BOLETÍN OFICIAL
DE LAS CORTES GENERALES

CONGRESO DE LOS DIPUTADOS

X LEGISLATURA

Serie D:
GENERAL **9 de abril de 2015** **Núm. 643** **Pág. 1**

Otros textos

COMISIONES, SUBCOMISIONES Y PONENCIAS

154/000007 Subcomisión de Estudio sobre las Redes Sociales.

Aprobación por la Comisión de Interior del Informe de la Subcomisión.

En cumplimiento de lo dispuesto en el artículo 97 del Reglamento de la Cámara, se ordena la publicación en el Boletín Oficial de las Cortes Generales del Acuerdo de la Comisión de Interior, relativo al Informe de la Subcomisión de Estudio sobre las Redes Sociales, aprobado en su reunión del pasado día 24 de marzo de 2015.

Palacio del Congreso de los Diputados, 30 de marzo de 2015.—P.A. El Secretario General Adjunto para Asuntos Parlamentarios del Congreso de los Diputados, **José Antonio Moreno Ara.**

cve: BOCG-10-D-643

APROBACIÓN POR LA COMISIÓN DE INTERIOR DEL INFORME DE LA SUBCOMISIÓN DE ESTUDIO SOBRE LAS REDES SOCIALES CONSTITUIDA EN LA COMISIÓN DE INTERIOR DEL CONGRESO DE LOS DIPUTADOS

PARTE EXPOSITIVA

I. Antecedentes y funcionamiento de la Subcomisión para el Estudio de las Redes Sociales constituida en el seno de la Comisión de Interior del Congreso de los Diputados (X Legislatura).

I.1 Solicitud de creación por la Comisión de Interior del Congreso de los Diputados.
I.2 Aprobación por el Pleno del Congreso de los Diputados.
I.3 Constitución de la Subcomisión.
I.4 Composición, objeto, método y calendario de trabajo.

II. Comparecencias efectuadas en la Subcomisión para el Estudio de las Redes Sociales.
III. Breve resumen de las materias más relevantes suscitadas en cada comparecencia.
IV. Relación de Documentación aportada a la subcomisión por los comparecientes.

PARTE DISPOSITIVA

V. Conclusiones del Informe aprobado por la Subcomisión.

I. Introducción.

1. Estructura.
2. Las recomendaciones de la Ponencia de estudio del Senado.
3. Especialización.
4. Medidas en marcha.
5. Concepto de redes sociales.
6. Tipos de redes sociales.
7. Situación actual de las redes sociales en España.
8. Situación en países de nuestro entorno.
9. Debate.
10. Publicación.

II. Conclusiones.

A) Consideraciones y Principios generales.

a) Valoración: 1.
b) Coordinación: 2, 3 y 4.
c) Medidas: 5, 6 y 7.
d) Regulación: 8. 9 y 10.

III. Recomendaciones y medidas concretas.

A) Organizativas: coordinación, cooperación y colaboración.

a) Coordinación de las Administraciones Públicas: 1.
b) Autorganización de las empresas y organizaciones privadas: 2 y 3.
c) Colaboración público-privada: 4.
d) Participación ciudadana: 5.
e) Cooperación internacional: 6, 7, 8, 9, y 10.

B) Educativas: formación, divulgación y prevención.

a) Educación de menores: 1, 2, 3, 4 y 5.
b) Formación de mayores: 6, 7, y 8.
c) Divulgación: 9.
d) Prevención: 10.

cve: BOCG-10-D-643

C) Regulatorias.

a) Penales: 1, 2, 3, 4, y 5.
b) Civiles: 6.
c) Otras Leyes: 7, 8, 9, y 10.

D) Policiales.

a) Contra la pornografía infantil o abusos a menores: 1, 2, 3, y 4.
b) En general: 5, 6, 7, 8, y 9.
c) Coordinación: 10.

