; muchísimas gracias, señor presidente. Antes que nada, quiero agradecer a todos los miembros de la ponencia la oportunidad que me dan para explicar una solución al problema que en esta ponencia y en todo el mundo se viene planteando desde hace años. Es gratificante para mí poder explicar hoy que ya existe una solución real.

Les voy a poner una diapositiva muy concreta que va a ser el pilar —ahí la tienen— de mi ponencia. Imagínense por un momento que cualquier usuario de cualquier parte del mundo, con su terminal móvil, tableta o PC pudiera obtener una información que quedara custodiada, encriptada, que tuvieran acceso cualquier cuartel o comisaría de la policía, y que paralelamente pudiera descargar esa prueba veraz en un juzgado. Ahí tenemos unos eslabones que son fundamentales a día de hoy para el descubrimiento o el esclarecimiento de un hecho delictivo.

Ahora mismo los menores, digamos que son los reyes de los *smartphone*. Básicamente, casi todos los delitos giran en torno a un *smartphone*, a una tableta y a las redes sociales. No quiero entrar ni voy a entrar en ese tema porque ya mis predecesores anteriores les han puesto en tela de juicio, con millones de estadísticas del aumento que hay de delitos cada año.

Yo vengo a presentarles esta solución, que además contiene un algoritmo innovador, con una patente internacional, que certifica el contenido de la información que se obtiene; el contenido, que es el punto clave, el punto principal, que es lo que a un policía le interesa, a un juzgado le interesa a la hora de detectar un delito y comprobar, por supuesto, si es veraz o no lo es.

Mis predecesores en las anteriores ponencias ya les han indicado suficientes estadísticas en cuanto al incremento de delitos en la red y sus diversas tipologías. Es por ello que yo les voy a hablar de una solución

con óptimas estadísticas que nos reporta la innovadora tecnología que hoy les presento. El Senado tiene la capacidad de contribuir a hacer una sociedad mejor, y es por ello que les voy a hablar de esta solución; es una solución global, una plataforma compuesta de un algoritmo, tecnología y *software* que certifica el contenido de la información que se obtiene. Porque no es manipulable por ningún usuario malintencionado. Esta información la podemos extraer a través de una web, de una fotografía, una vídeo, un audio, y nos aporta pruebas con el contenido visual y técnico. Esta es una parte muy importante y relevante, porque obtenemos pruebas técnicas (en cuanto a IP, etc., que ahora comentaremos) en una web, y la prueba visual, in situ y simultánea de lo que está ocurriendo en ese momento.

Esta tecnología, confeccionada en una plataforma transaccional que acoge la colaboración entre países para la agilización de pruebas veraces para la investigación policial y jurídica en la erradicación de todos los delitos en cualquiera de sus formas. Este *software* específico, creado con esta innovadora tecnología para usuarios particulares, para centros educativos, para las Fuerzas y Cuerpos de Seguridad del Estado y para los juzgados. *Software* que proporciona en sí mismo formación jurídica para profesores, alumnos y familias.

Internet es parte de la vida de todos los usuarios, de las empresas, de las instituciones y de los delincuentes, con la que se crea una relación entre sí de intercambio de un gran flujo de información a diario. Las redes sociales nos proporcionan una nueva forma de comunicación beneficiosa o nociva, según se utilicen, eliminando barreras temporales y geográficas.

Cuando ofrecemos información personal atentamos de forma totalmente inconsciente contra nuestra propia intimidad, por la gran desinformación en el uso de las nuevas tecnologías por parte de los usuarios. Pero tampoco podemos pretender que todos los usuarios se conviertan en expertos de las tecnologías. Pero sí es posible que adquieran unos conocimientos mínimos sobre las mismas y nuevas herramientas para su defensa, que hasta el día de hoy no las había, al menos que aportaran información veraz.

Dado que los usuarios no saben de tecnología, creé un sistema de *software* fácil, accesible y con un funcionamiento con el que se obtienen pruebas visuales y técnicas de lo que está ocurriendo en la red, con lo que

el usuario puede demostrar su verdad, la policía tiene pruebas veraces para comenzar su investigación, y los juzgados tienen la carga de prueba.

La innovación de este *software* para el usuario: creadas las aplicaciones ENOCH, MOISÉS Y THOR como herramientas para los usuarios, y creados los *softwares* FCSE para las Fuerzas y Cuerpos de Seguridad del Estado, e IUS para los juzgados, con esta innovadora tecnología, a través de la que pueden ver y descargar la información (pruebas) de los usuarios que ponen su denuncia certificada y contenido veraz con esta tecnología.

Esta tecnología agiliza los trámites de investigación, de usuarios, policías, jueces, y repercute directamente en educación.

Esta tecnología está disponible a día de hoy.

La información certificada obtenida por estas herramientas: datos de prueba, desde cualquier PC, móvil o tableta, con un solo clic se obtiene la información visual y técnica del suceso. Al enviarla a su panel de administrador llegan dos documentos: uno con los datos técnicos y otro con los datos visuales.

En cuanto a los datos técnicos que obtenemos: código de denuncia, la IP de donde se ha producido el hecho, la descripción de la denuncia (fecha y hora en la que se obtiene, fecha y hora a la que se envía, fecha y hora en que se queda encriptado el archivo de la prueba capturada, que puede ser un archivo audio, foto, vídeo o web), la latitud y la longitud, los datos del usuario (DNI, nombre, etc.), entre otros datos relevantes que únicamente pueden estar al alcance de policías y juzgados que son relevantes para sus investigaciones.

Las estadísticas obtenidas de centros educativos en el año 2012-2013: hay un gran número de centros educativos que vienen todavía negando este tipo de problemas como el acoso, ciberacoso, difamación, venta de drogas, etc., y esto es un gran error porque tarde o temprano, si no se pone una solución, estos problemas acaban saliendo a la luz, como está ocurriendo a día de hoy: suicidios, abusos sexuales, etc. Y lo que se podía haber evitado, ya no tiene marcha atrás.

El foco está en los centros educativos, y es en los centros donde ha de impartirse esta herramienta de defensa para formarles en una navegación responsable pero con libertad y de forma segura. ¿Por qué? Porque por muchas prohibiciones que a día de hoy hagamos a un menor, si no será

desde su casa será desde la casa del amigo o será desde la casa de quien sea, entrará a la página que quiera. Pues de este modo los alumnos aprenden a detectar, con esta herramienta, a prevenir, y en última instancia a defenderse de una conducta delictiva por parte de un usuario malintencionado, o de un delito.

La mayor problemática de incidencias radica en la gran desinformación por parte de los menores y sus tutores sobre qué es un delito en la red o lo que no lo es; y la falta de formación, y en cuanto a conocimientos mínimos para la navegación por la red.

Durante los doce años de investigación previa a la creación de este *software* observé la necesidad de proporcionar, junto con la herramienta de defensa, un material formativo adecuado para menores y sus tutores, en el cual se les indican las conductas más habituales de tipo delictivo en la red, con el fin de disminuir los casos de víctimas. Proporciona formación jurídica en nuevas tecnologías, en el uso de las redes sociales, tanto a profesores como a los alumnos y sus familias; los forma en la utilización de nuestro *software* Moisés para la obtención de las pruebas. De este modo los menores, los tutores y los padres aprenden a detectar, prevenir, y en última instancia a poder defenderse, poder denunciar con pruebas visuales y técnicas, el suceso.

El éxito que ha tenido en estos dos años esta herramienta, y en este último año 2012-2013, es el siguiente: hemos tenido a padres y alumnos informados sobre los riesgos de Internet, las penas que conllevan dichos delitos y cómo defenderse; toma de conciencia de los menores del daño psicológico que podrían estar ocasionando a los compañeros, y los riesgos a los que se exponen navegando y entrando a webs nocivas. Aprenden materia jurídica sobre los delitos en Internet, y cómo castiga la ley con su Código Civil y su Código Penal, etc., el *grooming*, el *sexting*, el *cyberbullying*, incitación al suicidio, estafas electrónicas, protección del derecho al honor, etc., propiedad intelectual, *phishing*, *pharming*, muy importantes, contratos falsos por Internet, LOPD, *spam*.

Los alumnos dados de alta en el centro encuentran asistencia psicológica, pudiendo estos entablar comunicación directa a través de su panel, el panel que les proporciona Moisés desde su administrador, directamente con el orientador de su centro, evitando así las barreras de comunicación que se producen en la adolescencia a la hora de contar algún problema personal cara a cara.

Acuerdos entre los padres y los centros antes de llegar a una situación grave con las pruebas que le proporciona Moisés, ya que el centro en sí mismo en ocasiones no es responsable del acto, sino el alumno o tutor que lo comete.

Disminución de las incidencias por parte de los menores en las redes sociales, y una navegación más responsable, en aquellos alumnos a los que les han impartido en clase este material didáctico-jurídico.

La falta de confianza en el seno familiar es complementada por Moisés. Los menores saben que, en el momento en que se vean en algún problema, pueden obtener esta información con tan solo un clic, que pueden decidir trasladarla, si lo necesitan, a la policía, a sus padres, a sus tutores, y resolver qué van a hacer con ella.

Ha sido una gran solución también para tutores, debido a las situaciones límite que están viviendo de acoso por parte de los alumnos.

Ahora les voy a contar las soluciones policiales y jurídicas en cuanto a tecnología forense en las que se aplica este algoritmo. Hasta el día de hoy no existía ningún modelo o método capaz de obtener una prueba y conservarla sin que existiese la posibilidad de manipulación. Hasta el día de hoy los mecanismos utilizados por la tecnología forense no pueden certificar que las pruebas obtenidas de un componente electrónico son veraces y no introducidas previamente por un usuario malintencionado, entendiendo que una prueba crucial para el esclarecimiento de un hecho puede ser introducida intencionadamente culpando a un inocente.

El área pericial que abarca, entre otras: delitos informáticos, propiedad intelectual, medios de pago, pornografía infantil, autenticación de *e-mails*, técnica criminalística y obtención de pruebas en las redes TOR.

La técnica criminalística o forense se ocupa del conjunto de medios y métodos científico-técnicos que se utilizan durante la investigación de los delitos a los fines del descubrimiento, fijación, ocupación e investigación de los distintos elementos, indicios, materiales o evidencias físicas halladas en el lugar del suceso o durante la realización dela inspección o de cualquier otra acción de instrucción que conlleve la búsqueda de estos elementos.

MSM Technology ofrece la garantía del contenido de la información, prueba, obtenido durante toda la cadena desde que el usuario la obtiene hasta requerimiento judicial.

El éxito obtenido en esta cadena: primero, se obtiene información veraz; segundo, obtenemos carga de prueba visual y técnica; tercero, ahorro para la administración en tiempo y costes económicos; cuarto, que el coste emocional de las víctimas sea el menor posible, algo que paralelamente repercute en un bien mayor en toda la sociedad; cinco, un uso ejemplar y responsable de las nuevas tecnologías y la seguridad de la información, adaptadas a policía y justicia, repercutiendo directamente como ejemplo para toda la sociedad a nivel internacional; seis, refleja socialmente una toma de contacto directa sobre la conciencia de los ciudadanos en la obtención, presentación de pruebas y sus consecuencias; siete, en delitos transaccionales se obtiene la carga de prueba visual y técnica que puede ser anticipada a otros países con los que se esté en colaboración mediante acuerdo firmado.

Esta tecnología custodia las pruebas vírgenes encriptadas con las que un ciudadano de cualquier parte del mundo demuestra lo que le está ocurriendo, avisando a las fuerzas y cuerpos de seguridad, pudiendo así solicitar ayuda a su país, en el caso de estar en el extranjero, si lo necesita.

Colaboraciones mantenidas hasta el día de hoy: el usuario es el propietario en todo momento de su información. Nuestro sistema ofrece la posibilidad de que el usuario decida compartir dicha información, colaborar, dada la situación del aumento de delitos año tras año. Por ello, pensando en la petición que tanto solicitan las Fuerzas y Cuerpos de Seguridad del Estado instando a la colaboración ciudadana y a empresas del sector, el *software* contiene un botón «Aviso» para avisar, si el usuario lo desea, sobre webs nocivas, ciberacoso, pornografía infantil, *grooming*, etc., terrorismo, ciberterrorismo..., con pruebas visuales y técnicas. En definitiva, ayuda o colaboración *online* sobre cualquier delito telemático con pruebas veraces simultáneas al suceso, contribuyendo así cada usuario a crear una red más sana y segura.

La aplicación de Moisés, conocida como Wave System S.O.S., colabora con el Grupo de Delitos Telemáticos de la Guardia Civil con el acuerdo firmado desde el 13 de febrero del año 2012; la Brigada BIT de Delitos Tecnológicos de la Policía Nacional fue informada de esta tecnología al mismo tiempo, no accediendo a dicha colaboración y servicio ciudadano.

Los resultados obtenidos por esta tecnología, la veracidad de la información obtenida, las ventajas en educación y formación, las ventajas de

toma de conciencia sobre las nuevas tecnologías, las ventajas policiales, las ventajas jurídicas y las ventajas transaccionales han quedado más que demostradas.

Tras dos años de colaboración con el Grupo de Delitos Telemáticos de la Guardia Civil en la recepción de las incidencias de los usuarios, y habiendo informado a Policía Nacional, como antes he mencionado, la propia secretaría de Estado publicó el 23 de junio de 2013 en Europa Press la noticia de una herramienta llamada SIMACS, aún sin desarrollar. Con dicha aplicación, el señor Francisco Martínez Vázquez, secretario de Estado de Seguridad, desde mi punto de vista parece que pretende apropiarse de estos éxitos obtenidos durante dos años de duro trabajo, doce años de mi investigación y mi grandísimo esfuerzo para realizar la puesta en marcha de esta innovadora tecnología como emprendedora.

La innovación que les he expuesto como solución fue presentada en la Unión Europea en el año 2009, la cual fue aprobada por todos los países miembros para su licitación en el programa SAFE, al cual no pude optar entonces por no ser empresa. Siempre he trabajado a contrarreloj para solucionar la problemática mundial en ciberdelincuencia y sabiendo que este *software* evitaría que más menores se convirtiesen en víctimas de acoso sexual, pornografía infantil, *cyberbullying*, difamación, suicidio, etc., en la red.

Lo positivo de todo esto a día de hoy es que es un hecho que existe esta solución, y ha quedado demostrado tras estos dos años la gran solución que reporta. MSM Technology dispone de toda la protección legal nacional e internacional en cuanto a su algoritmo y programas informáticos, para la obtención de dicha información, su contenido y su tráfico en cuanto a *softwares* específicos protegidos para policías y juzgados.

Tengo una petición para sus señorías, con toda mi inocencia. Y mi petición es la elaboración de una ley. Durante los doce años de mi investigación para la conclusión de este algoritmo también me quedó una visión muy precisa de la gran necesidad de la creación de una única ley global en la que —disculpen mi ignorancia—, en mi opinión, deberían sentarse los magistrados, mandatarios de todos los países que quisieran cubrir esta necesidad, recogerían todas y cada una de las leyes que castiga esta tipología de delitos de cada uno de los países participantes, y

llegar a una comunión entre todas ellas —sé que no es fácil—, creando así un nuevo tratado internacional en defensa de los usuarios en Internet. Yo lo llamaría «tratado internacional Cyberlaw».

Muchísimas gracias por escuchar mi exposición, y podemos comentar las diapositivas que he traído o pasar a preguntas.

COMPARECENCIA DE LA DIRECTORA DE RESPONSABILIDAD E INNOVACIÓN SOCIAL CORPORATIVAS DE TELEFÓNICA, DÑA. SOFÍA FERNÁNDEZ DE MESA ECHEVERRIA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 10 DE MARZO DE 2014.

La señora **DIRECTORA DE RESPONSABILIDAD E INNOVACIÓN SOCIAL CORPORATIVAS DE TELEFÓNICA** (Dña. Sofía Fernández de Mesa Echeverría): Muchas gracias, señores senadores. Quiero comenzar por agradecerles en nombre de Telefónica que nos hayan dado la oportunidad a través de esta comparecencia de trasladarles cuál es nuestra visión y cuál es nuestra posición sobre el tema relacionado con el buen uso de las tecnologías, Internet, por parte de los niños; y también sobre los riesgos que también existen, y somos conscientes de ello.

Efectivamente, nos enfrentamos ya desde hace varios años al reto de la educación de los niños y de los adolescentes para el uso adecuado de las nuevas tecnologías, por un lado, y por otro la implantación de medidas de protección frente a estos riesgos que ya se han identificado, derivados del uso de la red. Un riesgo que sobre todo se basa en la facilidad de acceso y en el anonimato que proporciona la red. Y ésta es una responsabilidad que compartimos con otros operadores de la industria y con otros agentes involucrados en este objetivo de protección de la infancia frente a la red.

Analizando un poco el perfil de estos usuarios, los niños han asumido con total naturalidad, mucho antes que nosotros, los teclados, pantallas y todo tipo de herramientas que les están permitiendo acceder a un mundo de posibilidades casi ilimitadas, yo diría, en cuanto a lo que es su formación, sus relaciones sociales y al inmenso número de habilidades extraordinarias que necesitan de cara a afrontar su futuro profesional y social.

Nosotros queremos destacar que, por un lado, somos conscientes de estas ventajas, y es el objetivo principal de Telefónica como operadora, potenciar este buen uso y estas ventajas que puede ofrecer la tecnología. Pero también somos conscientes de que existen determinados riesgos que se derivan de un mal uso de estas tecnologías, y que pueden llevar a cabo situaciones de difusión de contenidos ilegales (algunos no ilegales,

pero sí dañinos), contenidos ilegales de pornografía infantil, de abusos sexuales a menores, conductas también ilícitas, acoso escolar, y una serie de comportamientos que en sí no son nuevos; lo que es nuevo en esta nueva era digital, digamos, es la dimensión, el mayor alcance que tiene el hecho de que la red ofrezca la viralidad que todos conocemos.

Por tanto, para nosotros, habiendo hablado de ventajas y de riesgos, el objetivo es encontrar el punto de equilibrio entre ese temor y desconfianza hacia lo desconocido y los riesgos que entraña la red, y estos beneficios que comentaba brevemente derivados del uso de las tecnologías.

Telefónica agrupa su compromiso para el buen uso y para la disminución de estos riesgos en cuatro grandes bloques de actuación, que son: autorregulación, alianzas, educación, y la provisión de soluciones para un uso seguro y responsable, soluciones tecnológicas.

Yo, a continuación voy a exponer cómo se declinan actuaciones concretas en estos cuatro grupos que conforman la estrategia de Telefónica en esta materia, pero lo voy a hacer siguiendo un orden cronológico y no temático, no centrándome en los cuatro bloques sino en una secuencia de cuál ha sido el viaje de Telefónica a través de estos compromisos, muy marcados, por cierto, por la autorregulación sectorial. Y voy a empezar por hablar de ello.

El primer acuerdo sectorial de autorregulación data del año 2007, el 12 de febrero, cuando Telefónica firma junto a las principales operadoras europeas un acuerdo marco para fomentar el uso seguro de los móviles por parte de niños y adolescentes; un acuerdo auspiciado por la Comisión Europea. Este acuerdo se resumía en cuatro bloques.

En primer lugar, la clasificación de los contenidos para adultos. Nosotros aquí, en Telefónica, junto con otros operadores del sector en España hemos seguido la clasificación Wap Media Content Standards, un estándar de clasificación de reconocido prestigio internacional, a través del cual hemos trabajado conjuntamente en la gradación de los contenidos, la segmentación por edades.

Segundo compromiso dentro de este acuerdo marco: ofrecer mecanismos de control de acceso a aquellos contenidos que eventualmente puedan ser dañinos para los menores. ¿Qué quiere decir esto? Aplicación de medidas como es la verificación de edad, como es la oferta de servicios específicos, la oferta de terminales ad hoc, el establecimiento de filtros,

control de consumo de Internet por parte de los niños; son mecanismos, vuelvo a decir, de control de acceso a estas tecnologías.

Tercer bloque, importante y que van a ver que se repite en las distintas iniciativas de autorregulación: educar y concienciar en este uso responsable del móvil. Y hago aquí un inciso: la tecnología, probablemente no pueda dar respuesta a todo si no se combina con la debida sensibilización y uso adecuado de las tecnologías. Por eso este punto de la educación se repite sistemáticamente en casi todos los acuerdos de autorregulación.

Y el cuarto punto trata de la colaboración con los Cuerpos y Fuerzas de Seguridad del Estado para la denuncia de estos contenidos ilícitos. Y hago un nuevo inciso: la industria de las TIC extendida, no solo la de los operadores, sino fabricantes de terminales, productores de contenidos, etc., no pueden por sí solos gestionar este riesgo; es necesaria la colaboración con las Fuerzas y Cuerpos de Seguridad del Estado y en general con la administración pública y el legislador.

Como consecuencia de este acuerdo marco, el aterrizaje de este acuerdo marco en España data de finales del mismo año, 2007, cuando Telefónica, Vodafone, Yoigo y Orange firmamos el código de conducta nacional. Y quiero destacar aquí que España fue el primer país que declinó este acuerdo marco europeo en un código de conducta nacional. Es un código de conducta que está activo; hay reuniones cada dos meses, las operadoras nos reunimos y llegamos a acuerdos de implantación de medidas concretas. Les expongo algún ejemplo: la homogeneización en la categorización de los contenidos para adultos, que comentaba antes, todo esto para los portales Wap de los móviles; las inserciones en las facturas, donde aprovechamos para dar consejos sobre un buen uso de la tecnología de Internet en el móvil, o un icono común para la denuncia de contenidos ilegales, disponibles no solo en las webs, sino también descargables en los *smartphones* y en las tabletas. Este icono, de hecho, data de febrero de 2011, cuando este botón de denuncia que llamamos «Protégete» se desarrolla en colaboración con todos los operadores y se pone a disposición del público a través de nuestras páginas web. La idea era que los usuarios pudieran reportar contenidos potencialmente ilegales. Y este icono se negoció y se diseñó en colaboración con Protégeles, que es —probablemente conozcan— el nodo oficial del InHope en España, y también del InSafe. Por tanto, este icono enlaza con su página de denuncia, de tal forma que el usuario puede informar y buscar ayuda

también si tiene algún problema, alguna duda o alguna complicación en relación con las tecnologías.

Un año más tarde, en 2011, se presenta la versión para teléfonos inteligentes y tabletas, que es compatible con el sistema operativo IOS y Android. Aquí es importante, y vuelvo a insistir, el hecho de que en el propio código de conducta se vuelve a destacar la importancia de que la consecución de estos objetivos que perseguimos las operadoras implica no solo el compromiso de las operadoras, de los padres, de los educadores o de las organizaciones que conocen y que tienen esta vocación de proteger a la infancia, sino que es muy importante también contar con el apoyo de la administración pública y de las Fuerzas y Cuerpos de Seguridad del Estado.

Otra iniciativa de autorregulación sectorial fue esta vez promovida por el GSMA, la asociación de los móviles o GSM; fue una medida de autorregulación paralela a la que acabo de comentar, nace en 2008; y esta perseguía en concreto disminuir, frenar la distribución, el comercio y la venta de imágenes de abuso sexual a los niños a través de las redes móviles. Aquí los operadores móviles nos unimos para frenar precisamente esta circulación de contenidos. Y en concreto, lo que acordamos a través de esa alianza era, en primer lugar, un sistema de notificación y retirada de aquellos contenidos que, siendo ilícitos, pudieran estar alojados en los servicios que ofrecemos las operadoras.

En segundo lugar, una colaboración y una promoción de lo que son las *hotlines* nacionales, para que los clientes, los usuarios, los navegadores supieran que existe esta opción y se dirigieran a ellos para consultar y para denunciar estos contenidos.

Y en tercer lugar, la implantación de unos mecanismos técnicos que previniesen del acceso a contenidos que son ilegales o que hubieran sido identificados como ilegales por un organismo apropiado.

Por lo tanto, en primer lugar esta alianza persigue disminuir la frecuencia de exposición a estos contenidos, y por otro lado reducir su diseminación.

Estas medidas de autorregulación, he de decir que se basan en la supremacía del bien jurídico a proteger, que en este caso son los derechos de los niños, tal y como establece la Convención de Derechos del Niño de Naciones Unidas. Y además esta alianza, digamos que, aunque es una

medida de autorregulación, no por eso trabajó al margen de lo que son las iniciativas legales. Es decir, GSMA solicitó a los gobiernos el apoyo legal necesario precisamente para garantizar que los operadores móviles pudiéramos actuar de manera efectiva. Y esta alianza móvil, de hecho contó con el apoyo de la Comisión Europea y de otros organismos como Naciones Unidas o las Unión Internacional de las Telecomunicaciones. Les traía aquí una cita precisamente de Viviane Reding, entonces comisaria europea de la Sociedad de la Información y Medios de la Comunicación, donde decía literalmente: «doy la bienvenida a este acuerdo; es una señal muy clara de que la industria móvil tiene el compromiso de hacer que el Internet móvil sea un lugar más seguro para los niños. El hecho de que esta iniciativa haya surgido de la labor llevada a cabo por la industria de la tecnología móvil en Europa muestra que Europa es una vez más líder en la construcción de un ambiente confiable para hacer negocios». Es decir, contábamos, como vuelvo a decir, con el respaldo de la Comisión Europea.

Y esta solicitud de respaldo normativo desde el GSMA fue tenida en cuenta por la Comisión Europea, la cual era plenamente consciente del crecimiento de estas nuevas formas de acoso como son el *sexting*, el *grooming*, la proliferación de páginas con contenidos de pornografía infantil, la facilidad y la impunidad que ofrece Internet precisamente para cometer este tipo de crímenes, y la alta rentabilidad que estas organizaciones criminales obtienen de este tipo de negocio, digamos, asumiendo muy poco riesgo. La prueba de este compromiso por la Comisión Europea fue que en diciembre de 2011 lanza la directiva de la lucha contra la pornografía infantil. Lucha literalmente contra «los abusos sexuales y la explotación sexual de los menores y de la pornografía infantil». Esta, que debía trasponerse en todos los Estados miembros a partir del 18 de diciembre del año 2013, en España se hará a través de la reforma del Código Penal en curso, y esperamos, está previsto que se apruebe este año.

Para nosotros, esto supone definitivamente un refuerzo a todas estas medidas que voluntariamente ya habíamos empezado a adoptar los operadores y la industria en general. Nosotros mantendremos nuestro compromiso y trabajaremos junto con la globalidad de agente implicados, que como digo, no son solo las operadoras, en la lucha contra la pornografía infantil en la red, es decir, en colaboración con la Comisión Europea, el Parlamento Europeo, los gobiernos locales, ONG especializadas, autoridades judiciales y otros agentes involucrados.

Para nosotros, la solución que se considera más eficaz para combatir la pornografía infantil y la preferida por los operadores en general será siempre la eliminación de los contenidos en origen. Y únicamente cuando esto no sea posible, prevenir el acceso a esas *websites* que se han identificado como que alojan contenidos ilícitos de pornografía infantil. Por eso sería deseable para nosotros que existiera una lista única europea con todas esas websites y que fuera avalada por las autoridades judiciales y policiales; es decir, una mayor coordinación en ese sentido a nivel de las agencias o Fuerzas y Cuerpos de Seguridad del Estado.

Otra iniciativa de autorregulación sectorial es la de los principios TIC, también promovida a nivel europeo. Literalmente son los «Principios para el uso seguro de dispositivos conectados y servicios *online* para niños y jóvenes en la Unión Europea». Bien, durante 2011 hubo mucho diálogo entre empresas del sector de las nuevas tecnologías, se reunieron periódicamente, y elaboramos unos principios que fueron avalados y revisados por la sociedad civil. En enero de 2012 fue cuando cerca de treinta empresas del sector de las tecnologías de la información y de la comunicación anunciamos el lanzamiento de esta coalición. Estos principios están apoyados por empresas de distintos ámbitos del sector, es decir, los que somos operadores de la red, fabricantes de dispositivos, proveedores de contenidos, motores de búsqueda, etc., es lo que llamamos el sector TIC ampliado. Los firmantes de este documento nos comprometimos a, en primer lugar, desarrollar métodos innovadores que mejorasen las condiciones de seguridad *online*. En segundo lugar, a involucrar a padres y tutores en todo lo que son actuaciones de formación y de sensibilización. Importante: que los usuarios conocieran, tuvieran conocimiento sobre la información y las herramientas que ya están disponibles para mantenerse seguro en la red, y sobre aquellas obligaciones que tenemos en relación con un comportamiento responsable en Internet.

Nos comprometimos también a dotar de información clara y transparente en nuestras condiciones de uso de servicio, y de esta manera establecer cuáles eran los límites de un comportamiento aceptable y cuáles eran las reglas aplicables en el caso de que los contenidos sean generados por los propios usuarios, como ocurre en las redes sociales.

Y por último, acordamos crear mayor conciencia sobre qué tipo de contenidos son denunciables y cómo se pueden denunciar estos contenidos. Como ven, recurro a conceptos que ya se han ido discutiendo en medidas autorregulatorias.

Estas aspiraciones se tradujeron en seis líneas de trabajo: materia de contenidos, de control parental, mecanismos para el reporte de las situaciones de abuso y mal uso de la tecnología, lucha de la pornografía infantil en la red, la privacidad, y la educación y sensibilización.

La situación actual de la Coalición ICT es que hemos entregado todos los que hemos suscrito esta alianza un informe de situación respecto al grado de implantación a través de medidas de estos compromisos. Y hemos comisionado un verificador independiente que está haciendo una auditoría del avance de todos estos compromisos en las distintas operadoras, de los distintos miembros que hemos suscrito la alianza. Durante el mes de abril se publicará el resultado, será público y podrán ustedes comprobar cuál es el grado de avance de los distintos firmantes. La página web donde podrán comprobar este estado de situación es www.ictcoalition.eu, ahí podrán tener información pública.

Casi en paralelo, pero con una naturaleza un poco distinta, se firma la Coalición de los CEO, la que llamamos «Internet, un lugar más seguro para los niños». La Coalición de los CEO, que se lanza en diciembre de 2011, esta vez no estaba auspiciada por la voluntariedad del sector de las TIC, sino por la vicepresidenta de la Comisión Europea, por Neelie Kroes. Neelie Kroes llama a todos los CEO de las grandes empresas involucradas en el sector TIC para promover, de nuevo, un mejor uso de Internet desde cinco áreas, que van a sonar a lo que acabo de contar sobre la Coalición ICT, y que son de nuevo: herramientas para el reporte de situaciones de abuso y de contenidos ilegales en la red, privacidad por defecto, sistemas de clasificación de contenidos, controles parentales, y mecanismos para notificación y retirada de los contenidos de abuso a menores en Internet. Como ven, muy parecido a la ICT Coalition. Y ahora explicaré la diferencia entre una y otra.

En torno a estos cinco pilares se generaron cinco grupos de trabajo. Telefónica en concreto estuvo liderando el primero, precisamente el de generar un botón de denuncia, que es precisamente el que les he comentado que en España se aterriza con Protégete.

Con posterioridad a esa CEO Coalition, lanza la propia Comisión la estrategia europea, en mayo de 2012, acerca de un Internet más adecuado para los niños, que va en la misma línea; se basa en cuatro pilares, que son: potenciar los contenidos *online* de calidad para los niños, una mayor sensibilidad y dotarles de una mayor capacidad de reacción a través de

acciones de comunicación y de formación, crear un entorno *online* seguro con todas estas herramientas que he estado mencionando, como pueden ser la configuración de la seguridad por edades, un control parental, clasificación de contenidos, estándares de publicidad *online* para controlar y mejorar el consumo, que a veces es excesivo por parte de niños en Internet; y un cuarto bloque que se repite de nuevo, que es la lucha contra el abuso y la explotación sexual de los niños mediante la notificación y retirada de contenidos de pornografía infantil.

Bien, pues en Telefónica, a la luz de esta estrategia y de todo lo que he contado hasta ahora sobre las medidas de autorregulación sectorial, hicimos una revisión de nuestra propia política interna, y en 2013 definimos un reglamento interno en materia de buen uso de tecnologías, buen uso de Internet por parte de los menores, cuya implantación está siendo la base de toda nuestra actuación corporativa en las distintas unidades de negocio. Y destaco aquí, no solamente en Europa, donde tenemos operaciones, sino también en el resto de los países latinoamericanos.

Y como les decía, la CEO Coalition —en inglés— o coalición de los CEO y la Coalición ICT son muy parecidas en cuanto al contenido pero tienen algunas diferencias. La Coalición de los CEO es una iniciativa promovida por la Comisión Europea; en cambio, la ICT está promovida por la industria. Los contenidos son muy similares, pero la Coalición de los CEO dejó fuera un punto que para la ICT fue fundamental, que es todo lo que tiene que ver con la educación, la sensibilización en el buen uso de las tecnologías. Y por último, si la Coalición de los CEO nació, digamos, con fecha de terminación (la idea eran 18 meses, que vencían en enero de 2014), la Coalición ICT tiene vocación de permanencia, y quiere promover un debate sectorial donde se intercambien mejores prácticas y se promuevan iniciativas de mejora de la seguridad en Internet.

Esto es básicamente en relación con la autorregulación, pero quiero añadir un último punto que se ha descrito varias veces, y tiene que ver con la sensibilización. Telefónica, en el año 2008 constituyó el foro Generaciones Interactivas; no lo hizo sola, lo hizo junto con la Universidad de Navarra y la Organización de Universidades Interamericanas, y crearon así el Foro Generaciones Interactivas. El objetivo, la vocación del foro era conocer mejor los patrones de uso de las pantallas de Internet y trabajar, en base al conocimiento de esos patrones, en modelos educativos, formativos para potenciar el buen uso. Entre 2008 y 2011 se

llevaron a cabo una serie de estudios en varios países en Latinoamérica: Argentina, Brasil, Colombia, Chile, Ecuador, Guatemala, Perú, México y Venezuela. También se incluyó España. Participaron unos 2.300 centros educativos; hubo más de 300.000 alumnos que intervinieron a través de las encuestas explicando cuáles eran esos patrones de uso, y se publicaron varios libros en relación con esto.

A partir de esta investigación, el foro diseñó acciones educativas dirigidas a docentes, a educadores, también talleres para padres, y actividades para los niños en los colegios. Desde el año 2008 benefició hasta 50.000 personas que fueron formadas a través de estos programas.

A través de Foro Generaciones Interactivas, Telefónica también ha invertido en el desarrollo de contenidos para precisamente fomentar estos usos, y siempre lo hace en alianza con expertos del sector, en este caso, y a través de Foro Generaciones Interactivas, llegó a un acuerdo con «Pantallas Amigas» y lanzó una web, que es la de infancia y tecnología, es un recurso didáctico *online*, una web, que está orientado para niños y niñas de entre 6 y 11 años, y que combina historias animadas dirigidas a ellos, con otras series de cuestiones más orientadas a padres y a educadores.

No es la única web; hay otra interesante, que también se ha hecho con «Pantallas Amigas», y es la de «Cuidado con la *webcam*», que si se cliquea así, directamente, se puede encontrar en la web; y de nuevo son consejos en formatos de animación muy entretenidos, breves; pretenden llegar a explicar a los niños los riesgos donde ellos no los ven, donde solamente ven juego.

También lanzamos a través de este foro una colección de ocho vídeos que se llama *La familia digital* y que pretenden recrearse en lo que es la brecha digital que hay entre padres e hijos y en cómo la vida familiar se ha transformado por la introducción de las tecnologías de la información; es el uso que hacemos de los móviles, cómo gestionamos incluso las compras de las entradas de teatro en contraposición a lo que ha sido la manera tradicional de llamar a través de un *call-centre*; entonces, lo que hacen estos vídeos es que, de una forma medio cómica, intentan poner de manifiesto la brecha que hay entre padres e hijos y cuáles son las áreas que debemos cubrir en cuanto a la formación, y cómo afectan, por ejemplo, las redes sociales a la vida familiar.

Bien, a través de Foro Generaciones Interactivas también hemos abordado, en relación con la presencia en Latinoamérica, el objetivo de ex-

pansión de los acuerdos del InHope hacia Latinoamérica; es decir, hemos trabajado con ellos para crear líneas de denuncia, como es Protégeles, aquí en España, en Latinoamérica. El primer destino fue Colombia en 2012; y allí estuvimos trabajando para crear un canal de denuncia anónimo donde se pudieran reportar estas páginas con contenidos ilegales, y asegurando que el tratamiento posterior de estos contenidos llevara las garantías de unos procesos establecidos por el InHope, unas respuestas rápidas y eficaces y la posibilidad de atender a estas personas si tenían dudas. También se han hecho actividades de sensibilización, porque la población no sabe muchas veces que existen estos canales de denuncia.

¿Cómo se fundó este centro de denuncias? Es una alianza entre Telefónica, el Foro Generaciones Interactivas, el Ministerio de las Tecnologías de la Información y de la Comunicación colombiano, el Instituto Colombiano del Bienestar Familiar, la Fundación Telefónica allí en Colombia, y la red PaPaz, que es una ONG colombiana. Y a través de esto estamos ayudando al InHope a extender su campo de actuación, porque no solo están en Europa, sino que ya están presentes en unos cuarenta países en el mundo entero. En ese sentido, creemos que vale la pena seguir ayudando a la expansión de este tipo de iniciativas.

El último hito de Foro Generaciones Interactivas ha sido precisamente, la creación este año de una plataforma *online* alojada en la red comercial Movistar; hemos trabajado esto en España y también en Reino Unido. No hablo de Reino Unido porque no viene al caso, pero digamos que es una iniciativa corporativa de Telefónica que está intentando crear dentro de las páginas comerciales, no ya alojadas en las páginas típicas institucionales de responsabilidad corporativa, para que los clientes de Telefónica tengan acceso a estos contenidos, a estos recursos que les van a ayudar a entender con una clasificación por edades cuáles son las recomendaciones que hacemos de uso. Por estar en nuestras páginas comerciales, no están dirigidos a niños, están dirigidos a padres y a profesores, que son los clientes de Telefónica. Pero sí están segmentados los contenidos, los recursos, en base a esas edades. Incorpora un glosario de terminología que muchas veces para los padres es muy novedosa (el *texting*, el *grooming*, el *sexting*, el ciberacoso), y de ahí muchas palabras muy técnicas que no son conocidas habitualmente.

También está ahí instalado el icono de denuncia que decíamos antes, el Protégete. Cuenta con una colaboración de expertos a nivel europeo:

Universidad de Navarra, European Schoolnet, InSafe, EU Kids Online, Childnet International, Protégeles, PantallasAmigas. Hemos constituido un panel de expertos que nos ayuda a validar la línea editorial, a seleccionar los contenidos y los temas de mayor actualidad que creen que son de interés en este contexto europeo.

Esto fue presentado en el Safer Internet Day, y se le presentó a la Comisión Europea como uno de los trabajos resultantes precisamente de la CEO Coalition, esos grupos de trabajo, donde quisimos poner de manifiesto que era factible crear entornos de colaboración público-privados de autorregulación donde se promocionaran este tipo de esfuerzos. Somos conscientes de que además, cada vez más vamos a tender a montar plataformas —no me refiero solo a plataformas de Internet, físicas—, sino plataformas de colaboración multisectorial público-privadas para aunar esfuerzos, para racionalizar los recursos, que tienden a ser escasos hoy en día, y digamos, para alinearnos respecto de nuestra estrategia de sensibilización.

Por último, y antes de concluir, quiero comentarles, en relación con soluciones de control parental, una que Telefónica ha desarrollado internamente a través de su estructura de Telefónica Digital, que es una herramienta, en inglés «Protect my Kids»; esta está lanzada ya comercialmente en Brasil, y estamos en vías de ponerla a disposición de los clientes en España. ¿Qué hemos hecho? Antes de lanzar esta herramienta se llevó a cabo un estudio de lo que eran los patrones de uso y de consumo de las tecnologías, se hizo un estudio comparativo de lo que ofrecían otras herramientas, y se identificaron cuáles eran las funcionalidades más demandadas por padres, profesores, educadores, para establecer esa lista de funcionalidades.

Una de las características de esta solución es que ofrece una protección *online* integral. Es decir, imaginemos que desde el acceso, una especie de control de mando que podemos ver en Internet (y si tienen interés les puedo dejar una especie de demo que lo explica visualmente), el poder parametrizar o adecuar los mecanismos de control a las distintas edades o a los distintos perfiles de niños o de adolescentes sobre los cuales el padre o el adulto quiere establecer cierto tipo de control. Es decir, desde ella se puede gestionar el consumo de Internet a través del PC, de los móviles, las tabletas, el acceso a las redes sociales, el consumo, el gasto a través de Internet, etc.

Incluyen funcionalidades de protección contra contenidos inapropiados, lo que son los filtros, por supuesto, que es una funcionalidad básica

de casi todas las herramientas de control parental; protección frente al acoso y la amenaza en Internet; importante, el control del tiempo que los niños gastan en Internet, este también se puede gestionar a través de esta especie de control de mando o panel de control; creación de perfiles individuales para niños, depende esto de cuáles sean las normas internas de los padres o de los educadores; y todo esto a través de una gestión amigable del servicio con una página web que sea lo más intuitiva posible y donde sea muy fácil preestablecer todas estas funcionalidades.

Por concluir, reconocemos la responsabilidad que tenemos los operadores frente a estos nuevos retos que plantea Internet; no los omitimos, y estamos trabajando mediante medidas de autorregulación y desarrollo de servicios y herramientas para aumentar la seguridad.

Nuestros compromisos con la Unión Europea van en esta línea, y todo lo que hemos acordado a través de nuestras medidas de auto-regulación nos obliga, a través de nuestros propios códigos internos, a cumplir con todo ello.