E) Sectoriales.

a) Contenidos nocivos: 1, 2, 3, 4, y 5.
b) Protección de menores en general: 6, 7, y 8.
c) Seguridad en general: 9 y 10.

PARTE EXPOSITIVA

I. Antecedentes y funcionamiento de la Subcomisión para el Estudio de las Redes Sociales constituida en el seno de la Comisión de Interior del Congreso de los Diputados (X Legislatura).

Las Subcomisiones del Congreso de los Diputados, creadas por Resolución de la Presidencia de la Cámara de 1996, constituyen un órgano de trabajo parlamentario que ocupa una posición intermedia entre la Ponencia y las Comisiones, y que, con carácter general, desempeñan tareas de estudio y análisis de una materia que concluye con la elaboración de un informe que puede ser debatido, además de por la Comisión en cuyo seno se ha constituido la subcomisión, por el Pleno de la Cámara.

La Subcomisión de Estudio sobre las Redes Sociales se ha constituido en la X Legislatura en el Congreso de los Diputados y ha llevado a cabo su actividad de estudio y análisis a lo largo de 2013 y 2014 primer trimestre de 2015.

A continuación se recogen los antecedentes de la Subcomisión, la constitución de la misma, así como el método y calendario de trabajo adoptado por la Subcomisión.

I.1 Solicitud de creación por la Comisión de Interior del Congreso de los Diputados.

El 22 de noviembre de 2012 el Portavoz del Grupo Parlamentario Popular, D. Alfonso Alonso Aranegui, al amparo de la Resolución de la Presidencia de la Cámara sobre Subcomisiones de 1996, presentaba un escrito por el que se solicitaba la creación de una subcomisión de Estudio sobre las Redes Sociales en el seno de la Comisión de Interior. Como antecedentes de dicha solicitud se citaba la Proposición No de Ley del Grupo Parlamentario Popular, aprobada por unanimidad por el Pleno el 13 de marzo de 2012, en la que se instaba al Gobierno a «reforzar la prevención del acoso por internet, promoviendo acuerdo de protección de menores con las diferentes redes sociales, garantizando la protección de datos de carácter personal y revisando las posibilidades técnicas, operativas y jurídicas, tendentes a mejorar la seguridad de las fotografías que se cuelguen en la red, tanto por parte de las Fuerzas y Cuerpos de Seguridad del Estado y de las policías autonómicas con competencia en la materia, como de las redes sociales y servidores o proveedores de servicios informáticos».

Igualmente, «reforzar las Unidades Policiales competentes y de protección al menor, con el objetivo de intensificar la investigación de delitos relacionados con la utilización de la red, singularmente el "ciberbulling"».

Además de este antecedente parlamentario, el escrito del Grupo Popular aludía a la Comisión Europea, a determinados informes del Defensor del Menor de la Comunidad de Madrid y a los problemas detectados en la Unidades policiales de los Cuerpos y Fuerzas de Seguridad, «todo lo cual», precisaba, «aconseja fortalecer las medidas destinadas a la prevención del acoso por internet, mediante la formación de padres, profesores y los propios menores; así como, conseguir una respuesta rápida de los gestores de redes sociales, en casos de investigaciones desapariciones, extorsiones y otros hechos», por todo lo cual, el «petitum» del Grupo Popular proponía la creación de una Subcomisión de Estudio «como herramienta para establecer, de forma consensuada, una estrategia nacional de carácter integral que permita afrontar

cve: BOCG-10-D-643

la protección de educación de nuestros menores en la red y la prevención de delitos cometidos a través de las redes sociales». En el mismo escrito, y según pauta habitual en la solicitud de creación de Subcomisiones, se recogía propuesta sobre el objeto de la subcomisión, la composición, el método de adopción de acuerdos y los plazos de trabajo de la Subcomisión.

La Comisión de Interior debatió el 27 de febrero la creación de esta Subcomisión adoptándose el acuerdo por asentimiento, lo que equivale a unanimidad, de los miembros de la Comisión.

Esta propuesta de creación adoptada por la Comisión de Interior, fue elevada al Pleno por escrito de 12 de marzo de 2013, firmado por el entonces Presidente de la Comisión de Interior, D. Juan Carlos Aparicio.

I.2 Aprobación por el Pleno del Congreso de los Diputados.

El Pleno del Congreso, en sesión de 11 de abril de 2013, acordó aprobar por asentimiento la creación de la Subcomisión de Estudios sobre las Redes Sociales, en los términos de la calificación de la Mesa de la Cámara publicada en el «BOCG. Congreso de los Diputados», serie D, núm. 244, de 22 de marzo de 2013.

Conforme a ello, la Subcomisión sobre Redes Sociales se constituyó el 18 de abril de 2013, acordándose designar en esa misma fecha como coordinador de la misma al Diputado D. Conrado Escobar Las Heras.

I.3 Constitución de la Subcomisión.

En la misma sesión constitutiva de la Subcomisión el 18 de abril de 2013 el coordinador de la Subcomisión planteó algunos criterios generales sobre el funcionamiento de la Subcomisión, relativos a: en primer lugar, la flexibilidad de actuación; en segundo lugar, la conveniencia de que haya actas de las Sesiones y se transcriban las comparecencias, así como que se publiquen las transcripciones, o al menos un resumen, en la página Web de la Cámara, a cuyo fin se solicitaría la autorización correspondiente de la Cámara; y en tercer lugar, la necesidad de evitar solapamientos con una Ponencia de Comisiones Conjuntas constituida en el Senado que va a tender a cierta especialización en la protección de menores, lo que supondría por parte de la Subcomisión del Congreso inclinarse a la especialización en el análisis de la seguridad de las redes sociales con carácter general.

La Subcomisión, desde la sesión constitutiva abrió plazo para que los Grupos Parlamentarios presentaran propuestas de comparecencias en el bien entendido de que se trataría de evitar duplicidades en la materia. Dicho plazo finalizó el 10 de junio de 2013.

En las siguientes sesiones de la Comisión se analizaron las más de 100 comparecencias solicitadas por los Grupos Parlamentarios, acordándose la metodología, el formato y la cadencia de las comparecencias que, según se estableció, se llevaría a cabo de septiembre hasta junio y en la primavera del 2014. Asimismo, se solicitó a los Servicios Jurídicos de la Comisión, que prepararan un listado de comparecientes por bloques temáticos que se vería en próximas sesiones de la Subcomisión.

La metodología de trabajo de Subcomisión ha sido la propia de este tipo de órganos parlamentarios de estudio que funcionan sobre tres elementos: **comparecencias, análisis documental y trabajo de campo**.

Respecto de las **comparecencias** la Subcomisión acordó convocar del orden de 3 a 5 comparecientes por sesión, con carácter general, y el formato de las comparecencias, que se iniciarían, en primer lugar, con una breve exposición del compareciente, seguida de un turno de preguntas y respuestas por parte de los Diputados y las personas citadas a comparecer. A la vista de estas características, en la sesión de 19 de junio de 2013, se acordó la fecha de inicio de las comparecencias (el 26 de junio) y establecer tres grupos o bloques de comparecencias más un cuarto de autoridades, de los cuales, el primero se llevaría a cabo entre los meses de septiembre a noviembre de 2013 con el «leitmotiv» de comparecientes relacionados con tecnologías informáticas o electrónicas, redes sociales y protección a la infancia. El segundo bloque de comparecientes se pretendía que se llevara a cabo a lo largo de los últimos meses del año e incluiría tres diferentes grupos, el primero de profesores y académicos; el segundo, de representantes de comunicación y redes sociales; y el tercero, consultores; amén de un cuarto grupo con representantes de asociaciones y fundaciones.