Quiero destacar, aunque ya lo he hecho antes, lo importante que es para nosotros no ceñir este esfuerzo exclusivamente a las compañías operadoras de telecomunicaciones, no sería realista. Es necesario incluir a lo que llamamos la industria extendida, los proveedores de contenidos, por ejemplo, o los fabricantes de terminales, etc.; y también incluir a las autoridades judiciales y policiales, a la administración en general, de la cual necesitamos todo el apoyo para trabajar de una manera ordenada y en línea con lo que establezca la legislación de cada país.

Y por último, la tecnología no es suficiente; el control parental en el que estamos trabajando, pues es un avance más, tecnológicamente, hacia ese control; pero la tecnología va mucho más rápido que cualquier otra medida. Es importante, en paralelo, establecer medidas de concienciación, de educación, de formación en el buen uso de las tecnologías, igual que en la educación vial existen los semáforos, pero si queremos cruzar en rojo, lo más probable es que tengamos un disgusto; algo parecido nos ocurre con las tecnologías de la información. Y a veces es frustrante para los operadores sentir que la responsabilidad pueda estar enteramente volcada, por defecto, sobre nosotros, cuando tiene que darse una colaboración mixta, y además una combinación entre tecnología y formación, concienciación, sensibilización, padres, profesores, educadores en general.

Muchas gracias.

COMPARECENCIA DEL COFUNDADOR Y DIRECTOR DE MARKETING DE TALK2US COMUNICACIÓN, D. JOSÉ LUIS CASAL CASTRO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 2 DE ABRIL DE 2014.

El señor **COFUNDADOR Y DIRECTOR DE *MARKETING* DE TALK2US COMUNICACIÓN** (D. José Luis Casal Castro): (...) La verdad es que estoy superagradecido sobre todo porque les interese nuestra opinión al respecto; y después de lo que hablábamos, de que ya ha habido varias comparecencias, 42 en concreto, yo no he querido entrar ni ver lo que se hablaba, un poco para no estar ni posicionado ni viciado por opiniones. Y entonces, hice una primera comparecencia, preparé una pequeña presentación al principio, y a raíz del aplazamiento le quise dar una vuelta más y basarlo un poco en reflexiones.

Quiero hacer una pequeña composición de lugar, y es un poco ver lo que está pasando, ver dónde realmente pueden estar esos peligros, que yo no le enfocaría hacia peligros, yo siempre soy una persona muy positiva y constructiva; entonces, yo creo que es un tema bastante grande y global como para que el posicionamiento que se pueda tomar sea desde la base constructiva. Porque siempre vemos un poco que se habla de peligros, se habla de precauciones que hay que tomar, se habla muchas veces en tono negativo de esto. Y yo creo que la postura que debemos adoptar es positiva porque genera muchas ventajas, es un medio nuevo, pero es un medio que, como un día leía, no es un medio que haya aparecido un día por la mañana, que nos hayamos levantado y hayamos visto «señores, aquí hay una cosa que se llama Internet»; es una cosa que la ha fabricado el hombre, y es una cosa que la ha utilizado y se ha creado un poco para darle una utilidad y un servicio al hombre.

Entonces, hay cosas que llaman la atención dentro de esta composición de lugar que quiero comentar, y es un poco cómo somos los españoles. Casi 20 millones de españoles navegan diariamente por Internet, que es una barbaridad. Leía esta semana en *El País* y en *El Mundo*, venía la noticia de que la Unión Europea alerta de que España es el segundo país en el cual el acceso a Internet es el más caro. Estamos hablando de 40 euros mensuales, y Rumania, por ejemplo, que podríamos decir —con todos mis respetos— que es un país un poco de segunda división, está

con accesos a 10 euros el mes. Es curioso porque, pese a ser los segundos más caros, somos los líderes en adopción de nuevas tecnologías. En la forma en la que adoptamos los *smartphones*, las tabletas y todo eso, somos los líderes europeos, pero a saco.

Pero es curioso que la utilización que les damos está más enfocada muchas veces al ocio que a la posible utilidad profesional o educativa. Siempre hablo mucho de Apple, porque el enfoque que hacen ellos a nivel de *marketing* nunca hablan de características del aparato, hablan de las utilidades que tiene el aparato; y en un anuncio de una tableta de Apple siempre ves a la gente haciendo cosas, pero cosas productivas. Sin embargo, el perfil de usuario español no lo es tanto, es más orientado al ocio. Entonces, lo que decía, resumiendo: somos un país que tenemos un acceso muy caro, pero sin embargo adoptamos muy rápido las nuevas tecnologías.

En el tema de menores, tres datos: el 305 de los chavales de 10 años tiene móvil; el 70% de los de 12 años tiene móvil; y el 83% de los de 14 años tiene móvil. Por un lado, por la falsa sensación de seguridad y de control que puede tener de los padres hacia los niños, y la falsa sensación de libertad y de independencia que tienen los menores. Se crea un doble juego ahí.

Es curioso, porque todo esto es una nueva realidad, esto que estamos viviendo; a muchos nos ha pillado con el pie cambiado, otros realmente hemos nacido ahí... Hay que valorar un poco todo. Nosotros que estamos muy vinculados al tema, dentro de lo que es la agencia de comunicación que tenemos, tenemos una parte, una patita que está muy enfocada a la formación, tenemos, hemos diseñado un programa para colegios... Y la fase, vemos un poco lo que se hace por ahí. Muchas veces lo que vemos es que el enfoque que se le da a nivel educativo es de lo malo que pasa: cuidado con el *cyberbullying*, cuidado con el *sexting*, cuidado con todo esto. Eso es correcto, eso está ahí, pero tampoco les estamos diciendo lo bueno que se puede hacer con estas cosas. Nosotros vemos, por ejemplo, que hay iniciativas a nivel educativo, utilizando redes sociales, que están fantásticas pero que parten, a lo mejor, de un profesor, de forma individual; pero es un profesor que el propio sistema y su propia comunidad educativa lo etiqueta como friqui o como pirado, ¿y este qué hace?, con los niños con Facebook o no sé qué.

Entonces, ¿lo malo?: que lo consideras un enemigo, no a la persona, sino a lo que está haciendo y al medio que está utilizando, pero por

desconocimiento. Entonces, ¿qué nos da miedo?, que es una cosa que además tenía yo muchas ganas de decir aquí: que el desconocimiento provoca miedo. El miedo desencadena prohibición siempre. Entonces, lo que no nos gustaría es que la posible legislación que salga a raíz de este tipo de cosas y de este tipo de iniciativas genere prohibición o limitaciones, porque no es necesario; yo creo que de lo que tendríamos que partir es de una base, insisto como decía al principio, constructiva.

Si nos vamos un poco a los hábitos de lo que hacen los menores, es muy curioso, porque entre 11 y 14 años, lo que voy a decir, el 65% de estos chavales están dentro de grupos de WhatsApp; son grupos de usuarios —supongo que lo sabéis— en los cuales tiene una temática común y hablan dentro de ese grupo de este tema. Se genera un problema, y es que el que no está dentro se siente excluido del grupo a nivel social. Con lo cual hay un interés en estar en ese tipo de grupos. El 78%, 79% de los chavales estos entre 11 y 14 años utiliza mensajería instantánea; no están en grupos, pero sí utilizan programas del tipo Line, tipo WhatsApp y estas cosillas.

Es muy importante también: el 23% de los chavales entre 11 y 14 años publica periódicamente fotografías en Internet, y en sus redes; el 53% juega con su móvil; el 25% —son datos así, muy tal— tiene activado permanentemente la geolocalización en su móvil, con una doble lectura: por un lado les gusta utilizar aplicaciones tipo Foursquare y publicaciones en las cuales se vincula su publicación al lugar en el que están, que eso les puede hacer más populares o menos populares porque están en el sitio de moda y aparece que están en el sitio de moda, pero a la vez genera un posible control sobre esas personas, ya no solo de sus padres, sino de terceras personas que puedan estar controlando a esas personas.

Y lo más curioso: no llega a un 50% los chavales que utilizan Internet para buscar información. Con lo cual se está utilizando mal un medio como es Internet.

Por otro lado, ese dato tiene que ser también una señal de alarma para legisladores, por el hecho de que muchas veces estamos buscando el enemigo donde no está, porque el peligro no es las páginas a que puedan acceder o que no puedan acceder, porque estamos viendo que su mayor cantidad de tráfico no está en las páginas de Internet, porque no van a páginas de Internet, sino que están en aplicaciones; y de hecho, el tráfico

que se está generando, el 80% del tráfico se está generando a través de aplicaciones, no a través de navegación por Internet.

Y ojo con esto, que un 18% de chavales entre 13 y 14 años chatea habitualmente con desconocidos. Es un dado; de hecho, tengo aquí unos testimonios, he encontrado un estudio, y hay uno que es curioso: no sé si todos son usuarios de Twitter, pero hay un comentario, el segundo, de una niña de 4º de ESO, que dice que en Twitter solo me sigue gente de confianza, así que no veo el problema. Y es mentira: Twitter es una red que está abierta; puedes cerrar el perfil, pero inicialmente está abierta. Y un chaval de 1º de ESO que diga esto: ¿qué más da que sea delito o no? El daño ya está hecho. Tenemos ahí un problema.

Entonces, yo creo que los problemas —no sé si esto tiene audio; si pongo... o lo pego al micro, a lo mejor—.

[VÍDEO]

Es un vídeo durillo. Y con esto lo que quiero decir es que muchas veces, si algo me ha gustado de esta ponencia es que no solo estaba Interior, no solo está Educación, sino que se ha jugado un poco con varias. Y es que yo creo que un poco parte —la tecnología está ahí, el cómo la utilicemos está ahí—, parte un poco del perfil de la educación; esa madre no sabe lo que está haciendo su hijo porque está en una habitación, se llama Pablo, está con un ordenador, sabemos que está pero no sabemos qué está haciendo. Entonces, yo creo que parte un poco de la educación que se pueda fomentar. Estamos viviendo una situación que nos habrá venido grande —yo no quiero juzgar a nadie— en la cual todo el tema de videoconsolas, ordenadores nos ha venido a muchos padres como comodines; es decir, enchufo al niño, en vez de enchufar la videoconsola, y ahí está bien que está entretenido y a mí ni me marea, y estas cosas, ¿no? Llevo tres semanas buscando una viñeta que no la encuentro, que es muy ilustrativa y habla del sonido del recreo, en la cual se ve el recreo en los colegios en el año 1984, en el cual sale un grupo de niños en carrera de sacos, otros jugando al fútbol, el ruido de «gol» y tal, y otro que es el recreo en el año 2014; y se oye «tic, tic, tic, tic». Y todos los niños están sentados a la sombra de un árbol con el móvil. Entonces, yo creo que ahí tenemos un problema, y es eso: no se están utilizando los medios que tenemos y la potencia que puede tener Internet y sacándole el provecho que le podemos sacar.

Quería buscar yo, y he encontrado un estudio de una empresa que ha hecho para los usuarios de Internet de lo que hacen en Internet. Los menores, el contenido que hacen es colgar fotos y minivídeos, los famosos *shelfies*, utilizar mucha frase cita emotiva y muchas cosas, los famosos *memes*, chatear, publicar fotos de eventos a los que asisten y canciones. Volvemos a lo de siempre: es buscar popularidad, ser el más guay de su clase, buscar reconocimiento. Y una clave que va un poco asociada a este vídeo: el 60% de los menores prefiere consultar algo en Internet a sus amigos mediante WhatsApp o buscarlo en Google antes que preguntarles a los padres. Yo creo que ahí tenemos un problema.

Y si lo extrapolamos, la pregunta del millón: si predicamos con el ejemplo. Siempre decimos que muchas veces les soltamos la cháchara (esto no puedes hacer, no sé qué, y los primeros que estamos metiendo la pata somos los padres); hay un dato curioso, yo siempre hago la comparativa, y es que eso de buscar popularidad mediante los *memes*, mediante las fotos lo hacen los adultos igual. Analizamos las redes sociales de cualquier adulto, y tenemos la manía de publicar fotitos con el *gin-tonic*, pero claro, si es el bar cutre de tal no ponemos la foto del *gin-tonic*, pero si es el club de no sé qué o no sé cuántos, foto del *gin-tonic* con toda la frutería dentro. Conversación de persona, de alto directivo que se introduce en redes sociales, le encanta presumir del número de seguidores que tiene en Twitter —lo digo porque nosotros gestionamos alguna cuenta de algún directivo y tal, y las conversaciones son... si eso es importante—; luego es curiosísimo, porque en Twitter, el 78% de los *links* que van en un tuit no se abren, con lo cual estamos compartiendo contenido que no tenemos ni idea de lo que poner, 78%, eso somos los adultos; y para colmo de egos, yo siempre digo una cosa: que no entiendo cómo en este país hay tantos millones de parados con la cantidad de premios Nobel que hay en LinkedIn; porque hay perfiles que digo yo, ¡madre mía!; y luego, en búsqueda activa de empleo o tal, no me lo explico, o no hay empresas suficientes o no es normal esto. Entonces, lo que ves en casa, luego es muchas veces tu manera de actuar.

Y luego, una cosa muy curiosa, que hablamos de las fotos, de que si ten cuidado, de que no publiques fotos, no publiques... El 60% de los adultos españoles publica fotos subidas de tono y comparte fotos mediante WhatsApp, Line y sistemas de mensajería, 60%. Hay un vídeo también muy ilustrativo sobre este tema, y es que el famoso dicho aquel de que lo que pasa en Las Vegas se queda en Las Vegas, ahora dicen que

lo que pasa en Las Vegas se queda en Facebook, en Twitter, en YouTube, en todos lados; y es un poco lo que pasa en este vídeo, que es una cámara oculta en Bruselas.

[VÍDEO]

Yo creo que miedo no tiene que dar, pero sí respeto. Y sí tener un poco de sentido común en nuestras actuaciones, ¿no?

¿Qué es lo que está pasando y qué es lo que considero yo un poco que está pasando? Que en poco tiempo demasiados cambios; nos ha pillado a todos un poco... Hay una generación que sí, que son los famosos nativos digitales; hay una generación de transición que somos nosotros, que nos vamos adaptando como podemos; y luego hay los que han tirado la toalla y que pasan de todo y que no quieren saber nada. Pero es una realidad que está ahí, y que tenemos que adaptarnos como sea los que podamos, y que los otros vienen tirando y empujando muy fuerte.

Entonces, yo creo que la clave es adaptarnos a esa tecnología. Y luego, lo que decía hace un momento, que creo que a nivel educativo hay una dejadez muy grande por comodidad, porque es muy fácil eso, en vez de ponerte a jugar con el niño o tal, tú estás muy cansado que acabas de trabajar, y lo enchufo y así no me marea a mí.

Y una gran cosa, y entono el mea culpa yo también: una falta de ejemplo por parte de los mayores; no puedes estar diciendo que dejes ahí el móvil y estás tú con el Twitter, que no puede ser. Y creo que hay una falta de empatía y de respeto hacia estos menores.

Entonces, dentro de lo que a mí se me ha venido un poco a la cabeza, y fue por lo que rehice la presentación pensando en esto, pues se me ocurre de todo; lo primero, dar ejemplo, para mí es imprescindible, predicar con el ejemplo es fundamental. Creo que acompañar a los menores en el camino de esto es fundamental. ¿Cómo? Pues educando, enseñando, dando responsabilidad. Yo creo que eso lo consideran, es como un premio, dar esa responsabilidad. Vuelvo a decir, dar ejemplo. Dar confianza es fundamental; realizar actividades conjuntas. Yo creo que es un medio fantástico, lo que estaba hablando antes, que hay profesores que *motu proprio* están realizando y utilizando los medios sociales para colgar temarios en Internet; crean un grupo en Facebook, por ejemplo, o en Tuenti con sus alumnos para colgar material adicional del que están dando en clase;

y no son unos friquis. Sus alumnos tienen una motivación más. Hay un vídeo, lo que pasa es que dura mucho, y por eso no lo he querido incluir, que es de una escuela que está en Manchester, que mediante la adopción de la tecnología han pasado de un 30% de aprobados —es un barrio marginal de Manchester— a un 98%; han pasado de no recibir ni un duro de la administración porque los resultados eran los que eran a obtener dinero; de hecho, están cambiando el colegio de ubicación, están reformando no sé qué, intentando... ¿Por qué? Porque lo han adoptado. Son chavales que a la adopción de su tecnología le están viendo una utilidad real de lo que pueden tener y el poder que tienen en sus manos. No están metidos en líos, no están teniendo unos problemas de *cyberbullying* como el que pueda haber... ¿Por qué? Porque lo utilizan para trabajar. Es una herramienta más. No es la parte de ocio y en la cual se ven amparados por una pantalla y ese anonimato que ellos creen que tienen que les permite esa impunidad a la hora de meterse con compañeros y de machacar a compañeros. Llegan a casa y dejan la tableta; hacen los deberes o hacen lo que tengan que hacer y la dejan, hasta el día siguiente; es lo que nos pasa muchas veces a nosotros, que llegamos y, ¿ponerte un ordenador en casa?, ni de coña; ¿por qué? Porque llevo todo el día con un ordenador delante. Pues ellos han conseguido eso. ¿Por qué? Porque le ven la utilidad real a esto. ¿Que luego comparten fotos de sus fiestas y tal? Claro que sí, son chavales y son tal. Pero que le ven una utilidad real a todo esto.

Creo que los adultos debemos ser protagonistas en la adopción de las nuevas tecnologías, ser nosotros y que parta de nosotros. Yo creo que es importante tener en todas las casas, y en momentos muy concretos, zonas libres de pantallas; momentos a la hora de cenar, pues eso, que vuelva la comunicación como era antes, no que para pedirle patatas le tengas que mandar un WhatsApp a tu madre porque si no, no se entera, o lo que sea.

Hay que invertir tiempo en esto, no se puede dejar; yo creo que hay que aprender para poder educar, y que estemos los padres es una responsabilidad muy grande a la hora de esto. ¿Los educadores? Igual, yo creo mucho en la palabra «comunidad educativa», comunidad; yo creo que hay que implicar a todos; nadie es menos que nadie y todos los pilares son importantes para esto. Vuelvo a lo de siempre: creo que desde la administración están muy bien las charlas que puedan hacer policía, Guardia Civil... Pero creo que son demasiado negativas, creo que el tono siempre es «cuidado con esto, esto no, esto caca, esto, aquí no toquéis, esto no lo publiquéis, esto no lo hagáis», en vez de decirle «esto muy

bien, esto genial, esto fantástico, ¿por qué no lo hacéis así?». Creo que el tono debe ser un poco al revés de lo que se está haciendo.

Creo que hay que educar para cuidar la intimidad. Tenemos esa manía de exhibirnos, esa manía de mostrarnos vulnerables. Nos pasa a los adultos; cualquier perfil de Facebook de cualquier conocido vuestro, tenemos la manía, no sé por qué, el ser humano —bueno, es por un hecho de intentar buscar el aplauso, el ánimo y la palmadita en la espalda—, tienes un mal día y lo pones ahí, pero no te das cuenta de que lo leen tus amigos (que tendrás 300.000, que no son amigos), lo leen los amigos de los amigos porque te han contestado. Y entonces ahí tenemos un problema. No hay por qué mostrar esas vulnerabilidades, porque hay quien se puede aprovechar de ellas. Entonces, yo creo que educar un poco en materia de intimidad de la gente, es importante. No es que sea una cuestión de educación en ciertos valores.

Creo que hay que crear una serie de normas pero implicando a todos, padres sentados con hijos, creando unas normas, explicando los porqués y que se impliquen todas las partes.

Es muy importante sobre todo el tema de la identidad digital. Volvemos a lo de siempre, lo que pasa en Las Vegas ahora está en todos los lados. Todo lo mal que hagamos en Internet deja rastro. Cada vez se oye más el tema del *branding* personal, el tema de la reputación; empleadores, departamentos de recursos humanos están utilizando las redes sociales para rastrear a la gente, un poco para sacar sus perfiles y estas cosillas. El rastro que vayamos dejando, ahí queda; son pistas que le estamos dando a esta persona, que muchas veces se puede crear patrones equivocados de cómo somos.

Hay conceptos básicos que decía antes que estamos perdiendo un poco y que creo que habría que reforzar en casa y en el colegio, que son temas como el respeto y la empatía. Muchas veces, el tema de ponernos en el lugar; no sé, antes de que hubiese esto, siempre ha habido el vacilado de la clase, que todo el mundo se ensañaba con él y todo eso; el problema es que ahora el escaparate es mundial. Creo que un poco de empatía y fomentar la empatía de los chavales ayuda a disminuir un poco esos efectos de ataque hacia otros.

Vuelvo a decirlo: dar ejemplo, lo digo dieciséis veces en toda esta lista. Fundamental, enseñar. Otras aplicaciones que tienen las redes sociales, lo que hablábamos antes, que no se limiten los chavales a publicar

las fotos, a *memes*, a vídeos, que hay más cosas que se pueden hacer.

Desde las administraciones: intentar controlar lo que indexan los buscadores. Se pueden capar de alguna manera ciertas palabras para que desde Google, desde Bing no se pueda acceder a cierto tipo de páginas. Se ha legislado la ley de *cookies*, por ejemplo, ahora de forma fenomenal, superrápido, y todos amén. Se puede hacer también con el contenido que indexan las tal. ¿Para qué? Para evitar temas de pornografía infantil, enlaces, ese tipo de enlaces a través de palabras clave, eso se puede evitar, que un buscador funcione entrando por ahí.

El tema de la verificación: estamos en un momento en el cual por ley menores de 14 años no pueden tener perfiles en redes sociales. Todos tienen. El tema es que ahora mismo todos se están haciendo con esta tecnología. Coges a un niño con 2 años y maneja un iPhone mejor que ninguno de los que estamos aquí. Ahí tiene las aplicaciones, las descarga, baja, no sé qué y te la enseña, te vacila, y tiene 2 años o tiene 3 años o 4 años el niño. Yo creo que el problema no es la edad, yo creo que el problema es un poco de que sea verdad el que está ahí dentro, buscar fórmulas para aumentar la seguridad en el tema del acceso. Tenemos una cosa maravillosa que ha costado una pasta que es el DNI electrónico, que puede ser a lo mejor un canal fantástico para que sirva de barrera de entrada, para autentificar la entrada. Tenemos la doble verificación que es está empezando a utilizar ahora mediante un código que te llega al móvil, para que lo podamos hacer. No sé, se me ocurren varias cosas.

Creo que es importante el tema de que legalmente, no sé si a nivel estatal o a nivel europeo, una legislación común para que todos los proveedores de este tipo de servicios, redes, utilicen un paraguas legal único. Por ejemplo: aplaudo, y tenemos la suerte de que Tuenti es española y está bajo legislación española, con lo cual cualquier problema se puede atajar, a lo mejor incluso con una llamada. Facebook, es imposible, porque es imposible, si no está donde no sé qué, tienes que llamar a no sé dónde, mandar un e-mail, hablar con uno, el otro no sabe quién es... Es un lío. Twitter, ni os cuento; tenemos algún problema de verificación con alguna cuenta, y es una locura para que solucionen algo, y eso que han montado ahora una delegación aquí en España, pero son delegaciones meramente comerciales, para buscar anunciantes para que dejen pasta. Entonces, a nivel técnico y todo eso, es muy difícil de resolver. Yo creo que eso sería importante que hubiese establecimiento legal de alguna manera, que estuviesen bajo un mismo paraguas.

Insisto, no creo que sea una cuestión de edad. Y luego, no sé, es un guiño, no sé si político o qué, pero creo que a nivel educativo en los centros debería destinarse dinero, independientemente de la situación de recortes y tal de la que se habla, para formar en este tipo de cosas. Yo creo que es fundamental en este momento porque es una cosa que la estamos viviendo, porque está ahí y hacen falta medios.

No podemos sorprendernos y quedarnos con cara de tontos cuando vemos que en Corea del Sur están utilizando iPad los niños de tres años para aprender y todo eso; yo creo que eso lo puede implementar cualquier país. Hay que molestarse, pero hay que formar, hay que reciclar a profesorados, hay que reciclar a padres, hay que formar a los chavales para que vean, como decía antes, la utilidad mayor que tiene este tipo de medios, pero hacen falta medios. Y los medios es con dinero.

Luego, es fundamental volver a lo que decía antes: dar ejemplo. Y el tema de la divulgación es muy importante, ahí sí que también creo que la administración tiene que hacer un trabajo muy grande de divulgación, hablando con medios de comunicación, para que un poco fomenten este tipo de cosas. El tono negativo que muchas veces, cuando hay un caso de *cyberbullying* o hay que... tenemos la manía en este país un poco de ensañarnos en las noticias negativas y en lo malo, y pasa cualquier cosa y, ¡madre mía! Que sí que es malo, y que sí es incorrecto, pero también pasan muchas cosas buenas, y tenemos que contarlas también.

Entonces, yo creo que un fomento a nivel divulgativo; yo me quedo siempre con esta frase, que cuando empiezan a caminar los niños, les damos la mano, no los sentamos para que no se caigan. Entonces, yo creo que tenemos que darles la mano, porque así no se caerán, y avanzaremos nosotros también, que es la segunda lectura que saco de esto.

Y como campaña, un poco, de divulgación, el Ayuntamiento de Sevilla ha hecho esto, que me ha llamado mucho la atención, y os la pongo.

[VÍDEO]

Así que, como decimos en mi tierra, «sentidiño». Y con esto termino. Y cualquier pregunta o cualquier cosa, encantado de responderla. Y muchas gracias.

COMPARECENCIA DEL MÁNAGER DE SOSTENIBILIDAD Y CALIDAD DE VODAFONE ESPAÑA, D. JOSÉ MANUEL SEDES GARCÍA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 2 DE ABRIL DE 2014.

1. *Introducción*

1.1. Presentación

Buenas tardes, Señorías:

En primer lugar, deseo **agradecer** a la Comisión Conjunta de las Comisiones de Interior, de Educación y Deporte, y de Industria, Energía y Turismo del Senado, la **invitación** a Vodafone a comparecer ante la misma para **informar** en relación con las materias objeto de la «**Ponencia Conjunta** de **Estudio** sobre los **Riesgos** derivados del Uso de la **Red** por parte de los **Menores**».

Así mismo, deseo **felicitarles** por la **constitución** de dicha **Ponencia** y por la labor que vienen realizando en este ámbito, con el fin de estudiar y analizar en profundidad, y de forma colaborativa con las diferentes organizaciones implicadas, las **medidas de prevención** contra los potenciales riesgos derivados del uso de la Red por parte de los menores.

Para comenzar, permítanme realizar una breve **presentación de Vodafone**, así como de su **Estrategia de Responsabilidad Corporativa y Sostenibilidad**, en la que se enmarcan las diversas actuaciones que venimos desarrollando en el ámbito del **fomento del uso seguro y responsable** de nuestros productos y servicios por parte de **menores**.

1.2. Vodafone

Vodafone es una de las **mayores compañías** de telecomunicaciones del mundo **por ingresos** (44.445 millones de Libras en ejercicio 2012-13), con **presencia en 30 países y acuerdos en otros 50** países de todo

el mundo. El Grupo Vodafone proporciona un abanico completo de servicios de **telecomunicaciones móviles y fijas**, incluidas comunicaciones de voz y de datos, para el acceso de **419 millones de Clientes** proporcionales (dato a 31 de Diciembre de 2013; esto supone que 1 de cada 5 móviles en el mundo están conectados a una red de Vodafone).

De esta forma, los más de **13,6 millones** de Clientes de **Vodafone España** (a 31 de Diciembre de 2013) se benefician de la experiencia y capacidad de esta empresa líder mundial, que ayuda a sus Clientes —individuos, negocios y comunidades— a estar mejor conectados.

La **Estrategia de Responsabilidad Corporativa y Sostenibilidad** de Vodafone refleja nuestra **visión** de contribuir a lograr una **vida más sostenible** para todos los miembros de la sociedad. Para ello, nuestra Estrategia de Responsabilidad Corporativa y Sostenibilidad contempla **dos áreas** de actuación generales:

- El **Desarrollo de Productos y Servicios** para conseguir Sociedades más Sostenibles, lo cual incluye:
  - Tanto Productos y Servicios **Sociales** para mejorar la calidad de vida y la integración social de personas con necesidades especiales (personas con capacidades diferentes, personas mayores, enfermos crónicos, víctimas de la violencia de género, etc),
  - Como Productos y Servicios basados en soluciones inteligentes Máquina a Máquina (**M2M**) para ayudar a otros sectores a reducir su contribución al cambio climático.
- La aplicación de **políticas de comportamiento ético y responsable** en nuestra relación con Clientes, Proveedores, Empleados y el Medio Ambiente.

En este sentido, somos conscientes de que para conseguir la **confianza** de nuestros diferentes **Grupos de Interés**, es fundamental desarrollar nuestras actividades de una **forma ética y responsable**. De esta forma, nuestros clientes utilizarán nuestra tecnología, productos y servicios, y podremos contribuir a **mejorar la calidad de vida de las personas y a transformar las sociedades** en las que vivimos.

Por este motivo, en Vodafone la **seguridad en Internet** siempre ha sido una **prioridad**, y venimos ***fomentando el uso seguro y responsable*** de nuestros productos y servicios, en ***colaboración*** con las Administraciones, ONGs, otras empresas del sector, etc, durante ***más de una década***. A este respecto, desarrollamos e implantamos diversas **herramientas de seguridad e iniciativas educativas** y de concienciación, habiendo sido el ***primer operador móvil en lanzar controles parentales en 2005***.

2. *Antecedentes*

2.1. Uso de Internet por Menores

Las **nuevas tecnologías** se han convertido en una **parte fundamental de la vida diaria** de las personas y las organizaciones. Como evidencia de ello, según cifras del Instituto Nacional de Estadística, el 95,2% de los menores entre 10 y 15 años utilizan el ordenador, y el 91,8% **Internet**.[1]

Internet es una poderosa herramienta que ofrece multitud de plataformas, recursos e información, y durante los últimos años estamos siendo testigos de la amplia proliferación de las **redes sociales**. El **uso** de este tipo de plataformas por parte de los **menores** está **muy extendido**. Así, según el estudio del proyecto de investigación sobre Conductas Adictivas a Internet entre los adolescentes europeos (EU NET ADB), el 92% de los menores podrían ser miembros de al menos una red social[2]. Si comparamos este dato con el porcentaje de personas entre 25-54 años que tienen perfiles en redes sociales, que supone un 60% según el último Eurostat[3], podremos darnos cuenta de la elevada penetración que este tipo de plataformas tiene entre los menores.

---

[1] Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (TIC-H). Año 2013. Instituto Nacional de Estadística (http://www.ine.es/prensa/np803.pdf).

[2] Investigación sobre conductas adictivas a Internet entre los adolescentes europeos. Editores: Artemis Tsitsika, Eleni Tzavela, Foteini Mavromati and the eu net adb Consortium (http://www.protegeles.com/docs/estudio_conductas_internet.pdf).

[3] Eurostat http://www.theparliament.com/digimag/sid2014

Por ello, se puede considerar a los **menores** como un **colectivo que conoce y domina estas plataformas** (son expertos tecnológicos, mientras que sus padres se esfuerzan en mantenerse al día); aunque al mismo tiempo, se da la **paradoja** de que es un **colectivo vulnerable si no tienen** una correcta **formación y/o** no cuentan con **herramientas** para poder navegar de forma segura, ya que este ambos tipos de medidas son necesarias para prevenir y reducir los riesgos.

Por otra parte, estamos asistiendo a un rápido crecimiento en el número de «**Smartphones**» (o teléfonos inteligentes), que conlleva en paralelo un **significativo número de menores** que acceden a estos dispositivos. En este sentido, es preciso tener en cuenta que, según un estudio realizado por la GSMA (Asociación Internacional de Operadores Móviles)[4], el 65% de los menores entre 8 y 18 años tiene acceso a un teléfono móvil. En el caso de **España**, uno de los países con mayor penetración de Smartphones, el **63% de los menores posee un teléfono móvil**[5]. El **uso** que le dan a este dispositivo es principalmente el acceso a **Internet**, aunque también destacan otras actividades tales como la descarga y el uso de **Aplicaciones** móviles.

Estos datos suponen que las **familias** en general están ahora hiperconectadas, al estar **equipadas** con **diversos** tipos de **dispositivos conectados a Internet**; de hecho, se puede percibir la evolución creciente desde la disponibilidad de un único dispositivo compartido (ordenador de sobremesa, portátil o netbook), a un amplio abanico de otros tipos de pantallas personales (tablets, smartphones, video-consolas) con las que acceder a Internet, ver programas de TV o jugar online.

En definitiva, los **móviles,** y las preocupaciones por la seguridad de los menores, han **cambiado de forma sustancial en los últimos 5-10**

---

[4] Children's use of mobile phones 2012: An international comparison GSMA http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA-ChildrenES_Spanish2012WEB.pdf

[5] Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (TIC-H). Año 2013. Instituto Nacional de Estadística (http://www.ine.es/prensa/np803.pdf).

años, en términos de tipos de dispositivos a los que pueden acceder los menores, la forma en la que acceden a la información, y los tipos de comunicaciones. Ya no estamos hablando de voz, texto o portales de internet seguros. No es suficiente ubicar un PC en un lugar común del hogar para que los niños estén seguros.

En este contexto, y teniendo en cuenta los numerosos beneficios que representan las nuevas tecnologías (a los que me referiré posteriormente), su **uso seguro y responsable** se presenta como un **reto para las familias**, ya que en muchos casos se sienten desprotegidos por **carecer de las competencias digitales o conocimientos tecnológicos** suficientes en comparación con sus hijos.

Por otra parte, hay que tener en cuenta que la tecnología avanza cada vez más rápido, por lo que las **herramientas de control y los contenidos educativos** para el uso seguro y responsable, **deben ser flexibles y actualizables fácil y rápidamente,** para que se puedan adaptar a los cambios que se vayan produciendo.

Otro hecho relevante en el uso de las nuevas tecnologías por **menores** es que éstos hacen un **uso cada vez más temprano** de las mismas. Así, por ejemplo, el regulador de las comunicaciones en Reino Unido (Ofcom), ha realizado una investigación sobre los hábitos de consumo de las nuevas tecnologías por los menores entre 3 y 4 años, en la que se revela que este colectivo utiliza diferentes dispositivos para acceder a Internet, destacándose que más de una tercera parte (concretamente, un 37%) utilizan el ordenador (ya sea de sobremesa, portátil o netbook).[6]

Por otra parte, **Vodafone**, junto con **YouGov** (empresa de investigación de mercados a través de Internet)[7], realizó en **España** en Octubre de 2013 un **estudio** basado en una encuesta a padres y menores sobre el uso de Internet. Este estudio puso de manifiesto, entre otros aspectos, que el ***uso por menores de los dispositivos con acceso a Internet es elevado***, si

---

[6] Significant rise in children's texting and time spent online , 23 octubre, 2012 http://media.ofcom.org.uk/2012/10/23/significant-rise-in-children%E2%80%99s-texting-and-time-spent-online/

[7] Children's Internet Information Vodafone & YouGov 26 octubre 2013.

bien el ***conocimiento de los potenciales riesgos es reducido***. Así, entre los principales datos de este estudio cabe destacar que:

- El 51% de los niños entre 4 y 10 años utilizan Smartphones, un 57% tablets y otro 57% ordenadores (de sobremesa, portátiles o netbooks). Además, la **penetración de las tecnologías sigue en aumento**, ya que un 10% de los padres tenía previsto comprar en la Navidad de 2013 dispositivos con acceso a Internet para niños menores de 4 años (y en un 70% de los casos, los dispositivos serían tablets).
- Las **fuentes de información** que utilizan los **menores para aprender sobre el uso de Internet** son, en la mayor parte de los casos los **padres** (el 84%), un porcentaje muy por encima de los **profesores** (el 27%), o de los **hermanos o amigos** (el 24%). Estos datos reflejan la ***importancia*** que tiene ***proporcionar información a los padres sobre el uso seguro y responsable de Internet***, ya que, al mismo tiempo, un 35% de los padres indicó que no disponían de suficiente apoyo para informar a sus hijos.
- Este estudio también refleja la existencia de **reglas básicas de uso**. Las más comunes son las referidas a las **páginas que pueden visitar** los menores (el 75% de los casos) y al **tiempo** que pueden navegar por Internet (el 81% de los casos). Ahora bien, estas normas de uso en muchas ocasiones **no contemplan precauciones básicas** para la navegación segura en Internet, como por ejemplo, **cómo actuar ante contactos a través de internet:** así, aunque el 57% de los menores saben que no es tan seguro hablar con amigos conocidos a través de Internet, como con los conocidos en persona; sin embargo, sólo el 35% son conscientes de que los contactos de Internet podrían estar simulando ser alguien que no son.
- Como he comentado anteriormente, la **adopción de las nuevas tecnologías es cada vez más temprana**. Por ello, como se destaca en los grupos de trabajo («focus groups») llevados a cabo por Vodafone, es ***necesario informar a los menores sobre los aspectos de seguridad en Internet***. La educación puede evitar o reducir situaciones como la que refleja el estudio realizado por Vodafone y YouGov, en

el que un 72% de los niños de 6 años habían usado Internet, pero un 17% de ellos no había recibido información de sus padres sobre seguridad en Internet. Una de las mejores formas para que los menores hagan un uso seguro y responsable de Internet, es la existencia de un **diálogo continuo de los padres con los menores, mostrando interés en sus «vidas digitales»** y crear un nivel de **confianza** donde los menores puedan hablar con sus padres sobre los temas de seguridad en Internet.

2.2. Beneficios y Potenciales Riesgos

2.2.1. *Beneficios*

Son innumerables los beneficios que ofrece Internet en el **ámbito educativo** y en este sentido se han realizado diversas investigaciones sobre la **aplicación de las nuevas tecnologías al aprendizaje**. Por ejemplo, los estudios realizados por los proyectos National Writing Project y Pew Research Center's Internet & American Life Project, destacan que el 78% de los profesores afirman que **estas herramientas refuerzan la expresión personal y la creatividad** de los estudiantes.[8]

Internet es el repositorio de información más grande de la historia y la información contenida aumenta de forma exponencial. Por ello, se presenta como una **herramienta muy beneficiosa para los estudiantes**, ya que **les ayuda en sus necesidades de información**. Los profesores están de acuerdo en que la aparición de los **motores de búsqueda ha facilitado la obtención de información** de manera más rápida y cómoda. En este ámbito, una parte importante de la **labor de los docentes** debe ser enseñarles a diferenciar lo valioso de lo que no lo es, las fuentes que son fiables de las que no, evitando así que los estudiantes puedan sentirse abrumados por la cantidad de contenidos disponibles.[9]

---

[8] National Writing Project and Pew Research Center's Internet & American Life Project http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_NWP%20Writing%20and%20Tech.pdf

[9] http://www.pewinternet.org/2012/11/01/how-teens-do-research-in-the-digital-world/

Por otra parte, las **Redes Sociales** son una **importante herramienta de comunicación**: ayudan a los menores en sus necesidades de socialización, parte fundamental en su desarrollo como personas. Además, permiten establecer comunicaciones de una manera directa y bidireccional con la gente de su entorno.

2.2.2. *Potenciales Riesgos*

El **uso incorrecto** de Internet, puede suponer algunos **riesgos**, y una **parte significativa** de ellos están relacionados con **daños contra la imagen y el honor** de las personas.

Así, uno de los problemas más comunes a los que se pueden enfrentar los menores es el «**cyberbullying**» o acoso online. Según los datos del estudio realizado por el proyecto de investigación sobre conductas adictivas a Internet entre los adolescentes europeos (EU NET ADB), el 21,9% de los menores han experimentado en algún momento acoso a través de las nuevas tecnologías, y aunque **España es uno de los países con niveles más bajos de «cyberbullying»**, es una cuestión que conviene abordar[10].

Además del acoso online, existen otros potenciales riesgos para los menores si no utilizan las TIC de manera segura. Uno de ellos es el «**grooming**», que consiste en acciones que lleva a cabo una persona sobre un menor, con un objetivo fundamentalmente sexual. El objetivo puede tener como fin último desde la obtención de imágenes del menor en situaciones sexuales o pornográficas, hasta la posibilidad de establecer contacto físico y presencial con el menor para consumar un abuso sobre éste.

Las **principales preocupaciones** de los **padres** en cuanto a los potenciales **riesgos** del uso de Internet se refieren a:

- **Comportamientos Inadecuados**: ya sea que afecten a sus menores como víctimas o culpables de cyberbullying

[10] Investigación sobre conductas adictivas a Internet entre los adolescentes europeos. Editores: Artemis Tsitsika, Eleni Tzavela, Foteini Mavromati and the eu net adb Consortium (http://www.protegeles.com/docs/estudio_conductas_internet.pdf).

- **Interacción con Extraños**: «Grooming»; malas influencias; reunirse con gente contactada a través de Internet
- **Acceder a Contenidos Inadecuados** para los menores: contenidos para adultos, violentos, sexting
- **Control del Coste**: Facturas elevadas; costes por descargas y usos de Aplicaciones
- **Uso Excesivo**: Distracciones; Adicción
- **Perfil Digital**: Consecuencias futuras de un comportamiento inadecuado en Internet, tales como dejar una «huella digital» de la que no se pueda librar y que afecte a su reputación
- **Difusión de Información Personal**: Nombre, dirección, email, ubicación, etc.

Si bien los potenciales riesgos existen, es necesario destacar que la ***concienciación y sensibilización*** sobre la utilización de las nuevas tecnologías de una forma segura y responsable, ***ayuda a reducir estos potenciales riesgos***.

La concienciación y sensibilización es una ***tarea a realizar conjuntamente*** entre los distintos actores dentro de la sociedad, tales como: empresas del sector, fundaciones, organismos públicos, administraciones, padres, instituciones educativas, fuerzas y cuerpos de seguridad, etc.

3. *Iniciativas Sectoriales*

3.1. Internacionales

Promover el **uso seguro y responsable** de Internet y las Nuevas Tecnologías por parte de los **menores** es uno de los objetivos principales de la **Comisión Europea** y uno de los pilares de la **Agenda Digital Europea**, que está cobrando una especial relevancia en la actualidad, tanto por el intenso trabajo de la propia Comisión, como por la cantidad de iniciativas de autorregulación del sector.

Desde nuestro punto de vista, la **función principal** del **sector** en esta materia debe ser **ofrecer las herramientas** y los recursos necesarios a

padres y menores para conseguir que estos últimos utilicen las TIC de forma segura y responsable.

Además, el sector de las TIC está especialmente **implicado en la sensibilización y concienciación** en el uso seguro y responsable de las nuevas tecnologías por parte de los menores. En cualquier caso, hay que destacar, como indicaba anteriormente, que ésta es una ***cuestión de responsabilidad compartida*** entre todas las partes involucradas, que requiere la implicación y colaboración entre todos los agentes. Así, el sector está desarrollando en el ámbito internacional multitud de iniciativas orientadas a la **sensibilización.** A continuación enumero brevemente algunas de ellas:

- En primer lugar, es preciso señalar las **iniciativas** de la Asociación Internacional de los Operadores Móviles (**GSMA**). Esta Asociación **fomenta entre sus miembros la adopción de un *enfoque auto-regulador*** en materia de uso seguro y responsable por parte de los menores, que es reconocido por la Comisión Europea. La auto- regulación es un enfoque ***eficaz porque permite adaptarse con agilidad a los cambios tecnológicos*** que son cada vez más rápidos debido al continuo desarrollo de plataformas y servicios (audiovisuales, contenidos, aplicaciones…).
  - Así, la rama europea (GSME) de esta Asociación estableció en 2007, a solicitud de la Comisión Europea, un documento de autorregulación denominado **Acuerdo Marco Europeo** («European Framework») **para el uso más seguro del móvil por los menores**. Este Acuerdo fue firmado el 6 de febrero de 2007 (aprovechando el Día de Seguridad en Internet) por 15 operadores móviles de la GSME ante la Comisión Europea, y se comprometían a implantarlo a través de **Códigos de Conducta nacionales**, que debían ser desarrollados antes de febrero de 2008.
  - Otra iniciativa internacional relevante de la GSMA es la «**Alianza Móvil contra Contenidos de Abusos Sexuales a Menores**» («Mobile Alliance against Child Sexual Abuse Content»), de la que Vodafone es miembro fundador. Esta Alianza, fue presentada durante el Congreso Mundial de Móviles («Mobile World

Congress») de 2008 y la integran los **principales operadores de telefonía móvil** (más de 90 operadores, en más de 30 países, apoyan esta Alianza). Sus objetivos son, por unas parte, proporcionar consejos sobre mejores prácticas y apoyo a los operadores móviles en el mundo con el fin de obstruir el uso de las redes y servicios móviles por individuos u organizaciones que desean consumir o beneficiarse de los contenidos de abusos sexuales a menores, y por otra parte, proporcionar apoyo y colaboración a las fuerzas y cuerpos de seguridad de los diferentes países que investigan tales actividades.

Cumpliendo con dicho objetivo, Vodafone dispone de sistemas que, como detallaré posteriormente, impiden el acceso a este tipo de contenidos ilícitos en el entorno de Internet móvil, siguiendo los criterios de las Bases de Datos de la Internet Watch Foundation (IWF), Fundación auspiciada por la Unión Europea que identifica y registra las url's con contenido de abusos sexuales a menores.

- Por otra parte, para dar respuesta a las necesidades de los menores en el mundo digital, la Comisión Europea ha puesto en marcha la **Coalición de los Consejeros Delegados** («CEO Coalition»), una iniciativa promovida por la Comisaria Neelie Kroes, **lanzada del 1 de diciembre de 2011** y basada en **cinco objetivos**, en cuya implantación se establecía un periodo de 18 meses. Los **cinco objetivos** se refieren a:
  - La **Clasificación de Contenidos** por Edad: Especial atención a los generados por usuarios y los de Apps Stores; Fomento de tecnologías que etiqueten contenidos.
  - La disponibilidad de **Controles Parentales** de fácil configuración.
  - El desarrollo de **Botones de Denuncia** de Contenidos de Abusos Sexuales a Menores: Direccionando a una Línea de Denuncia o «Hotline»; Visible, fácilmente reconocible e identificable en todas las pantallas (PC, TV, smartphones, consolas, etc).
  - Los Mecanismos de **Notificación y Retirada** de Contenidos: Implementación de la Directiva de Lucha contra los Abusos Sexuales, la explotación sexual de los niños y la pornografía infantil.

– **Privacidad por Defecto**: Centrado en Redes Sociales; Información y Advertencias Comunes ante cambios en la configuración de privacidad

- Entre las iniciativas sectoriales internacionales también merece ser destacada la denominada **Principios TIC** («ICT Principles»), de la que también forma parte Vodafone. Estos Principios establecen un Código de Conducta común para el desarrollo de productos y servicios que promueven el uso seguro y responsable de dispositivos y servicios online por menores en la Unión Europea. Esta iniciativa aspira a ayudar a los usuarios de Internet a enfrentarse a los potenciales retos o riesgos que puedan derivarse de su uso. Los Principios considerados son:
  - Clasificación de Contenidos no adecuados y control de Acceso
  - Controles Parentales: Herramientas y distintos niveles de seguridad para operadores, fabricantes de terminales y proveedores de contenidos
  - Notificación y Bloqueo de contenidos o comportamientos inadecuados
  - Contenidos de Abusos Sexual Infantil: Retirada de contenidos en colaboración con autoridades judiciales
  - Gestión de la Privacidad de menores
  - Educación y Concienciación

Siendo Internet una de las principales fuentes de información, educación y entretenimiento, desde la iniciativa Principios TIC se ***considera vital una colaboración conjunta de todas las partes implicadas***. Por ello, son miembros de esta iniciativa los agentes más importantes del Sector de las Telecomunicaciones e Internet, y en 2012 firmaron los Principios a seguir para promover la seguridad de los menores que usan productos y servicios que las compañías de esta iniciativa ofrecen, tales como, plataformas de conectividad, servicios online, conexión a Internet, videojuegos, etc.

- Por último, también es preciso mencionar la celebración anual del **Día Internacional de la Internet Segura** (Safer Internet Day): iniciativa de las organizaciones **Inhope e Insafe**, con la **Comisión Europea**, y en la que colabora Vodafone. Por ejemplo, la edición celebrada este año 2014, con el lema «Juntos por una Internet mejor», ha tenido por objetivo hacer un llamamiento a todos los públicos de interés para crear juntos una Internet mejor y más segura para los menores. Esta iniciativa **implica a los diferentes agentes** (sector TIC, padres, educadores, menores, Administraciones, Fuerzas y Cuerpos de Seguridad, etc) que deben trabajar conjuntamente para conseguir su objetivo principal. En palabras de la vicepresidenta de la Agenda Digital Europea, Neelie Kroes, *«hay que avanzar juntos; la seguridad de los menores debe ser una colaboración y no una competición.»*

El evento «Safer Internet Day» comenzó realizándose sólo en Europa y ahora se realiza en más de 100 países. Desde esta iniciativa **se considera Internet** como una **poderosa herramienta**, que **ayuda** a los menores **a aprender, a jugar, a interactuar con otros y a explorar**. Si bien hay que ser conscientes de que no está libre de **algunos potenciales riesgos**. Por ello, esta iniciativa busca crear un Internet mejor, asegurando unos **contenidos de calidad y seguros** en la red.

3.2. España

A nivel nacional, deseo destacar la gran evolución en las **iniciativas** desarrolladas desde la **Administración** en respuesta a la necesidad de una mayor **concienciación y protección de los menores** ante los potenciales riesgos de las nuevas tecnologías. A este respecto, me consta que les han sido presentadas a sus Señorías excelentes iniciativas desarrolladas por Red.es, chaval.es, INTECO, etc.

Como decía anteriormente, el **sector** está facilitando **herramientas** para ayudar a que se utilicen los dispositivos con acceso a Internet de manera segura y responsable, y está participando en iniciativas de **sensibilización y concienciación**.

En este sentido, Vodafone firmó en Diciembre de 2007, junto con los principales operadores móviles en España, el denominado **Código de Conducta** para el Fomento del Uso Seguro y Responsable del móvil en el acceso a contenidos, en cumplimiento del compromiso del anteriormente citado Marco Europeo de implantar este Marco en cada país de la UE, convirtiéndose **España** en el **primer país de la UE en disponer de un Código de Conducta en aplicación del Marco Europeo**.

Este Código de Conducta tiene por objetivo la promoción y fomento de un uso seguro y responsable de las telecomunicaciones móviles y los contenidos, propios y de terceros con los que haya suscrito un acuerdo contractual. En él se incluyen **cuatro líneas de actuación** generales: sistemas de clasificación de contenidos comerciales; mecanismos de control de accesos; educación y concienciación; y lucha contra contenidos ilícitos en Internet.

- En la primera línea de actuación, los operadores hemos acordado unos **criterios de clasificación de contenidos,** basados tanto en estándares internacionales como en la clasificación del Ministerio de Cultura. Además, se anima a las **asociaciones de proveedores de contenidos** a colaborar activamente en el etiquetado de contenidos según la clasificación acordada por los operadores.
- En línea con dicha clasificación de contenidos, los operadores móviles ponemos a disposición de nuestros clientes **herramientas** para facilitar el **control de acceso** a contenidos clasificados como no adecuados para menores
- Las herramientas y soluciones de control de acceso deben ir acompañadas de iniciativas de **educación y concienciación**. Por ello, los operadores móviles hemos puesto a disposición de nuestros clientes mecanismos, orientados fundamentalmente a padres y tutores, para ampliar la información sobre uso seguro y responsable de los dispositivos móviles por parte de los menores. Siendo conscientes de que fomentar un uso seguro y responsable de las nuevas tecnologías es **trabajo de diferentes actores** de la sociedad, los operadores móviles venimos colaborando con administraciones públicas, centros

educativos, instituciones de investigación sobre menores y adolescentes, asociaciones y ONGs expertas en la materia. En esta línea se incluyen por ejemplo actividades de **Voluntariado Corporativo,** en las que nuestros empleados participan en jornadas de formación y sensibilización en colegios dirigidas a menores.

- Los operadores móviles además venimos **colaborando con las Fuerzas y Cuerpos de Seguridad en la lucha contra los contenidos ilícitos**, como por ejemplo, la tramitación de mandamientos judiciales en los que se solicitan la retirada o el bloqueo del acceso a contenidos ilegales. En el ámbito de la lucha contra los contenidos ilícitos, se pueden destacar los lanzamientos por los operadores móviles, junto con la organización Protégeles, de la iniciativa «**Protege a la Infancia**» en febrero de 2011, que consiste en un **botón** que permite **denunciar**, a través de las **web de los operadores**, imágenes sobre abuso infantil de forma anónima, simple y directa. Este lanzamiento fue complementado en 2012 con el desarrollo de la **aplicación móvil «Protege a la infancia»** diseñada para dispositivos con sistema operativo Android.

Este Código de Conducta cuenta con un **Comité de Seguimiento** que se reúne periódicamente para asegurar el cumplimiento de los compromisos del Código.

4. *Iniciativas de Vodafone*

4.1. Grupo Vodafone

Uno de los objetivos de la **Estrategia de Responsabilidad Corporativa y Sostenibilidad** de Vodafone consiste en que el **uso** que hagan los menores de nuestras tecnologías, productos y servicios se enmarque **dentro de la seguridad y la responsabilidad**. Por ello, hacemos especial hincapié en proporcionar **herramientas y recursos** desarrollados **para padres, tutores y los propios menores,** que sean **fáciles de usar y de diseño atractivo** para el público al que van dirigidos. De esta forma, pretendemos realizar una labor conjunta con estos públicos para ***reducir***

o evitar una brecha entre los conocimientos que sobre las nuevas tecnologías tienen respectivamente los menores y los padres.

Entre las **actividades** que se vienen realizando por **Vodafone** se pueden destacar:

- El desarrollo de **herramientas e iniciativas educativas**, según las necesidades de los públicos.
- La participación activa en el diseño de la **auto-regulación del sector**, de la cual he hablado anteriormente («European Framework», o Código de Conducta en España), con el fin de garantizar que todos los implicados (fabricantes, proveedores de acceso a Internet, proveedores de contenidos, etc) asumen su responsabilidad por sus productos y servicios.
- La **colaboración** en iniciativas del sector, compartiendo recursos para aumentar la eficacia, especialmente en relación con los temas de educación. En este ámbito es preciso señalar la colaboración del Grupo Vodafone con el Instituto sobre Seguridad Online de las Familias (FOSI, «Family Online Safety Institute»).

Por ejemplo, en Reino Unido colaboramos con «The Parent Zone» (reconocida organización en Reino Unido que proporciona información, ayuda y recursos para padres, profesores, policía, etc) para crear la **revista «Digital Parenting»,** de la que se imprimen más de un millón de ejemplares (de las cuales, 843.000 son distribuidas a colegios), o la **aplicación «Guardian»** que está implantada en 23 países, con más de 500.000 descargas (en España se llama «Vodafone Safety Net», de la que posteriormente ampliaré información).

En cuanto a **auto-regulación**, es preciso destacar que Vodafone es miembro de diferentes organismos e iniciativas relacionadas con la promoción del uso seguro y responsable de los productos y servicios de telecomunicaciones por los menores, tales como:

- El **Marco Europeo** («European Framework») para el fomento del uso seguro y responsable de dispositivos móviles por menores.
- La iniciativa **Principios TIC** («ICT Principles») y la **Coalición de los Consejeros Delegados** («CEO Coalition», establecida por la

Comisión Europea) que comparten los mismos principios en cuanto a la promoción de una Internet segura para los menores,

- La **Alianza Móvil contra los Contenidos de Abusos Sexuales a Menores** («Mobile Alliance against Child Sexual Abuse Content»), establecida por la GSMA, donde Vodafone ofrece apoyo, buenas prácticas e información en esta materia, o
- La **Internet Watch Foundation** (IWF), especializada en la lucha contra los contenidos en la red sobre abusos sexuales a menores, y que mantiene actualizada permanentemente Bases de Datos de este tipo de contenidos, y que Vodafone utiliza en sus sistemas para impedir el acceso a los mismos Vodafone lleva **una década desarrollando herramientas** para que los menores naveguen de forma segura. Así, en **2004 Vodafone Reino Unido fue el primer operador móvil en ofrecer un filtro online en toda su red 3G para proteger a los menores**, en el que se incluían la lista de contenidos bloqueados sobre abusos sexuales a menores, desarrollada por la Internet Watch Foundation. En 2007 se implantaron filtros similares en las redes de Vodafone de otros países, adecuándolos a la ley y a la cultura de cada país.

También, se pueden destacar los **procedimientos** denominados **«Notificar y Eliminar»** («Notice and Takedown») implantados por Vodafone, con el objetivo de asegurar que el contenido ilegal o inapropiado se borra o se gestiona de manera adecuada en servicios propios como «Vodafone Cloud».

4.2. Vodafone España

En el caso concreto de Vodafone España, hemos desarrollado **3 tipos de controles parentales** para dispositivos móviles con el fin de clasificar y proteger a la infancia de contenidos no adecuados para ellos.

- El primer tipo de control parental es el denominado **«Perfil Joven»,** que bloquea el acceso a aquellos **contenidos propios** clasificados como **no recomendados para menores de 18 años**.

- El segundo tipo de control es el **«Filtro Off-net»,** que bloquea el acceso a las **páginas de Internet** que están clasificadas para **adultos**.
- El tercer tipo de control parental consiste en la **aplicación móvil** para «Smartphones» con sistema operativo Android, llamada **«Vodafone Safety Net».** Esta aplicación, sencilla y gratuita, permite a los padres personalizar la configuración del dispositivo móvil que usen los menores en base a la edad y madurez de éstos, y el proceso de configuración está gestionado a través de una contraseña establecida por los propios padres.

Con esta aplicación los padres tienen mucho más control sobre cómo y cuándo sus hijos usan el «Smartphone». Así, los padres pueden permitir, limitar a ciertas horas, o bloquear funcionalidades del dispositivo, tales como: llamadas entrantes y salientes, mensajes entrantes y salientes, wifi, bluetooth, cámara, navegador, configuración del teléfono, así como añadir, usar o eliminar aplicaciones.

También permite a los padres o tutores configurar un contacto telefónico del responsable, el cual recibirá un mensaje de texto en determinadas ocasiones, como por ejemplo, cuando se realice una llamada de emergencia desde el teléfono o cuando la aplicación se elimine o se desactive.

Por otra parte, y como complemento a las herramientas anteriores, Vodafone España ha desarrollado en su web un **«Portal para Padres»,** que contiene información sobre:

- Las actividades de Vodafone en esta materia y sobre las **herramientas de control parental** que pone a disposición de padres y tutores,
- Las **iniciativas sectoriales** en las que Vodafone participa,
- Información sobre la **configuración** de la aplicación «Vodafone Safety Net», y de otras herramientas como los controles de privacidad de Facebook o los controles parentales integrados en Microsoft, así como información para descargarse los filtros de «Google Safesearch», e

- Información práctica y **recomendaciones** dirigidas especialmente a los padres y tutores que tienen niños y jóvenes a su cargo. Esta información es proporcionada en forma de **Decálogo** con consejos útiles para que los padres y tutores estén mejor informados a la hora de ayudar a sus hijos a navegar de manera segura.

Como decía anteriormente, la **educación** en nuevas tecnologías es **siempre necesaria**, si bien es aún **más importante** cuando los menores son **más pequeños**, ya que a medida que se hacen más mayores son menos receptivos a los consejos de padres y tutores. Es **mucho más fácil sensibilizar sobre el uso seguro y responsable de las nuevas tecnologías a niños entre 5 y 8 años, que a adolescentes**.

Por ello, hemos creado la **aplicación «Vodafone Kids»,** que consiste en un espacio con actividades educativas para menores entre 2 y 6 años, en donde se incluyen inicialmente 27 juegos, 10 cuentos, 6 canciones, 12 colecciones para pintar y colorear, y 16 muestras para crear su «foto-aventura» animada; todo ello orientado a acercar la tecnología móvil a menores de estas edades.

En esta línea de la educación mediante el juego, en Noviembre de 2013 Vodafone España desarrolló un conjunto de **tarjetas** denominadas **«Súper - Poderes en la Web»**, que enseñan a los niños diferentes conceptos sobre la seguridad en Internet. Esta iniciativa de protección a menores hasta unos 10 años, se desarrolló a partir de las opiniones de los padres, y la información, que se presenta en forma de juegos sencillos y divertidos, proporciona consejos sobre:

- La importancia de no compartir datos personales con desconocidos en Internet,
- La diferencia entre amigos reales y virtuales,
- Cómo se debe tratar a las personas en la red, o
- Cómo deben actuar los niños cuando encuentren un contenido inapropiado.

Estas tarjetas no están sólo **dirigidas** a los **menores**, ya que también incluyen información útil para **padres y tutores**, sobre las herramientas y materiales que Vodafone España pone a su disposición para favorecer el

acceso adecuado y seguro de los menores a Internet. De esta forma, se pretende proporcionar un **diálogo entre padres y sus hijos** sobre seguridad en Internet en la edad en que los menores lo usan por primera vez, y ayudar a los padres con los **mensajes sencillos** que se requieren para esa edad.

Los **mensajes** de estas tarjetas han sido **creados por expertos** en el uso seguro y responsable por menores de dispositivos con acceso a Internet, y **revisados por Protégeles**, representante en España del Centro de Seguridad en Internet.

Las tarjetas se ofrecen en nuestras **tiendas propias** y también están disponibles a través de nuestra **web**.

5. *Conclusiones*

Para finalizar, me gustaría resumir las **conclusiones** en los siguientes **puntos** que consideramos **clave**:

- El uso de **Internet** proporciona **numerosos beneficios** para los **menores**, aunque al mismo tiempo es necesario que sean conocedores de **potenciales riesgos**. Para ello, es fundamental ***ayudarles a usar Internet de forma segura y responsable***. Como en cualquier nueva experiencia para los menores, el uso de Internet requiere **herramientas y concienciación/formación** en aspectos de **seguridad y supervisión** por los **adultos** para minimizar/mitigar los riesgos.
- Los **operadores móviles** venimos realizando con el desarrollo de ***herramientas e iniciativas para fomentar y concienciar en el uso seguro y responsable*** de nuestros productos y servicios. Ahora bien, esta tarea no es sólo del sector, ya que como destacaba la Comisaria Neelie Kroes, *«hay que avanzar juntos, la seguridad de los menores debe ser una colaboración y no una competición»*. Por ello, es necesario la **colaboración** y trabajo conjunto de operadores móviles, fabricantes, empresas proveedoras de servicios de Internet, administraciones, centros educativos, organizaciones del tercer sector, padres y los propios menores, aportando cada parte sus fortalezas.

- La visión de Vodafone sobre la concienciación y fomento del uso seguro y responsable de las TIC, está basado en dos pilares: Herramientas y Educación.
  – Herramientas como los **controles parentales** que ofrecemos (App Safety Net, Perfil Joven, Filtro Off- net), y
  – El **Material Educativo** que ponemos a disposición de padres, educadores y los propios menores, para que éstos puedan hacer un uso seguro y responsable de las nuevas tecnologías. En esta línea se encuentran el Portal Padres, las Guías o Recomendaciones, el Decálogo para padres o las iniciativas como las Tarjetas «Súper-Poderes en la web». En este sentido, es importante la **involucración y escucha activa con los padres y tutores** para poder ofrecerles los materiales educativos que más les ayuden.
- Aunque el sector TIC, gobiernos, familias, educadores y ONGs vienen realizando esfuerzos para enseñar a los menores cómo usar Internet de forma responsable y dirigirles hacia contenidos apropiados, **queda camino por recorrer,** tanto por la dificultad de los menores para identificar los **nuevos riesgos** derivados de los usos y hábitos inadecuados, como por la **limitación de soluciones tecnológicas y servicios diseñados para ellos, cuestiones en las que el sector está poniendo foco**

Finalizada mi exposición, quería **reiterar el agradecimiento** a esta Comisión su amable **invitación a Vodafone** para presentar nuestros **puntos de vista y actuaciones** en esta materia, y estoy **a su disposición para responder a las cuestiones** que consideren oportuno plantear.

Muchas gracias por su atención.

COMPARECENCIA DE LA DIRECTORA GENERAL DE LA COALICIÓN DE CREADORES E INDUSTRIAS DE CONTENIDOS DIGITALES, DÑA. CARLOTA NAVARRETE BARREIRO, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 2 DE ABRIL DE 2014.

La señora **DIRECTORA GENERAL DE LA COALICIÓN DE CREADORES E INDUSTRIAS DE CONTENIDOS DIGITALES** (Dña. Carlota Navarrete Barreiro): Buenas tardes. En primer lugar, realmente quiero agradecer de forma muy intensa la propuesta de comparecencia y que tengan la tarde de hoy para atender y escuchar de alguna manera las inquietudes que desde las industrias de contenidos nos gustaría que se tomasen en cuenta en los trabajos de esta subcomisión.

Hemos estado observando que es verdad que, constituida ya hace meses, ha sido muy amplio el número de comparecientes y de expertos que han venido trasladando sus inquietudes, y en este contexto quisiera no reiterarles en demasía los contenidos de los que ya se han hecho eco, aunque inevitablemente los mencione de forma puntual nuevamente.

En este sentido, nos ha resultado muy valioso también contemplar que no solamente se ha estudiado desde la vertiente que tenía que ver con la Comisión de Interior, donde está integrada esta subcomisión, sino que se han incorporado también aportaciones desde otro tipo de perspectivas, sea el ámbito de la educación, el ámbito de la cultura, el de la industria o desde otras perspectivas, que sí es verdad que se contemplan en este escenario que tiene que ver con las redes sociales, y para los contenidos creativos en concreto, mucho más que ver.

En esta cuestión les voy a hacer un apunte simplemente, aunque me consta que sus señorías conocen a la perfección, y por eso nos convocan también, la realidad de la Coalición de Creadores, constituida en el año 2008, en abril, con una serie de asociaciones que en el ámbito de los contenidos protegidos por propiedad intelectual comparten una visión crítica de los índices de piratería y de vulneraciones de la propiedad intelectual que cada vez alcanzan unos ratios mayores en el ámbito del Estado español; y contemplando también una vertiente por comunidades autónomas, que yo creo que desde la perspectiva del Senado tiene una gran importancia, que luego comentaré, al final, en las conclusiones, a

raíz de algunas medidas y propuestas que nos gustaría trasladar a esta subcomisión en esta Cámara.

Realmente el objetivo y la misión que tiene la Coalición es potenciar, e impulsar todas aquellas medidas que puedan favorecer una mejor protección de los derechos de propiedad intelectual en el ámbito de Internet, y también fomentar aquellas medidas que puedan entorpecer o dificultar las vulneraciones a los mismos.

En este contexto, y con el ámbito del menor, nos preocupa también de forma muy especial que este ámbito de las redes sociales utilizadas por los menores muchas veces tienen un uso fraudulento para vulnerar estos derechos. En esa concepción, desde luego para las industrias de contenidos a las que represento, que es el sector del libro, el sector del videojuego, el sector del cine y de la música, contemplan al menor como público pero también como sujetos de especial salvaguarda. Ahí todos los productores de contenidos entienden que los menores, a través de los clubes de fans, de sus preferencias culturales, participan en redes sociales que les permite comunicarse con sus ídolos en cualquiera de este tipo de manifestaciones, participar en línea con los videojuegos, participar en foros de literatura, sea Harry Potter o sea de las ediciones del Barco de Vapor; hay todo un universo que valoramos muy positivo del entorno de Internet por cuanto que fomenta el apego desde las primeras edades a los contenidos creativos.

Ahora bien, debemos tener presentes las salvaguardas que tienen que prevalecer respecto del desarrollo del menor y de su personalidad, y un amplio espectro de detalles que sobre esa regulación pueden tener las redes sociales y que también nos inquietan a la hora de proponer medidas y cautelas que puedan mejorar la situación de protección del menor.

En este sentido, nos ha parecido también relevante un informe que les han presentado sobre «**menores en internet**» desde las ONGs de ACPI y Protégeles para el Defensor del Menor, que da cifras sobre para qué acceden los menores a Internet. Veíamos que ahí había casi un 40% que accede a las redes sociales para consumir productos culturales: para compartir música, para compartir videojuegos, para compartir cine.

En este sentido, y contemplando que luego, estos mismos menores se convierten en adultos, manejamos las cifras del último Observatorio de piratería y hábitos de consumo de contenidos digitales que publicaremos

la semana que viene, el 9 de abril, con datos de 2013 de descargas ilegales, y que reflejan que hemos alcanzado un 84% del consumo en España es ilegal. El estudio realizado por la consultora independiente GfK a instancias de las industrias de contenidos representadas en La Coalición, confirma la gravedad de la situación y evidencia un panorama desolador.

En el estudio se detallan **las razones principales** que señala el internauta para acceder a los contenidos de manera ilegal, poniendo de manifiesto la ausencia de un mensaje claro a los ciudadanos por parte de los poderes públicos y la cada vez mayor necesidad de programas pedagógicos. Uno de cada cuatro dice hacerlo porque lo hace todo el mundo y porque no hay consecuencias para ninguna industria y tampoco para el pirata. Esos dos grupos de datos cruzados, de que cuando el niño, el menor accede a Internet el 40% del uso que hace de la red es para ese consumo, y posteriormente, a partir de los 18 años, que es cuando nosotros valoramos ya la encuesta, el 84% consume contenidos no autorizados, nos hace ver que si no tiene una formación y no tiene una educación sobre cómo debe consumir esos contenidos, posiblemente vayamos consolidando una tendencia a que el mercado de las descargas ilegales se afiance en nuestro país. Somos un referente negativo en ese sentido. En otros países del entorno europeo y de los países desarrollados, de los que nosotros siempre hacemos referencia para contemplar las prácticas y usos que funcionan para imitarlas o para incorporarlas a nuestro ordenamiento, tanto las redes sociales como el uso de Internet por menores tienen ciertas salvaguardas respecto a propiedad intelectual.

Para nosotros, las industrias culturales, sería fundamental que en esta subcomisión se pudiesen estudiar estas iniciativas que se toman en el ámbito de los países desarrollados de nuestro entorno, para tratar de aprovechar su experiencia y que hubiese cierta trazabilidad: unas guías prácticas de utilización, unas recomendaciones de qué páginas son adecuadas y cuáles no para menores; realmente por lo que he podido observar en las comparecencias previas, creo que han sido advertidos ya y puestos en conocimiento la mayoría de todos aquellos usos arriesgados que en la red se pueda exponer al menor por contener pornografía, porque puedan obtener datos personales o de los padres, porque a través de lo que parece una simple utilización de una red social por un menor, van aparejados otro montón de cuestiones aparentemente subordinadas, en esa utilización y sin embargo sean estrictamente en ellas las que asociamos a toda una serie de riegos graves para su desarrollo.

Aparecía también en el informe de la Fiscalía de este año, publicado en julio, que había aumentado el número de vulneraciones y de infracciones respecto a la propiedad intelectual, y estas mismas relacionadas con la adquisición de datos personales y de posteriores delitos asociados a esa adquisición de datos personales, como suplantación de personalidad, como robo de datos bancarios, etcétera.

En esta misma línea queríamos comentar que, igual que hemos obtenido el dato de que el 84% del mercado español es realmente contenido ilícito, se dan los datos de que casi se han dejado de crear durante el último año (2013) 26.000 puestos de trabajo en el sector de las industrias culturales; se ha dejado de ingresar por contribuciones de IRPF y por contribuciones de IVA en un escenario sin piratería 526 millones de euros para las arcas del Estado; e igualmente, el valor de lo pirateado ha superado los 16.000 millones de euros.

Esas cifras, relacionadas nuevamente con el ámbito de lo que puede ser unas posibilidades para la valoración de la creatividad, del trabajo creativo, de la cultura en un Estado, nos parecen muy significativas y que realmente reflejan una carencia de formación y de valor en si mismo en el espacio del menor.

Nos gustaría también reseñar a este respecto que hay una serie de recomendaciones que se hicieron por la Comisión Europea, concretamente por la comisaria Neelie Kroes en el año 2012, que casi no hemos incorporado y que nos quedaría trabajo por hacer en ese sentido, y que me gustaría detenerme un momento porque son cuatro apuntes sobre qué se podía hacer en el ámbito de los menores e Internet y que tiene que ver con el espacio en común con las industrias culturales:

En este sentido, según la Comisión Europea:

— En primer lugar, habría que facilitar y fomentar la información, la publicidad y el acceso a los contenidos intelectuales adecuados para el perfil del menor;

— buscar mecanismos de autorregulación con los prestadores de servicios que permitan vías fáciles y ágiles con las denuncias de las infracciones de manera instantánea, y que pudiese evidenciar y detener cuanto antes, de que se constituyan delitos en esta materia;

— reforzar la seguridad y la no vulnerabilidad del menor desde la vertiente del riesgo y de la identificación de estos como usuarios,

accesos a los perfiles de estos, utilización de esta información para el envío de la publicidad y ofertas de todo tipo;

— evitar el riesgo de intrusismo o captación de datos personales o económicos de padres y familiares del menor, vía el registro o el contacto de estos en el acceso de la oferta de contenidos.

En este fomento de la producción de contenidos creativos y educativos en línea destinados a los niños, se podrían desarrollar plataformas que ofrezcan acceso a contenidos adaptados por edad y que pudieran servir de etiquetado. De esta manera aumentar la sensibilidad y la enseñanza de la seguridad en línea en todas las escuelas, con el fin de desarrollar la alfabetización digital y mediática de los niños y la autorresponsabilidad en línea. En este sentido me parece muy importante.

Al menos en la Comunidad Autónoma de Madrid, por ejemplo, ha desaparecido la figura del Defensor del Menor propiamente dicha; y el Defensor del Menor en otras comunidades sí contempla un espacio para este tipo de denuncias.

Creemos que a nivel autonómico es algo que desde el **Senado** sí se podía potenciar, que hubiese algún tipo de agencia de control a nivel de comunidad autónoma que pudiese facilitar y fomentar que, bien desde las escuelas o desde las instancias públicas, si uno conoce que hay una infracción en Internet frente a derechos de propiedad intelectual, que se están utilizando datos de manera irregular, se pudiese poner en contacto o pudiese haber simplemente un seguimiento desde esa institución para que fuese más ágil y rápido detectarlo y actuar al respecto en beneficio del menor.

Aquí, desde las industrias de contenidos, consideramos que el que haya todos los mecanismos de autorregulación y a nivel administrativo, además de poder siempre recurrir al sistema judicial, que desde luego es el más garante, pero que quizá puede tardar años, mientras que el menor ya es mayor de edad y ha tenido que superar todos sus conflictos. Para evitar ese tipo de cuestiones, realmente que pudieran ser muchísimo más participativas, más activas, más instantáneas estas puestas en conocimiento de vulneraciones o usos fraudulentos.

Me consta que hace un par de semanas han tenido la oportunidad de escuchar también al representante de la Federación Antipiratería, FAP, en la que les hacía traslado de muchos de los riesgos que puede haber

en páginas de descargas ilegales de contenidos, tales como pornografía, oferta de juego en línea, acceso a datos personales ...en los que el menor, simplemente por su condición, no es capaz de discriminar esa información, aprovechándose de que les parece atractiva sin contemplar que para ello existe una clara necesidad de madurez intelectual y personal, para poder asimilarla y discriminar que no se pide en ningún momento que acredite.

En ese sentido, también nos gustaría que esta subcomisión, que entendemos que tiene una gran responsabilidad y va a tener un reto de conformar unas conclusiones importantes en la materia, pudiese hacer hincapié o trabajar en esta línea, y en la de exigir el respeto a los contenidos protegidos para contribuir a un escenario dónde los menores respeten la Creatividad y la valoren de forma inherente en el desarrollo de su formación como adultos.

Hagan las preguntas que consideren, les felicitamos por su labor, ha sido un placer poderles compartir nuestras inquietudes. Muchas Gracias.

COMPARECENCIA DEL DIRECTOR GENERAL DE SYMANTEC ESPAÑA, D. JOAN TAULÉ VALDEPERAS, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 2 DE ABRIL DE 2014.

Señores y señoras senadores, me llamo Joan Taule y soy el director general de Symantec para España y el director regional de Symantec para la península ibérica.

Symantec se encuentra en la lista de empresas de Fortune 500 y es líder mundial en seguridad de la información. Nuestras punteras soluciones tecnológicas hacen que el mundo sea un lugar más seguro ayudando a personas, empresas y gobiernos a proteger y gestionar su información para que puedan centrarse en conseguir sus objetivos. Symantec dispone de una amplia red de inteligencia que recopila información procedente de más de 240 000 sensores repartidos por 200 países. Para mejorar la seguridad y la protección, Symantec procesa más de ocho mil millones de correos electrónicos y más de mil millones de solicitudes web cada día.

Me gustaría aprovechar esta presentación para agradecerles en nombre de Symantec esta oportunidad para hablarles hoy sobre este tema de crucial importancia: la protección de las familias y los niños online, y nuestros roles y responsabilidades como padres y madres, sector industrial y legisladores a la hora de proteger a los miembros más vulnerables de nuestra sociedad. Nuestros hijos.

La posición de Symantec sobre este tema se puede resumir diciendo que tenemos la necesidad real de asegurarnos de que protegemos a nuestros hijos en el mundo de internet de la misma forma que lo haríamos en el mundo fuera de internet.

Para ello, todos debemos desempeñar un papel activo. Los padres tienen una responsabilidad fundamental a la hora de educar a sus hijos en el uso de la tecnología y en los peligros relacionados con su utilización. Por supuesto no se puede esperar que los padres y las madres sean expertos en tecnología. El papel de la industria debe ser educar y proporcionar las herramientas necesarias, mientras que los legisladores deben crear un entorno propicio para permitir que estos intercambios se realicen dentro de un robusto marco jurídico y de aplicación de la ley que proteja a los niños.

Cuando hablamos de proteger a las familias y a los niños en internet, hablamos de educarlos siguiendo prácticas recomendadas y utilizando las herramientas tecnológicas apropiadas. Pero nunca se trata de algo exclusivamente tecnológico.

Los padres suelen tener muchas ideas incorrectas sobre cuáles son los verdaderos peligros de internet para sus hijos. Algunos están atemorizados por los agresores sexuales que acechan a los niños en internet. Otros se preocupan por el ciberacoso y otras conductas antisociales; otros por su exposición a contenidos inadecuados o por la pérdida de privacidad. Si bien todas estas preocupaciones están justificadas y, en cierto modo, están influidas por la prensa generalista, lo que posiblemente se acerque más a la realidad es que, dependiendo del grupo de edad del niño, es posible que se tenga que enfrentar a diferentes riesgos.

Los grupos más jóvenes se suelen tener que enfrentar a contenidos inadecuados, mientras que es más probable que los grupos de secundaria tengan que lidiar con conductas sociales inapropiadas, como el ciberacoso en las redes sociales. Es más probable que nuestros hijos mayores se enfrenten a usos inadecuados de las redes sociales pero, además de estos, también deben ser conscientes de los problemas de la privacidad y el cibercrimen.

Sea cual sea el riesgo y el grupo de edad, la primera responsabilidad y línea de defensa de nuestros hijos están en hogares y escuelas. Es el deber de padres y profesores educar a nuestros hijos sobre los riesgos y las amenazas online y sobre lo que representa un comportamiento social adecuado en internet y en las redes sociales con el fin transmitirles que lo que esperamos en su comportamiento fuera de internet se debe reflejar en su comportamiento en internet.

No es tarea fácil. La tecnología evoluciona y los dispositivos habilitados para Internet son algo más que el PC. Ponemos estas tecnologías a disposición de nuestros hijos y, a menudo, ellos son capaces de utilizarlas desde muy pequeños mejor que los padres y maestros.

Sin embargo, es fundamental que a los niños se les enseñen «las reglas de la casa» sobre cómo se espera que usen los dispositivos habilitados para internet de una manera segura y sobre los riesgos a los que se pueden enfrentar online. Symantec anima a padres, maestros y tutores a que se formen sobre algunos consejos básicos y las prácticas recomendadas con respecto a los peligros de internet. También les animamos a

que hablen con sus hijos, de una forma habitual y sincera, para hacerles entender los peligros, para explicarles cómo deben comportarse en internet y para identificar cualquier problema que el niño se pueda haber encontrado en sus interacciones online. Algunas de las tecnologías de Symantec para proteger a las familias online están diseñadas específicamente para fomentar y facilitar un debate y formación transparentes en lugar de llevar a cabo una vigilancia encubierta.

El sector debe desempeñar un papel fundamental en estos esfuerzos por poner a disposición de todo el mundo las tecnologías necesarias para proteger a nuestros hijos en internet. Se deben implantar y utilizar estas tecnologías tanto en el ámbito del hogar y del dispositivo individual como en el nivel de la infraestructura (proveedor de servicios de internet o red de telefonía móvil). Symantec es un proveedor de este tipo tecnologías y las ofrecemos actualmente en España.

También trabajamos con proveedores de servicios de telecomunicaciones y de software de filtrado en la nube. Así, ofrecemos el servicio GURÚ para proteger a todos los usuarios de Telefónica con N360, especialmente para los dispositivos móviles y el uso doméstico en España. También participamos en el proyecto de la fundación BT para educar a las familias sobre cómo comportarse y en la iniciativa de Inteco para la protección de los niños HYPERLINK «http://seguridadinternet.wordpress.com/tag/inteco/» **inteco** | Seguridad en Internet estudios | Redes **Sociales** Móviles)

No obstante, la tecnología no es la solución dorada para todos los males. Es un componente necesario en la construcción de un entorno seguro para los niños. La formación de padres y profesores también es un paso importante. Nuestro sector, en un trabajo conjunto con los gobiernos y la sociedad civil, también desempeña una función fundamental.

Symantec ha trabajado con varias organizaciones no gubernamentales (ONG) de todo el mundo para impulsar la seguridad online y el desarrollo de materiales educativos (sin relación directa con las empresas) para educar e informar a los padres, profesores y niños. En los últimos años, los empleados de Symantec han ofrecido conferencias y charlas sobre este tema en colegios de muchos países de Europa y la empresa ha participado en numerosas iniciativas de concienciación en Europa (en España específicamente con www.Protegeles.com, la asociación Te Veo me Ves, *Fundación Aliad2, fundación BT* y Unicef). Además, Symantec ha involucrado a las ONG en el diseño y desarrollo de algunas de sus

tecnologías de seguridad como Norton Online Family y en el diseño de algunos de sus materiales educativos.

Por último, Symantec publica todos los años el Informe Norton sobre Cibercrimen. Es un exclusivo informe mundial sobre el cibercrimen y sus efectos en los consumidores, la economía y la confianza en internet. El Informe Norton 2013 (llamado antes Informe Norton sobre Cibercrimen) es uno de los estudios más grandes del mundo sobre delitos informáticos que afectan a los consumidores. El informe se basa en la experiencia personal de más de 13 000 adultos en 24 países, incluidos Brasil, Colombia y México. La investigación busca comprender el efecto de los delitos informáticos sobre los consumidores y el impacto producido por la adopción y evolución de las nuevas tecnologías en relación a la seguridad de los consumidores.