El tercer bloque, previsto para 2014, se integraría con un primer grupo de abogados especializados; un segundo grupo, de especialistas en protección de derechos; y un tercer grupo de comparecientes con representantes de consumidores y usuarios.

cve: BOCG-10-D-643

Por último, el cuarto bloque, a celebrar en 2014, estaría integrado por comparecencias de autoridades de diferente ámbito.

Desde el día 26 de junio de 2013 hasta el día 3 de septiembre de 2014 se han celebrado durante el periodo de vigencia de la Subcomisión 13 sesiones de comparecencias con 48 comparecientes en total.

Respecto del **análisis documental** consistente en el estudio de la información preparada por la Cámara a través del Departamento de Documentación y los servicios de la Comisión que, en este caso, ha comprendido lo siguiente:

— Legislación española**:** Constitución; L. O. 10/1995, de 23 de noviembre, del Código Penal; Ley Orgánica 5/2000, de 12 de enero, reguladora de la Responsabilidad Penal de los Menores; R. D. Legislativo1/1996 de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual; Ley 2/2012 de 4 de marzo, de Economía Sostenible; R. D. 1889/2011 de 30 de diciembre, por el que se regula el funcionamiento de la Propiedad Intelectual; Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen; e instrumento de ratificación del convenio sobre ciber delincuencia hecho en Budapest el 23 de noviembre de 2001 («BOE» núm. 226, de 17 de septiembre de 2010).

— Legislación española autonómica**:** Leyes y Reglamentos relativos a redes sociales y menores.

— Jurisprudencia**:** Auto de la Audiencia Nacional de 27 de febrero de 2012, planteando cuestión prejudicial de interpretación sobre la protección de datos de un particular frente a Google.

— Información de la Unión Europea sobre la materia**:** Documentos COM: *«Hacia una política general de lucha contra la ciber delincuencia»* COM (2007)/267 final de 22 de mayo; *«La protección de los menores en el mundo digital»* COM (2011)/556 final, de 13 de septiembre; *«La represión del delito en la era digital: creación de un centro europeo de ciber delincuencia»* COM (2012)/140 final, de 28 de marzo; *«Estrategia europea en favor de una internet más adecuada para los niños»,* COM (2012)/196 final, de 2 de mayo; «Informe del Parlamento Europeo (Comisión de Desarrollo Regional, Ponente Ms. Lisabeth Schroedter), *Sobre las consecuencias locales y regionales del desarrollo de redes inteligentes»,* de 10 de enero de 2014; «Informe del Parlamento Europeo (Comisión del Mercado Interior y Protección del Consumidor, Ponente: D. Pablo Arias Echeverría) *Sobre un mercado integrado de los Servicios de entrega para impulsar el comercio electrónico en la U.E.»; «Resumen del dictamen del Supervisor Europeo de Protección de Datos»,* de 29 de junio de 2012, sobre la comunicación de la Comisión Europea al Consejo y al Parlamento Europeo sobre *«creación de un centro europeo de Ciber delincuencia»; «Dictámenes del CES europeo sobre la estrategia europea en favor de un internet más adecuada para los niños»* (18-9-2012) y sobre *«Uso responsable de las redes sociales y prevención de trastornos asociados»* (de 19-9-12); Estrategia de Ciber seguridad de la Unión Europea, presentada por la Comisión Europea y por la Alta Representante de la Unión para Asuntos Exteriores y de Política de Seguridad (2013).

— Sentencia de la Gran Sala del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en asunto C-131/12 (Cuestión prejudicial planteada conforme al articulo 267 TFUE por la Audiencia Nacional mediante Auto de 17 de febrero de 2013, recibido en el Tribunal de Justicia el 9 de marzo de 2012, en el procedimiento entre Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos.