Principales temas del Informe:

Coste global del cibercrimen.

Escala del cibercrimen.

Los usuarios están adoptando la movilidad pero dejan de lado la seguridad.

La línea entre el trabajo y el entretenimiento es cada vez más delgada).

Utilizando nuestra información, el Informe Norton sobre Cibercrimen ofrece una visión única sobre los diferentes tipos de ciberamenazas y peligros a los que se enfrentan los consumidores en regiones específicas del mundo.

En este esfuerzo colectivo por crear un entorno seguro para nuestros hijos, los gobiernos también tienen un papel fundamental. Se deben concentrar en la creación de las condiciones necesarias para permitir una óptima colaboración entre el sector, el gobierno y las ONG en este tema tan importante. Las actividades de concienciación apoyadas por la administración pública de forma regular son una parte fundamental del papel del gobierno. La concienciación se debe desarrollar en los colegios y entre los profesores, como capa adicional de formación sobre la conducta en internet, pero ahora se trataría de educar a grupos de niños, en lugar de familias independientes. De este modo, los niños pueden debatir, compartir experiencias e interactuar sobre este tema en un entorno en el que pasan mucho tiempo y suele ser el lugar donde reciben la influencia de sus compañeros.

Por último, los gobiernos pueden desempeñar su papel como reguladores y fuentes de financiación de iniciativas políticas específicas. En este sentido, el gobierno de España tiene que asegurarse de que existe el marco legal necesario que permita el filtrado de los contenidos inadecuados para los niños. La ley de la competencia debe garantizar la igualdad de condiciones en el mercado de la seguridad entre los proveedores. Al mismo tiempo, debe existir un marco legal eficaz sobre el cibercrimen que garantice que la policía y el poder judicial sean eficientes y dispongan de la financiación necesaria (en términos de instrumentos legales y herramientas técnicas) para capturar a los cibercriminales y llevarlos ante la justicia. (Colaboramos de forma puntual y esporádica con la Policía, la Guardia Civil y otros departamentos de la administración pública.

En las instituciones europeas se está trabajando intensamente en la protección de los niños mediante la financiación de proyectos de protección de la infancia y de una red de líneas de ayuda para recibir informes sobre contenidos inadecuados. Además, existe una amplia legislación europea sobre cibercrimen, que también cubre la pornografía infantil y los discursos que incitan al odio. En la Unión Europea también se está trabajando en la autorregulación del sector en cuestiones tales como los contenidos apropiados y la publicidad. La legislación sobre la privacidad es otro de los ámbitos específicos de trabajo de la UE en la actualidad. El proyecto de reglamento que se debate en estos momentos prevé disposiciones específicas sobre los niños, aunque en este tema Symantec considera que es preciso trabajar más para alcanzar un resultado significativo que proteja la privacidad de los niños en diferentes grupos de edad, al mismo tiempo que se encuentra un equilibrio óptimo para el papel de padres y educadores.

En nombre de Symantec me gustaría agradecerles la oportunidad de tratar estos temas tan importantes con ustedes. En Symantec apreciamos la atención que los legisladores prestan a esta cuestión porque creemos que es fundamental para un desarrollo saludable de nuestra sociedad «digital». Quedo a su entera disposición para responder a cualquier preguntar y ofrecer información adicional.

COMPARECENCIA DE LA RESPONSABLE DE CONSUMIDORES Y USUARIOS E INTERCEPTACIÓN LEGAL DE LAS COMUNICACIONES DE JAZZTEL, DÑA. MARÍA JOSÉ GALLEGO MORALES, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 7 DE ABRIL DE 2014.

Para mí es un auténtico honor estar aquí con todos ustedes y la verdad es que estoy encantada de tener esta oportunidad.

En primer lugar quiero felicitar la iniciativa por la creación de estas ponencias por parte de las Comisiones de Interior, de Educación y Deporte y de Industria, Energía y Turismo, ponencias que abordan la prevención y la lucha contra los nuevos delitos cibernéticos a los que se encuentran expuestos nuestros menores.

Brevemente, informarles que una de mis funciones principales en JAZZTEL no es otra que la de atender, coordinar y desarrollar las actuaciones necesarias para cumplir con el Deber de Información y colaboración que nuestra compañía JAZZTEL tiene con el conjunto de la Sociedad. Que este deber se materializa a través de solicitudes Judicializadas que nos llegan a través de las distintas Fuerzas de Seguridad del Estado, así como de los Juzgados. Si tienen interés, desarrollaré brevemente más adelante, el medio, las herramientas y la forma en la que actualmente se desarrolla esta actividad en JAZZTEL, que consideró será la principal aportación que pueda hacerles llegar.

El aumento del uso de la Sociedad de la Información y de las nuevas tecnologías se encuentra en constante desarrollo y avances. Estamos viviendo una auténtica revolución que afecta a todos los niveles, en nuestros trabajos, en las comunicaciones con la Administración, en el día a día, y por supuesto, estos avances afectan directamente a nuestros menores.

Es un hecho que las Redes Sociales se han convertido en parte de nuestras vidas y más concretamente en una parte muy importante de la vida de nuestros jóvenes y a muy pesar nuestro, de nuestros menores. Los jóvenes españoles pasan más de 5 horas al día utilizando dispositivos que les permiten el acceso a las redes sociales, chateando, utilizando el Wasap.

En la actualidad existen multitud de páginas que están dirigidas a los menores, páginas de actividades y juegos, que en muchos casos requieren un registro de datos previo, que ya quedarán incorporados en los servidores de estos dominios. Los menores se encuentran particularmente expuestos al uso de su información personal constantemente, incluso en su actividad cotidiana, siendo titulares de cuentas de correo a través de las que gestionan tareas, trabajos, etc.. por ejemplo, con los propios centros escolares. Esta incorporación de las nuevas tecnologías en ámbitos educativos y de ocio para nuestros menores, supone un cambio muy importante que deben comenzar a tener en cuenta los educadores y padres, debiendo prestar especial atención y disponer de información contrastada y actualizada en todo momento.

En internet existen muchos riesgos y peligros, siendo los menores mucho más vulnerables que los adultos a su exposición. Entre los riesgos más comunes que últimamente venimos atendiendo y que empiezan a convertirse en una pieza fundamental de las solicitudes judicializadas de información que se requiere a entidades como la que represento son:

CIBERACOSO ⇒ Es una situación en que un niño o adolescente es atormentado, acosado, humillado o de alguna manera molestado por otro niño o adolescente a través de mensajes de texto, de correo electrónico, mensajería instantánea, o cualquier otro tipo de tecnología de comunicación. Este acoso NO necesariamente debe tener un objetivo sexual.

CYBERDATING ⇒ Es una cita virtual, generalmente con un desconocido y a ciegas acordada por algún medio tecnológico.

GROOMING ⇒ (término anglosajón que se refiere al acoso de carácter sexual hacia un menor). Las acciones llevadas a cabo tienen el objetivo de establecer una relación y control emocional sobre un niño/a para luego abusar sexualmente.

PHISHING ⇒ Es la actividad de atraer al usuario hacia un delito de fraude informático, para atraer su atención y/o información. El objetivo del delito es robar información personal.

SEXTING ⇒ Es generar contenidos eróticos o pornográficos por medio de teléfonos móviles por parte del propio remitente, y su posterior envío.

El auge de las tecnologías de la información han dado una nueva orientación a las formas en las que se comenten los delitos, estos medios «tecnológicos», suponen un nuevo escenario, que precisa una mayor respuesta y colaboración en la investigación de este tipo de ilícitos.

Es necesario el esfuerzo y el trabajo conjunto, en primer lugar desde la Administración fortaleciendo e incorporando a todos los niveles campañas de prevención e información. Campañas que deben adecuarse y cuidarse mucho, para que cumplan el objetivo que perseguimos, evitar la exposición a contenidos «inadecuados» y minimizar cualquier riesgo de nuestros menores en la red.

En un segundo lugar las familias y los educadores, con información, herramientas y medios en los que puedan consultar, acceder, poner en conocimiento de los Agentes Facultados, incluso pedir ayuda a las Organizaciones que tienen estas finalidades y objetivos en su actividad cotidiana, cualquier duda o denuncia, les pueda ser planteada.

En un tercer lugar el trabajo conjunto y coordinado de las Fuerzas de Seguridad del Estado y nuestros Juzgados con los Operadores de telecomunicaciones, que como JAZZTEL, realizan una investigación paralela y facilitan datos, dentro del marco de la ley, a los Agentes que les permiten llevar a cabo sus funciones.

En el caso de JAZZTEL, empresa a la que represento, en los últimos tiempos ha tenido un incremento aritmético en el número de requerimientos / solicitudes Judiciales, donde las Fuerzas de Seguridad del Estado, al amparo siempre del obligado Mandamiento Judicial, solicita diferentes datos con el objetivo de esclarecer e investigar la comisión de un posible delito.

En la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas, se establece que dentro del plazo de 72 horas, a excepción de que es establezca otro distinto por parte del Juez que instruye la causa, tienen que proporcionarse la información solicitada, siendo esta tarea a veces compleja no sólo por la información que pueda ser requerida, sino también por el volumen de datos que en muchos casos hay que preparar convenientemente a los Agentes Facultados para que tengan la información precisa y alcancen con los mismos el objetivo propuesto.

La colaboración o el valor añadido que presenta JAZZTEL, consiste en facilitar información que va, desde la titularidad de un teléfono, lista-

dos de llamadas, identificación de una IP ya sea fija o dinámica en un día y hora determinado, el bloqueo de una página web por considerar que a través de la misma se están cometiendo ilícitos, ya sea por su contenido o porque en ella se alojan anuncios, fotografías u otros datos e información que puedan suponer una infracción a la Ley de Propiedad Intelectual, del Código Penal etc…

En este sentido, los operadores de telecomunicaciones, y JAZZTEL en este caso, preocupados con la situación en la que nos encontramos, en la que cada vez existen más tipos delictivos que se cometen a través de Internet, suscribió el «Protocolo de alto nivel para la operación en la cesión de los datos prevista por la ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas», de forma activa y voluntaria, suponiendo un desembolso y esfuerzo muy importante para una compañía como JAZZTEL.

Este Protocolo, que tiene como objetivo garantizar la eficacia de las operaciones en la cesión de los datos especificados en el artículo 3 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones en plazos inferiores a los recogidos en la norma.

La firma de este acuerdo supone la colaboración por parte JAZZTEL en cualquier momento, los 7 días de las semana las 24 horas del día en aquellos supuestos que se plantean en situaciones de criticidad extrema, por ejemplo, cuando se ponen en peligro la vida de una o varias personas y son necesarias las actuaciones de urgencia, situaciones de secuestros, atentados terroristas, etc… en las que entendemos, debe primar la colaboración sobre la regulación. En la actualidad la firma de este protocolo y las actuaciones que se han coordinado a través del mismo, han supuesto operaciones muy importantes dentro del conjunto de la Sociedad.

En relación a la Interceptación Legal de las Comunicaciones, JAZZTEL dispone de un Sistema Automático «no intrusivo» que permite, previo Mandamiento Judicial, intervenir las comunicaciones de un abonado de una forma prácticamente inmediata, esto ha supuesto un gran avance sobre la eficacia en la persecución en determinados delitos, considerados críticos, como pueden ser los secuestros. En JAZZTEL existe un grupo especializado de agentes que se encarga de esta tarea, operando a cualquier nivel y en cualquier momento que fuere necesario. Se cuida mucho la formación y la importancia de estas actuaciones, que deben ser

especialmente cautelosas por la confidencialidad de los datos tratados y la discrecionalidad que debe existir de cara al objetivo interceptado, o sobre el que se está recabando información.

Mucho más sensible se muestra JAZZTEL, cuando la víctima del ilícito es un menor, como ya hemos dicho, nuestros menores son aún más vulnerables que los adultos y se encuentran expuestos en muchas ocasiones, sin que se den cuenta por su inexperiencia, vulnerabilidad e inocencia, a situaciones que inicialmente se les pueden plantear de una forma natural.

Es por ello que la colaboración que viene realizando JAZZTEL no sólo con todas la Fuerzas de Seguridad del Estado sino también con los Juzgados y en algunos casos con las propias familias y organizaciones que persiguen este tipo de ilícitos, son de una gran beneficio para la Sociedad, máxime cuando en muchos de los casos que hoy se vienen planteando, requieren de conocimientos técnicos avanzados por parte de los propios Agentes Facultados, siendo necesaria una colaboración muy estrecha con los técnicos, soportes y abogados de las Operadoras de Telecomunicaciones.

Esta colaboración permite conocer la tecnología sobre la que pueda ir soportado un determinado servicio de un Cliente, las características técnicas del mismo, y tras un análisis del supuesto que está siendo objeto de la investigación, complementar, acometer de una u otra forma, las actuaciones tendentes a desencriptar, descodificar, desenmascarar los eventos de voz y datos de un objetivo, facilitando la identificación por parte de JAZZTEL a los Agentes Facultados / Juzgados.

Con lo expuesto anteriormente, quiero insistir en que debemos «entre todos» proteger a los menores, ya que existen riesgos y peligros que se están extendiéndose progresivamente en nuestra Sociedad. Internet es un medio con infinitas posibilidades para encontrar información, aprender, expresar opiniones subir fotografías de nuestros menores. Existe un deber social de protegerlos de esas posibles amenazas y peligros, motivo por el que hoy estamos aquí.

Es necesaria una colaboración internacional en la protección de los menores, la creación de unos estándares internacionales de protección, aunque estos sean mínimos, pero que suponga unas reglas y garantías comunes para todos. Internet no tiene fronteras.

Es necesario identificar y castigar a las personar que realizan un mal uso de las redes, y así proteger a nuestros menores, adolescentes etc..

La proliferación de los dispositivos móviles, hace que sea más necesaria la prevención y que nuestros hijos dispongan de una información correcta y contrastada.

Según los datos que obran en poder de JAZZTEL asociados a los años 2011, 2012 y 2013 en relación al número de clientes activos:

— 2011 ⇒ 1122675

— 2012 ⇒ 1339966

— 2013 ⇒ 1449625

La base de Clientes se incrementó en un 22.3 %

Poniendo en línea este dato, con las solicitudes de información recibidas en Jazztel, tenemos que manifestar que el crecimiento ha sido exponencial, duplicándose el número de solicitudes tramitadas durante el año 2013 en relación con las atendidas en años precedentes.

Hay una tendencia a la utilización de Internet como un nuevo medio a través del cual es más sencilla la comisión de delitos, por la complejidad que existe en la identificación, porque permite enmascarar identidades e incluso suplantarlas, facilita el anonimato.

Según datos de la Policía Nacional, hubo 266 detenciones durante el año 2013 asociados a delitos contra menores.

Estamos hablando que cada vez se accede durante más tiempo (en minutos) a la red, cada vez se dispone de dispositivos móviles con edades más tempranas y con mayores facilidades en las tecnologías que se ponen al alcance de los usuarios, y nuestro deber es proteger a los menores de las personas que hacen mal uso de la red, incluso de ellos mismos, que por su ingenuidad y vulnerabilidad a veces no son conscientes de las consecuencias que pueda tener un determinado acto, como pueda ser, la exposición de una foto o la subida de un video.

Internet no es el enemigo, ya que la tecnología es neutra y hay una tendencia por parte de las Operadoras de Telecomunicaciones de orientar sus productos a las necesidades de sus destinatarios, como muestra de ello, se lanzan productos pre-pago y post-pago con límites de crédito o saldo, se limitan los servicios denominados «servicios de adultos», de

tarificación especial o de llamadas internaciones, es decir, muchos de los servicios que se proporcionan, requieren una solicitud expresa del responsable del servicio para su activación.

Como dato añadido, actualmente, cada habitante dispone de 1.3 dispositivos, España es el país europeo con mayor tasa de penetración de teléfonos inteligentes, según el informe proporcionado por la Entidad «*Spain Digital Future*».

Las encuestas del Instituto Nacional de Estadística sobre equipamiento y uso de tecnologías de la información en los hogares españoles, reflejan una continua expansión del uso de los ordenadores y de Internet por parte de los menores, que ya está casi a punto de convertirse en universal.

Según los datos disponibles por la CNMC (Comisión Nacional del Mercado y de la competencia)

- Existen 50,2 millones de líneas móviles en España
- Las líneas de banda ancha móvil ascendieron a 29,9 millones, con un crecimiento interanual del 34,6%
- La penetración de la banda ancha fija continuó aumentando hasta alcanzar 25,3 líneas por cada 100 habitantes
- Desde 2005 han aumentado sólo las líneas móviles de 39.547.520 hasta 50.222.144.

Desafortunadamente, muchos de estos datos contrastan con el volumen tan importante de menores que son los usuarios de estas líneas, usuarios desinformados y en muchos casos, con servicios a su disposición que en todo momento deben tener una supervisión o control por parte de un adulto responsable y convenientemente informado.

Cualquier tipo de información que los niños publican en sus páginas, en sus chat, en sus perfiles en las redes sociales, pueden hacerlos vulnerables y exponerles a delitos de estafas, de suplantación de identidad, de engaños, ciberacoso, etc…

En este sentido, entiendo personalmente, como madre de tres hijas menores, que deben promoverse a todos los niveles, las campañas de concienciación sobre ciberseguridad, que ya empiezan a incorporarse en los colegios, pero que de forma continuada, ordenada y formativa debe comprender un hábito continuo en el conjunto de la Sociedad, al igual

que lo hace las campañas de concienciación de la Dirección General de Tráfico, prevención del uso del alcohol a menores, etc…

Nuestros educadores deben tener a su alcance información adaptada, herramientas que le permitan consultar, plantear o incluso denunciar los supuestos que muchas veces son los primeros en conocer a través de los propios menores.

Una prevención eficaz a través de estas campañas de concienciación sobre la seguridad de niños y adolescentes en las redes sociales y en Internet en general, es necesaria y permitiría a los educadores y padres conocer los riesgos, y por tanto, minimizarlos.

Creo que aún estamos a medio camino, pero que entre todos, podemos conseguir el Objetivo ⇒ «Proteger a los menores», a nuestros hijos de los riesgos y peligros, que por desgracia bastantes veces, entraña el uso de las nuevas tecnologías, siempre mediante fórmulas, protocolos de actuación, de colaboración entre entidades, asociaciones, Agentes Facultados, Padres y Profesores que permita aunar los esfuerzos y alcanzar el objetivo.

Me gustaría poner a disposición mil ejemplos que todos los días tratamos y atendemos en compañías como JAZZTEL y que permiten orientar e informar de las actuaciones y pasos que deben darse. Ejemplos de la eficacia y ayuda que proporcionamos diariamente a los Agentes Facultados, Juzgados y en algunos casos, a las familias de alguna manera han sido objeto de un depredador en Internet.

Garantizando que nuestros tiempos de respuesta, nuestros mecanismos de colaboración no sean nunca un impedimento, sino todo lo contrario, seamos una pieza más, en este caso, la más Técnica, la que conoce junto con los Agentes Facultados especializados, los medios en los que se mueven los «malos», nuestro objetivo.

Quedo a su disposición para cualquier cuestión que quieran formularme.

COMPARECENCIA DE LA DIRECTORA DE POLÍTICAS PÚBLICAS, EMEA, DE TWITTER, SINÉAD MCSWEENEY, Y DE LA DIRECTORA DE SEGURIDAD DE TWITTER, PATRICIA CARTES, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 5 DE MAYO DE 2014.

La señora **DIRECTORA DE POLÍTICAS PÚBLICAS, EMEA, DE TWITTER** (Sinéad McSweeney): Maybe I'll just say a few words of introduction first. My name is Sinead McSweeney, as the chairman said. I look after public policy for twitter in the near region which includes Europe, the Middle East and Africa. Up until very, very recently it was just me. One person looking after that region which is one of the reasons why unfortunately it has taken me such a long time to come to Spain, which is unfortunate, not just because we have many users here in Spain and we like to ensure that safety messages etc. are available wherever we have lots of users, but also because I like Spain. It would have been much nicer to have been here sooner.

So in terms of my role, I look after government relations, relationships with regulators the beginning of relationships with police to ensure that they are aware of our policies about how to acquire information from us which may be helpful with an investigation and I deal with our privacy issues and other regulatory issues.

We have a very strong and committed trust and safety team. Up until very recently, Patricia was part of our trust and safety team but I have been very fortunate to welcome her to the public policy team and she has many years of expertise and experience although you wouldn't think so when you look at her in the area of safety particularly online safety for young people and she is now heading up our global safety outreach so but we are fortunate that we have her in Europe. So we will get more of her time and then the rest of the world.

I think one thing that is important to understand is that very often people say Google/ Facebook / Twitter as if it was one word or as if we were all the same company or the same size. The reality is that while the word Twitter is known far and wide, the company itself is still quite small and its growth as a company in terms of actual human beings trying to keep the company going has only happened, really in the last 12 to 18

months, so I often draw the parallel that Google has more employees in Dublin than Twitter has in the whole world, so that might give you some sense of how small we are and the efforts we are making to catch up with the platform.

Patricia is going to take you through our safety policy. She will touch on the size of the platform but mainly our safety policies and safety procedures and the work that she and colleagues from trust and safety do. Hopefully that will cover a lot of the questions that you are likely to have but between us we will take care of any outstanding issues once she has gone through the presentation.

La señora **DIRECTORA DE SEGURIDAD DE TWITTER** (Patricia Cartes): Sin más dilación, comenzaré. Y hoy quería empezar intentando ilustrar un poco las dimensiones de Twitter. Y como bien decía Sinéad ahora, Twitter es una plataforma en crecimiento, si bien la empresa es mucho más pequeña, y siempre estamos intentando seguir la estela de la plataforma, pero a veces es difícil.

En cuanto a visitantes únicos, tenemos 400 millones al mes; de esos 400 millones, 230 suelen entrar de forma muy regular, eso quiere decir que entran a visitar el sitio por lo menos de forma diaria. Y vemos 1.000 millones de tuits cada dos días. Para que se den una idea de lo que esto significa, tardamos tres años, dos meses y un día en ver el primer millón de tuits, y sin embargo ahora vemos un millón de tuits cada dos días. Por lo que cuando nos enfrentamos a abuso en la plataforma, muchas veces cuando llegamos a la denuncia de abuso ese tuit ya no es importante, porque ha habido muchos tuits que le han seguido. Entonces, es primordial que intentemos dar soporte al usuario inmediatamente cuando ocurre cualquier problema en el sitio web.

La página web está disponible en 35 idiomas, tanto en la versión web como en la aplicación. Eso quiere decir que un usuario francés puede acceder a twitter.com y ver la interfaz en francés, y también puede contactar con los equipos de soporte al usuario en su idioma nativo y recibir asistencia en el idioma nativo.

Y en cuanto a empleados, tenemos unos 2.000 empleados a nivel global. Como decía Sinéad, por ejemplo Google tiene 3.000 solo en la oficina de Dublín, que es su sede europea, y nosotros tenemos 2.000 en

todo el mundo, por lo que se pueden imaginar que son muchos menos empleados de los que tenemos en cuanto a usuarios, por lo que nos toca hacer a todos mucho trabajo día a día.

Para los que estén aquí que no utilicen Twitter, esto será útil; para los que utilicen Twitter, lo siento, igual se aburren ahora un momento conmigo, pero quería captar lo que es la anatomía de un tuit. Todas las cuentas en Twitter tienen un nombre que va seguido del símbolo de la arroba. Por ejemplo, aquí estamos mostrando el de uno de nuestros colaboradores en el campo de la seguridad en España, que es la asociación PantallasAmigas. Entonces, @pantallasamigas es el nombre del usuario, que les identifica, y para conectar con ellos lo único que hay que hacer es escribir @ más ese nombre, para poder conectar con ellos directamente.

El tuit tiene 140 caracteres, o menos, y es la forma que la gente tiene de comunicarse con sus seguidores. Se pueden imaginar: 140 caracteres es muy poco espacio, por lo que cuando recibimos denuncias de abuso a veces nos falta mucho contexto; es muy difícil para nosotros juzgar qué es realmente lo que está pasando, por lo que siempre les pedimos a los usuarios que nos den cuanto más contexto mejor a la hora de realizar las denuncias de abuso.

También tenemos la verificación, que es esa marca azul que se ve al lado del nombre de PantallasAmigas, en este caso, y la verificación muestra cuando hemos marcado una cuenta como auténtica en la plataforma. Y eso nos sirve para que los usuarios sepan que están interactuando con la persona o la entidad a la que realmente siguen. Por ejemplo, si yo soy fan, no sé, de Pep Guardiola, quiero asegurarme de que estoy interactuando con Pep Guardiola, y no con, igual, un fan o alguien que está haciendo una parodia de Pep Guardiola. Y la forma de saber que realmente él es con quien estoy interactuando es buscar ese símbolo azul al lado del nombre del usuario.

Y finalmente tenemos la forma de interactuar con un tuit, que está al final del tuit, en el que podemos responder, podemos retuitear, y lo que hace retuitear es simplemente mostrar ese mismo contenido en mi cuenta; es una forma de compartir el mismo contenido en mi cuenta. De forma que si yo ahora quisiera compartir este mensaje en mi cuenta, lo único que tendría que hacer es clicar en retuitear para que apareciera en la cuenta de Patricia Cartes.

También puedo marcar un tuit como favorito, y si le doy a los tres botones de más —lo veremos más adelante— tendré las opciones de denuncia de abuso, que es de lo que se encarga mi equipo. Y eso enlaza bastante bien con el equipo de Trust & Safety. No hemos conseguido traducir el nombre al castellano, porque en realidad el campo de «safety» en castellano se suele traducir como «seguridad», pero implica algo mucho más allá de la seguridad; no estamos hablando solo de recuperación de contraseñas o de cuentas comprometidas y haqueadas, estamos hablando de la protección al menor en un sistema de una forma más amplia.

Entonces, este equipo está especializado, hay diferentes áreas de especialización. Y entre ellas quería recalcar la de propiedad intelectual e identidad. Como decía antes, tenemos mecanismos para asegurarnos de que las cuentas que tenemos en el sitio son reales, y cuando nos encontramos con usurpación de marcas o suplantación de identidad es importante que tomemos acción.

También tenemos el equipo que se encarga de llevar los derechos de usuario y privacidad, que son temas como menores de 13 años que estén en la plataforma, derechos de imagen (alguien que sube una foto mía a Twitter y yo no quiero que esa foto esté en Twitter, cómo puedo denunciarlo y qué pasos vamos a seguir para eliminar esa imagen). Lo mismo con cualquier otro tipo de elemento de privacidad, como direcciones, números de teléfono que sean privados, etcétera.

Las políticas para anunciantes: este equipo se encarga de ver qué productos hay que restringir en qué países (por ejemplo, los anuncios de alcohol en según qué países nórdicos están prohibidos en línea), de forma que se encargan de realizar todo el estudio de mercado para todos los mercados en los que facilitemos anuncios a nuestros usuarios.

El equipo de seguridad de usuario, que es con el que yo trabajo de forma más cercana, se encarga del abuso y el acoso a un nivel bastante general, cosas como amenazas, el lenguaje de incitación al odio, autolesiones, contenido que tenga relación con el suicidio; miran todas las denuncias que recibimos sobre esas áreas y se encargan de responder a los usuarios y de atenderles.

Y finalmente, el equipo que se encarga de las solicitudes legales: ellos se encargan día a día de las relaciones con fuerzas de seguridad (en el caso de España, Guardia Civil, Policía Nacional y todas las policías re-

gionales). Reciben las solicitudes de información, cuándo ha ocurrido un crimen, o si se quiere saber más del usuario. Y también se encargan de bloquear el contenido a nivel geográfico. Es algo que podemos hacer. Imaginémonos un contenido que sea ilegal, por ejemplo, en Turquía: podemos bloquear ese contenido para el territorio turco pero dejarlo en el sitio para el resto del mundo. Entonces, se encargan mucho de mirar este tipo de solicitudes.

Y finalmente, en la explotación de menores se encarga junto con el equipo de seguridad del usuario de mirar cualquier tipo de denuncia que nos llegue de este tipo de contenido, pero también de nuestros esfuerzos proactivos a la hora de combatir cualquier tipo de contenido relacionado con la explotación al menor. Y sobre esto voy a hablar un poco con más detalle en unos minutos.

Hay otro equipo, que es el de atención al usuario, que complementa a este primer equipo del que hablaba. Y entre estos dos equipos, que están situados tanto en Dublín como en San Francisco, podemos hacer soporte al usuario 24 horas al día, 7 horas a la semana, de forma global. Por lo que, cuando Dublín se va a dormir, San Francisco toma el relevo y se encarga de seguir con las denuncias de abuso que nos llegan.

El equipo de atención al usuario hace un soporte más genérico: se encargan del centro de ayuda, mirar cualquier tipo de errores del sistema que estemos viendo de forma sistemática. También se encargan de ver las etiquetas, que son las palabras claves que van precedidas del símbolo del sostenido, y que permiten a los usuarios agrupar conversaciones por un tema. Por ejemplo, si yo quisiera hablar del partido del Real Madrid ayer podría utilizar ese símbolo más «partido del Real Madrid», y empezaría a conectar con cualquier usuario que esté hablando de ese tema. Es una forma realmente de agrupar las conversaciones a través de palabras clave. Pero, como se pueden imaginar, en ocasiones se dan caso de abuso con etiquetas; puede haber etiquetas abusivas e incluso ilegales, y es algo con lo que tenemos que tener mucho cuidado.

También se encargan de *spam*, *phishing*, *malware*, toda la parte técnica de cuando una cuenta es vulnerada, e intentar restablecer esa cuenta, el cambio de contraseñas y asegurarse de que ningún usuario que haya interactuado con esa cuenta también haya sido infectado por los virus que sean.

Fotos y multimedia: hay mucho contenido multimedia en Twitter. Twitter te permite subir imágenes al sitio, y este equipo se encarga de asegurarse de que esas imágenes son legales, pero también de que no haya abuso en general con las imágenes.

Acceso a cuentas, cuentas haqueadas, restablecimiento de contraseñas, cualquier persona que tenga un problema de inicio de sesión, que tal vez ha perdido la dirección de correo asociada a su cuenta, etcétera, este equipo se encarga de restablecer todas esas cuentas.

Y finalmente, el equipo de traducción, que se asegura de que el sitio esté disponible en esos 35 idiomas de los que hablábamos antes, tanto el centro de ayuda como el sitio web como las aplicaciones a las que se puede acceder a través del teléfono o del iPad.

Hay dos formas de denunciar abuso en la plataforma, porque hemos hablado de los equipos que se encargan de mirar estas denuncias, y la forma que tiene el público de dar con ese equipo es a través de dos mecanismos principales.

El primero es el centro de ayuda, que contiene muchísima información; información muy simple, como cómo cambio el nombre de mi cuenta o cómo subo una foto a la cuenta, a información más compleja, como cómo denuncio terrorismo en Twitter.

El segundo mecanismo de denuncia es el tuit. A nivel de tuit también hemos implementado un mecanismo de denuncia. Como decía antes, en el botón de «Más», cuando clicamos en «Más», y esto ya sea desde el sitio web, desde el teléfono móvil o desde la aplicación, tengo la opción de bloquear o reportar. Es importante marcar —esto es lo que se ve una vez que clico en bloquear o reportar—, recalcar la opción de bloquear, porque queremos que el usuario también sea capaz de protegerse a sí mismo. Y una de las recomendaciones que compartimos es siempre, si estás interactuando con alguien o alguien interactúa contigo de forma abusiva, es muy importante bloquear y no interactuar con ellos, porque muchas veces, cuanto más se interactúa, es como echar leña al fuego.

Pero aparte de la opción de bloquear, que te permite acabar con esa interactuación de forma inmediata, también puedes denunciar el tuit en particular. Y hay varias opciones: puedes denunciar el tuit como *spam*, puedes denunciar la cuenta por estar comprometida si lo que estás viendo son tuits de *spam*, y esto ocurre muchas veces, que igual ves a un amigo

que está compartiendo tuits de adelgazar diez kilos en tres días, y toda la cuenta tiene ese tipo de tuits, lo más lógico es que hayan sido haqueados. Y entonces, es importante denunciar la cuenta como comprometida para que nosotros podamos restablecerla.

Y la última opción, que es realmente la opción que nos ocupa aquí, es la de cuando un usuario es ofensivo. Y cuando clicas en este enlace te vamos a preguntar exactamente qué tipo de violación de nuestras reglas estás observando. ¿Estamos hablando de acoso o estamos hablando de incitación al odio o estamos hablando de una violación de la privacidad de alguien? Y como decía antes, como 140 caracteres es muy poco espacio, siempre le pedimos al usuario que nos dé, cuanto más contexto, mejor. Y dependiendo de la opción que elijas, eso le irá a un equipo o a otro. Y tenemos la gran suerte de tener especialistas en los diferentes equipos. Por ejemplo, el equipo de privacidad está conformado de gente que realmente ha trabajado en el campo de la privacidad y de la protección de datos durante muchos años, y son capaces de ver el tuit, saben cuáles son las reglas de Twitter, cuál es la legalidad vigente en el país en el que se encuentra el usuario y tomar la acción apropiada.

Pero podemos hablar más de eso ahora, porque hay un par de reglas de las que realmente quería hablar hoy. La primera, la de abuso, acoso y amenazas, y es importante decir que el abuso y el acoso están prohibidos en Twitter, y siempre que nos llegan denuncias de este tipo, lo que hacemos es evaluar la situación. Muchas de las interactuaciones que vemos en el sitio, la gran mayoría de las interactuaciones que vemos en el sitio web son positivas. Pero de vez en cuando tienes la situación de dos amigos, que igual se han peleado, y uno empieza a tuitear al otro de forma abusiva. Y en estos casos nos viene muy bien poder mandarle advertencias al usuario y compartir con ellos las reglas de Twitter. Y vemos que en la gran mayoría de los casos los usuarios reaccionan muy bien a estas advertencias y suelen rectificar el comportamiento que han estado mostrando en la plataforma.

Hay casos más severos en los que se crean cuentas solo para abusar de alguien, y está claro porque cuando te metes en la cuenta ves la arroba y el nombre de alguien que de forma muy consistente se ve que está haciendo abuso. Esas cuentas, obviamente, no las queremos en el sitio, y en esos casos tenemos que suspender la cuenta de forma permanente y asegurarnos de que ese usuario no está creando otras cuentas para conti-

nuar ese abuso. Y para asegurarnos de que eso no ocurre mantenemos un diálogo constante con el usuario y le vamos preguntando si ha observado en alguna cuenta nueva, si han recibido contacto nuevo por parte de ese usuario desde cualquier otro canal, para poder tomar acción.

Y en el medio también tenemos las cuentas que tal vez son abusivas, pero no es el único objetivo de la cuenta; puede ser una cuenta que estaba bien y por el motivo que sea se ponen a abusar de alguien, y en esos casos podemos hacer una suspensión temporal, y avisar al usuario, y tienen que leerse las reglas antes de ser restablecidos en el sitio web.

Entonces, tenemos muchas acciones disponibles a la hora de enfrentarnos al abuso.

El caso de las amenazas ya es más complicado. No permitimos amenazas directas, es obvio eso. Y siempre estamos mirando cuál es la posibilidad de que una amenaza en Twitter cause daño en el mundo real. Y si hay realmente elementos que nos preocupan, y creemos que la integridad de alguien está en peligro, no solo tomaremos acción en el contenido, sino que también le recomendaremos a la persona que contacte con las fuerzas de seguridad, y entonces nosotros continuaremos esa conversación con las fuerzas de seguridad. Entonces, digamos, si a mí me ha amenazado hoy alguien y hay suficientes elementos en el tuit, como por ejemplo el lugar de la amenaza, en armas que se van a utilizar, quién va a participar en el ataque y demás, y yo voy a la Guardia Civil, nosotros podemos luego mantener la conversación con la Guardia Civil para realmente llegar al meollo de la cuestión, por así decirlo.

Ha habido últimamente muchas conversaciones sobre la explotación infantil en línea, y quería aclararlo también hoy: tenemos tolerancia cero para el contenido de explotación al menor y trabajamos de acuerdo con las leyes, sobre todo las americanas, que claramente nos marcan que tenemos que denunciar cualquier tipo de contenido de este nivel a NCMEC (que es el National Center for Missing and Exploited Children). NCMEC se encarga de trabajar con las diferentes fuerzas de seguridad en los diferentes países, de diseminar la información necesaria para que la persona que haya compartido este tipo de contenidos sea llevada a la justicia. En España trabajamos mucho sobre todo con la Guardia Civil, también con Policía Nacional y las fuerzas de seguridad regionales, pero siempre es a través de NCMEC. Y en particular la Guardia Civil tiene una conexión VPN con NCMEC, que es la forma que tienen de obtener

los datos específicos de un usuario que esté compartiendo este tipo de contenido.

Este tipo de contenido es complicado. En Twitter, al ser una plataforma abierta, vemos menos de este tipo de contenido que otras redes sociales, porque no hay mucho sitio por el que esconderte, no hay muchos lugares en los que te puedas esconder. Y lo que es obvio es que los explotadores de menores no suelen compartir este contenido de forma abierta.

Aun así, es importante que seamos proactivos, porque si bien la comunidad denuncia este tipo de contenido, entre ellos los explotadores no lo van a denunciar, por lo que no podemos confiar solo en la comunidad para denunciar este tipo de tuits.

Por eso tenemos una tecnología que se llama Photo DNA, que fue desarrollada por Microsoft con Dartmouth College y es usada por todas las empresas de este tipo de industria (Facebook, Microsoft, Yahoo, Google, etcétera), que es una base de datos de imágenes que están escaneadas; funciona por un *hash*, y los *hashes* de las imágenes son un poco como el ADN de una imagen. Entonces, cuando tienes el mapa de ese ADN de la imagen, cuando una imagen es subida a un sitio web, si hay una imagen que le corresponde en la base de datos nos alerta inmediatamente, la cuesta es suspendida y le pasamos la información a NCMEC. O sea, es una tecnología proactiva que siempre está funcionando por detrás de la plataforma, y nos permite a veces llegar a los casos antes de las denuncias.

Y otra regla de Twitter que quería subrayar aquí hoy es la de suplantación de identidad. Porque, si bien consideramos cuentas de parodia, y hay muchas en el sitio, hay muchas cuentas, incluso por humoristas famosos, que hacen cuentas de parodia sobre políticos y gente de la vida pública, no permitimos la suplantación de identidad, y es algo que siempre estamos mirando, cuál es el objetivo de la cuenta y si el objetivo es engañar al usuario o hacerse pasar por alguien, ahí es cuando tenemos que eliminar el contenido, eliminar la cuenta y ver qué acciones tomar.

Pero hay un mecanismo específico de denuncia. Como mostraba antes, cuando denuncias a un usuario como usuario abusivo, también te preguntamos si lo que estás denunciando es una suplantación de identidad, en cuyo caso vamos a mirar elementos como el nombre, la imagen, pero también si los tuits están siendo producidos en primera persona y si hay una intención paródica o no. Y a veces la línea entre la parodia y el

abuso es muy delgada. Entonces, es algo que llevamos juntos el equipo de propiedad intelectual y el equipo de abusos, porque en los casos en que, sobre todo a personajes privados, la suplantación de identidad es abusiva (que es lo que suele pasar, no suplantas a alguien por la broma, sobre todo cuando son personajes privados), en ese caso tenemos que suspender la cuenta del usuario y advertirles de que están en violación de las reglas de Twitter.

Estas son las que había elegido que pensé que serían más relevantes para este grupo, pero ahora tenemos tiempo y Sinéad y yo vamos a responder cualquier pregunta que tengan, si ha quedado algo que no ha sido claro.

6. ANEXO
(Versión en lengua inglesa del Informe de la Ponencia)

REPORT ISSUED BY THE JOINT SUBCOMMITTEE TO STUDY THE RISKS DERIVED FROM USE OF THE WEB BY MINORS

I. INTRODUCTION: COMPOSITION AND ACTIVITY OF THE SUBCOMMITTEE

Further to a motion[1] endorsed by all the Groups in Parliament (Grupo Parlamentario Popular en el Senado, Grupo Parlamentario Socialista, Grupo Parlamentario Catalán en el Senado Convergència i Unió, Grupo Parlamentario Entesa pel Progrés de Catalunya, Grupo Parlamentario Vasco en el Senado (EAJ-PNV) and Grupo Parlamentario Mixto), the Plenary Sittings of the Senate, at meeting number 24 in the X Legislature, held on 19 December 2012, unanimously agreed (through the Senators in attendance) to create a Joint Subcommittee representing the Home Office, Education and Sports and Industry Energy and Tourism Committees, to study certain fields related to Internet use by minors:

«a. Prevention measures against risks derived from the use of social networks by minors. These measures should be applied by schools and by the education sector in general, based on the training of teachers and educators. Responsibilities for each school should be determined, for risk control.

b. Determination of responsibilities and self-control in social network management companies, in relation to access by minors and the use of personal and private information.

[1] Motion whereby the Senate has agreed to create a Joint Subcommittee amongst the Home Office, Education and Sports and Industry, Energy and Tourism Committees, to study various matters related to the prevention and fight against new cybercrime («B.O.C.G., Senado», no. 142, of 27 December 2012).

c. The instruments available to security forces and corps to fight against new cybercrime, including the training of professionals and specialized units to fight against this time of crime»[2]

The Bureau of the Senate, at its meeting held on 29 January 2013, agreed to establish a Joint Committee amongst these Committees, consisting of their members and chaired by the Speaker of the Senate. At its meeting held on 5 February 2013, the Joint Committee of the Home Office, Education & Sports and Industry, Energy & Tourism Committees agreed to designate the following Senators as members of the Joint Subcommittee created by the Plenary Sitting of the House:

— His Excellency Mr. Emilio Álvarez Villazán (GPS).

— His Excellency Mr. Iñaki Mirena Anasagasti Olabeaga (GPV).

— His Excellency Mr. José María Ángel Batalla (GPS).

— Her Excellency Ms. Carmen Azuara Navarro (GPP).

— His Excellency Mr. Francisco Boya Alós (GPEPC).

— His Excellency Mr. Tomás Pedro Burgos Beteta (GPP).

— His Excellency Mr. José María Chiquillo Barber (GPP).

— His Excellency Mr. Andrés Gil García (GPS).

— Her Excellency Ms. Amalur Mendizábal Azurmendi (GPMX).

— His Excellency Mr. Jordi Miquel Sendra Vellvé (GPCIU).

The Subcommittee has been coordinated by His Excellency the Senator Mr. Tomás Pedro Burgos Beteta, and all assistance and support has been entrusted to Mr. Eugenio de Santos Canalejo, Legal Adviser to Parliament, and the Secretary of the Home Office and Industry, Energy & Tourism Committees, Ms. Isabel Jalvo García.

Between February-April 2013, the Subcommittee held four preparatory meetings to clarify various relevant issues:

— It determined, as a suitable title, the «Joint Subcommittee to study risks derived from Web use by minors».

— A fundamental premises of its work was to consider minors as a group with specific Internet needs, which need to be comprehensively

[2] «Diario de Sesiones, Senado, Pleno», no. 47, of 19 December 2012.

studied, based on the many different approaches, interested parties and existing levels of action.

— A time limit was established for its work –September 2014– as well as a work plan essentially based on the participation of prominent members of public and private entities and renowned experts, designated on the grounds of their connections with the subject matter, amongst other proposals presented by the Subcommittee Senators. Specifically, four relevant fields were defined in this appointment:

  • The scope of public powers, specifically in sectors with competence related, from various angles, to the subject matter.

  • The scope of private organizations specifically aimed at the protection of minors or representing educational and Internet user associations.

  • The range of experts in various fields, such as new technologies and cybersecurity, psychology or digital communication.

  • The scope of the industry and creators of digital contents.

— Subject to prior authorization from the Bureau of the Senate, the Subcommittee encouraged a novel policy whereby, without prejudice to meetings being held without direct publicity, as is usual practice in the operation of these types of bodies, the text of all dissertations presented by the participants, subject to the prior consent, would be uploaded onto the Senate website.

The Subcommittee has held a total of thirty-three meetings, of which nineteen consists of hearings; fifty-three guests attended, listed below, in the chronological order of the meetings attended[3]:

Meeting of 9 May 2013

— Mr. Víctor Calvo-Sotelo Ibáñez-Martín, State Secretary of Telecommunications and the Information Society.

---

[3] The speeches of the participants are published on the Senate website: http://www.senado.es/web/actividadparlamentaria/sesionescomision/detallecomisiones/ponencias-deestudio/index.html?id=S030001&id2=S020009&legis=10&tab=t

Annex 1 hereto includes a list of the participants in alphabetical order.

— Mr. Borja Adsuara Varela, General Manager of Red.es.

— Mr. Manuel Escalante García, General Manager of *Instituto Nacional de Tecnologías de la Comunicación* (INTECO) [National Institute for Communication Technologies].

Meeting of 16 May 2013

— Mr. Ignacio Cosidó Gutiérrez, General Manager of the Police.

— Mr. Juan Miguel Manzanas, Head Officer of the Technological Investigation Brigade, General Station of the Judicial Police, General Directorate of the Police.

— Ms. Carolina González García, Chief Inspector of the Press and Social Networks Department, Press and Informative Relations Office, General Directorate of the Police.

Meeting of 20 May 2013

— Mr. Arsenio Fernández de Mesa Díaz del Río, General Manager of the Civil Guard.

— Mr. Óscar de la Cruz Yagüe, Chief Commander of the Telematic Crime Section, Central Operating Unit [*Unidad Central Operativa* (UCO)] of the Civil Guard.

— Mr. Carlos Igual Garrido, Captain of the Minors and Children's Sexual Exploitation Section, Technical Unit of the Judicial Price [*Unidad Técnica de Policía Judicial* (UTPJ)] of the Civil Guard.

Meeting of 6 June 2013

— Mr. Alfonso González Hermoso de Mendoza, General Manager of Evaluation and Territorial Cooperation.

— Ms. Ana María Román Riechman, Head of *Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado* (INTEF) [National Institute for Educational Technologies and Teacher's Training]

Meeting of 17 June 2013

— Mr. Manuel Viota Maestre, Head of the Central Department of IT Crime, Criminal Investigation and Judicial Police Unit, Ertzaintza [Basque Police].

— Mr. Joaquim Bayarri i Nogueras, Head of the Technical Division for Citizen Security Planning, Mossos d'Esquadra [Catalonian Police].

Meeting of 27 June 2013

— Ms. Elvira Tejada de la Fuente, State Prosecutor, Coordinating Chamber to fight Computer Crime.

— Ms. Consuelo Madrigal Martínez-Pereda, State Prosecutor, Coordinating Chamber for Minors.

— Ms. María Salomé Adroher Biosca, General Manager of Family and Children's Services.

Meeting of 12 September 2013

— Mr. Guillermo Cánovas Gaillemín, Chairman of the Internet Security Centre, «*Protégeles*» Association.

— Mr. Francisco Javier Martos Mota, Executive Director of UNICEF, Spanish Committee.

— Mr. Jorge Flores Fernández, Manager of «*PantallasAmigas*».

Meeting of 26 September 2013

— Ms. Liliana Orjuela López, Coordinator of Children's Rights, «Save the Children».

— Mr. Miguel Comín Hernández, Manager of the Alia2 Foundation.

— Mr. Luis Carbonell Pintanel, Chairman of the National Catholic Confederation of Family Representatives and Alumni Parents [Confederación Católica Nacional de Padres de Familia y Padres de Alumnos] (CONCAPA).

Meeting of 10 October 2013

— Mr. Josep Manuel Prats Moreno, Chairman of the Catalonian Federation of Associations of Parents of Free Schools [*Federació d'Associacions de Pares i Mares d'Escoles Lliures de Catalunya*] (FAPEL).

— Mr. Jesús Salido Navarro, Vice Chairman of the Spanish Confederation of Associations of Alumni Parents [Confederación Española de Associations de Padres y Madres de Alumnos] (CEAPA).

— Mr. José Luis Rodríguez Álvarez, Manager of the Spanish Data Protection Agency [Agencia Española de Protección de Datos] (AEPD).

Meeting of 24 October 2013

— Mr. Carlos Represa Estrada, Manager of the School ITC Security Centre [Centro de Seguridad TIC Escolar] (CTIC) and Head of the Internet Security and Protection of Minors Department, UNIR (Universidad Internacional de La Rioja) Foundation.

— Mr. Miguel Pérez Subías, Chairman of the Internet Users Association [Asociación de Usuarios de Internet] (AUI).

— Mr. Miguel Errasti Argal, Chairman of the National Association of Internet Companies [Asociación Nacional de Empresas de Internet] (ANEI).

Meeting of 4 November 2013

— Mr. Javier Urra Portillo, First Ombudsman for Minors, Autonomous Community of Madrid.

— Mr. Juan María Martínez Otero, Member of the Advisory Board of the Federation of Media Consumer and User Associations [Federación de Asociaciones de Consumidores y Usuarios de los Medios] (iCmedia).

— Mr. José Miguel Rosell Tejada, Managing Partner of S2 Grupo.

Meeting of 27 November 2013

— Mr. Antoni Gutiérrez Rubí, Communications Advisor and social network analyst.

— Mr. Mariano Chóliz Montañés, Lecturer, Faculty of Psychology, University of Valencia.

Meeting of 30 January 2013

— Mr. Eugenio Fontán Oñate, Chairman of the Official Association of Telecommunication Engineers.

— Ms. Dolors Reig Hernández, Social Psychologist, specializing in social networks; head of «*El caparazón*» programme.

— Mr. Félix Brezo Fernández, Software Engineer and Industrial Organization Engineer.

Meeting of 10 February 2013

— Mr. Francisco Ruiz Antón, Manager of Public Policy and Institutional Matters, Google Spain and Portugal.

— Ms. Natalia Basterrechea Oñate, Manager of Public Affairs, Facebook Spain and Portugal.

— Mr. Jesús Guijarro Valladolid, Manager of Corporate Social Responsibility, Orange.

Meeting of 24 February 2014

— Mr. Héctor Sánchez Montenegro, Technology Manager, Microsoft Ibérica.

— Mr. Sebastián Muriel Herrero, General Operations Manager, Tuenti.

Meeting of 10 March 2014

— Mr. José Miguel Tourné Alegre, General Manager of the Federation for Intellectual Property Protection [Federación para la Protección de la Propiedad Intelectual] (FAP).

— Ms. Salud Martínez Monreal, expert in innovation for information security.

— Ms. Sofía Fernández de Mesa Echeverría, Head of Corporate Responsibility and Social Innovation, Telefónica.

Meeting of 2 April 2014

— Mr. José Luis Casal Castro, Co-Founder and Head of Marketing, Talk2Us Comunicación.

— Mr. José Manuel Sedes García, Sustainability and Quality Manager, Vodafone España.

— Ms. Carlota Navarrete Barreiro, General Manager of the Coalition for digital content creators and industries.

Meeting of 7 April 2014

— Mr. Íñigo Polo González, Head of Institutional Relations, Ono.

— Mr. Francisco Javier Santos Ortega, Corporate Security Manager, Ono.

— Mr. Joan Taulé Valdeperas, General Manager of Symantec España.

— Ms. María José Gallego Morales, Head of consumers and users and legal interception of communications, Jazztel.

Meeting of 5 May 2014

— Ms. Sinéad McSweeney, Head of Public Policy, EMEA, Twitter.

— Ms. Patricia Cartes, Head of Security, Twitter.

In addition to the informative meetings of the participants, the Subcommittee made two institutional visits. The first, further to an invite from the General Manager of the Police, Mr. Ignacio Cosidó Gutiérrez, to the police complex located in Canillas (Madrid), on 3 July 2013, as a result of which the Subcommittee got to know the

facilities of the General Station of the Scientific Police and attended a presentation made by the Technological Investigation Unit. The second visit was made on 8 July 2013, further to an invite from the General Manager of the National Institute of Communication Technologies [Instituto Nacional de Tecnologías de la Comunicación] (INTECO), Mr. Manuel Escalante García, in order to hold a work meeting at the Institute's offices in León, during which the latter presented its strategic lines; a visit was made to the INTECO-CERT security incident response centre and INTECO's security technologies were presented.

During the course of the Committee's work, specifically on 11 February 2014, a «Day for a Safer Internet» was held; this event, under the auspices of the European network for Internet safety centres (INSAFE), is held each year since 2003 and there is a growing number of participating countries. As a result of this event, the Subcommittee approved an Adhesion Declaration, particularly in support of holding the «III National Conference for Young People and the Web», arranged by the Spanish Internet Safety for Minors (Protégeles/Cesicat), as the central act of the Day. The content of this Declaration is attached hereto as Annex 2.

Next, this Report provides the Subcommittee's analysis about the subject matter, in light of the contributions made by the participants and complementary documentation consulted, systematically structured into five main titles, with the following headings:

— Web Use by Minors.

— Existing risks in Web Use by Minors.

— What to do?: minors as a centre for digital citizenship strategy.

— Conclusions.

— Recommendations.

First, a methodological comment should be made. Without prejudice to existing bibliography related to the subject matter being studied, this Report has been based on institutional documents, accordingly cited throughout. As an exception, certain statistics are cited that represent initiatives financed by the European Union and provide a comparison

basis amongst several European Countries, including Spain, which the Subcommittee considers of particular interest[4].

The Report was approved by the Subcommittee at its meeting held on 30 September 2014.

II. WEB USE BY MINORS

1. *Global scenario*

The safety of minors on the Web cannot be adequately analysed outside the global Internet and technological evolution scenario.

Churchill's words in a speech delivered in 1943 before the House of Commons –«We shape our buildings, and afterwards our buildings shape us»– in a citation made by José Miguel Rosell in his speech before the Subcommittee, is a good description of how the Internet has evolved.

Since ARPAnet (a collaboration network jointly created in the 60's by the U.S. Department of Defense and leading U.S. universities) and until the TCP/IP protocol was adopted in 1973 (marking the beginning of the Internet, by allowing connection of ARPAnet connected computers and those in another networks existing at the time), and the subsequent

---

[4] Livingston, S., Haddon, L., Görzig, A, Ólafsson. (2010). «Risks and safety for children on the Internet: The perspective of European children. Full Findings». LSE London. EU Kids Online, 2011. Available at http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf

By the same authors, «Final Report, EU Kids Online II», 2011. Available at http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

How results are read amongst Spanish minors, Maialen Garmendia, Carmelo Garitaonandia, Gemma Martínez & Miguel Ángel Casado, «Riesgos y seguridad en Internet: los menores españoles en el contexto europeo» [«Internet risks and safety: Spanish minors in the European scenario»]. Universidad del País Vasco, Bilbao, 2011. Available at http://www.prentsa.ehu.es/p251-content/es/contenidos/noticia/20110328_internet_kids/es_interkid/adjuntos/Informe_Espa%C3%B1a_completo_red.pdf

Tsitsika, A., Tzavela, E. & Mavromati, F. (Ed.). «Investigación sobre conductas adictivas a Internet entre los adolescentes europeos», [«Research on Internet addictions amongst European adolescents»], EU NET ADB Consortium, 2011-2012.

Available at www.eunetadb.eu

generalization of the Internet amongst the public at large, and since then until the Web 2.0 showed up in the early 2000's (i.e. the interactivity era) and the social network breakthrough (in 2004 when Facebook was born), already at the beginning of the «Big Data» and «Internet of things» era (storage, processing and massive data exchange and connection of objects to the Internet), man has designed a scenario –Internet and the digital world–, based on technological progress at staggering speed, with revolutionary consequences for human and social relations.

Some of the main features of the current scenario are: connectivity, interactivity and media convergence.

As pointed out to the Subcommittee by Antoni Gutiérrez, the key is no longer Internet access but connectivity. This is a consequence of broadcasting through high-speed networks (broadband and fibre in fixed lines, and UMTS and LTE (third and fourth generation, respectively) mobile telephony lines, basically tablets and smartphones), providing gradually broader layers of the population with potentially continuous Web access and connection; and, above all, access is provided to advanced Web services (to include social networks, amongst others), with total ubiquity (pocket Internet, with a smartphone) all over the planet.

According to Eugenio Oñate, in his speech made to the Subcommittee, Internet is «a pan-communication tool».

The figures speak for themselves: there are high rates of growth worldwide in Internet access, broadband access and mobile telephony. By late 2012, approximately 2,500 million persons were connected to the Web, registering a 10.70% growth during the year all over the world. It is estimated that, by 2013 40% of the world's population will be connected to the Internet[5].

Furthermore, intelligent portable devices, particularly Tablets and Smartphones, have become the main connectivity terminals (over 1,000 million Smartphones were sold in 2013 all over the world and, as a consequence of the foregoing, mobile application users are expected to grow from approximately 1,200 million in 2012 to 4,400 million in 2017[6]).

---

[5] Telefónica Foundation. «La Sociedad de la Información en España 2013» [The Information Society in Spain 2013»], p. 34. Available at: http://www.fundacion.telefonica.com/es/arte_cultura/publicaciones/sie/sie2013.htm

[6] Ibidem, p. 42.

And Spain is no exception. According to 2013 INE[7] data:

— 69.8% of all homes have Internet access (nearly three percentage points more than in 2012) and a similar number of homes (68.9%) has broadband connection (ADSL, cable network, etc.).

— In population terms (16 to 74 years old), 71.6% used the Internet in 2013 (24.8 million, nearly two percentage points more than in 2012); age was a relevant differentiating factor, given that Internet use was more popular the younger the segment considered; the lowest age range analysed (16-24 years) reflected a quasi-universal use (97.4%) (4 million persons, nearly two percentage points more than in 2012).

— In turn, of the total Internet users 75.1% has daily access (which, in addition to 16.9% of users with weekly access, even if not daily, amounts to 92% frequent Internet use) and, again, the 16-24 year range registered the highest percentage of daily Internet use (88.5%).

— Mobile telephone use is practically universal (96.1% of all homes with a mobile phone and 94.2% of mobile phone users). This figure is related to the sale of Smartphones which, back in December 2012, already represented 80% of all mobile telephones, turning migration from a traditional mobile phone to a Smartphone into an accomplished fact[8].

— Amongst Internet users, the main type of device used to access the Internet outside the home or work centre is a mobile phone (63.2% of Internet users, which increases to 82.7% in the 16-24 age range).

Essentially, Internet connectivity and its mobility has become part of Spanish citizens' lives and is particularly relevant amongst the younger population.

A second characteristic of the current scenario is interactivity, i.e. users' potential to act as content creators and to share it on-line with other users. As an example taken from the European Commission Green

[7] Instituto Nacional de Estadística (INE) [National Statistics Institute]. Survey on home equipment and use of IT and communications 2013.

[8] Telefónica Foundation, op. cit., p. 42.

Papers, «Preparing for a Fully Converged Audiovisual World», each minute 72 video hours are uploaded on YouTube[9].

From this perspective, social networks are at the forefront. The National Institute for Communication Technologies [*Instituto Nacional de Tecnologías de la Comunicación*] (INTECO) and the Spanish Data Protection Agency [*Agencia Española de Protección de Datos*] (AEPD), in a 2009 study, both defined on-line social networks as «Internet services that are able to generate a user profile, used to publicize data and personal information, providing tools for interaction with other users and traceability based on published profile characteristics»[10].

Sebastián Muriel, in his speech before the Subcommittee, proposed an idea of a social network adjusted to the Smartphone and mobility breakthrough; «any application enabling user communication and the exchange of information and contents between them»; this idea includes mobile applications such as WhatsApp, Line, WeChat, etc. and is relevant in terms of the actual situation faced by regulatory and self-regulation frameworks.

The National Observatory for Telecommunications and the Information Society [*Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información*] (ONTSI), in its study of December 2011, highlighted the dynamism resulting from social network penetration in Spain, which was then two decimal percentage points above the average penetration of social networks in Europe[11].

According to INE data for 2013, amongst the most popular services of Internet users in Spain is participation in social networks (64.1%), which increases up to 94.5% in the 16-24 year age range.[12]

---

[9] European Commission.·»Green Papers, Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values». COM(2013) 231 final, p. 5.

[10] INTECO/AEPD, «*Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online*» [«Study on data privacy and information security in on-line social networks»], 2009. Available at:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf

[11] National Observatory for Telecommunications and the Information Society, «*Las redes sociales en Internet*» [«Social networks on the Internet»], 2011, p. 27. Available at:

http://www.ontsi.red.es/ontsi/sites/default/files/redes_sociales-documento_0.pdf

[12] INE, survey cited.

Another characteristic of the current technological scenario is convergence of the audiovisual world, understood as the «progressive merger of traditional and Internet radiobroadcasting services»[13]. There is a blurred line between linear radiobroadcasting services for TVs and on-demand services provided by the Internet for PCs. By 2016, it is expected that most European Union homes with a TV will have a hybrid unit, enabling the receipt of linear and Internet contents. It is also expected that over this same period of time most consumer Internet traffic will be video-based and that most of the traffic will be basically channelled through mobile devices.

2. *Minors and use of the Web*

Minors are not an exception to this Web use and ICT scenario. For the purposes of this Report and further to the 1989 United Nations Convention on the Rights of the Child, ratified by Spain, minors will be those under 18 years of age, although the available statistics analysed use variable age ranges, making it difficult to make a comparison and diagnosis.

It is very common to treat minors as «digital natives». However, the meaning of this term needs to be clarified.

The term is correct in direct and literal terms. As manifested in a 2009 INTECO study[14], whereas adults use the Internet for something, with a specific purpose, for children the Internet is a vital reality; they simply are and live for the Internet, which is why, as pointed out by Héctor Sánchez before the Subcommittee, they are «always on». We need to refute a false belief held by the adult world: that a virtual world exists separately from the real world. There is only one reality, to which the digital world belongs, which all minors naturally apply.

Further to the foregoing, there is a second interpretation of the «digital natives» term. All minors are intensive users of new technologies, and this intensity varies according to age.

---

[13] European Commission, «Green Book…», document cited, p. 3.

[14] INTECO. «*Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres*» [«Study on safe habits in ICT use by children and adolescents and their parents' e-trust»], 2009, p. 46. Available at:

http://www.inteco.es/guias_estudios/Estudios/Estudio_ninos

The foregoing is reflected in the data already commented on above in relation to the 16-24 age group.

Due to its scope (25 European countries) and link to the European Commission's «Safer Internet Programme», we will now reproduce some of the results of the latest survey conducted as part of Phase II of the EU Kids Online Project amongst European minors between 9 and 16 years of age[15]. These results, though obtained in 2010 and presented in 2011, point towards trends that are still valid overall.

a) Starting age and frequency of Internet use

Both in Spain and in Europe the trend is that users begin to access the Internet at an earlier age. Specifically, the average age of a Spanish minor connecting to the Internet for the first time was the same as the European average (i.e. 9 years, confirmed by the fact that the youngest age group –9-10 years– began connecting to the Internet at 7 years of age, whereas 15-16 year olds claimed to do so at 11).

The frequency in Internet use by Spanish minors was slightly below the European average. Thus, 58% claimed to use the Internet every or nearly every day (60% for all of Europe) and 34% used it once or twice a week (33% in Europe). The total of these percentage figures registers a high percentage (92%) of minors who are frequent Internet users.

There were clear differences by age group. Whereas in the youngest group (9-10) a third (33%) accessed the Internet daily, amongst older users (15-16) daily access was 82%; this difference is very similar to the one existing in Europe (33% and 80% on average, respectively).

The study also measured the length of daily Internet use, despite acknowledging the difficulty inherent to this measurement given that, amongst other factors, minors carried out various activities at the same time («multitask») without totally signing off; consequently, the average length of daily Internet use of Spanish minors was 71 minutes (under the European average of 88 minutes), and a notable difference existed by age group (45 minutes in the 9-10 year range, over 97 minutes in the 15-16 year range, which in European average terms was 58 and 118, respectively).

[15] Vid. citation 4.

To conclude, back in 2010 use of the Internet was already commonplace in the daily life of Spanish and European minors.

b) Signing on

Most minors signed onto the Internet at home (84% of Spanish minors, very close to the European average; 87%), followed by school (70% of Spanish minors, a figure higher than the European average; 63%).

In relation to the home, the respective percentage figures of Spanish minors who used the Internet in their room and those who did so elsewhere in the house were the same (42%, reflecting a difference with the European average, where such average percentage figures were 49% and 38%, respectively).

Age was also a clear differentiating factor: «private» use in the minor's room took place more often amongst adolescents than younger minors.

If, until recently, Internet access was limited to laptops, explaining the generalized advice given to parents to place the computer in shared quarters, with the breakthrough of mobile devices, the place and means with which Internet is accessed have changed.

c) On-line activities

The main activities for which minors used the Internet were: for schoolwork (83% Spain, 85% Europe), games (e.g. videogames played against the computer, 80% Spain, 83% Europe), video clips (78% Spain, 76% Europe) and communications (through instant messaging, social networks or e-mail, 68%, 59% and 62%, respectively; these figures slightly differ in Europe: 62%, 62% and 61% on average, respectively). Other activities were also carried out related to the creation of contents, in lower and variable percentage figures.

It has been pointed out that data on the matter would lean in favour of an «opportunities ladder», whereby certain basic activities tend to be completed first by more children, whereas more creative and participative activities are carried out later by less young people.

In any case, participation in social networks is considered the most rapidly growing «on-line» activity amongst young people.

56% of all Spanish minors surveyed stated to have a private profile on a social network (50% on average in Europe). Age difference was, again, a differentiating factor in an 11%-42% range in the 9-10 year and 11-12 year segments, respectively, and between 74% and 89% were present on the networks in the top range, 13-14 years and 15-16 years, respectively.

Based on the foregoing data, and the legal threshold applicable in Spain to consent to personal data assignments and, consequently, to obtain a social network profile (14 years), it is likely that this age restriction is not being met.

These data, which reflect trends in Europe and elsewhere (Internet access at a gradually earlier age, progressively intensive use by age; home and school as the main points of on-line connection; many different on-line activities, with particular emphasis on communications and the breakthrough of social networks), will probably remain significantly valid.

There is, however, a factor related to the on-line devices used, particularly the use of mobile devices, which will probably mean that our figures are outdated.

In fact, whereas the percentage figures in this study amongst Spanish minors accessing the Internet through a PC were close to the European average (59% through a shared PC, 30% through a private PC, over 58% and 35% on average in Europe, respectively), the use of mobile devices by Spanish minors in order to access the Internet was in 2010 well below other European countries, although at more similar levels to Southern countries and some in Eastern Europe (9% use of mobile phone or other portable device, over 34% use of other devices, on average, in Europe).

The widespread use of mobile telephones, to particularly include Smartphones, very popular in Spain over the last few years, now raises doubts as to whether these figures are up to date.

According to INE data for 2013[16], 91.8% of the children's population between 10-15 years old uses the Internet, and 63% has a mobile phone (on a growing scale, ranging from 26.1% amongst 10 year olds to 90.2% amongst 15 year olds). And although the survey refers to mobile phone availability, Smartphone sales figures (representing 8 out of 10 mobile

[16] INE, survey cited.

phones) indicate that they are widely used by minors to access the Internet. According to Jesús Guijarro, in his speech before the Subcommittee, the current scenario seems to be defined by access to mobile devices at gradually earlier ages, which converge in terms of service with small PCs.

These devices help parents feel that their children are safe and in control, and their children consequently feel free and independent.

Although two of the meanings of the term «digital natives» seem unquestionable (Internet as a natural reality for minors and intensive online access), there is a third meaning that almost operates as a myth, not backed up by empirical evidence: digital competences. In the plausible opinion of Jorge Flores presented to the Subcommittee, minors are not advanced users but, rather, intensive and often compulsive users. Along these lines, it has been upheld that speaking in terms of digital natives means overlooking the need to support children in developing their digital skills.

In the aforementioned survey, minors between 11 and 16 years of age were asked about certain digital competences, focusing on critical examination and safety abilities.

Most of those questioned in Spain confirmed that they knew how to mark a website in the favourite toolbar (76%), to block messages from unwanted correspondents (70%), to find information about how to use the Internet safely (63%), or to compare different websites to contrast information (61%); these figures are slightly higher than the European average (64%, 64%, 63% and 56%), respectively.

On the other hand, approximately half or less claimed to know how to change the privacy parameters of a social network profile (55%), to erase the log of visited pages (45%), to block ads or unwanted spam (52%) or to change the preferences of content filter (27%) (similar percentage figures to the average for Europe).

There are relevant differences by age. Adolescents (13-16 years) claim to have more skills than younger users (11-12 years).

In addition, the 9-16 year population was asked about its level of awareness in relation to that of their parents. Almost half (47%) claimed that it was «very true» to affirm that they knew more than their parents (above the European average, 36%). Age differences in this regard are

very relevant; minors tend to be more in agreement with this statement the greater the age.

Other relevant data are the use of privacy parameters in social networks.

Amongst minor users of social networks in Spain, a private profile (only accessible to friends), a partly private profile (visible by friends and networks) or a public profile (accessible to all) was confirmed by 67%, 17% and 14%, respectively (these percentage figures are higher than the European average– 43%, 28% and 26%, respectively). Although these data seem to indicate greater awareness amongst Spanish minors, they reason may be prevalence of the Spanish network Tuenti, amongst the participating networks, where a private profile is configured by default.

Complementary data are the relatively low percentage of minors who show their address or telephone number (9% in Spain, 14% on average in Europe). although it is common to post some information that is able to identify them in their profile (in Spain, 2.4 data on average, over a total of six, when asked about photo, surname, address, telephone, school, exact age– slightly below the European average, 2.8), and the relatively high percentage of Spanish minors who have incorrectly stated their age in their profile, the highest amongst European Union countries (27%, over an average of 16% in Europe), probably as a result of great restrictions on the age required to have a profile in Spanish networks.

III. RISKS INHERENT TO WEB USE BY MINORS

1. *Opportunities and risks. Type of risk.*

It is undisputed, as highlighted by all the Subcommittee participants, that both opportunities and risks co-exist in Web use. Furthermore, to be exact, *prima facie* one and the other are only possibilities, respectively entailing benefits or disadvantages, depending on many different circumstances, either based on the nature of certain situations (e.g. some, such as bullying, clearly constitute risk factors, whereas others, e.g. visiting pages that host videos, are ambiguous, and may entail opportunities or risks), the closest social surroundings (parents, school, friends) and broader social surroundings (economic, social and cultural factors).

Furthermore, there is a complex relationship between opportunities and given their inter-dependence, i.e. as in other aspects of life, the acceptance of a certain risk level is inevitable in order to reach opportunities, and the challenge consists of finding the right balance, without an excessive emphasis on opportunities, without protection, increasing risk possibilities, or an excessive emphasis on risks removing the former.

In this context, minors have specific needs that are gradually demanding more attention, both in terms of opportunities and risks; this approach is present in Europe both in the «Digital Agenda for Europe» and in the «European Strategy for a Better Internet for Children»[17].

In fact, minors are claiming special needs in relation to games, education and knowledge, creativity, communication and participation, according to age, in group or community tasks. From this point of view, ICT offers huge opportunities, as pointed out by all the Subcommittee participants.

Thus, Alfonso González referred to the Internet as «the great city of the XXI century», a city based on the intensive use of global CIT, open and undergoing constant change, entailing the challenge of integrating school (*per se*, «the most powerful technology developed by man to reach the highest levels of justice and prosperity») with learning possibilities offered by new technologies, consequently serving both children (in equal terms, in order to leave no-one out of basic digital competences, and integrating those with different, and sometimes more creative, intelligence) and teachers («the huge discovery of educational transformation»), for those who, as stated by Ana María Román, use these competences as a key resource in managing improvement in educational quality, encouraging a collaborative and open policy in school surroundings, enabling individualized education and, in general, supporting intermediation when transferring and procuring an interest in knowledge.

Salomé Adroher, Francisco Javier Martos and Liliana Orjuela highlighted this two-fold perspective (opportunities and risks) in relation to the United Nations Convention on the Rights of the Child.

In turn, Dolors Reig emphasized the potentiality of information and communications technology (ICT) as empowerment and participation technologies (EPT), to the extent that they trigger change in intellectual

[17] «Digital Agenda for Europe». COM(2010) 245 final, and «European Strategy for a Better Internet for Children». COM(2012) 196 final.

and relational capacities, of a positive nature, such as fluent (as opposed to crystallized) intelligence, diversity and collaborative and participative activities.

Minors constitute a special-needs group in the digital world, also from a risk point of view. In addition to ongoing training, their individual physical and psychological development characteristics make them particularly vulnerable. As affirmed by Mariano Chóliz to the Subcommittee, in relation to adolescents, minors have not developed their prefrontal cortex areas, responsible for behaviour control, planning and evaluation of the consequences of their acts; the trend is to manifest extreme affective reactions, from excitement to boredom, from pleasure to frustration, and impulsiveness.

Studies conducted further to the EU Kids Online project mentioned above have extended a risk typology, distinguishing between content risks (where the minor plays a recipient role) and contact risks (where the child has a somewhat active, even if involuntary, role, in an adult's activity) and conduct risks (where the child is the author or victim of a certain conduct in a relationship between peers).

Beyond the academic utility of this classification, for our purposes and based on the rich information contributed by all the Subcommittee participants, there is a primary division distinguishing between risks of the Internet and risks on the Internet. Risks of the Internet are risks inherent to the Internet, i.e. not avoidable but the existence of which is inseparable from the Internet, whereas risks on the Internet are those associated to situations that are likely to arise in this scenario, although they may also be present outside.

In turn, risks of the Internet make a difference between, on the one hand, general risks affecting the way in which we receive and apprehend information and the way in which we relate to others (cognitive and relational changes) and Internet use (excessive use); and, on the other, specific risks related to situations where computer systems or tools *per se* are the object of malicious conduct, which may eventually constitute crime and, in turn, be used to commit other crimes (malicious acts involving computer systems or tools).

By simplifying EU Kids Online typology, risks on the Internet should be divided into risks derived from the circulation of contents on the

Internet (content risks), associated to particularly serious conduct (child pornography) or conduct that is generally harmful for minors (exposure to adult pornography or other inappropriate contents), and risks derived from certain conducts where the minor voluntarily or involuntarily participates (contact risks) which, in turn, may be basically divided into those somehow affecting a minor's physical or mental integrity (cyberbullying, cybergrooming, gender-based digital violence, on-line games), those affecting the privacy and protection of personal data (sexting, long-term image difficulties, objectification of digital identity, malicious use of personal data) and those associated to intellectual property (digital piracy).

Before continuing with our individualized examination of the risks of and on the Internet for minors, we should highlight that this is a difficult task, both because the risks are «dynamic and constantly evolving, powered by new technical possibilities that arise nearly on a daily basis»[18], and due to the difficulty in basing an examination on generally recognized objective terms.

Differences in perception and evaluation are evident amongst parents and children. In the EU Kids Online research project, conducted amongst European minors between 9-16 years old, more than half (55%) of European minors who used the Internet manifested that there are situations on the Internet that disturb their peers, a perception that is compatible with that of a vast majority (90%) who considered that certainly there are many positive situations on the Internet for minors their own age. There was a minority, albeit relevant, percentage (one out of every eight, 12%) of European minors who claimed to find situations on the Internet that personally disturbed them (14% in Spain).

However, although earlier studies have disclosed, along with a «digital gap», relevant differences in the percentage of parents and children, these differences tended to decrease. The study indicated that 8% of all parents believed that their children were being disturbed by an on-line situation, over 12% of minors who confirmed disturbing situations, reflecting that parents tended to underestimate their children's harmful experience.

Beyond a perception about the risks affecting Internet users, including minors and their parents, in objective terms there are two types of threats

[18] INTECO. «Study on safe habits …», 2009, op. cit., p. 71.

or risks, based on the global concern generated and reflected in the European Union analyses.

First, those risks inherent to the Internet or which, using it as a platform, are included in the cybercrime phenomenon which, further to European Union's Cybersecurity Strategy, «is one of the fastest growing forms of crime, with over a million daily victims all over the world»[19], and is also very lucrative. According to Ignacio Cosidó in his speech to the Subcommittee, cybercrime is «currently the most lucrative type of crime worldwide after prostitution and drug trafficking».

As stated to the Subcommittee by Ignacio Cosidó, Manuel Escalante, Elvira Tejada and Óscar de la Cruz, this form of crime has specific characteristics: from the offender's point of view, it is a low-risk activity, to the extent that is now professionalized and has generated a business model based on «multi-crime platforms», the use of sophisticated technical resources that enable anonymity, and the difficulty in combating the same, given the global scope of the Internet (the victim and offender may be located in different countries, thousands of kilometres apart) and, from a victim's point of view, it is a threat that may affect the general population and, above all the vulnerability faced by all Web users, if a safety policy is lacking and due to how Internet amplifies the consequences of a crime.

The second risk phenomenon that attracts a lot of attention and concern, as it affects the entire population, revolves around privacy and personal data. José Luis Rodríguez highlighted that the combination of digital memory (allowing all kinds of information to be saved at low cost), the Internet (which allows all these memories to be connected irrespective of geographical location and to transfer and share information in real time), and search tools (which gather and provide access to information with extraordinary capacity) have overcome two barriers –space and time– which until now had very effectively protected people's privacy.

In this technological scenario, Internet governs the self-establishment of interests; it is an unregulated matter, except for certain technical issues, and has been essentially related to the legal system, focusing on traditional means of communication; as Eugenio Fontán pointed out, its

[19] «*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*». JOIN(2013) 1 final, p. 10.

cost-free nature adds another risk factor, as it may be used by on-line service providers to exclude quality parameters.

In this context, personal data protection, applied to the digital world as protection of digital identity, has become a fundamental challenge. This was specifically highlighted by José Luis Rodríguez (personal data protection is a fundamental right, albeit connected to others, with its own autonomy, recognised in the European Union Charter of Fundamental Rights, which should be upheld), Eugenio Fontán («Europe should fight to protect our right to hold any data of our concern»; «in order to achieve a fair society in the data era, we should reach a new data agreement, essentially treating personal data as an asset, over which individuals have a proprietary right», citing Alex Pentland), or Antoni Gutiérrez and José Luis Casal (when highlighting the importance of learning over the value of digital identity).

Surveys conducted in Europe and Spain indicate that there is an extended view amongst the public of a lack of information and mistrust in relation to personal data provided on the Web.

According to the Special 390 Eurobarometer Cybersecurity, 40% of all users are concerned about the risk to which their on-line personal data are exposed.

The CIS barometer published in May 2013, which included questions on personal data protection, has indicated the following: 66% of those surveyed declared that Internet security in relation to personal data protection is low or very low; 70.3% declared to hardly agree or totally disagree with the fact that privacy and information policies, announced on Internet sites, on data processing, are clear and easy to understand (although at the same time 13.8% claims to always or nearly always read the privacy policies published on the website visited); 65.5% declares to totally or sufficiently agree with the fact that websites try to conceal what will be done with our personal data, or 76.5% declares to be very much or sufficiently in agreement with the fact that privacy policies announced on the website try and disclaim any liability in law rather than providing accurate information; 74.6% declared to hardly or to not at all agree with the fact that social networks ensure the safety of their users' personal data; 69.2% declared to be quite or very much in agreement with the fact that it is difficult to control who can see information entered into one's profile; 89.1% declared to be quite or very much in agreement with the fact that social networks should not be allowed to change their privacy policies without their users' consent; 94.8%

declared to be quite or very much in agreement with the fact that social networks should not provide personal data to third parties.

In any case, security and trust are necessary presumptions for the effective development of an information society and, thus, are a strategic cornerstone of two European Union initiatives, which are complementary: the «Digital Agenda for Europe», adopted in August 2010 and updated in December 2011 (Europeans are not in favour of technology they cannot trust; «the digital era hardly operates as a Big Brother or a «cybernetic wild west»[20]; «the European Union should be the world's cutting-edge centre in terms of network and information security, on-line security and the protection of on-line privacy»[21]) and the European Union's Cybersecurity Strategy, adopted in February 2013 (which, amongst other premises, is based on the fact that «European Union essential values are found in both the physical and digital world», the priorities of which include «a huge reduction in cybercrime»[22].)

2. *Cognitive and relational change*

A factor inherent to new technologies, without a time limit for examination purposes, is the way in which users obtain and assimilate information provided by the digital world; it seems undisputed that this factor entails cognitive, even physical changes, of uncertain diagnosis and evaluation, which were highlighted to the Subcommittee by Guillermo Cánovas, Dolors Reig and Miguel Pérez. The first gave an example of these changes with some references, such as the alleged «multi-task» capacity pointed out by young users in participating Committees, referring to the deployment of various tasks at the same time, the cognitive overload caused by excessive Web information or the new form of «f» reading, encouraging on-line information; for all these issues, to cite a few, it is still early to obtain a positive or negative balance but, in G. Cánovas's opinion, they all lead not only to a digital or even generational gap, but also to an evolutionary gap.

For D. Reig, the highlight of changes in cognitive processes resides in development of the working memory, very closely linked to fluent

[20] COM(2010) 245 final, p. 18.

[21] «Digital Agenda for Europe -An engine for European growth». COM(2012) 784 final.

[22] JOIN(2013) 1 final, p. 4.

intelligence and imagination. In turn, Miguel Pérez vouched for alternative activities to somehow compensate the gaps produced by the use of new technologies.

In addition to cognitive changes, new technologies are apparently causing profound changes in the way in which we relate to others and, according to D. Reig, are affecting the various needs of a human being in the well-known Maslow pyramid, referring to «belongingness», «esteem» and «self-actualization».

In this regard, Internet generates a special attraction amongst adolescents by encouraging the need for information, socialization and leisure at this stage of growth. According to the EU Kids Online project, 50% of all European minors between 11-16 years said they found it easier to be themselves on the Internet that face-to-face, a slightly higher percentage than the figure for Spain (40%).

One of the main concerns for the security of minors on the Internet refers to the contacts held through this means, given the absence of warning signals in terms of time, place and context that is characteristic of the Internet, as opposed to the physical world. In this regard the same study disclosed that the vast majority of European minors between 11 and 16 years (87%, 94% in Spain), claimed to be connected on-line to known persons in the outside world (evidencing that Internet connections complemented pre-existing ones established in social circles), although a minor yet significant percentage (39%, also in Spain), claimed to communicate with persons they met on the Internet but who were connected to relatives or friends in the outside world, and a smaller proportion (25%, 19% in Spain) claimed to hold Internet contact with persons without a prior connection in pre-existing social circles.

In turn, given the broader age spectrum analysed by the study (between 9 and 16 years), 30% of all European minors (21% in Spain) pointed out to have held Internet contact with someone not known in a pre-existing relationship, and 9% (same proportion in Spain) claimed to have met up with someone they met on the Internet, although in this latter percentage the majority (57%, 67% in Spain) stated that the person met belonged to his/her social circle– friend or relative of someone personally known. Also amongst this 9% claiming to have dated someone they met through the Internet, 11% (17% in Spain) said they were uncomfortable with the outcome; these percentage figures,

albeit low in relation to the overall number of minors surveyed, are the cause for most concern.

Finally, it has been observed that, based on the minors who met up with an on-line contact, 61% of all parents (70% in Spain) were not aware of the situation.