— Documentación extranjera. Derecho Comparado**.** La Subcomisión ha manejado entre otra información y documentación, la siguiente:

Canadá: *Ley sobre el sistema de Justicia Penal para los adolescentes, Parte VI, protección de la vida privada de los adolescentes,* actualizada a 23-10-2012»; Documentación: *«Cada imagen, cada niño: la facilidad de internet para el abuso sexual de niños en Canadá».* Gobierno de Canadá, 2009; *Sentencia de la Corte Suprema de Canadá, de 27 de septiembre de 2012.*

Estados Unidos: *Ley sobre amenazas electrónicas, de 16 de diciembre de 1997; Ley de protección de la privacidad Online de los niños, de 1998; Ley de 13 de octubre de 2008, sobre mantenimiento internet a salvo de los depredadores sexuales; Ley 13 de octubre de 2008, para erradicar las amenazas cibernéticas a nuestros niños; Ley de 17 de enero de 2013, de protección de privacidad Online de los niños.* Documentación: *Cuadro general de la normativa y políticas sectoriales de los Estados de la Unión sobre «bulling», «ciberbulling» ataques electrónicos, vulneraciones electrónicas, sanciones penales, sanciones escolares, políticas escolares y comportamiento en los campus; Dosier con las conclusiones del estudio sobre victimización Online juvenil.*

Francia: *Ley de 12 de junio de 2009, favoreciendo la difusión y protección de la creación en internet; Código Penal Libro II, Título II, Cap. 7, Sec. 5 De la puesta en peligro de los Menores; Código de la*

cve: BOCG-10-D-643

Propiedad Intelectual, apartado relativo a la difusión de obras y protección de derechos en internet. Documentación y Estudios: *«Guía práctica para luchar contra las ciberamenaza entre alumnos».* Ministerio de Educación Nacional Juventud y Vida Asociativa. Año 2011; *Estudio de modelo económico de sitios o servicios de distribución de contenidos ilícitos* (marzo de 2012).

Italia: *Ley de 8 de febrero de 2006 de lucha contra los ataques sexuales a los niños y la pedo-pornografía a través de internet.*

Reino Unido: *Ley de 1988 de comunicaciones maliciosas; Ley de 2010 sobre economía digital,* modificada en 2012 en materia de Copyright. Documentos: *«Mantener a salvo a los niños en un mundo digital».* Informe de la Revista Byron marzo de 2008; *«Protegiendo a los niños del "ciberbulling" y la violencia virtual»,* Londres 2009 y Londres 2012. *«Respuesta del Gobierno a la consulta sobre control parental en internet».* Departamento de Educación de diciembre de 2012. *«Nota de la Cámara de los Comunes de 15 de enero de 2013, sobre la protección de los niños en Internet».*

— Documentación de Organizaciones Internacionales. La Subcomisión ha manejado entre otra información y documentación, la siguiente:

Consejo de Europa: Recomendación (2006/12), del Comité de Ministros a los Estados miembros, sobre responsabilidad y autonomía de los niños en torno al medioambiente de la información y de la comunicación; Declaración del comité de Ministros de 20 de febrero de 2008 sobre protección de la dignidad, seguridad y vida privada de los niños en internet.

OCDE: *La protección de los niños Online,* documento de 2 de mayo de 2011;

Fondo de las Naciones Unidas para la Infancia (UNICEF): *Seguridad Online de los niños: cambios globales y estrategias,* diciembre de 2011.

Unión Internacional de Telecomunicaciones (ITU): *Uso de la información y la comunicación tecnológica por parte de los niños y jóvenes del mundo* (junio de 2008); *Guía para políticas sobre protección Online de los niños* (Año 2009);

Memorándum de Montevideo de 28 de julio de 2009, «Seminario Derechos Menores y Redes sociales en internet», sobre la protección de datos personales y la vida privada en las redes sociales y en internet en particular de niños, niñas y adolescentes: Recomendaciones para los estados y entidades educativas de carácter preventivo; Recomendaciones para Estados sobre marco legal; Recomendaciones para aplicación de las leyes por parte de los Estados; Recomendaciones en materia de Políticas Públicas; Recomendaciones para la industria.