An analysis of contacts with strangers over the Internet discloses a feature that constitutes a risk factor *per se*, i.e. a decontextualization of situations and relationships, highlighted by some Subcommittee participants (Consuelo Madrigal, Antoni Gutiérrez or Dolors Reig). Decontextualization is not only relevant in relation to these possible contacts, by making it difficult to obtain a clear image of the other users with whom minors interact (the screen excludes warning signals existing in the physical world), also in relation to the minor's image in space and over time, as this image is inevitably distorted. The existence of a long track record of Internet information provided by minors, disconnected from the specific circumstances in which the information was given at the time, could have involuntary negative consequences in the long term.

In short, decontextualization affects the way in which we relate to others, in the same way as the influence of new technologies on certain traits of human behaviour, such as polarization, with multiplying effects.

On the matter, some participants referred to the importance of stressing the value of silence (Javier Urra) or signing off (Dolors Reig), and basic communication rules in Web surroundings. According to Consuelo Madrigal, this constitutes a «virtual semiology».

3. *Excessive Internet use*

A risk factor that is inherent to the Internet and becoming a growing concern, given its effect on minors, is excessive use. Opinions exist indicating that excessive use may cause an addictive disorder, as specifically upheld before the Subcommittee by Professor Mariano Chóliz (although there were other participants who referred to technoaddictions, such as Salomé Adroher, Juan María Martínez, Luis Carbonell, Antoni Gutiérrez, Guillermo Cánovas, Jorge Flores and Dolors Reig). In this regard, there is an «Internet addiction disorder» (IAD), defined in a research study conducted between 2011-2012, which interviewed adolescents between

14-17 years old in seven European countries, including Spain, as a «behavioural pattern characterized by the loss of control over Internet use»[23]. This same study make a distinction between Internet addiction disorder (IAD) and the risk situation of this conduct, encompassing both under the expression «Dysfunctional Internet Conduct» (DIC).

As manifestations of the loss of control generated by addictive conduct, Mariano Chóliz referred to tolerance (the need to use the Internet more and more), abstinence (unease when not using the Internet), use in spite of awareness of the damage caused, inability to stop using the Internet against one's will, excessive time spent in activities related to Internet use and abandonment or negligence in other activities.

Amongst the companies studied, Spain had the highest prevalence of dysfunctional Internet conduct, although the greater ratio in this conduct refers to the 21.3% risk situation, not to IAD in strict terms, which represents 1.5% (the average in the countries examined was 12.7% and 1.2%, respectively).

This same study reveals that boys have a greater tendency towards this disorder, as well as older adolescents and those belonging to parents with little education, and certain activities are more closely associated to this disorder, such as games of chance with on-line betting (which triple the risk of IAD), the use of social networks (for more than two hours a day or having more than 500 on-line «friends») and computer games (playing more than 2.6 hours/day is associated to IAD).

According to Dolors Reig, there is an addiction not to the Internet as such but to certain activities carried out by these means.

This risk factor shows a curved-line relationship between Internet use and benefit, in such a way that greater use is beneficial up to a point, after which it could become problematic.

Juan María Martínez in his speech to the Subcommittee referred to certain recommendations made public in October 2012 by the American Paediatrics Association, to encourage a healthy use of digital tools by minors; this included the need to establish clear rules on their use, to guarantee aspects such as the minor's concentration ability, adequate diet or sleep cycles. Mr. Martínez recalled that the

[23] «Research on Internet addictions amongst European adolescents», see note 4.

Department of Health of the British Government had also manifested itself along these lines.

M. Chóliz, based on the premise that adolescence is critical in the prevention of addictions, explained to the Subcommittee that a «technological addiction prevention plan» was being implemented, launched by the Autonomous Government of Valencia, based on three basic principles: the plan should apply before the problematic conduct appears; it should apply universally and, consequently, at school, given that all adolescents use these technologies; and it should be based on information, awareness and action guidelines.

4. *Malicious acts that involve computer systems and tools*

Web use may entail exposure to spyware and other forms of malware, immediately aimed at interfering or intruding in computer systems or tools, with ultimately varying purposes: hindering equipment operation or, even, a loss of information; making it difficult for users to legitimately access a computer or network (Denial of Service (DoS)); intrusion in order to take over control of an individual or set of computers («botnets» or «zombie networks»), or activating webcams or obtaining passwords.

In turn, computer falsification and fraud exist, where action over computer systems and tools is respectively aimed at generating false data that may be treated and used as authentic, or the fraudulent procurement of an economic profit and correlative material loss for the victim.

All minors, as Web users, may be affected by these situations; according to INTECO[24], these situations refer to spyware, computer locking, or the loss of information (most frequent), and fraud rates are not often declared (amongst European minors between 11 and 16 years old, surveyed in the EU Kids Online project, only 1% claimed to have lost money due to Internet fraud).

From a regulatory point of view, in 2010 (specifically on 20 May, Official State Gazette Number 226, of 17 September) Spain ratified the Convention on Cybercrime, signed in Budapest on 23 November 2001, under the auspices of the European Council, which contemplated two

[24] INTECO. «Study on safe habits...», op. cit., p. 81.

categories in its cybercrime typology, covering many of these situations: «crimes against confidentiality, integrity and availability of data and computer systems», referring to intrusion, interception and interference in computer systems and data, and «computer-based crime», such as falsification and computer fraud.

5. *Child pornography*

Sexual abuse and the sexual exploitation of minors, child pornography included, constitute serious manifestations of violence against children that are universally repudiated, as reflected in various international instruments such as the 1989 United Nations Convention on the Rights of the Child, of which Article 34 demands that all signatory States protect children against all forms of sexual exploitation and abuse, the 2000 Optional Protocol to the UN Convention on the Rights of the Child, on the sale of minors, child prostitution and pornographic use of minors, the 2001 European Council Convention on Cybercrime (Budapest Convention) and the 2007 European Council Convention on the protection of children against sexual exploitation and abuse (Lanzarote Convention), all of which have been ratified by Spain.

In line with these instruments, the European Union approved a Directive in 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (Directive 2011/92/EU of the European Parliament and Council, of 13 December 2011, replacing Council Framework Decision 2004/68/JHA). The Directive constitutes a huge step forward in the adjustment of criminal and procedural laws in Member States so as to contemplate the incidence of ICT in the commission of offences related to the abuse and sexual exploitation of minors, articulating effective devices to fight against the same. The deadline established by the Directive for its implementation into domestic law of each Member State ended on 18 December 2013.

Specifically as regards child pornography, its seriousness arises both from the type of pictures involved, often representing real crimes (pictures of sexual abuse to minors by adults, including rape, as eloquently described to the Subcommittee by Carlos Igual; pictures of minors participating in explicit, real or simulated sexual conduct, or involving their sexual organs, with sexual purposes; or even realistic pictures of minors participating

in sexually explicit conducts, or involving their sexual organs, even if not reflecting an occurrence), and the perverse consequences this entails, referred to by C. Igual, such as cognitive distortions amongst consumers, its use as a means to bully and corrupt minors, and the creation of a supply-demand circle to such an extent that as more and more people demand these pictures the greater the supply, particularly in those countries where children are more socially disadvantaged.

Although the term «child pornography» is commonplace, organizations for the protection of minors (as manifested by Liliana Orjuela to the Subcommittee) prefer the term «pictures of children's sexual abuse», as this better describes the infringement of rights, avoids any comparison with adult pornography pictures and removes any margin of action for paedophiles when promoting and legitimating their criminal activities. The On-Line Safety Report issued by the Culture, Media and Sport Committee, House of Commons, approved in March 2014, has upheld the foregoing[25].

It is difficult to estimate the magnitude of pictures of sexual abuse against minors on the Internet due to the anonymity involved in this criminal activity. However, according to UNICEF, there are millions of pictures of abuse against minors and there are probably thousands of child victims[26]. One of the priorities applied by police corps in this regard (as indicated by Juan Miguel Manzanas and Carlos Igual) is precisely victim identification, given that until victims are identified abuse will continue and assistance may not be provided.

As commented by Óscar de la Cruz to the Subcommittee, currently most child pornography is exchanged in peer-to-peer networks, at the base of a pyramid where the narrowest part consists of closed forums (concealed Internet), where the most violent and serious contents are exchanged and where organized crime is in charge of circulating money.

In Spain, Article 189 of the Criminal Code establishes that it will be a crime to produce, sell, distribute, exhibit, offer and enable the production,

---

[25] House of Commons. Culture, Media and Sport Committee. Report «Online safety», 2014, p. 6. Available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/729/729.pdf

[26] UNICEF. «Child Safety Online. Global Challenges and Strategies», 2011, p. 1. Available at http://www.unicef.es/sites/www.unicef.es/files/Child_Safety_online_-_Global_challenges_and_strategies.pdf

sale, dissemination or exhibition by any means of pornographic material involving underage or disabled children, or possession of the foregoing for these purposes, and to hold this material for personal use. Furthermore, it will be a crime to produce, sell, distribute, exhibit or otherwise provide pornographic material, not directly involving minors or disabled persons, but which use their altered or modified voice or image. As announced to the Subcommittee by Elvira Tejada, we are witnessing an increase in these types of crimes due to the incidence of information and communications technology. According to the 2011 Annual Report of the State's General Prosecution Office, 12.52% of all judicial proceedings filed in Spain for conducts associated to CIT use involved child pornography crimes or others related to disabled persons, and 368 charges were brought by the Public Prosecution Service for illegal events of this kind in the same year.

At present, the Spanish Parliament is processing a Draft Organic Act to amend the Criminal Code that entails certain novelties on the matter, which were positively viewed by Liliana Orjuela and Elvira Tejada. Specifically, the latter referred to the incorporation of a child pornography definition, taken from Directive 201/93/EU, in turn based on the one included in the Budapest and Lanzarote Conventions of the European Council, criminalizing the on-line access to child pornography files, also further to this Directive, to include viewing through «streaming», albeit without an effective download; until now, this circumstance was being required by the courts in order to uphold possession for personal use.

A relevant issue partly affecting the authorities in charge of applying the Act, particularly the judges, in procedural law terms but also in relation to the liability of Internet operators, is the removal of child pornography pictures or locked access thereto. This is crucial in achieving a drastic reduction in circulating pictures on the Internet.

There are two main obstacles to achieve this objective. On the one hand, there is a generally applicable principle that waives liability as to contents in favour of Internet service providers that are usually classified as «intermediaries»: this is the case of telecommunications network operators and access providers (insofar as they merely provide an intermediation service involving data transmission along a telecommunications network or providing access thereto), hosting service providers, to include social networks (as regards the storage

of data) and service providers that enable links to contents or search tools («search engines»). According to the Spanish Act on Information Society and E-Commerce Services (Act 34/2002, of 11 July), which enshrines this principle, these last two types of Internet service providers are not liable for the information stored or addressed to users, as long as «they lack effective awareness that the activity or information stored (in relation thereto) is illegal» or, if aware, «they act diligently to remove the data or to prevent access thereto» (or «to erase or deactivate the relevant link») (Articles 16 and 17 of Act 34/2002).

In practice, «effective awareness» entailing liability of the service provider will either depend on the decision adopted by the competent body, ordering a removal of the illegal information or locked access (i.e. through an external action), or on procedures to detect and remove contents, applied by providers under voluntary agreements, i.e. self-regulation.

The other obstacle to achieve reduced Internet circulation of child pornography, or to limit access thereto, is represented by the global scope of the Internet, in relation to the principle of territoriality in national legislations. Usually, the place where the service provider is established or connection point is what determines the law applicable and the authorities competent to enforce compliance; consequently, the possibilities of response by a country's authorities differ depending on whether the contents are hosted in the country or outside[27]. This is also the case in Spain, where Act 34/2002, of 11 July, is based on the same connection principle (it applies to «service providers belonging to the information society that are established in Spain» and to services offered «through a permanent establishment in Spain», specifying that «the use of technological means located in Spain, to provide a service or access thereto, may not be used, alone, to determine the provider's establishment in Spain»: Article 2), which not only conditions the possibilities of response against those responsible for illegal contents, but also the scope of the duty to collaborate binding «intermediation» service providers, which is limited to those established in Spain (Article 11 of the Act); those located outside Spain will depend on international cooperation channels, and the greater or lesser degree of commitment of the service provider.

[27] See «Online Safety», op. cit., p. 12.

6. *Other content risks*

In addition to child pornography and other criminal contents (e.g. incitement to hate or terrorism) there is a wide range of contents to which minors are exposed on the Internet; these, also licit and protected by the freedom of expression, are harmful to minors insofar as they are potentially damaging in physical, mental or moral terms (adult pornography, sites in favour of anorexia or bulimia, sites defending paedophilia, self-injuring or suicide, etc.).

It is necessary to first make a distinction, given that at present anybody with an Internet connected device is a potential editor, between self-generated contents and those offered by a programmer or editor as part of a business activity. The first are practically devoid of control; the challenge with the second type is the difficulty of translating restrictions to the virtual world which, according to age, operate in the outside world to enable access to adult contents.

Pornographic material is probably the best illustration of such difficulties. Administrative regulations on the classification or sale of this type of material, and a generally accepted criminal sanction of certain conducts (in Spain, the Criminal Code punishes as a crime the sale, dissemination or exhibition of pornographic material amongst minors or disabled persons, «by any direct means»: Article 186) provide an effective set of restrictions on minors' access to this material in the physical world.

However, these restrictions are difficult to apply on the Internet.

First of all, due to possible business models through the Internet that offer pornographic contents and are theoretically uncontrolled as on-line services which, due to their similarity with TV, are covered by audiovisual communication laws.

Thus, for example, there are «on-demand» (or «à la carte») audiovisual communication services, which differ from traditional «linear» television services (which follow a broadcasting schedule) in the possibility of viewing programmes at a time chosen by the spectator and at its request, based on a previously selected catalogue by the editor; these fall within the scope of application of Community law (Directive 2010/13/EU, of 10 March 2010, known as the Audiovisual Media Services (AMS) Directive) and applicable national laws (in Spain, General Act 7/2010, of 31 March,

on Audiovisual Media [*Ley General de Comunicación Audiovisual*] (LGCA)). According to Article 12 of the Directive, Member States shall take appropriate measures to ensure that on-demand audiovisual media services provided by media service providers under their jurisdiction which might seriously impair the physical, mental or moral development of minors «are only made available in such a way as to ensure that minors will not normally hear or see such on-demand audiovisual media services». According to Spain's General Act on Audiovisual Media, Article 7 regulates at length the protection of minors, although it starts off with a general statement that is apparently applicable to all audiovisual contents, prohibiting «the broadcasting of contents that could seriously hinder the physical, mental or moral development of minors, to particularly include programmes that involve pornography, abuse, gender-based violence or gratuitous violence» (section 1), beyond the effectiveness of such statement, the rules contained in this section (focusing on time slots for protection) suggest that it was conceived for traditional or linear television media services; nevertheless, the article makes explicit reference to on-demand programme services, specifically in section 5, which imposes an obligation on service providers to «establish separate catalogues for those contents that may seriously harm the physical, mental or moral development of minors», establishing «devices, programmes or effective systems, updatable and easy to use, which enable parental control by preventing access to harmful contents». In this regard, all audiovisual products offered by an editor, including on-demand products, should be classified by age, based on a digital coding system enabling parental control, certified by the audiovisual authority (Article 7.2 and 6 of the LGCA).

There are, however, other Internet business models through which pornographic contents are available, such as those based on YouTube (usually referred to as «Tube sites»), which offer hard pornography videos at no cost and without restrictions as a window enabling spectator access to other paid pornographic services or advertising space for other services[28], which are not affected by the obligations and control measures foreseen in audiovisual media sector laws.

To this factor we need to add another obstacle, already referred to in relation to child pornography: the global scope of the Internet which,

[28] See «Online Safety», op. cit., p. 21.

in the case of adult contents that are harmful for minors, has a two-fold consequence. On the one hand, whether in relation to on-demand programming services or other on-line services, the possibilities of action by national authorities are limited to what is established within their barriers; consequently, any established outside are able to evade national control (see the territorial scope of application of the LGCA, Article 3). Furthermore, one of the main devices used to restrict access by minors to harmful on-line audiovisual contents is digital tagging which, based on metadata, is conducted by content providers and operates independently from the broadcasting media (television or the Internet). However, as pointed out by Borja Adsuara or Miguel Errasti, whilst also highlighting their relevance as a future action, the foregoing would only be really effective in a global scenario, as an «Internet protocol for content tagging» (B. Adsuara).

7. *Contact risks: «cyberbullying», «cybergrooming», gender-based digital violence, Internet games, «sexting», long-term image difficulties, objectification of digital identity, malicious use of personal information and digital piracy.*

Within the risks present on the Internet, i.e. associated to situations that use this means for production but which also existed and still exist outside, we usually distinguish between two main types: content risks (already referred to above) and contact risks, derived from certain conducts where the minor voluntarily or involuntarily participates and which, in turn, may be broken down into three main categories, according to the legal asset affected.

In relation to contact risks affecting a minor's physical or mental integrity, one of the types that has generated most concern and social alarm is «cyberbullying»: a specific manifestation of general cyberbullying arising amongst minors, referring to threats, harassment, humiliation and other forms of abuse produced through telematic communication technologies[29].

Taken as a whole, of European minors between 9 and 16 years of age who were questioned further to the EU Kids Online project 6% declared

[29] Definition taken from INTECO. «*Guía de actuación contra el ciberacoso*» [«Action guide to fight cyberbullying»], 2012. Available at http://www.chaval.es/chavales/sites/default/files/editor/guia_lucha_ciberacoso_menores_osi.pdf

to have been bullied on-line (4% in Spain) and 5% (as in Spain) confessed to have perpetrated this type of conduct; the rate increased in relation to those claiming to be victims or offenders both on the Internet and outside (19%-16% in Spain– and 12%-9% in Spain–, respectively). But perhaps the most relevant figure is how minors have perceived this situation, and who felt it was most damaging. There is also a relatively high proportion of parents who were unaware of the situation, amongst minors claiming to have been bullied (56% on average in Europe, 67% in Spain).

Elvira Tejada drew the Subcommittee's attention to the increase in the number of threats, duress, humiliation and, in general, acts that degrade minors carried out through new technologies.

This increase is explained by less intense psychological resources of social control and the veil of anonymity and impunity associated to the Internet; however, bullying through and outside the Internet are not separate, nor is there a migration from a school playground to a «virtual» playground; rather, both are connected, in a kind of vicious cycle where offenders pursue their victims through different means and victims have difficulty in escaping from this situation.

Nevertheless, the consequences are not the same: the Internet amplifies the harm in two ways, as indicated to the Subcommittee by Manuel Viota: first, it removes a division amongst the minor's social groups, which previously existed in the outside world; second, it «democratizes» bullying, very often entailing a secondary form of victimization: school drop-outs.

The means in which bullying operates mainly involve instant messaging and social networks, and many different specific actions, as pointed out by E. Tejada: humiliating or degrading messages, recording of the victim in difficult situations or that offend his/her dignity, which are later distributed, identity theft, attributing to the victim certain expressions or conducts in order to damage his/her relations with third parties, etc. These conducts may eventually be criminal, covered by different legal offences, depending on the specific circumstances of the case; in fact, this is being applied by the Public Prosecution Service, as explained by E. Tejada: offence of threat or duress (Articles 169-172 of the Criminal Code) and, even, in the most serious cases, offences against moral integrity (Article 173 of the Criminal Code).

A particularly serious form of cyberbullying is «cybergrooming» (the term «child grooming» is also used, though vaguely, without referring to use of the Internet), which may be defined as «actions (through the Internet) carried out deliberately (by an adult) in order to establish a relationship and emotional control over a child, laying down the ground for the minor's sexual abuse»[30].

The *modus operandi* takes various forms; as indicated by M. Viola, it may consist of appropriating a minor's e-mail account, through which it is able to access his/her digital life and control more accounts, or stealing the identity of an adolescent pursuing the victim's «enamourment».

Cybergrooming was specifically regulated in a reform of the Criminal Code carried out in 2010, consequently implementing the Council of Europe's Lanzarote Convention (Article 23). Article 183.bis) of the Code provides that «anybody using the Internet, telephone or other ICT to contact a thirteen-year old minor, proposing to meet up in order to commit any of the offences described in Articles 178-183 and 189, provided that this proposal is accompanied by material acts aimed at making this approach», will constitute a crime.

Along the lines of the General State's Prosecution Office, in its 2011 Annual Report, on the rigid articulation of this criminal offence, Elvira Tejada pointed out to the Subcommittee that is possible application has been considerably limited; the criminal offence only contemplates thirteen-year olds as victims (this is the age limit currently established in Spain to provide sexual consent) and it is necessary for a proposed meeting with the child to be accompanied by «material acts aimed at making this approach». As a result this crime does not cover –and consequently needs to resort to other criminal provisions– a common situation where the offender does not pursue a physical encounter with the minor but a virtual encounter in order to achieve pornographic material, directly obtained, or by inducting the minor to carry out sexual acts in front of a webcam.

The Draft Organic Act to reform the Criminal Code, which is currently being processed by Parliament, would overcome both limitations: by increasing the age of sexual consent it will extend the scope of application of the provision; and conduct is also criminalized when the offender does

[30] INTECO. «Action guide…», see above, p. 11.

not pursue a physical approach but the procurement of pornographic material.

In turn, Consuelo Madrigal pointed out that the Criminal Code, when defining conducts, also applies to minors if they are also the offenders, albeit with different consequences. This is why when reforming legal crimes, such as sexual abuse, in relation to minors, different ages should be considered which, in Ms. Madrigal's opinion, should be at least five years.

In addition to the cyberbullying situations described, some participants have declared their concern about what Jorge Flores refers to as «digital gender-based violence», as a result of which female minors could suffer twice as victims. Patriarchal patterns and gender stereotypes that seemed to be forgotten are now reappearing, encouraged by new means of connectivity which, as indicated by Antoni Gutiérrez, enable «vigilant use, inquisitive use, protective use and proprietary use of human relations».

Another risk factor of growing concern is on-line games, an activity regulated in Spain since 2011 (Gaming Act 13/2011, of 27 May) which, since then, shows a tendency to increase (in 2012, it is the only form of gaming that increases, and its related expenses are estimated at approximately five thousand million Euros, nearly doubling the expense of the previous year).

The risk associated to gaming is its ability to become an addiction. Professor M. Chóliz explained to the Subcommittee that gambling addiction or pathological gaming is considered an addictive disorder, categorized by the American Psychiatry Association as drug dependence, due to «evidence indicating that gambling activates the brain's system of reward in a similar way to drug abuse and the fact that clinical symptoms of gambling disorders are similar to those of drugs». From this perspective, according to M. Chóliz, on-line gaming has already become the second type of gaming that causes addiction, after slot machines. This is so because on-line gaming has structural characteristics that make it very dangerous: accessibility (users may play with mobile phones), immediate rewards and use of all the resources offered by new technologies (e.g. welcoming vouchers, which work as a «reinforcement sampler» in psychology terms, a strategy used to encourage a certain conduct by reinforcing it in advance).

Unlike traditional games, usually played by adults, on-line games constitute a market niche amongst adolescents and young people that is cause for concern.

Certainly, gaming is forbidden for the underaged, who are protected in Gaming Act 13/2011, of 27 May and its implementing regulations, whereby betting houses, including on-line houses, need to articulate identification and age verification devices. However, in Professor Chóliz's opinion, all identification should be authentic and, furthermore, such protection should be developed further by regulatory means in order to regulate types of games and publicity.

Félix Brezo had the same opinion, when he mentioned that the main gaps in the regulatory framework implemented by Act 13/2011 refer to the existence of platforms located outside Spain, which are beyond control, and unstoppable advertising of on-line games through sports websites or, surprisingly, over the radio; this advertising easily reaches minors, who often include these sites amongst the pages they visit daily. According to F. Brezo, this problem could be handled in legislative terms, similarly to the case of smoking or drinking.

Internet has encouraged other forms of games that fall outside the regulatory framework, such as multiplayer on-line videogames which, according to Jorge Flores, achieve a social network function, beyond any control, and which, due to their playful purpose, attract paedophiles, given that due to their nature both players and their parents are less wary; or videogames with micropayments or new increased reality surroundings, such as «Second Life» or social games where the use of cryptocurrency, as advised by F. Brezo to the Subcommittee, generates speculative exchange beyond state control and tax regulations, giving rise to markets for illegal services or products.

A second group of contact risks is related to privacy and, specifically, personal data protection. We have previously made a general reference to a growing interest in this latter topic. Now we will focus on a more particular topic: certain risks that may particularly affect minors.

Based on the results obtained in certain surveys, amongst the risks to which minors are exposed, considered the most common by the adult population, is the dissemination of disturbing photos or videos. According to the CIS barometer of May 2013, this is the risk, followed by giving too

much personal information to strangers, to which minors are exposed on the Internet, as indicated by a greater number of interviewed persons (39.6% and 22.9%, respectively), followed by harassment in order to obtain sexual favours –17.1%– cyberbullying –6.7%– and the future damage caused by data uploaded on the Web –4.5%– and identity theft– 2.4%.

The term «sexting» (a combination of «sex» and «texting») specifically refers to the exchange of self-generated texts or pictures, of a sexual content; although this is commonplace in private relations, this practice may have unexpected negative consequences due to the high probability of such data or pictures extending beyond the scope of such relationships, becoming public, with the disseminating and long-lasting consequences of the Internet.

The potential damage caused by the publicity of this type of contents, even if generated by the victim, has however occasionally increased the relevance of this type of conduct (based on the results obtained by the EU Kids Online survey, amongst European minors between 11 and 16 years old, 15% claimed to have seen or received through the Internet messages of a sexual content, and 3% apparently sent or uploaded this type of message; Spain is particularly one of the countries with the lowest incidence in this type of practice, with 9% and 1% respectively).

The proposed reform of the Criminal Code, which is currently being processed by Parliament, includes amongst its novelties the criminalization of conducts where, once another person's pictures or recordings are obtained, voluntarily issued in personal surroundings, these are later broadcast without the victim's consent, seriously damaging his/her privacy. Irrespective of how this legislative proposal is evaluated, we should carefully examine, as stated by J.M. Martínez to the Subcommittee, the specific issue of «sexting» amongst minors.

Even if particularly problematic self-generated contents are not exchanged, persons leave a trace on the Internet in many different ways and for vicarious reasons (automatic or semi-automatic capture through cookies when websites are visited, data provided when completing on-line forms or accessing certain services, information downloaded onto social network profiles, blogs or other interactive applications, etc.) that may entail far-reaching risks, which are becoming a greater cause for concern and which particularly affect minors, due to the early age at which digital track records are established and their vulnerability.

One of these risks refers to long-term difficulties in self-image or reputation, caused by personal information downloaded on the Internet. For example, a selection process for a job opening may be based on a prior search of the candidate's digital biography, which may disclose texts, photos or videos from which a negative opinion may be inferred on the candidate's personality, even if they do not correspond to reality due to the data being disconnected from the specific circumstances in which they were created.

In relation to this risk factor, the so-called «right to be forgotten» is very relevant: a specific projection on the Internet of the right of cancellation, which is part of the essence of the fundamental right to personal data protection, consisting of a person's right to apply for removal of any personal data held by a processing third party.

The effectiveness of this right, however, has been questioned until now not only due to the ubiquity of personal and other information circulating on the Internet, but specifically as a result of doubts raised in Europe, and indirectly in Spain, by the application of personal data protection regulations to certain Internet service providers, either based on their activity or location of their parent company; these laws, in Europe, refer to Directive 95/46/EC and, in Spain, to Organic Act 15/1999, of 13 December, on Personal Data Protection, which strictly gathers the Directive's standards, and Royal Decree 1720/2007, of 21 December, approving the Regulations that implement the Act.

A recent decision of the European Court of Justice, dated 13 May 2014, resolving on various preliminary rulings filed by the «Audiencia Nacional de España» (Spanish National Court), further to a lawsuit between Google, on the one hand, and the Spanish Data Protection Agency and an individual, on the other, in relation to the Agency's decision upholding the individual's claim and ordering Google to adopt the necessary measures to remove certain personal data from its index, preventing any future access thereto, contains statements of interest. It states that companies managing search engines (which seek information published or placed on the Internet by third parties, automatically indexing it, provisionally storing the data and, finally, making them available to Internet users following an order of preference), insofar as this activity involves personal data, are responsible for the data processing and, consequently, their activity is materially encompassed by the European

(and Spanish) regulatory framework on personal data protection; furthermore, although the parent company of the search engine and its data processing activity were located outside the European Union, the existence of an establishment in a Member State, as was the case here, used to promote and sell advertising space amongst the citizens in that country, meant that, insofar as both activities are inevitably linked, the regulatory data protection framework of the affected State applied. This two-fold statement meant that the search engine cannot evade the obligations and guarantees foreseen in this regulatory framework, to include removing links to web pages published by third parties, containing personal information, from a list of results obtained further to a search based on the person's name, even if such information is not erased from the websites and even if its publication was legal in itself.

This decision will without a doubt be reflected in the terms eventually adopted by the draft European Union Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[31] (on which the European Parliament already pronounced itself in the «first reading», in a resolution adopted on 12 March 2014). Amongst other novelties with respect to the current Directive (in addition to its nature as a regulatory instrument), it incorporates a wide principle as to its territorial scope, by including, irrespective of the company's main location, any data processing activities that constitute «a supply of goods and services to European Union citizens» or related to «control over their behaviour», and expressly recognises the «right to be forgotten», expressly referring to its relevance for minors (Article 17 and Whereas 53: «*This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet*»).

Another risk which, albeit unknown or insufficient weighted until now in statistics analyses[32], is gradually drawing more attention, is what in this Report will be referred to as the objectification of digital identity,

[31] COM(2012) 11 final.

[32] These exceptions include, for example, the OECD Report entitled «The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them», *OECD Digital Economy Papers*, No. 179, 2011, p. 27. Available at http://dx.doi.org/10.1787/5kgcjf71pl28-en.

derived from a change in the paradigm that Internet has represented for commercial and advertising activity, turning personal data in sought-after raw material for the tracing of gradually more accurate profiles used to provide personalized advertising.

A lack of sufficient awareness about the business model of many Internet services, including search engines or social networks, which are apparently cost-free but are actually paid for with personal information, specifically affects minors which, from a very early age, may involuntarily become the object of invasive monitoring, profiling and conductual advertising; this was pointed out to the Subcommittee by various participants, to include Alfonso González (for whom the basic challenge of integrating school with the learning possibilities offered by new technologies should invoke the danger of turning learning «into information merchandise for Web giants»), Josep Manuel Prats («We have assigned our own image and that of our children without limitation and without the right to be forgotten»), or Consuelo Madrigal (who used a thought-provoking comparison to a «virtual coup d'état» when referring to the threats to freedom caused by industrial solicitations of the imaginary, advertising and the market).

The draft European Union Regulation indicated above, on the protection of individuals with regard to the processing of personal data, foresees an individual's right to challenge the processing of his/her personal data for direct marketing techniques, and to not be the object of profile creation measures using automated processing (Articles 19 and 20, and Whereas 57 and 58).

A third type of risk is the one derived from the malicious use made by other persons of personal information on minors existing on the Internet, consequently enabling trusted and common practice amongst them (such as providing their password to friends, in order to be able to access their mail accounts and social network profiles), and the abundance of such information, not only on the minors themselves but also covering family groups and friends, obtained not only at the minor's initiative but also through the popular «tagging» of photos, and even inadvertently as a result of the geolocation print usually attached to digital photos or the same type of functionality, currently included by Smartphones, providing information on the minor's whereabouts or route followed.

Malicious use may entail criminal conduct worthy of various legal appraisals, such as duress, crimes against honour or crimes against

mortal integrity (see above), or the discovery and disclosure of secrets, if they fall within the circumstances foreseen in Article 197 of the Criminal Code; despite the alarm generated, some crimes are not specifically contemplated by law, such as identity theft.

Elvira Tejada, in relation to this second situation, stated to the Subcommittee that, unless foreseen in other crimes due to its defamatory or libellous content, appropriating another person's identity on the Web and, in general, by electronic means, is not specifically contemplated by criminal law, as it falls outside the closest figure related to «usurpation of civil status» (Article 401 of the Criminal Code), due to not meeting the requirements of the crime, as interpreted by Supreme Court case-law. However, in line with the 2011 Annual Report of the State's General Public Prosecution Service, E. Tejada stated that taking over another person's identity in certain conditions, e.g. on a permanent or actually misleading basis, may seriously infringe one's privacy and serious affect the victim's relations with third parties, which is why it merits a specific criminal response. Identity theft may also be used to harm the minor in his/her relations with third parties, and may also be aimed at accessing information or private data on the minor, on the part of an adult, as preliminary steps for sexual harassment.

To end this chapter on contact risks we will refer to those affecting intellectual property, derived from the illegal activity of certain website allowing users to either directly download films, shows, music or videogames, or to connect to or share links with servers allowing such downloads. The harmful effects of this website activity take various forms, as indicated to the Subcommittee by José Manuel Tourné and Carlota Navarrete.

Perhaps the clearest form is an infringement of copyright, resulting from this activity; more serious is the erosion of collective awareness of the value of intellectual property, not only as an individual asset but also in terms of general wellbeing and employment. In this regard, the data provided by Carlota Navarrete, given that Web use by minors to consume digital contents is now used by adults on the illegal contents market, indicate a consumer trend that is cause for concern.

Another less well-known effect is derived from the highly lucrative business behind this activity, in breach of rules governing the establishment of any Internet services provider (particularly Article 10 of Act 34/2002,

of 11 July, on Information Society and E-Commerce Services), which is consequently performed in unfair competition terms in relation to the legal Internet contents sector.

Also relevant are implications as to collateral risks affecting minors who visit these website, such as exposure to adult contents (links to pornographic contents, extremely violent films), to the advertising of on-line betting houses, or even the risk of being the victim of fraud.

Infringements of intellectual property which, in the criminal law field an according to the 2011 Annual Report of the State's General Prosecution Office, «only enjoys very scattered minority case-law, which is very often contradictory», have been affected by the entry into force of the Regulations approved by Royal Decree 1889/2011, of 30 December, implementing the forty-third final provision of Sustainable Economy Act 2/2011, regulating the operation of the Intellectual Property Committee, a section of which is entrusted with filing administrative proceedings in the event of a «breach of intellectual property rights by the head of an Information Society service, as long as said person is directly or indirectly acting for a profit or has caused or is able to cause material damage to the right holder».

The relevance of social networks as privileged platforms for communications between persons and groups means that they are now the centre of attention in relation to the approach adopted to handle some of the contact risk factors examined.

The Subcommittee has been provided with the opinion of three important social networks: Tuenti, Facebook and Twitter.

Tuenti is a Spanish technological company which, according to Sebastián Muriel, has close to two hundred highly qualified employees; its business model is focused on social communication tools, and its centre of gravity has changed from an initial web service to Smartphones. Currently, there are 16 million registered users and between 5-6 million users are active in relation to the mobile operator, of which 75% are of legal age.

In relation to Facebook, Natalia Basterrechea pointed out that there are more than 1,200 million active users on the platform, including approximately 18 million in Spain, and that approximately half sign on daily, very often through mobile phones.

Twitter, according to data provided by Sinéad McSweeney and Patricia Cartes in their speech to the Subcommittee, has 400 million visitors a month, reaching 1,000 million «twits» every two days.

As already seen, interaction not only through instant messaging and social networks is part of the main activity carried out by minors through the Internet, but also the age thresholds established for their presented are often not met; these thresholds usually coincide with the minimum age imposed by applicable law to provide consent to personal data assignments.

In this regard the general regulatory framework on personal data protection should be taken into account; in Spain, this is represented by Organic Act 15/1999, of 13 December, on Personal Data Protection, and by Royal Decree 1720/2007, of 21 December, approving the Regulations implementing the Act. Specifically, Article 14 of the Regulations sets fourteen as the age below which it will be necessary to obtain the consent of parents or tutors to agree to personal data processing; consequently, minors under fourteen years of age cannot provide their consent themselves in order to create a profile on a social network. Furthermore, the «file or processing manager» (of the social network) will «articulate procedures to guarantee that the minor's age has been effectively checked and the authenticity of consent provided by parents, tutors or legal representatives (Article 13.4).

The Spanish company Tuenti has set fourteen years of age as the threshold for minors to register by themselves on this social networks, whereas the age determined in social networks of the U.S. parent company is thirteen, precisely the age determined in the U.S. in the «Child Online Privacy Protection Act» (COPPA). By the way, this is also the age proposed in the European Union Regulation, currently being processed, on the protection of individuals as regards personal data processing and the free circulation of these data[33].

As regards Facebook, José Luis Rodríguez announced that in Spain, at the request of the Spanish Data Protection Agency, the age for access has increased from 13 to 14 years in order to adjust to Spanish regulations.

The problem resides in articulating an age verification procedure when registering on a social network; this procedure does not exist *de*

[33] COM(2012) 11 final, Art. 8.

facto in any social networks, and only leading networks have established devices for *ex post facto* action, usually based on reports filed by the user community. The social network that has made the most progress in this regard is Tuenti, whose verification protocol and erasing of under-fourteen profiles includes an electronic Spanish Identity Card (DNI) (DNIe) for a subsequent identity check.

Sinéad McSweeney and Patricia Cartes (Twitter) informed the Subcommittee that the minimum age to be present on Twitter is thirteen, and that the platform is based on a «data collection minimization» principle; consequently, in order to open a real account no details as to age, location or other are requested, and a reporting device is entrusted with the task of advising and eventually withdrawing under-thirteen accounts.

Tuenti, Facebook and Twitter informed the Subcommittee of their «community» policies in order to handle harassment situations in a broad sense, amongst others. The common denominator of all these policies, based on self-regulation, is to entrust the users with detecting and reporting, through the relevant devices, any inappropriate contents or conducts on the social network.

Specifically, Sebastián Muriel, on behalf of Tuenti, explained that the company's commitment to the protection of minors is based on three cornerstones: to provide tools to minors, parents and educators (available at the Assistance and Safety Centre), in order to report any content or profile that does not meet the terms of use, which could entail a locking or removal of the reported account; the adoption of agreements with security corps and forces and with organizations for the protection of minors; and information and education for minors, parents and educators on all available tools. Furthermore, Tuenti's security strategy includes a device to check compliance with the principle to only allow real identity, by associating a profile created on the network either to a prior invitation from another user or to an e-mail address or telephone number.

Natalia Basterrechea, on behalf of Facebook, explained that the platform's rules of conduct are based on a «Declaration of Rights and Responsibilities» and on «Community Rules», and that, specifically, bullying, intimidation or harassment are forbidden, as well as to share and update content related to a speech that incites hatred, threats, pornographic content, content that incites violence or contains nudity or graphic violence. Any illegal, deceitful, malicious or discriminatory activity is forbidden.

In order to guarantee effective compliance of these rules, many tools are available, including «social reporting» tools, based on an innovative line of research («Compassion Research») aimed at designing a more compassionate and humanized interface, enabling Facebook users to establish more significant connections and to resolve conflicts in an effective manner. Consequently, «social reporting» is a tool that tries to amicably settle a conflict between two persons, with the held of a third party in their surroundings and without having to file a report as such. In 85% of these cases, the system has been able to resolve the matter raised.

The reporting channel, available to users, is another tool, where examination of a situation is entrusted to an operating team, working 24x7, able to provide assistance in more than 24 languages through offices distributed between the U.S., Ireland and India.

Ms. Basterrechea completed her description of Facebook's security policy by referring to the «Family Security Centre», to which there is even free access, containing abundant educational and informative material, with specific guidance for adolescents, and the profuse collaboration between Facebook and many different agents, through the «Advisory Council for Global Security», represented by five large U.S. and European organizations, advising Facebook on matters related to Web security, through specific relations with many different organizations and state security forces.

Sinéad McSweeney and Patricia Cartes explained that Twitter has two main teams: the «Trust & Safety» team, with different specialities (including user rights and privacy –in charge of under-thirteen minors present on the Network and privacy components–, user safety –in charge of situations related to abuse, harassment, self-injury, suicide–, legal application –in charge of relations with security forces– and the exploitation of minors– which, along with the user security team, is not only in charge of examining any report on the matter but also actively collaborates to combat contents related to the exploitation of minors), and user assistance (providing more general support, including a help desk, and the solution of technical problems related to spam or malware). Both teams, both in San Francisco and Dublin, provide user assistance 24x7.

The procedure to ensure compliance with terms of use is the reporting device, which may be channelled through the help desk or by sending a «twit»; when the «More» key is selected, a menu is displayed where it is

possible to «lock» or «report» and, in this latter option, there arte various possibilities.

Ms. Cartes specifically referred to two types of situations: (i) situations of abuse and harassment which, based on their prohibition and after evaluating the relevant report, may entail a mere warning that reiterates the rules, to which the vast majority of users react positively, or even a provisional suspension of an account and, in the most serious cases, a permanent suspension of the account, and in the case of threats, a recommendation to contact the security forces; (ii) exploitation of minors, for which Twitter has zero tolerance; the company is committed to not only reporting any content of this kind to the National Center for Missing and Exploited Children (NCMEC), with which the Civil Guard has VPN connection –the way in which to obtain specific details on a user that is sharing this type of content–, but also actively collaborates, as reflected in its PhotoDNA technology. Furthermore, Ms. Cartes referred to the prohibition of identity theft, for which a reporting device may also be activated and which may entail suspension of an account.

In privacy matters, minors (and many adults) often tend to overlook declarations, conditions or terms of use for Internet services, including social networks; in turn, these declarations often do not include the special characteristics of this user group, neither formally speaking, i.e. clear information policies, nor with respect to other service configuration issues, which would endow the experience of minors on the Web with greater levels of safety.

The Spanish company Tuenti is very committed in this regard, as shown in the following basic principles referred to by Sebastián Muriel:

- Maximum privacy applied by default for all users; as commented by José Luis Rodríguez, this principle is being recommended by data protection authorities and means that data access to third parties will depend on the user's conscious and voluntary decision.
- Non-indexation of user data and personal information in search tools.
- Encrypting and encoding of chats (SSL protocol).
- Distinction between «contacts» (only for chatting) and «friends» (to chat and share information, contents, notice board, etc.), in such

a way that a user may add another user by choosing one category or the other.

- The foregoing is completed with a privacy policy which, from an informative point of view, should be user-friendly, and a simple Privacy Subcommittee, with which to configure a level of privacy and help and safety centre– «tuenti.com/privacy», with informative and educational help resources, including audiovisual space and recommendations on responsible use for parents, educators and users.

As stated by Natalia Basterrechea, Facebook is subject to the European data protection framework, through its establishment in Ireland, which means it is supervised by the data protection authority in charge of this establishment, i.e. the Irish authorities.

In relation to Twitter, Sinéad McSweeney and Patricia Cartes highlighted the public nature of the platform, as to contents («twits» are, as a whole, public or private, and there is no possibility of choosing the addresses of each specific content), which is compatible with user privacy; it is possible for accounts to be anonymous, and a data minimization principle applies, evidenced by the company's early decision to remove any photos uploaded onto the platform, and information on geographical location.

IV. WHAT TO DO?: MINORS AT THE HEART OF A DIGITAL CITIZENSHIP STRATEGY

1. *Five key ideas*

In a Report like the present one, which acts as a report for political action, this is a decisive chapter; its purpose is related to the powers of a parliamentary chamber, such as the Senate, to provide general political guidance to the Government. This means that the object matter is approached in a specific way.

According to the information provided by all the participants and the documentation examined, five key ideas may be pointed out:

— Although, from many points of view, Internet provides huge opportunities, it also entails a series of greater or smaller risks;

public policies therefore face the challenge of finding an adequate balance between one and the other. In this content, minors have special needs, from one or the other perspective.

— The values that enshrine fundamental human rights, acknowledged in the Spanish Constitution and in international treaties, should govern both the physical and digital world; in the case of minors, they guarantee their «higher interest» as a «priority» for public authorities or private institutions in any related acts (Article 3 of the 1989 United Nations Convention on the Rights of the Child and Article 24 of the European Union Charter of Fundamental Rights).

— The existence of different agents with relevant interests in this subject matter (public powers, children and parents, schools and educators, private organizations in the social action sector, various kinds of companies related to the Information Society), raises the basic issue of the role played by the two main circles where the agents operate –State and society– representing two different regulatory perspectives (regulation and self-regulation, respectively). The answer to this question is based on a shared responsibility system.

— The existence of many different agents and regulatory approaches (regulation and self-regulation) requires a national strategy on the needs of minors on the Internet.

— The dynamic and global nature of the Internet means that national objectives and actions cannot ignore the international sphere, both as regards political and regulatory decisions and in operational terms.

2. *Self-regulation and regulation for the protection of minors on the Internet: public-private alliance*

The evolution of the Internet has granted undisputed protagonism to the self-establishment or self-regulation of interests, relegating the State to a minor role, due to the overwhelming speed of technological evolution and international accessibility of the Web; as a result, the law is generally not adapted to the digital world, a point made by several participants in the Subcommittee.

This statement is not a negative opinion on self-regulation, which is ordinarily granted a main role in protecting minors in this field; it does, however, raise the issue of the position that the State should ideally have and, specifically, how to adequately connect self-regulation and regulation.

There is a very wide range of self-regulation and co-regulation initiatives, and the boundaries between both terms are unclear; the latter would seem to refer to a combination of public and private regulations, whilst the former refers to a voluntary commitment of the private sector with no governmental participation. The formulae most broadly accepted at present are public-private partnerships, at the intersection of co-regulation and self-regulation, where the Government actively negotiates the commitments raised in order to be voluntarily adopted by participating private enterprises. The outcome of these formulae contain self-regulation characteristics, but the process is catalysed within a public-private alliance.

The European Union and its Member States tend to follow a model that combines various approaches –regulation and self-regulation and co-regulation– highlighting one or the other depending on the type of risk.

Self-regulation has been, and still is, important in the European Union, given its ability to adjust to technological development and social trends, with relevant initiatives such as those related to mobile telephony communications, social networks and on-line games. Thus, in 2007, the European Commission sponsored an agreement between Europe's leading telephony operators and content providers, the so-called «European Framework for Safer Mobile Use by Younger Teenagers and Children»[34], which describes principles and measures, classified into four groups (contents, access control devices, education and awareness and collaboration with police forces and the courts in the fight against illegal contents), to be implemented in each country, a copy of which was adopted in Spain by leading telephony operators; before the end of 2007 a code of conduct was adopted which, as recalled by Sofía Fernández de Mesa, is still in force and has enabled, amongst other initiatives, the development of a common icon to report illegal contents, available not only on company websites but also downloadable in Smartphones and tablets.

[34] Available at http://www.gsma.com/gsmaeurope/wp-content/uploads/2012/04/saferchildren.pdf

Soon after, in 2009, the «Safer Social Networking Principles for the European Union»[35] came to light, proposed by leading social networking operating in Europe, after a consultation process with the European Commission and non-governmental organizations, focusing on making recommendations in seven fields (to increase awareness; to encourage an appropriate range of services by age; to train in the use of technology; to provide user-friendly devices to report contents or conducts in breach of the terms of use; to effectively respond to earlier reports; to evaluate the review of reports on illegal or prohibited contents or conducts).

The PEGI («Pan-European Game Information») On-Line Security Code, adopted in 2003, is another relevant example of European self-regulation with a broader scope than that of the European Union as an organization, whereby the signatories, amongst other commitments, adhere to a content classification system.

These are not the only self-regulation initiatives in Europe that focus on the protection of minors on the Internet. We may also refer to the ICT Coalition for the Safer Use of Connected Devices and On-Line Services by Children and Young People in the EU– launched by the so-called «extended» ICT sector (telecommunication operators, content providers, search engines, device manufacturers[36]) or the CEO Coalition to make the Internet a Better Place for Kids[37], further to an announcement called by the European Commission amongst the CEOs of large ICT companies.

The self-regulation approach is now intertwined in the European Union with regulatory frameworks that identify the protection of minors on the Internet amongst their basic principles. Such is the case of the 2010 Directive on Audiovisual Media Services (Directive 2010/13/EU), indicated above, which extends the protection of minors with respect to inappropriate contents to commercial communication or à la carte (on-demand) audiovisual services offered by the Internet, or the 2011 Directive on combating the sexual abuse and sexual exploitation of children and child pornography (Directive 2011/92/EU).

Under Spanish law, self-regulation should be encouraged by the Public Administrations. Thus, according to Article 18 of Act 34/2002, of

[35] Available at http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf

[36] Available at www.ictcoalition.eu

[37] Available at http://ec.europa.eu/digital-agenda/self-regulation-better-internet-kids

11 July, on Information Society and E-Commerce Services, the Public Administrations «will encourage (…) voluntary codes of conduct», adopted by «corporations, associations or commercial, professional and consumer organizations», and «will particularly take the protection of minors into account», «stimulating, in particular, the setting of common criteria agreed by the industry for the classification and labelling of contents and the adhesion of content providers».

On this second issue, leading television channels executed a Self-regulation Code for Television Contents and Children in 2004, which General Act 7/2010, of 31 March, on Audiovisual Media, expressly recognises for the implementation of the obligations imposed by the Act on all providers of television audiovisual media services, including on-demand services, content classification and labelling (Articles 7 and 12).

In turn, Act 34/2002 also imposes certain obligations on the industry to inform users about technical tools to increase Internet safety, including «any existing tools for filtering and restricted access to certain undesirable Internet contents and services, or which may be harmful for young people and children», and each user's responsibility «if the Internet is used for illegal purposes, particularly to commit criminal offences, and a breach of intellectual and industrial property laws», although these obligations are limited to Internet access providers (Article 12.bis) of the Act).

3. *Leverage for action: strategy, coordination, consistency and international cooperation*

In its «European Strategy for a Better Internet for Children», issued in 2012, the European Commission recognised that the various policies launched until now in Europe in favour of minors have not merged into a consistent network; it claimed that «Europe needs a strategy that avoids market fragmentation and creates safer on-line surroundings that are enriching for all European Union children»[38].

At a national level, the adoption of a strategy is also an instrument or indispensable leverage of public policies related to the needs of minors in Internet surroundings, where many different agents co-exist, as well as

[38] COM(2012) 196 final.

regulatory frameworks (self-regulation and regulation) and action levels (national and international).

Several participants in the Subcommittee have highlighted the value of strategy as leverage to handle the challenges raised by the needs of minors on the Internet.

In the governmental field, this was upheld by Víctor Calvo-Sotelo, Manuel Escalante and Salomé Adroher when they referred to the main instruments approved by the Government with an impact on the matter: the Digital Agenda for Spain, approved by the Council of Ministers on 15 February 2013, where objectives 4.1 and 4.2 respectively refer to «boosting the trustworthy services market» and «reinforcing capacities for digital trust»; and the «II National Strategy Plan for Children and Adolescents 2013-2016 (II PENIA)», approved by means of a Resolution adopted by the Council of Ministers on 5 April 2013, where objective 2 is to «encourage children's rights and protection in relation to the media and IT in general»

On an individual basis, Ignacio Cosidó and Arsenio Fernández de Mesa highlighted the relevance of a strategy to fight against cybercrime, which should be transversal due to the special characteristics of crimes committed on the Web.

In relation to child protection organisations, Liliana Orjuela and Jorge Flores specifically referred to the ned to adopt a national strategy.

Liliana Orjuela claimed that this strategy should fall within a more general one to protect children against violence, in line with the «Council of Europe Policy Guidelines on integrated national strategies for the protection of children from violence», approved in 2009 through a Recommendation of the Committee of Ministers (REC(2009) 10), and in the broader scope of commitments for signatory States derived from the United Nations Convention on the Rights of the Child.

Jorge Flores highlighted the importance of designing an integral, effective and flexible plan, meeting three conditions: determination and consistency over time; coordination and optimization of resources, and conditions for efficiency; and rapid adaptation. In this sense, he encouraged the public powers to overcome their operating limits and to act in advance.

In effect, the conceptual keys of a strategy in the matter are coordination and consistency. Coordination seeks to bring together with

decision and management processes of the various agents in the field; and consistency seeks to avoid both internal contradictions in actions individually considered in relation to the objectives each one pursues, and to align all actions in all sectors in light of the objectives laid down.

Coordination and consistency should be encouraged through specific organisational formulae that constitute a firm step forward from a mere aggregation of many different public and private initiatives to a high leadership strategic view and long-term commitments; this idea may be considered one of the guiding lines of practically all the Subcommittee participants, which Óscar de la Cruz specified as the creation of a «national coordination centre» to bring together all competent bodies in the matter, also integrating the private sector and enabling a flow of information for all.

An interesting example is provided by the United Kingdom; based on the recommendations of an independent report (known as the Byron Report), the UK Council for Children's Internet Security (UKCCIS) was established, where more than two hundred agents are represented, both public and private, the task of which is to design and implement a Security Strategy for Minors on the Internet (a first version was published in 2009).

It is more common to create work groups, with governmental leadership or where the government participates with other interested parties, as is the case in Spain where, in addition to bilateral coordination in specific matters, e.g. between two Ministerial Departments, some general work groups exist. Borja Adsuara, Manuel Escalante and Salomé Adroher referred to the «Internet and Minors» group created in May 2013 and directed by the National Institute for Communication Technologies (INTECO), which coordinates the work of different participating bodies from the Central Administration.

The issue raised is whether this level of articulation is sufficient or whether another step should be taken towards requirements inherent to strategy, coordination and consistency. In turn, the matter should be viewed specifically in terms of children's needs on the Internet, or should be subsumed into a broader perspective of the organisational model to be adopted in governmental terms in Internet matters.

There is open debate on this last point, with different opinions, such as those who are in favour of a High Digital Commissioner (along the lines

of the Chief Digital Officer (CDO) in some Administrations in the U.K./ U.S., referred to by Antoni Gutiérrez in his speech to the Subcommittee, or those who are in favour of more standard organisational formulae applied by the Spanish Administration.

Presently, the Spanish model places public competences in Internet matters in the ministerial sphere, specifically the Secretary of State for Telecommunications and the Information Society, belonging to the Ministry of Industry, Energy and Tourism (with the support of Red.es which, amongst other duties, is in charge of serving as an «observatory in the telecommunications and information society sector», «the issue of studies and reports and, in general, advice from the General State Administration in anything related to the information society», and «development and progress in the information society», as established in the sixteenth additional provision of Telecommunications Act 9/2014, of 9 May, and the National Institute for Communication Technologies (INTECO), identified by the Digital Agenda fort Spain as the reference centre in digital trust and cybersecurity); in addition, action is also taken by the Secretary of State for Education, the Secretary of State for Social Matters, the Secretary of State for Security, through the State Security Corps and Forces, and the Ministry of Justice, complemented with those applicable to the National Commission Markets and Competition (created by Act 3/2013, of 4 June, which combined the tasks of various regulatory bodies, to include the Telecommunications Market of Commission and the State Council for Audiovisual Media) and the Spanish Data Protection Agency (regulated in Organic Act 15/1999, of 13 December, on Personal Data Protection). In addition to this organisational unit are the tasks assigned to the Advisory Council for Telecommunications and the Information Society, contained in Act 9/2014 (fifth additional provision).

One last lever for action, which is essential in all Internet matters, and also as regards the needs of minors, is international cooperation, both in terms of political-regulatory decisions or influence (in European Union member states this is a natural platform for action, without forgetting other regional bodies such as the Council of Europe or the OECD, ITU or the Forum for Internet Governance itself) or operating bodies, where the importance of cooperation takes on various forms: harmonization of national statistic frameworks, in order to consistently measure the access, use and prevalence of Internet risks amongst minors; cross-border cooperation of police authorities to prosecute and fight against crime;

activity of on-line help networks and Internet security centres, respectively, INHOPE and INSAFE, originally European but which have now become international cooperation models; awareness and information, a notable example of which is the Safer Internet Day arranged by INSAFE, the yearly edition of which is gradually becoming more important; or initiatives that promote international standards for the interoperability of many techniques, such as parental control on platforms or devices.

4. *Objectives and actions*

The «European Strategy for a Better Internet for Children» raises four basic objectives, around which specific actions are articulated:

1) To stimulate quality on-line contents for young people.
2) To intensify awareness and skills.
3) To create a safe on-line environment for children.
4) To fight against sexual abuse and the sexual exploitation of children.

This Report will basically follow this outline although, based on the participants' contributions, who have unanimously indicated that education is the priority to cover the specific needs of minors on the Internet, both in terms of opportunities and risks, proposes that minors be trained in digital competences and that awareness be the primary objective; this objective is related to encouraging quality on-line contents for minors and should be complemented with double outside protection provided to the minor through an acceptable level of safety in on-line surroundings, and a regulatory and law enforcement system that provides an effective response to illegal Web contents and conducts.

Thus, the Subcommittee has proposed the following objectives for a strategy of opportunities and safe and responsible Internet use for minors:

1) Enablement in terms of digital skills and general awareness.
2) Promoting quality on-line contents for children and adolescents.
3) Protection through an acceptable level of security on the Internet.
4) Protection through a regulatory and law enforcement system that provides an effective response when there are illicit contents and conducts found on the Internet.

4.1. Enablement in terms of digital skills and awareness

One of the cornerstones of the «Digital Agenda for Europe» precisely consists of «encouraging digital skills, abilities and inclusion»; in relation to the foregoing, it has been affirmed that «digital competence is one of the eight key competences that are essential for persons in a knowledge-based society...», and part of this is to «guarantee safety on-line»[39].

The Agenda thus applies an approach on «key competences for lifelong learning», contained in the Recommendation of the European Parliament and of the Council of 18 December 2006, which defines these competences as «all those required by individuals for their personal achievements and developments, and for active citizenship, social inclusion and employment», to include «digital competence», which «entails the safe and critical use of technologies of the information society for work, leisure and communication», and «is backed up with basic ICT competences: the use of computers to obtain, evaluate, store, produce, present and exchange information, and to communicate and participate in collaboration networks through the Internet».[40]

Likewise but with a broader scope, for a «European Strategy for a Better Internet for Children» «digital and media skills and related abilities are crucial for children's Internet use» and for the future of society itself, given that, ultimately, «the way in which children now behave on-line will help define the digital world of tomorrow»[41].

Digital skills (which includes digital security, but is not exhausted here) and media skills, which extends the former's scope, indicate a new concept –digital citizenship– which emphasizes creative and participation opportunities on the Internet for minors.[42]

If coordination as a means to pool objectives and actions, translatable into organisational formulae that are consistent with the principle's requirements, was one of the main lines followed by all the Subcommittee participants, another recurrent idea was the importance of learning at school on the safe and responsible use of new technologies, which some

[39] COM(2010) 245 final, p. 28.

[40] Recommdendation of the European Parliament and of the Countil of 18 December 2006 on key competences for lifelong learning (2006/962/EC).

[41] COM(2012) 196 final, pp. 9 and 18.

[42] OECD, op. cit., p. 73.

participants connected to the idea of citizenship and status of minors as rights holders, to particularly include the right to intimacy or privacy and personal data protection (Francisco Javier Martos, Liliana Orjuela, Jorge Flores; focusing on the need to learn how to protect and manage digital identity, José Luis Rodríguez, Eugenio Oñate, Antoni Gutiérrez, José Luis Casal, Consuelo Madrigal, Joaquim Bayarri), communication abilities in general (Josep Manuel Prats, Javier Urra, Consuelo Madrigal, who even referred to a «virtual semiology», regarding communication skills in the digital world) or abilities usually assigned to «social and civil competences», which include psychological resouces such as resilience (or capacity to face adversity –also referred to in relation to Internet risk factors–), respect and empathy, or civic values that help a person belong to the community (Dolors Reig, Javier Urra, José Luis Casal, Joaquim Bayarri, Jorge Flores; particularly focusing on the need to uphold intellectual property, Miguel Pérez, José Manuel Tourné, Carlota Navarrete).

However, this learning raises different possibilities in the way it is implemented; it may be included in the educational syllabus as a subject or specific course, or as a transversal component (where the participants gave different opinions, at least generically speaking) and, in turn, in one way or the other, it should be included in primary education or at a later educational stage (the general opinion was favourable to including the subject at the first stage of mandatory education).

Organic Act 2/2006, of 3 May, on Education, points out that both respect for values and cohabitation rules and the adequate use of information technologies are a priority at the various stages of basic education and secondary school (as foreseen in Articles 17.a) and i) in relation to Primary Education, 23.a) and e), for Secondary Education, and 33.a) and g), for University Entrance Studies) This idea is reiterated in the Preamble to Organic Act 8/2013, of 9 December, to improve the quality of education («the responsible and orderly use of these new technologies by pupils should be present throughout the education system» –section IX of the Preamble–), although the Act does not make any changed as to how to articulate this learning in the syllabus (given that new Article 111.bis) introduced by the Act into Organic Act 2/2006, of 3 May, on Education, refers to ICT viewed as an educational tool); in this regard, the rules established in the regulations should apply, which establish the basic syllabi applicable at each education stage.

From these rules (currently consisting of Royal Decrees 126/2014, of 28 February, 1631/2006, of 29 December, and 1467/2007, of 2 November, on primary education, secondary education and university entrance studies, respectively), learning is primary seen in the use of ICT (in the same way as civic values) as transversal learning, which should be present in all subjects, without prejudice to specific treatment in some subjects taught during each educational stage.

Initially, transversality seems inherent to the idea of «key competences» referred to in the Recommendation of the European Parliament and of the Council; it is the line of argument gathered in the valuable Preamble to Royal Decree 126/2014, which establishes the basic syllabus of Primary Education (the first and only syllabus, until now, to develop basic syllabi in educational stages, following the entry into force of Organic Act 8/2013, on the improvement of education), which claims to be based «in line with Recommendation 2006/962/EC, of the European Parliament and of the Council, of 18 December 2006, on key competences for lifelong learning, on the enablement of competence-base learning», «characterised by its transversality, dynamism and comprehensiveness».

A different matter which should probably be analysed further is the level of effective consolidation, throughout the itinerary followed during various educational stages, of digital competence asserted as a basic or key competence in the syllabus.

The articulation in a syllabus of digital competences (to search, prioritize, store, use, produce and share information, communicate and participate in collaboration networks, management of digital identity and awareness of risks of and on the Internet, and the ability to face these, are basic components) has been practically unanimously upheld as the epicentre of all actions aimed at training minors in these competences; however, other related actions appear, as a presumption or necessary complement thereof.

As specifically indicated by participants from the field of education and child protection organizations, it is necessary to train teachers and professors, already at the university stage (university programmes should be updated– José Miguel Rosell), particularly in order to remove the barriers that still exist in ICT learning and in continuous education (Miguel Comín, Carlos Represa), adjusting to the evolution of technology.

A necessary extra consists of training parents; as in other activities entailing risks, parents «lend a hand, teach the rules and work alongside their children» (Antoni Gutiérrez, Luis Carbonell, Josep Manuel Prats, Jesús Salido).

Whereas actions related to the school syllabus of university study programmes –constituting regulated learning– refer to regulatory measures, all other actions are related to informal learning; this is not only of interest for parents, but also for children and adolescents (to complement their regulated education) and for their teachers (as part of continuous training), and are part of actions for general awareness.

It could be said that, to a large extent, the effort made to train minors in a safe and responsible use of ICT has been present in this type of awareness action through multiple initiatives, either public –launched by bodies in various fields– or private –deployed by organisations in the social action sector and companies in the ICT sector as part of their corporate social responsibility (those who participated in the Subcommittee on behalf of these companies provided information on these initiatives).

The challenge in this field is to bring all these initiatives into a strategy which, based on formal learning at the epicentre of digital competence training actions, is complementary, coordinating and aligning them, using public-private alliances and also involving the media (Salomé Adroher and Antoni Gutiérrez), consequently ensuring that everyone (children, parents, teachers and educators) are effectively informed. All coordination should also take into account any effort made in Europe, particularly through the Commission programmes and events such as a «Safer Internet Day», arranged each year in February, promoted by INSAFE, the European network of Internet security centres, held in an increasingly number of countries.

Two relevant aspects for the effectiveness of awareness initiatives refer to the need to take age differences amongst minors into account and the participation of young people.

Thus, the «European Strategy for a Better Internet for Children» points out that «awareness strategies should take into account the different development levels of the youngest children and adolescents, paying particular attention to the youngest and most vulnerable, including mentally disabled children or with learning difficulties», and the fact that

«peer education is a valuable strategy for children of all ages to know their rights and responsibilities on line»[43].

As regards the participation of young people in awareness actions, some participants announced some interesting case studies, either in virtual surroundings («*Ciberresponsables*» platform referred to by Salomé Adroher; «cybermanagers» initiative pointed out by Jorge Flores, minors as «active solution agents»), or through workshops or on-site activities at school (Joaquim Bayarri, to train students who in turn are able to train students below them).

Some participants also insisted on the importance of quality and appealing contents used in awareness initiatives (Manuel Escalante); it was also mentioned that specific topics should be examined («capsules», Joaquim Bayarri; «informative pills», José Miguel Rosell, based on case studies, following the example of campaigns launched by Traffic Regulation Authorities).

A specific dimension of training and awareness actions that are naturally performed at school refers to situations where children are aggressors, as in «cyberbullying»; these situations need clear action protocols, which need to be defined, as declared by Manuel Escalante and Carlos Represa. The latter, even, in more general terms, referred to the «Security Manager» figure, who would need specific training, as a means of transferring «Data Protection Representatives» to the school world,, foreseen in the European Union Regulation on the protection of individuals as regards personal data processing[44].

4.2. Encouraging quality on-line contents for children and young people

One of the objectives of a «European Strategy for Better Internet for Children», closely related to training in digital competences, consists of encouraging high-quality Internet contents for children and young people. The Strategy has specified two interlinked lines of action, one referring to the stimulus of instrumental digital contents for teaching, aimed at games and education, by age, encouraging creativity and critical

[43] COM(2012) 196 final, p. 10.

[44] COM (2012) 11 final, Arts. 35 ff.

thought; and another stimulus for children and adolescents to act of their own accord, encouraging them not to just use the Internet but to apply it positively and creatively. Both lines of action will also favourably impact the single European digital market and technological innovation.

The national actions described in this chapter should encourage innovation and developments aimed at creating this type of content, and initiatives taken by young people themselves, and should be jointly coordinated with European actions.

4.3. Protection through an acceptable level of Internet safety

Given that digital and media skills for minors, taught at schools as the pivot of this action, and complemented with teacher and parent training and awareness, encouraging their positive experience in the field, constitute (again) the heart of a strategy on the needs of minors on the Internet, it is generally thought that their protection should also be provided through an acceptable level of security on the Web.

In this sense, basically technical measures may be adopted, usually entrusted to self-regulation; the public powers are given larger or smaller room for participation, ranging from development, with or without financial support, to regulations requiring that affected companies establish certain measures.

Based on the type of risk that technical measures aim to reduce or mitigate, filtering tools are particularly useful to block access to illegal contents (particularly pictures of child sexual abuse) or harmful contents for minors.

Filtering techniques may be based on «blacklists», which allow general access to Web contents other than those identified as rejectable) or «whitelists», which generally block all access except for admissible sites). They may apply at different levels of a technical communication process (either in the infrastructure, in access to the Web provided by the provider or access to a local network, or access to the server of a certain platform, or on the user terminal).

Although filters are not an absolute remedy, given failures in effectiveness due to excessive blockage (accidental blocking of non-adult sites) or blockage by default (not all adult sites are blocked), and

many young people are reluctant to use them, and occasionally evade them (if filters are not installed in the terminal), the general opinion is that they are useful, particularly in blocking Web contents included on a «blacklist».

A specific type of filtering tool is parental control software, which may work at different levels but has a broader scope; it not only filers contents but also controls the use of certain applications (e.g. webcam, instant messaging), providing detailed information on on-line use by minors and allowing the length of use to be shortened, thereby covering a wider range of risks that are not just content-related. This is one of the main advantages of this type of tool, along with entrusting families with value-based decisions on which type of contents and activities are admissible, as well as when and how often Internet should be used by their children.

The «European Strategy for a Better Internet for Children» treats parental control as a «complementary measure that helps protect the youngest children from damaging on-line contents, as contents may be filtered and on-line activities supervised».[45]

Sofía Fernández de Mesa gave an example to the Subcommittee of an infrastructure filtering tool, apparently developed by her company but not yet available in Spain which, in her own words, provides «comprehensive (…) on-line protection upon access».

Joan Taulé referred to the industry's obligation to develop technologies required for the protection of minors and was in favour of implementing and using them «both in the home and individual devices and in infrastructures (Internet services provider or mobile telephony network)».

Since July 2013, the British Government has made a huge effort, including a summit sponsored by the Prime Minister himself on 18 November 2013[46], held with leading Internet service providers, to encourage both the blocking of access to child pornography contents and removal thereof, and the blocking of harmful contents.

---

[45] COM(2012) 196 final, p. 13.

[46] News item available at https://www.gov.uk/government/news/internet-safety-summit-at-downing-street-communique.

As a result of this effort, Google and Microsoft have made changes to their search engines (explained to the Subcommittee by Héctor Sánchez and Francisco Ruiz), in order to prevent, on a global scale, the use of certain terms (up to 100,000 combinations) being able to lead to child pornography pictures. After this was announced last November, Google informed that changes would be gradually introduced in 159 languages over a period of six months. Google and Microsoft's initiative also includes key warning messages that will always be displayed if someone uses any of the «blacklist» search terms, informing the user of the consequences of his actions and proposing contact with help organisations, and changes in text anticipation functions («self-completion») to avoid suggestions leading to child pornography search results.

Héctor Sánchez also informed the Subcommittee of the PhotoDNA technology developed by Microsoft to create identifiers that are able to remove pictures of child abuse and any copy thereof through the Internet; this technology will be shared with other companies.

All action taken by Internet service providers to avoid the circulation of child pornography on the Internet should focus both on developing the technical lines of action provided by search engines, to block access and remove this type of material, and a more general active and firm collaboration by these companies to detect and rapidly inform the police, in order for these contents to be removed.

The British Government is also firmly committed to stopping children's access to harmful contents, using infrastructure filtering tools: it is encouraging all new broadband clients to include a family filtering tool (unless the account holder rejects this solution), on a comprehensive basis, i.e. covering any device connected to the client's Internet account, which may only be changed by the account holder. In turn, Internet service providers will have until late 2014 to contact their current clients and propose an «inevitable» decision about whether or not they wish to install this tool[47].

The «European Strategy for a Better Internet for Children» invites all Member States to:

— encourage the availability and use of parental control tools;

[47] «Online Safety», op. cit., p. 28.

— back up the industry in its efforts;

— conduct trials and certification cycles for this type of tool.[48]

With respect to adult Web contents, the possibility has also been raised of implementing age verification methods; if theoretically imposed by the public powers, this would at least cover users located within their jurisdiction. There is currently a legal difference between the on-line gaming industry and the adult contents industry, in which the former must conduct an age check. This difference is partly explained by the fact that an age check is rendered more difficult if service access does not involve a direct financial transaction, where the holding of a valid credit card provides both a financial guarantee and an implicit confirmation of the age, and consequent right, of the betting party.

The following examples were provided as adequate age verification methods:[49]

— Confirmation of holding a credit card or other method of payment, for which legal age is a requirement for issue.

— A professional service to manage personal digital identity, with verifications supported by an independent and reliable database, such as an electoral census.

— Other comparable evidence confirming ownership of an account, effectively checking the holder's age.

In any case, whether in the case of age verification systems or other procedures, it is generally considered that adult content providers are particularly responsible for avoiding child access, and that this was may be imposed to the extent of national jurisdiction. The «Online Safety» Report proposes a novelty related to a national authority that assigns Internet domains: «no .uk site should offer adult pornography without preventing the visit by minors» [50]

In relation to filtering tools, age classification and content labelling measures exist.

According to Act 34/2002, of 11 July, on Information Society and E-Commerce Services, the Public Administrations «will particularly

[48] COM(2012) 196 final, p. 13

[49] «Online Safety», op. cit., p. 22.

[50] Ibidem, p. 22.

encourage the establishment of common criteria, agreed by the industry, for content classification and labelling» (Article 18).

The challenge here is interoperability, at lease in European terms, or, in the words of the «European Strategy for a Better Internet for Children», to have a «generally applicable, transparent and consistent approach in Europe with respect to age classification (…) for various contents and services (including on-line games, applications and educational and cultural contents in general) and to explore innovative solutions (e.g. user or automatic qualification)»[51].

In this regard, Spain's public powers should intensify their effort along the lines laid down by the Act on Information Society and E-Commerce Services and the General Act on Audiovisual Media Services, within the framework of the classification and labelling systems promoted by the European Union.

In relation to risks affecting privacy or personal data protection and other contact risks, it has been discussed whether to implement age verification mechanisms and to configure privacy parameters in social networks.

Several participants, such as Víctor Calvo-Sotelo, Borja Adsuara or Manuel Escalante, pointed out the risk entailed by stricter Spanish laws on age verification, in terms of penalties imposed on Spanish companies. Sebastián Muriel upheld this and stated that, apart from this effect, there is a paradoxical situation due to restrictions in national regulations existing in a social context that favours the growing use by minors of new technologies –which results in situations that were intended to be avoided (user reports for age-related reasons, as a form of harassment, in order to cause a social vacuum and exclusion, parents' complaints due to the shutting down of their children's accounts; reluctance of parents to provide their DNI and family record in order to authorise a Tuenti entry for their under-fourteen children)– as well as a further paradox in the context of rapid technological evolution, with the breakthrough of new networks (WhatsApp, Line, WeChat, etc.) that are not governed by common conduct and control patterns used by leading networks. S. Muriel concluded that «it is gradually making less sense to focus on age registration and verification, particularly in mobility surroundings; it is more important to focus on a safe and responsible use of ICT by minors».

[51] COM(2012) 196 final, p. 14.

In this chapter, self-regulation is still the main action tool; the public powers should encourage it whilst also implementing regulations, in Spain, as a European Union member, within the EU framework established. One of the regulations in this framework that is particularly relevant is personal data protection, currently contained in Directive 95/46/EC but which is presently under review; a proposed Regulation to replace it exists (which, as such, would be directly applicable in all Member States), covering relevant matters, some of which we have already referred to, as its territorial scope, the «right to be forgotten» (Whereas 53 and Article 17), treating minors for the first time as a group with special protection needs (Whereas 25 and Article 13, amongst others), the principle of data protection in terms of design and by default (Article 23) or the «one-stop-shop» principle, in relation to which a defined and clear position of Member State Governments is particularly relevant.

Finally, both in relation to content risks and contact risks (to particularly include cyberbullying and cybergrooming), reporting devices have become an essential technical measure, provided by social networks and other Internet service providers.

This self-regulatory measure should be given more attention and supervision by the public powers, not only to ensure that it is generally implemented but also to meet adequate visibility, accessibility, clarity and human support conditions, and to provide speedy connection with help lines managed with child protection organisations or police and judicial authorities. These tools, according to the «European Strategy for Better Internet for Children» would also help citizens report cybercrimes[52].

In addition to these reporting devices are parallel resources provided by child protection organizations and police web sites, which were declared as scarcely visible by some participants (Manuel Escalante) or, event, that a cyber emergency number [«ciber112»] would be necessary (José Miguel Rosell).

As well as the foregoing technical measures, an acceptable level of Web security is also related to the protection of minors in on-line games and advertising. In the first, the public powers should ensure that companies apply effective age verification devices, as well as implementing regulations in the protection of minors, particularly from

[52] COM(2012) 196 final, p. 11.

an advertising point of view. With respect to on-line advertising risks, self-regulation and the supervision of public powers and, if necessary, regulatory action, should be aimed, according to the «European Strategy for a Better Internet for Children», at guaranteeing that «advertising rules for children's websites provide a level of protection that is comparable to advertising in audiovisual services and which, as regards conduct-oriented advertising, does not create segments for children»[53].

Another step in the actions taken to protect minors based on an acceptable level of Web safety, referred to by some participants (Eugenio Oñate, Jorge Flores), consists of the measurement by an independent third party of the quality parameters imposed on Internet service providers, in order for Internet users (to also include minors and their parents or tutors) to have easily accessible information on such parameters that is complete, comparable and reliable.

4.4. Protection through a regulatory and law enforcement system providing an effective response to illegal Web contents and conducts

Another idea that was also repeated throughout the speeches to the Subcommittee was that the Information Society has appeared so suddenly as to exclude a safety policy to prevent the new risks arising from Web use (Manuel Escalante: «the revolution is so huge that we have decided to turn our backs to the risk») or an adequate institutional and regulatory protection framework, i.e. adapted to the reality of such risks.

In addition to the review and adjustment required of the Criminal Code, particularly as regards the obligations binding Spain both under the Budapest and Lanzarote Conventions of the Council of Europe, on cybercrime and child protection against exploitation and sexual abuse, respectively, and the Directive to combat sexual abuse and the sexual exploitation of minors and child pornography (Directive 2011/92/EU) and the recommendations provided by the scientific community or law enforcement authorities, the participants in the Subcommittee, particularly in relation to State security forces and corps and the Public Prosecution Service and child protection organisations, were in favour

[53] Ibidem, p. 15.

of reviewing the filed of procedural law in order to render investigation more effective, whilst also guaranteeing citizens' rights and the integrity and authenticity of any evidence obtained; this review is particularly important in relation to child pornography, but may be justified with respect to other types of crimes (e.g. «child grooming»), committed through the Internet, consequently raising a particular challenge.

In general, the «European Strategy for a Better Internet for Children» encourages Member States to put into practice «effective investigation instruments that increase investigation capacity to identify the victims of sexual abuse, along with effective guarantees to ensure that they are used with democratic responsibility»[54].

In this sense, many participants leaned in favour of an undercover agent, currently regulated in Article 282.bis) of the Criminal Procedure Act, when investigating certain crimes insofar as linked to organised crime, which could be very effective in the technological investigation field.

Óscar de la Cruz referred to this figure as a necessary technique to solve the asymmetric nature of cybercrime, e.g. in order to climb up the ladder represented by child pornography file exchange, beyond peer-to-peer networks, accessing concealed areas where extremely violent and serious contents are exchanged. This concern with prosecuting concealed crime has resulted in the United Kingdom and U.S. Governments creating a specific work group to find solutions.

Along these same lines, Elvira Tejada was in favour of extending the possible applications of this figure; in relation to crimes committed through ICT, in addition to the figure's basic and essential lines (the need for judicial authorisation or approval from the Public Prosecution Service, based on criteria of need and proportionality appraised in each case, and total control of the undercover agent's activity by a due), it would be necessary to specifically regulate matters such as a definition of the type of crimes this figure would apply to (which, in E. Tejada's opinion, would refer to all crimes generally committed through ICT, given that very often illegal activities are not linked to organised crime, such as in the case of harassment), a difference between free navigation, protected by other identities or nicknames, usually used on the Internet,

[54] Ibidem, p. 17.

and that of the undercover agent as such, which would need judicial authorisation, or the extent to which the undercover agent in the exercise of his investigation tasks is exempt from criminal liability.

Also in relation to procedural law, E. Tejada pointed out that the withdrawal of child pornography contents or blocked access thereto, currently requested by the courts further to Article 13 of the Criminal Procedure Act and Articles 8 and 11 of Act 34/2002, on Information Society and E-Commerce Services, is backed up more strongly in the draft Organic Act to reform the Criminal Code, currently underway, by including amongst its novelties an express right of the Judges and Tribunals to act in this regard.

Finally, E. Tejada was also in favour of amending Act 25/2007, on the preservation of data related to e-communications and public communication networks, in order to not be limited to the criminal scope defined by law, when investigation ICT crimes, nominally referring to serious crimes and, furthermore, to oblige not only «communication service operators» (to be exact, «operators providing e-communication services available to the public or that exploit public communication networks»: Article 2 of the Act) but, in general, Internet service providers.

A decision issued by the European Court of Justice on 8 April 2014 declared as invalid Directive 2006/245/EC, of the European Parliament and of the Council, of 15 March, on the preservation of data generated or processed in relation to the provision of e-communication services with public access or public communication networks, amending Directive 2002/58/EC, of which the implementation into Spanish law is the main aim of Act 25/2007; although this statement does not affect the validity of Spanish law which, in turn, contains some of the components (e.g. the need for prior judicial authorisation to assign data files) which were absent in the Directive and justified to a large extent the decision to declare it invalid, it is undoubtedly a mandatory reference if the Act is reviewed in the future.

In operating terms, the «European strategy in favour of more appropriate Internet for children» emphasizes the aim of fighting any sexual abuse and exploitation of children, where international cooperation is crucial, although national actions may be intensified as follows:

— Reinforcing police resources aimed at combating Internet child pornography, including R&D in technical solutions for police

investigations, enabling an identification of child pornography materials, in order to be rapidly removed, the identification and rescue of victims and handing the offenders over to the courts, based on procedures that guarantee the procurement and integrity of evidence.

— Reinforcing coordination between specialised units in various State and Autonomous Security Forces and Corps.

— Reinforcing cooperation between service providers, reporting lines of private organisations and police corps, in order to rapidly remove illegal material.

V. CONCLUSIONS

1. Within the global scenario of high-speed technological change which is being brought about by high-speed networks, new mobile devices, the Web 2.0 and the convergence of media for connectivity and interactivity on the Internet, children, adolescents and youths are appearing to become «digital natives,» at least in the dual sense that, for them, the Internet is a natural reality not in opposition to that of the physical world, both forming part of one single reality, and in the sense that they are intensive users, showing certain trends well-reflected in the changes seen in statistics: they gain access to the Internet at increasingly younger ages, display growing use with increasing age and a wide range of on-line activities, with a notable presence of those used for communication and participation in social networks, and are undergoing a transformation of the location and means of connectivity as a result of the advent of mobile devices.

However, their status as «digital natives» does not mean *per se* that they possess a high level of digital skills. Quite the contrary, speaking of this condition and the existence of a «digital divide» between minors and their parents, though it does have some basis in reality, has also been exaggerated quite often and conceals the need to take the proper action to ensure that appropriate enablement is provided to them in terms of these skills.

2. The Internet offers huge opportunities, but at the same time it presents a series of risks, and therefore it brings up a precise challenge in terms of seeking out public policies that create the right

balance between the two, ensuring that an excessive emphasis on opportunities without proper protective measures does not increase the potential for risk, while also avoiding an excessive emphasis on measures which hinder the opportunities.

Within this context, we can see that minors have specific needs, from both the perspective of opportunities and that of risks.

3. The types of risks which may affect minors as a result of their Internet use is quite varied, and from the large amount of information provided by the participants it is emerging that there is a primary division which makes it possible to distinguish between risks *from* the Internet and risks *on* the Internet. The risks from the Internet are those intrinsic to the Internet, not in the sense that they cannot be avoided, but rather in the sense that their existence is inseparable from that of the Internet, whereas the risks on the Internet would be those associated with situations that find in this medium the ideal means for taking place, though they already existed and continue to exist outside of the Internet.

4. Amongst the risks from the Internet, or intrinsic to this medium, the Subcommittee shares the concern expressed by certain participants in relation with the decontextualisation which characterises the process of communication by way of the Internet, due to the greater repercussions which this may have for minors, from both the perspective of on-line contacts with new people, by making it harder to get a proper image of them, given that the mediation of the screen does not make it possible to view signs which provide warnings about location, time and context that can help prevent certain risks in the physical world, and from the perspective of the problems which the image projected by the minor through the Internet may have in the long term, disconnected from the specific circumstances in which the minor's information is provided at each given moment.