— Otra Documentación y Estudios en relación con la materia. La Subcomisión ha manejado entre otra información y documentación, la siguiente:

Instituto Nacional de Tecnología de la Comunicación. Observatorio de Seguridad de la Información: *Estudio sobre la privacidad de los datos personales y la seguridad de la información de las redes sociales Online* (2009); *Guía de actuación contra el ciber-acoso para padres y educadores* (octubre de 2012); *Guía legal sobre «ciberbulling» y «grooming»* (año 2009).

Ciberbulling and the Law. De T. A. Jacobs. (State bar of Arizona, 2013)

El «bulling» (acoso escolar) y el «ciberbulling», prevención y soluciones desde la vía judicial y las extrajudiciales. De R. Pérez Martel. Diario La Ley, N.º 7978 de 4-12-2012.

Buscadores de internet y protección de datos: La cuestión prejudicial de la audiencia Nacional sobre Google. P.A. de Miguel Asensio. Diario La Ley, 7860. Año 2012.

El ciber-acoso con intención sexual y el «child grooming». V. Panizo Galenca. *Quadernos de Criminología.* n.º 15, de 2011.

Ciber-piratas, administración y jueces. D. Ordoñez. *Diario La Ley.* n.º 7822, de 21-3-2012.

Ciberbulling. V. B. Worley. Criminal Law Bulletin. Primavera 2011.

Los derechos de autor en los medios y soportes electrónicos y digitales. J. Massaguer Fuentes. *Diario La Ley* 7800, de febrero de 2012.

El fenómeno de las Redes Sociales y los cambios en la vigencia de los Derechos Fundamentales. A. M. Gil Antón. *Revista de Derecho de la UNED.* nº 10. 2012.

Intervención de comunicaciones electrónicas. J. M. Suárez Robledano. *Foro Nueva Época*, n.º 14, 2011.

Sexting Sexual Expression or Child Pornography. V. B. Worley. Criminal Law Bulletin. Verano 2012.

cve: BOCG-10-D-643

El tercer elemento de trabajo es el denominado trabajo de campo, habida cuenta de la naturaleza de la materia objeto de estudio, se ha realizado desde los propios sistemas online de los Diputados miembros de la Subcomisión y mediante un fluido intercambio de informaciones online, a través de los Diputados y las Redes Sociales.

En un momento de la actividad de la Comisión (11 de julio de 2013) se llegó a solicitar autorización para publicar en la web de la Cámara los resúmenes entregados por los comparecientes respecto de las comparecencias que se llevaron a cabo en la Subcomisión, si bien, por la naturaleza de este órgano parlamentario, y dado el régimen de publicidad aplicable a las Subcomisiones de la Cámara, no resultó procedente, ya que sólo se publican los Diarios de Sesiones y éstos se corresponden con las Comisiones Parlamentarias (Acuerdo de la Mesa de 24 de julio de 2013); en todo caso, se ha producido este fluido intercambio de información entre los miembros de la Subcomisión, los comparecientes y otras personas, a través de las redes sociales.

La Subcomisión no ha llevado a cabo desplazamientos de estudio lo que supone un coste cero en las tareas de la Cámara en este ámbito.

I.4 Composición, objeto, método y calendario de trabajo.

La composición de la Subcomisión.