Likewise, attention must be paid to the problem of excessive use, which can lead to a disorder of addiction. Although the rates of this risk are not high, this problem must not be underestimated, due to the negative consequences it may have on the minors' development.

5. Special concern is brought up by certain risks which, though they are not inherent to the Internet, do find an ideal medium for taking

place through this platform. It is possible to distinguish between the risks caused by the circulation of contents on the Internet (content-related risks) associated with particularly serious behaviours (child pornography and other illicit contents), or behaviours which, though legal, are harmful to minors, insofar as they may cause physical, psychological or moral harm to them (exposure to pornography for adults and other inappropriate contents), and risks caused by certain forms of conduct in which the minor participates in one way or another, be it voluntarily or involuntarily (contact-related risks), which may involve various legal figures, such as the minor's physical or psychological integrity («cyber-bullying,» «cyber-grooming,» digital gender violence, on-line gaming), privacy and the protection of information of a personal nature («sexting,» problems in the long term related with the minor's personal image, objectification of the digital identity, malicious use of personal information) and intellectual property (digital piracy).

Some of the above risks may be associated with criminal behaviours, and as such, they form part of the phenomenon of «cyber-crime,» and therefore the prevention thereof and effective response thereto constitute an objective that cannot be ignored, resulting from the importance which the legal system places on the protection of certain legal figures. However, this does not decrease the importance of other risks, which include exposure to harmful contents, digital gender violence, on-line gaming, certain risks which involve privacy and personal information protection (long-term problems which may be caused by the personal information put on the Internet and the objectification of one's digital identity as a result of the invasive practices carried out in behavioural advertising) and the habit of consuming digital contents through illicit downloading websites, all of which was subject to an individualised analysis by the Subcommittee in the preceding sections above.

6. The values enshrined by the fundamental rights of individuals, acknowledged by the Spanish Constitution and international treaties, must govern both the physical world and the digital world, and in the case of minors they must ensure the «higher interest» of those minors as a «priority» for public authorities and private institutions in all of the acts which concern them.

7. The existence of different role-players with relevant interests in the topic subject to study (the public authorities, children and parents, schools and educators, private organisations in the field of social action, and those companies of different types related with the information society), brings up basic questions about the respective roles which are to be played by the main circles in which those role-players work, State and society. This allows us to distinguish between the two different regulatory focuses available (regulation and self-regulation), though the response to this question aims towards a system of shared responsibility.

The path taken by the European Union, in which there has been a mixture, in accordance with the various categories of risk, of self-regulation and co-regulation using regulatory frameworks which identify the protection of minors on the Internet amongst their basic principles (Year 2010 Directive on audiovisual communication services, 2011 Directive on the fight against sexual abuse and the sexual exploitation of minors and child pornography, and, still undergoing the process of examination, the draft Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data), constitutes a plausible model at the national level, at which, from the perspective of self-regulation, public-private alliances must be promoted, regarding the active participation of the Government in the negotiation of the commitments proposed for voluntary adoption by the participating private companies as inherent to such a figure.

8. The existence of different role-players and diverse regulatory focuses (with regulation and self-regulation) highlights the need, parallel to that proposed at the European level («European strategy to promote a more appropriate Internet for children»), for a strategy at the national level to provide essential leverage for the public policies involving the needs of minors on the Internet, in the understanding that their main conceptual factors are coordination and coherence.

Coordination and coherence must also be promoted through specific organisational formulas which translate into a decisive shift from the mere aggregation of various public and private initiatives to a strategic vision with good leadership and long-term commitments, an idea which may be considered one of the common threads

running through practically all of the statements made before the Subcommittee.

9. This leverage for action is also essential to everything related with the Internet, and therefore international cooperation is also indispensable as regards the needs of minors, both in terms of political and regulatory decision-making and the influence on that decision-making process (a level for which the member countries of the European Union have a natural platform for action in the EU's institutions, without leaving out others, either regional like the Council of Europe, or of a broader scope –OECD, ITU and the Forum for Internet Governance itself), as well as at the operational level, in which the importance of cooperation is projected in various aspects: the harmonisation of national statistical frameworks, to consistently measure the factors of access, use and prevalence of risks on the Internet amongst minors; cross-border cooperation by police authorities for the persecution of and fight against this crime; the activities of the networks of help lines and safety centres on the Internet –INHOPE and INSAFE, respectively–, which were originally European but today have become models of international cooperation; the activities to increase awareness and sensitivity, a notable example of which is «Safer Internet Day», organised by INSAFE, the holding of which is increasing in importance each year; or the initiatives which promote international standards for the interoperability of many technologies, including parental controls on platforms or devices.

10. The Subcommittee has stated four objectives that form part of a strategy of opportunities and safe, responsible Internet use by minors:

1) Enablement in terms of digital skills and general awareness.

2) Promoting quality on-line contents for children and adolescents.

3) Protection through an acceptable level of security on the Internet.

4) Protection through a regulatory system in application of the Law that provides an effective response when there are illicit contents and conducts found on the Internet.

11. The main focus of the activities which are aimed at enabling minors with digital skills –and this was repeatedly stated by the participants

in the Subcommittee– consists of education to provide digital skills in schools, with content that includes, but is not limited to, digital safety. Searching, creating hierarchies, storing, using, producing and sharing information, communicating and participating in cooperative networks, managing one's digital identity and being aware of the risks existing on the Internet, as well as being able to deal with them: these are the basic components of the educational content which is comprised of the concept of «digital citizenship,» which places on emphasis on creative and participatory opportunities for minors on the Internet.

Building digital skills, «key competences,» in the sense of the term created by the Recommendation of the European Parliament and of the Council of 18 December 2006 on «key comptences for lifelong learning,» the primary focus in terms of creating a backbone with the educational curriculum must be based on a multi-subject system, without prejudice to how the topic is dealt with in the specific classes throughout the different levels within the educational system.

12. The budgeting and complements necessary for creating the backbone of the educational curriculum for digital skills consist of, respectively, training teachers and professors, which must begin with university schools themselves, whose study plans have to be reviewed, above all from the perspective of creating skills for adapting to technological change and training parents who, as with other activities that may cause risks, must accompany their children throughout the learning process.

13. The digital skill-building activities based on officially regulated education which make reference to regulations and laws must be complemented by activities to increase general awareness about the safe, critical use of information society technologies, based on informal learning, aimed at both children and adolescents, as well as parents, teachers and all of the other role-players involved.

The challenge in this sense consists of framing the wide range of existing initiatives and those which may arise in the future within a strategy to coordinate and align them, making use of public-private alliances that also involve the media. Moreover, the contents must be high-quality and appealing, as well as bearing in mind the differences in developmental advancement depending upon the minors' ages,

while promoting the participation of youths themselves and the main role-players in those activities.

Likewise, the existence of protocols for action at schools must be promoted, as related to the situations in which children appear as aggressors, such as those cases which involve «cyberbullying.»

14. Closely related with the objective of digital skill building is the promotion of high-quality on-line contents for children and adolescents, which means encouraging innovation and developments aimed at the creation of this type of contents and initiatives by children and teenagers themselves, encouraging in them an attitude which is not limited to consumerism, but also to a positive use of the Internet and to creativity.

15. Even after the digital and media-related literacy of minors, with the school as the cornerstone thereof, comes to form part of the core of a strategy aimed at the needs of minors on the Internet, the Subcommittee shares the opinion that their protection must also result from an acceptable level of security on the Internet.

The activities aimed at achieving this goal are fundamentally of a technical sort and are usually entrusted to self-regulation, though the public powers can do a lot in this field, even through the mere activity of promotion alone, without ruling out the enactment of regulations that force those companies involved to implement certain measures if self-regulation does not achieve the proposed objectives.

For instance, the efforts made by the British Government since the month of July 2013 to obtain a firm commitment from the main search engines regarding the blockage of access to images of child pornography and the removal of such images, which has led to these companies' development of filtering and image identification technologies, demonstrate that governmental promotion can lead to significant advancements in the cooperation by Internet service provider companies to raise the level of safety on-line for the protection of minors.

16. The activities by the public authorities in this sense are not limited to the fight against the scourge of sexual child abuse, of which child pornography is just one of the manifestations, but must also include the promotion of technical measures which safeguard

minors from the risk of exposure to harmful contents. Amongst these measures, the following must be considered.

— Tools for parental control, the usefulness of which is generally acknowledged, above all for protecting the smallest of children, and not only from content-related risks, so its availability and use must be promoted while also encouraging the industry's commitment in this sense, without ruling out their use through the infrastructure itself so as to provide all-encompassing solutions for families that can be applied to all of the devices which are used to access the Internet through the same account.

— The rating and labelling of contents by ages, which must move forward along with the objective of interoperability and, therefore within the framework of systems promoted at the European Union and international levels.

— The mechanisms for age verification and other procedures which are effective for restricting access by minors to websites that offer contents for adults, which it must be possible to require those responsible for such websites to put in place, at least as far as the national jurisdiction applies.

17. Also aimed at the goal of protecting minors by creating an acceptable level of safety on the Internet are those measures which may be adopted through social networks in relation with age verification and privacy settings, an area in which the public authorities must promote the highest possible level of advancement through self-regulation, while at the same time their regulatory activity in a country like Spain, a member of the European Union, must be implemented within the framework that is established at that level. In this respect, unique importance is taken on by the clear, well-defined position of the governments of the Member States with regard to the process for reviewing the regulatory framework that governs personal information protection, a process laid down in a proposal for a Regulation to replace current Directive 95/46/EC, dealing with important aspects such as its scope of territorial applicability, the «right to be forgotten» (with a plausible explicit mention of its importance for minors –Article 17, Whereas 53, which states: «*This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks*

involved by the processing, and later wants to remove such personal data especially on the Internet»), receiving minors as a group with special needs for protection (Whereas 25 –«children require specific protection of their personal information»– and, in addition to others, Article 8, which sets the age of 13 years as the threshold under which parents or guardians must give their consent for the handling of the child's personal information, it being established that the party responsible for handling said information is required to make «efforts within reason to obtain verifiable consent, bearing in mind the available technology»), adoption of the principle of information protection through design and by default (Article 23), or the principle of the «one-stop shop» as regards the relationship with national information protection authorities.

18. The reporting tools enabled by social networks and other Internet service providers are essential in terms of both the content-related risks (illicit contents and harmful contents) and contact-related risks (in particular, cyber-harassment and «cyber-grooming»), and therefore, though entrusted to the realm of self-regulation, they must receive greater attention and tracking by the public authorities, so as to promote not only their widespread implementation, but also so that they meet the proper conditions of visibility, accessibility, clarity and human support, as well as providing a user-friendly connection when appropriate with the help lines for which organisations for the protection of minors are responsible, or with the police and court authorities.

19. An acceptable level of safety on the Internet also has to do with protecting minors in terms of on-line gaming and on-line advertising. In the case of the former, the action by public authorities must ensure use of effective age verification mechanisms by the liable companies, in addition to taking the regulation of the protection of minors even further in terms of the effects of the different types of games and advertising.

To deal with the risks associated with on-line advertising, self-regulation and oversight by public authorities and, if necessary, regulatory action by them must be aimed at ensuring that the rules on advertising in websites for children allow for a level of protection comparable to that of the advertising in audiovisual

services, which does not create segments for children in terms of behavioural advertising.

20. The protection of minors on the Internet may not do without a regulatory system and application of the law that provides an effective response when there are illicit contents and conducts found on the Internet.

In this respect, in addition to the review and adaptation which is needed in the Criminal Code, above all within the framework of the obligations which are incumbent upon Spain pursuant to both the Conventions of the Council of Europe of Budapest and Lanzarote on cyber-crime and the protection of children from exploitation and sexual abuse, respectively, and pursuant to the Directive on combating the sexual abuse and sexual exploitation of children and child pornography (Directive 2011/92/EU), and the recommendations indicated by the scientific community and the authorities responsible for enforcement of the law, widespread amongst the participants in the Subcommittee, especially those from the State's securities forces and corps and the Public Prosecutors' offices, as well as the organisations for the protection of minors, was the opinion in favour of review in the field of procedural law, making it possible to achieve greater effectiveness in the work to investigate cyber-crimes, while at the same time ensuring the rights of the people and the integrity and authenticity of the evidence which is gathered; this review is of particular interest as regards child pornography, but with a justification that can be extended to include other types of crimes (for example, «cyber-grooming»), the perpetration of which through the Internet is a special challenge in the fight against such crimes.

21. International cooperation is crucial in the fight against sexual child abuse, though activities at the national level may be intensified in several directions, as well:

— Reinforcing the police resources used in the fight against child pornography on the Internet, which include the research and development of technical solutions for police investigations that make it possible to identify child pornography materials with a view to their swift removal, the identification and rescue of any victims, and the apprehension of the perpetrators so as to

hand them over to the Justice system, based on procedures which ensure that evidence is obtained and its integrity is ensured.

— Reinforcing the coordination amongst the specialised units of the different State and Autonomous Regional Security Forces and Corps.

— Reinforcing the cooperation amongst service-providing companies, hotlines for reporting crimes set up by private organisations and police entities, so as to take swift action to have any illicit materials taken down.

VI. RECOMMENDATIONS

1. *Public-private alliances*

The Subcommittee believes that self-regulation constitutes an essential focus with regard to protecting minors on the Internet, due to the ability to adapt it in accordance with technological development and social trends, and it believes that the Government must go further in terms of this focus, to which a commitment was made by way of the Information Society and E-Commerce Services Act (Article 18) and the General Act on Audiovisual Media Services (Article 12); this includes the promotion of public-private alliances, regarding as inherent to this concept the active participation of the Government in the negotiation of the commitments proposed for voluntary adoption by the participating private companies.

The contributions by companies in any of the realms which have to do with the protection of minors on the Internet must be promoted by creating specific awards or «seals» of social responsibility.

The focus of self-regulation must be linked together with the State's initiative or regulatory activities, when necessary on the basis of the nature and seriousness of the risks which the minors face on the Internet, from the perspective of the «higher interest» of minors as a «priority» for public authorities and private institutions in all of the acts which concern them, in accordance with the United Nations' Convention on the Right of the Child (Article 3) and the European Union Charter of Fundamental Rights (Article 24).

2. *International cooperation*

The dynamic, global nature of the Internet means that objectives and activities at the national level must be framed as part of those proposed at the international level, and therefore international cooperation takes on a fundamental role as a form of leverage for action by Governments.

At the political/regulatory level of decision-making or influence thereupon, the institutions of the European Union constitute the primary platform for action for a member country of the European Union like Spain, it being particularly important at the present time for the Government to have a clear, well-defined position with regard to the process for reviewing the regulatory framework that governs personal information protection, a process laid down in a proposal for a Regulation to replace current Directive 95/46/EC, which, in addition to dealing with other important aspects, deals with classifying minors as a group with special needs for protection, the «right to be forgotten,» and the adoption of the principle of information protection through design and by default.

International cooperation must include other relevant platforms, which may be regional, such as the Council of Europe, or of a broader scope (including the OECD, ITU, and the Forum for Internet Governance).

International cooperation must also play an important role in terms of operations, with different fields in which the Government's efforts must be made: harmonisation of the national statistical frameworks, to consistently measure the factors of access, use and prevalence of risks on the Internet amongst minors; cross-border cooperation by police authorities for the persecution of and fight against this crime; the activities of the networks of help lines and safety centres on the Internet –INHOPE and INSAFE, respectively–which were originally European, but today have become models of international cooperation; the activities to increase awareness and sensitivity, a notable example of which is «Safer Internet Day»), organised by INSAFE, the holding of which is increasing in importance each year; or the initiatives which promote international standards for the interoperability of many technologies, including parental controls on platforms or devices.

3. *Strategy, coordination and coherence*

The Subcommittee acknowledges the contribution made by those strategic instruments approved by the Government with effects in the field of the needs of minors on the Internet, which include the Digital Agenda for Spain and the «Second National Strategic Plan for Childhood and Adolescence of 2013-2016 (II PENIA),» though, from the ensemble of statements made to the Subcommittee, one can infer that there is a need to highlight the value of the strategy to create leverage for action in relation with the challenges brought up by those needs.

In this sense, a renewed governmental strategy in this field must be of a global nature, or in other words, it must foresee the opportunities and risks on the Internet for minors and understand the actions by the entire General Administration of the State, as well as including the following two basic objective types:

A) Action objectives:

1) Enablement of minors in terms of digital skills and general awareness.
2) Promoting quality on-line contents for children and adolescents.
3) Protection of minors through an acceptable level of security on the Internet.
4) Protection of minors through a regulatory system in application of the law that provides an effective response when there are illicit contents and conducts on the Internet.

B) Leverage for action:

1) Increasing the coordination of all the actions which are being performed by the Government, with a particular emphasis on the Ministries of the Interior, Industry, Energy and Tourism, Health, Social Services and Equality, Justice, and Education, Culture and Sports.
2) Providing all of the actions by the Government with proper coordination and coherence, by taking advantage of synergies.
3) Promoting an *ad hoc* organisational model designed specifically for this purpose.

4) Promoting the actions by the General Administration of the State in the Autonomous Regions, within the scope of their duties and responsibilities.

In this sense, though an interest in figures such as that of a «High Digital Commissioner» has been acknowledged, in the style of the «Chief Digital Officer» (CDO) existing in certain Administrations within the English-speaking world, the Subcommittee believes that, without parting ways with the organisational formulas typical of Spain's public administration, it is possible to move ahead on public policies related with the information society as a whole and with the protection and needs of minors on the Internet in general, in a direction which allows a strategic outlook with a high level of leadership and commitment in the long term.

While, in the current model, the public competences related with the Internet fall within different ministerial centres, more specifically through the State Secretariat of Telecommunications and for the Information Society, which forms part of the Ministry of Industry, Energy and Tourism, with the support of an important entity, RED. ES, whose activities are coupled with those of the State Secretariat of Education, the State Secretariat of Social Affairs, the State Secretariat of Security, through the State Security Corps and Forces, and the Ministry of Justice, complemented by those which are appropriate from different perspectives in the National Commission of Markets and Competition (created by Act 3/2013 of 4 June 2013, which grouped together the roles of different regulatory entities, including the Telecommunications Market Commission and the State Audiovisual Media Council) and the Spanish Data Protection Agency (regulated by Organic Act 15/1999, of 13 December 1999, on Personal Data Protection), the Subcommittee believes that the Government must review, in line with the models existing in the European Union and its member countries, including reflection on a figure of the type of a High Digital Commissioner, the relationship amongst all of these various parts so that its structure and functions include the risks and opportunities of minors on the Internet as a high-priority area, while ensuring that the requirements resulting from the ideas of strategy, coordination and coherence are fulfilled.

At the same time, the Subcommittee believes that, while Organic Act 1/1996, of 15 January 1996, for the Legal Protection of Minors, with a partial amendment of the Civil Code and the Civil Procedure Act,

foresees that one of the Assistant State Ombudsman will be permanently responsible for those affairs related with minors, a further step could be taken by creating, within the State Ombudsman's Office, as a High Commissioner for the Spanish Parliament to defend the rights included under Title I of the Constitution (including those recognised for children in Article 39), a Third Assistant Ombudsman with specific tasks as a «Minors' Ombudsman,» which would explicitly include the field of protecting minors on the Internet, requiring an amendment of Organic Act 3/1981, of 6 April 1981, on the National Ombudsman.

4. *Digital literacy and general awareness*

From the perspective, shared by the Subcommittee, which considers the promotion of digital literacy amongst minors, or in other words, their enablement by providing digital skills, to be the core of a strategy on the needs of minors on the Internet, with school as the cornerstone in providing these skills, which are not limited to just digital safety, but rather aim for a broader concept (which entails safe, critical use of information society technologies for work, entertainment and communication, and also include knowledge of the risks from and on the Internet, and the means for dealing with those risks, as well as the opportunities for creativity and participation available on the Internet), the Subcommittee believes that the Government, regardless of the competences held by the Autonomous Regional Governments, must guarantee the effective learning of the aforementioned skills when creating the backbone of the educational curriculum, from the earliest levels of education, based on a multi-disciplinary focus in terms of key skills, in line with the Recommendation of the European Parliament and of the Council of 18 December 2006, on «key competences for lifelong learning,» without prejudice to how the topic is dealt with through specific classes throughout the different levels within the educational system.

Likewise, given that training for teachers and professors is a necessary factor in the learning of digital skills in schools, the Government must promote such training so that universities, in exercising their independence, can bring up the review of study plans for the Bachelor's and Master's degree programs of the university schools where future teachers are educated, and in a more general manner, because «safety

through design» is a concept that can be applied not only to products and the rendering of services, but also to training, Bachelor's degree study plans and technical graduate studies, so as to include professional enablement involving cyber-safety.

As a complement to the above actions, aimed at the officially regulated education system, the Subcommittee, after listening to all of the participants who made statements before the Subcommittee, believes that awareness about the safe, critical use of information society technologies must be promoted, because the problem of protecting minors when they use the Internet is a problem of society as a whole, and it is a key aspect in achieving a safer Internet, because preventive actions are the most effective.

This objective must be aimed at increasing awareness amongst all role-players and be based on the following coordinates:

— The universal nature of the target groups: minors, parents, grandparents, educators, the State Security Corps and Forces, public prosecutors, judges and media professionals.

— Public-private cooperation that involves the media, and television in particular.

— A broad base of contents, referring not only to digital safety, but also to psychological resources (such as disconnecting, resilience, respect and empathy), the right to privacy and the protection of personal information, civil values, and the current laws in force and their effects, above all on minors and their parents.

— Diversified contents, or in other words, contents which bear in mind the different development levels of minors, including those who have intellectual or learning disabilities.

— Contents which are appealing due to the way in which they are distributed: education by peers, getting young people to take responsibility in this area; practical workshops based on the use of technology; information based on real cases made anonymous; awareness campaigns which alert to specific dangers such as cyber-harassment, in the style of those which have been used effectively by Spain's Directorate General of Traffic, or the more recent ones related with alcohol and drug use.

In this direction, the Government will be promoting campaigns for information, awareness and education with the cooperation of the autonomous regions.

In all of the informational and educational campaigns at centres of learning, the participation of experts on this topic will be promoted, such as agents from the National Police Force, the Civil Guard and the autonomous regional police forces in their respective regions.

Likewise, the Government must promote the existence of protocols for action at schools, as related to the situations in which children appear as aggressors, such as those cases which involve «cyber-bullying.»

The Government must also promote the availability and dissemination of innovations and developments aimed at creating high-quality contents on the Internet for children and youths, and initiatives by these children and adolescents, encouraging in them an attitude which is not limited to consumerism, but also to a positive use of the Internet and to creativity.

5. ***Internet Safety***

The Government's efforts must be aligned with those of other advanced countries in terms of the fight against the scourge of sexual child abuse, of which child pornography is just one of the manifestations, the commitment of service-providing companies constituting one of the protective barriers in this fight, in both the direction already followed towards the development of filtering and image identification technologies to block access and having this type of images removed, and the more general direction of achieving active, decisive cooperation by these companies in the detection of such images, effectively reporting them to the police forces and swiftly removing them.

Likewise, the Government's activities must include the promotion of technical measures which safeguard minors from certain risks on the Internet such as exposure to harmful contents, «cyber-bullying» or «cyber-grooming,» amongst which the following should be considered:

— Tools for parental control, such decisions based on their values about what type of contents and activities are acceptable and the time and frequency of Internet use for their children. The Government must decisively promote the availability and use of these tools,

promoting the commitment of industry in the development and offerings thereof, which must include their application through the infrastructure so as to provide all-encompassing family-based solutions that can be applied to all of the devices which access the Internet through the same account, in the direction promoted by the British government.

— The rating and labelling of contents by ages, which the Government must continue to promote, without prejudice to the responsibilities and duties of oversight and control held by the National Commission of Markets and Competition, along the lines determined by Article 18 of the Information Society and E-Commerce Services Act and Article 7 of the General Act on Audiovisual Media Services, promoting the industry's establishment of criteria based on interoperability, within the framework of systems promoted at the European Union and international levels.

— The mechanisms for age verification or other procedures which are effective for restricting access by minors to websites that offer contents for adults, which it must be possible to require those responsible for such websites to put in place, at least as far as the national jurisdiction applies.

— The permanent response at any time of day to any problem that might affect the physical, psychological or moral integrity, or the privacy of minors as a result of their Internet use, which may be brought up by the minors themselves, or their parents, guardians or educators, using the reporting tools made available by organisations for the protection of minors and police forces, tools which the Government must analyse in order to promote their visibility and complementary nature.

6. *Age and privacy parameters and reporting tools on social networks*

Potentially putting in place age verification mechanisms, either at the time of creating a profile or at some later time, as well as the selection by default of the strictest option in terms of privacy on social networks, constitute, in the Subcommittee's judgement, an indisputable field of discussion in which self-regulation, with the Government's active participation, remains a main tool for action, without setting aside the

fact that regulatory action, as well, due to its effects on the digital market, must move ahead in a country like Spain which forms part of the European Union, within the regulatory framework that is established at that level.

At the same time, the reporting tools provided by social networks and other Internet service providers are essential in terms of both the content-related risks (illicit contents and harmful contents) and contact-related risks (in particular, cyber-harassment and «cyber-grooming»), and therefore, though entrusted to the realm of self-regulation, they must receive greater attention and tracking by the Government, so as to promote not only their widespread implementation, but also so that they meet the proper conditions of visibility, accessibility, clarity and human support, as well as providing a user-friendly connection, when appropriate, to the help lines for which organisations for the protection of minors are responsible, or to the police and court authorities.

In this sense, the Subcommittee proposes that it be the Government that promotes political action which, through the European Union, gets Internet service provider companies to fulfil their obligations to guarantee safety when accessing social networks, by putting in place age verification mechanisms and providing the police forces and justice system with information.

At the same time, the Subcommittee, with a view to meeting the essential need for specific protection of minors' personal information, as a fundamental part of their safety on the Internet, positively views the criteria of the «one-stop shop» as regards national information protection authorities, from the perspective of both the companies which do business in more than one European Union member state and that of the people as individuals with the right to protection of their personal information, in the direction determined by the European Parliament in its Resolution of 12 March 2014, issued in the proceeding on the proposal of a Regulation for the protection of individuals as regards the processing of their personal data and the free circulation of such data.

7. *Safety on the Internet related with on-line gambling and on-line advertising*

The Government must ensure the effective enforcement of the prohibition against minors' participation in gambling governed by Gaming

Act 13/2011, of 27 May 2011, , including on-line gambling, through the use of effective age verification mechanisms. Moreover, it must develop the provisions of the aforementioned Act with the objective of ensuring the effective protection of minors, above all in terms of the advertising of this type of gambling.

At the same time, self-regulation and regulatory action, the latter framed within that which is issued at the EU level, must be linked together in order to ensure a proper level of protection for minors against advertising on the Internet, in particular, so as to ensure that the rules on advertising in websites for children allow for a level of protection comparable to that of the advertising in audiovisual services, and to prevent the creation of behavioural advertising that targets children.

8. *Regulatory system in application of the Law that provides an effective response when there are illicit contents and conducts on the Internet*

Spain has a regulatory framework for the protection of minors in which their protection against the risks from and on the Internet must be placed, the basis of which is the Constitution itself, through the general mandate established in Article 39.4 thereof, which refers to the international agreements that seek to ensure children's rights, including the 1989 United Nations Convention on the Rights of the Child, the 2000 Optional Protocol of the United Nations Convention on the Rights of the Child, regarding the sale of minors, child prostitution and the use of minors in pornography, the Council of Europe Convention on Cyber-crime of 2001 (Budapest Convention) and the Council of Europe Convention for the protection of children against exploitation and sexual abuse of 2007 (Lanzarote Convention), all ratified by Spain. In line with these instruments, the European Union enacted the Directive on the fight against sexual abuse and the sexual exploitation of minors and child pornography in 2011 (Directive 2011/92/EU), which added notable momentum to the adaptation of the criminal and procedural law of Member States in such a way that they may foresee the effect of Information and Communication Technologies on committing crimes involving the abuse and sexual exploitation of minors, and to ensure that effective, consistent instruments are created in the fight against these crimes. Similarly, certain laws include the protection of minors

amongst their basic principles, as is the case with the Organic Act for civil protection of the right to honour, personal and family privacy and self-image (Article 3), as well as the Organic Act for Legal Protection of Minors (Article 5) and the General Act on Audiovisual Media Services (Article 7), the review of which must be carried out within the context of today's information society, in the Subcommittee's judgment.

In particular, as a result of the current legislative proceedings under way in the Spanish Parliament for the Draft Organic Act to amend Organic Act 10/1995, of 23 November 1995, on the Criminal Code, it will become possible to adapt that regulatory text from the perspective of protecting minors on the Internet from contents and conducts which, due to their serious nature, merit a response through the State's punitive system, above all within the framework of the obligations which are incumbent upon Spain pursuant to both the Conventions of the Council of Europe of Budapest and Lanzarote, on cyber-crime and the protection of children from exploitation and sexual abuse, respectively, and pursuant to the Directive on the fight against sexual abuse and the sexual exploitation of minors and child pornography (Directive 2011/92/EU), and the recommendations indicated by the scientific community and the authorities responsible for law enforcement.

At the same time, in line with the «European Strategy for a Better Internet for Children,» which encourages Member States to put into practice «effective investigation tools that increase the ability of investigators to identify the victims of sexual abuse, along with effective safeguards to ensure democratic responsibility in the use thereof.» In line with the widespread view amongst the participants in the Subcommittee, they expressed their opinion in favour of carrying out a review in the field of procedural law, with a view to making it possible to achieve greater effectiveness in the work to investigate cyber-crimes, while at the same time ensuring the rights of the people and the integrity and authenticity of the evidence which is gathered; this review is of particular interest as regards child pornography, but with a justification that can be extended to include other types of crimes (for example, «child grooming»), the perpetration of which through the Internet is a special challenge in the fight against such crimes.

In particular, the Subcommittee advocates a broadening of the scope of cyber-crime, or at least a broadening of the part related with sexual

child abuse and «child grooming,» through the figure of the undercover agent, currently regulated under Article 282 *bis* of the Criminal Procedure Act, in relation with the investigation of certain crimes as they are related with organised crime. This expansion would require, in addition to maintaining the basic, essential guidelines of this figure (requirement of obtaining authorisation from a Judge or the Public Prosecutor's Office, in accordance with criteria involving the need for an investigation and proportionality and oversight of the undercover agent's activities by the Judge), a specific system governing aspects such as the delimitation of the crimes committed through the Internet to which the application of this figure could be extended (bearing in mind that they are frequently not related with organised crime, as is the case, for example, with «child grooming»), the distinction between instances of free browsing under the aegis of assumed identities through the use of nicknames, which is typical on the Internet, and that of the undercover agent as such, which would require court authorisation, and the scope of the exemption from criminal responsibility for the activities by the undercover agent in carrying out the investigation.

Likewise, the Subcommittee believes that possibilities must be studied for modification of Act 25/2007, of 18 October 2007, on the preservation of information related to electronic communications and public communications networks, so as to increase the ability to investigate those crimes committed using Information and Communication Technologies that affect minors, a modification which would in any case have as a necessary reference the ECJ Decision of 8 April 2014, which declared invalid Directive 2006/24/EC, of the European Parliament and Council of 15 March 2006, on the preservation of information generated or processed in relation with the rendering of electronic communication services with public access or public communication networks, and which modified Directive 2002/58/EC, the implementation of which into Spanish law constituted the main objective of Act 25/2007.

As for all else, an effective response of the system in application of the Law to deal with illicit contents and conducts on the Internet that stalk minors must include, and therefore must be promoted by the Government, a determined commitment to ongoing education on the technologies of the information society, amongst both the State and Autonomous Regional Security Corps and Forces, as well as the Public Prosecutors and the Judicial powers.

The Subcommittee proposes that the Government of Spain promote the creation, of a «Charter for the People's Rights on the Internet» which deals above all with protecting the rights of minors within the European Union, through a participatory process, with a special emphasis on the regulation of on-line safety and the right to users' privacy.

9. *Operational capabilities in the fight against sexual abuse and child pornography*

In addition to the indispensable international cooperation, the Subcommittee believes that action at the national level must be strengthened in the fight against sexual child abuse in three different directions:

— Reinforcing the police resources used in the fight against child pornography on the Internet, which include R&D on technical solutions for police investigations that make it possible to identify child pornography materials with a view to their swift removal, the identification and rescue of any victims, and the apprehension of the perpetrators so as to hand them over to the Justice system, based on procedures which ensure that evidence is obtained and its integrity is ensured.

— Reinforcing coordination amongst the specialised units of various State and Autonomous Regional Security Forces and Corps.

— Reinforcing the cooperation amongst service-providing companies, hotlines for reporting crimes set up by private organisations and police entities, so as to take swift action to have any illicit materials taken down.

ANNEX 1

ALPHABETICAL LIST OF PARTICIPANTS IN THE JOINT SUBCOMMITTEE TO STUDY THE RISKS DERIVED FROM USE OF THE WEB BY MINORS, INDICATING THE POSITION OR STATUS HELD BY EACH PERSON AS IT APPEARS ON THE AGENDA OF THE CORRESPONDING MEETING IN WHICH THEY INTERVENED.

ADROHER BIOSCA, María Salomé. General Manager of Family and Children's Services.

ADSUARA VARELA, Francisco de Borja. General Manager of Red.es.

BAYARRI I NOGUERAS, Joaquim. Head of the Technical Division for Citizen Security Planning, Mossos d'Esquadra [Catalonian Police].

BASTERRECHEA OÑATE, Natalia. Manager of Public Affairs, Facebook Spain and Portugal.

BREZO FERNÁNDEZ, Félix. Software Engineer and Industrial Organisation Engineer.

CALVO-SOTELO IBÁÑEZ-MARTÍN, Víctor. State Secretary of Telecommunications and the Information Society.

CÁNOVAS GAILLEMIN, Guillermo. Chairman of the Internet Security Centre, «Protégeles» Association.

CARBONEL PINTANEL, Luis. Chairman of the National Catholic Confederation of Family Representatives and Alumni Parents [Confederación Católica Nacional de Padres de Familia y Padres de Alumnos] (CONCAPA).

CARTES, Patricia. Head of Security, Twitter.

CASAL CASTRO, José Luis. Co-Founder and Head of Marketing, Talk2Us Comunicación.

COMÍN HERNÁNDEZ, Miguel. Manager of the Alia2 Foundation.

COSIDÓ GUTIÉRREZ, Ignacio. General Manager of the Police.

CRUZ YAGÜE, Óscar de la. Chief Commander of the Telematic Crime Section, Central Operating Unit [Unidad Central Operativa (UCO)] of the Civil Guard.

CHÓLIZ MONTAÑÉS, Mariano. Lecturer, Faculty of Psychology, University of Valencia.

ERRASTI ARGAL, Miguel. Chairman of the National Association of Internet Companies [Asociación Nacional de Empresas de Internet] (ANEI).

ESCALANTE GARCÍA, Manuel. General Manager of Instituto Nacional de Tecnologías de la Comunicación (INTECO) [National Institute for Communication Technologies].

FERNÁNDEZ DE MESA DÍAZ DEL RÍO, Arsenio. General Manager of the Civil Guard.

FERNÁNDEZ DE MESA ECHEVERRÍA, Sofía. Head of Corporate Responsibility and Social Innovation, Telefónica.

FLORES FERNÁNDEZ, Jorge. Manager of «PantallasAmigas.»

FONTÁN OÑATE, Eugenio. Chairman of the Official Association of Telecommunication Engineers.

GALLEGO MORALES, María José. Head of consumers and users and legal interception of communications, Jazztel.

GONZÁLEZ GARCÍA, Carolina. Chief Inspector of the Press and Social Networks Department, Press and Informative Relations Office, General Directorate of the Police.

GONZÁLEZ HERMOSO DE MENDOZA, Alfonso. General Manager of Evaluation and Territorial Cooperation.

GUIJARRO VALLADOLID, Jesús. Manager of Corporate Social Responsibility, Orange España.

GUTIÉRREZ RUBÍ, Antoni. Communications Advisor and social network analyst.

IGUAL GARRIDO, Carlos. Captain of the Minors and Children's Sexual Exploitation Section, Technical Unit of the Judicial Price [Unidad Técnica de Policía Judicial (UTPJ)] of the Civil Guard.

MADRIGAL MARTÍNEZ-PEREDA, Consuelo. State Prosecutor, Coordinating Chamber for Minors.

MANZANAS MANZANAS, Juan Miguel. Head Officer of the Technological Investigation Brigade, General Station of the Judicial Police, General Directorate of the Police.

MARTÍNEZ MONREAL, Salud. Expert in innovation for information security.

MARTÍNEZ OTERO, Juan María. Member of the Advisory Board of the Federation of Media Consumer and User Associations

[Federación de Asociaciones de Consumidores y Usuarios de los Medios] (iCmedia).

MARTOS MOTA, Francisco Javier. Executive Director of UNICEF, Spanish Committee.

McSWEENEY, Sinéad. Head of Public Policy, EMEA, Twitter.

MURIEL HERRERO, Sebastián. General Operations Manager, Tuenti.

NAVARRETE BARREIRO, Carlota. General Manager of the Coalition for digital content creators and industries.

ORJUELA LÓPEZ, Liliana. Coordinator of Children's Rights, «Save the Children.»

PÉREZ SUBÍAS, Miguel. Chairman of the Internet Users Association [Asociación de Usuarios de Internet] (AUI).

POLO GONZÁLEZ, Íñigo. Director of Institutional Relations, ONO.

PRATS MORENO, Josep Manuel. Chairman of the Catalonian Federation of Associations of Parents of Free Schools [Federació d'Associacions de Pares i Mares d'Escoles Lliures de Catalunya] (FAPEL).

REIG HERNÁNDEZ, Dolors. Social Psychologist, specialising in social networks; head of «El caparazón» programme.

REPRESA ESTRADA, Carlos. Manager of the School ITC Security Centre [Centro de Seguridad TIC Escolar] (CNTiC).

RODRÍGUEZ ÁLVAREZ, José Luis. Manager of the Spanish Data Protection Agency [Agencia Española de Protección de Datos] (AEPD).

ROMÁN RIECHMAN, Ana María. Head of Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF) [National Institute for Educational Technologies and Teacher's Training].

ROSELL TEJADA, José Miguel. Managing Partner of S2 Grupo.

RUIZ ANTÓN, Francisco. Manager of Public Policy and Institutional Matters, Google Spain and Portugal.

SALIDO NAVARRO, Jesús. Vice Chairman of the Spanish Confederation of Associations of Alumni Parents [Confederación Española de Associations de Padres y Madres de Alumnos] (CEAPA).

SÁNCHEZ MONTENEGRO, Héctor. Technology Manager, Microsoft Ibérica.

SANTOS ORTEGA, Francisco Javier. Corporate Security Manager, Ono.

SEDES GARCÍA, José Manuel. Sustainability and Quality Manager, Vodafone España.

TAULÉ VALDEPERAS, Joan. General Manager of Symantec España.

TEJADA DE LA FUENTE, Elvira. State Prosecutor, Coordinating Chamber to fight Computer Crime.

TOURNÉ ALEGRE, José Manuel. General Manager of the Federation for Intellectual Property Protection [Federación para la Protección de la Propiedad Intelectual] (FAP).

URRA PORTILLO, Javier. First Ombudsman for Minors, Autonomous Community of Madrid.

VIOTA MAESTRE, Manuel. Head of the Central Department of Information Technology Crime, Criminal Investigation and Judicial Police Unit of the Ertzaintza [Basque Police].

ANNEX 2

DECLARATION ON THE OCCASION OF «SAFER INTERNET DAY» (11 FEBRUARY 2014), BY THE SENATORS WHO ARE MEMBERS OF THE SUBCOMMITTEE ESTABLISHED WITHIN THE SENATE OF SPAIN TO STUDY THE RISKS DERIVED FROM USE OF THE WEB BY MINORS

The Senators who are members of this Subcommittee**, established within the Senate of Spain to study the risks resulting from Internet use by minors**, express their participation in the holding of *«Safer Internet Day» –SID–*, promoted within the framework of the European Committee, the year 2014 edition of which was held on 11 February.

In particular, they welcome the holding of the «Third National Youth and On-line Congress,» organised by the Centre of Internet Safety for minors in Spain (Protégeles/Cesicat), as the central event of that Day.

The Senators who are members of the Subcommittee completely accept as their own the Day's slogan: «*Let's create a better Internet together*,» stated in the program and by the participants in that Congress.

The Subcommittee was created precisely with the clear awareness that the opportunities and risks which arise from the Internet have a specific way of being projected amongst minors and must be dealt with by all. The minors themselves, along with their families and educators, are key role-players from the perspective which places the basic focus on prevention in order to deal with the threats or risks originating on-line, and therefore awareness and skill-building actions must be carried out so as to promote a responsible attitude towards the Internet.

Effective coordination within the realm of public authorities, a steadfast alliance between those authorities and the private sector, for both social action and business activities, with the participation of all role-players, including youths, and a strategy with a European and international outlook: these are the essential tools needed to build a better and safer Internet, of which the initiatives described above are valuable examples.

At the Palace of the Senate, on September 30, 2014. Emilio Álvarez Villazán, Iñaki Mirena Anasagasti Olabeaga, José María Ángel Batalla, Carmen Azuara Navarro, Francisco Boya Alós, Tomás Pedro Burgos Beteta, José María Chiquillo Barber, Andrés Gil García, Amalur Mendizabal Azurmendi, Jordi Miquel Sendra Vellvè.