De conformidad con la propuesta de creación de la Subcomisión de estudios sobre las redes sociales y en los términos del apartado tercero de la Resolución de la Presidencia del Congreso de 26 de junio de 1996, la Subcomisión ha estado compuesta por cuatro representantes de los Grupos Parlamentarios con más de 100 Diputados, lo que, según la Composición de la X Legislatura, equivale a decir 4 representantes del G. P. Popular y 4 del G. P. Socialista, en tanto en cuanto estos dos grupos son los únicos que cuentan en la Cámara con más de 100 Diputados; dos representantes de Grupos Parlamentarios con más de 6 Diputados, esto es, dos representantes del Grupo Parlamentario Izquierda Plural, dos del Grupo Parlamentario CiU y dos del Grupo Parlamentario Mixto; y un representante de los restantes Grupos Parlamentarios, que son un representante del Grupo PNV y otro del Grupo UPyD (Grupos con menos de seis Diputados cada uno de ellos). A su vez, cabe la posibilidad de que haya designación de suplentes, lo que así ha efectuado por el Grupo Parlamentario Popular, quien ha designado como suplentes a D. Javier Puente y D.ª Julia de Micheo Carrillo-Albornoz. Por otra parte, al haber sido designada como Alto Cargo en el Gobierno la Diputada D.ª Susana Camarero Benítez fue sustituida por D.ª Macarena Montesinos de Miguel como representante del Grupo Parlamentario Popular.

En total los componentes titulares y suplentes de la Subcomisión han sido: 18 Diputados, asistidos por los servicios jurídicos y administrativos de la Comisión de Interior, conforme a la lista que figura a continuación.

Vocales:

Agirretxea Urresti, Joseba Andoni (sustituyó desde el 06/02/2014 a D. Emilio Olabarría Muñoz)-Grupo Parlamentario Vasco (EAJ-PNV).

Álvarez Álvarez, Ángeles, Grupo Parlamentario Socialista.

Ciuró i Buldó, Lourdes (sustituyó desde el 12/12/2013 a D. Jordi Jané i Guasch)-Grupo Parlamentario Catalán (Convergència i Unió).

Escobar las Heras, Conrado, Grupo Parlamentario Popular.

Escudero Berzal, Beatriz Marta, Grupo Parlamentario Popular.

Guillaumes I Ràfols, Feliu-Joan, Grupo Parlamentario Catalán (Convergència i Unió).

Larreina Valderrama, Rafael, Grupo Parlamentario Mixto.

Llamazares Trigo, Gaspar, Grupo Parlamentario IU, ICV-EUiA, CHA: La Izquierda Plural.

Marcos Domínguez, Pilar, Grupo Parlamentario Popular.

Martín González, María Guadalupe, Grupo Parlamentario Socialista.

Martínez Gorriarán, Carlos, Grupo Parlamentario Unión Progreso y Democracia.

Montesinos De Miguel, Macarena (sustituyó desde el 01/04/2014 a D.ª Susana Camarero Benítez)-Grupo Parlamentario Popular.

Salvador Armendáriz, Carlos Casimiro, Grupo Parlamentario Mixto.

Sánchez Amor, José Ignacio, Grupo Parlamentario Socialista.

Sixto Iglesias, Ricardo, Grupo Parlamentario IU, ICV-EUiA, CHA: La Izquierda Plural.

Trevín Lombán, Antonio Ramón María, Grupo Parlamentario Socialista.

cve: BOCG-10-D-643

Vocales suplentes:

Micheo Carrillo-Albornoz, Julia de, Grupo Parlamentario Popular
Puente Redondo, Javier, Grupo Parlamentario Popular

Letrada de la Comisión de Interior:

Ripollés Serrano, María Rosa

Servicios administrativos:

Bravo García, José Luis
Martínez Esteban, Laura

Objeto de la Subcomisión.

La Subcomisión, conforme al escrito de creación de la misma, aspiraba a alcanzar seis objetivos de trabajo: primero, analizar la situación actual en España de las redes sociales; segundo; analizar la situación en países de nuestro entorno; tercero, estudiar el papel que las Administraciones Públicas tienen en el mundo de las redes sociales e intensificar la cooperación e intercambio de información con los administradores de las redes sociales mediante la activación de canales de comunicación ágiles; cuarto determinar qué modificaciones legislativas se deben llevar a cabo para mejorar la protección integral de nuestros menores y la educación en su utilización; quinto, determinar qué otras medidas, además de las citadas, son necesarias para que nuestra sociedad dé un tratamiento acorde con las necesidades actuales, mejorando la formación y concienciación de los usuarios; y sexto, determinar las medidas necesarias para la protección de los derechos de propiedad intelectual en el entorno de las redes sociales y para la promoción de conductas respetuosas con estos derechos por parte de los usuarios de las citadas redes.

Metodología de trabajo y fórmula de adopción de acuerdos.

En los términos habituales de estos órganos parlamentarios, la metodología de trabajo de la Subcomisión ha sido la tradicional de esta clase de órganos parlamentarios, ya referida anteriormente, esto es: análisis documental, comparecencias, y trabajo de campo circunscrito, en este caso, a la utilización de las redes sociales en la indagación y en los planteamientos de comunicación con los usuarios.

Desde el día 26 de junio de 2013 hasta el día 3 de septiembre de 2014 se han celebrado durante el periodo de vigencia de la Subcomisión 13 sesiones de comparecencias con 48 comparecientes en total.

Por lo que atañe al sistema de adopción de acuerdos y según viene siendo habitual en esta clase de órganos, los acuerdos se adoptan por asentimiento y, en el supuesto de tener que recurrir a la votación, por aplicación del denominado «voto ponderado», es decir, cada grupo en la Subcomisión, si todos los miembros del Grupo votan en el mismo sentido, expresa un resultado general equivalente al número total de votos con los que cuenta el Grupo Parlamentario en la Comisión de Interior.

Calendario o plazo de trabajo de la Subcomisión.

En el escrito de constitución, se indicaba que la Subcomisión habría de culminar sus trabajos dentro de los dos próximos periodos de sesiones. Toda vez que la Subcomisión se constituyó el 18 de abril de 2013, esto es, en el primer periodo de sesiones del año 2013, la fecha originariamente previstas para finalizar los trabajos de la Comisión, comprendía hasta el 30 de junio de 2014.

Teniendo en cuenta que la Subcomisión es un órgano de la Comisión de Interior y ha de convivir con la actividad ordinaria de esta Comisión Legislativa permanente, y que en 2013 se tramitaron dos proyectos de Ley (Reforma de la normativa de Tráfico, Seguridad Privada) y en 2014 se tramitó el Proyecto de Ley de Régimen de Personal de la Guardia Civil y el PLO de Protección de la Seguridad Ciudadana, ello supuso, suspender en diferentes etapas los trabajos de la Subcomisión por la dedicación prioritaria que requiere el trabajo legislativo.

Esta fue la razón por la que la Comisión solicitó, de conformidad con el punto Tercero. 2 de la Resolución del Presidente del Congreso de 26 de junio de 1996, la autorización de una prórroga del plazo para la finalización de sus trabajos hasta el 31 de marzo de 2015.

cve: BOCG-10-D-643

El Pleno del Congreso de los Diputados acordó en su sesión de 26 de junio de 2014 autorizar la prórroga del plazo de ampliación de sus trabajos hasta el 31 de marzo de 2015.

Desde la sesión constitutiva el 18 de abril de 2013, hasta la sesión de aprobación del Informe, el 10 de marzo de 2015, la Subcomisión, además de diversas reuniones preparatorias de trabajo, ha celebrado diecinueve sesiones.

Procedimiento parlamentario para la adopción del Informe.

Una vez constituida la Subcomisión y finalizado su trabajo de análisis la Subcomisión ha de aprobar el Informe en el plazo previsto y con el límite de 31 de marzo de 2015.

El Informe, acompañado de los votos particulares si los hubiera, (esto es, las discrepancias formalizadas de los grupos parlamentarios al texto del Informe aprobado) se ha de someter a debate y a aprobación por la Comisión de Interior. El debate del Informe de la Comisión, conforme a la Resolución del Presidente del Congreso de 26 de junio de 1996, y demás disposiciones concordantes del Reglamento del Congreso, se inicia con la presentación del Informe aprobado por un miembro de la Subcomisión, a continuación, intervienen los Grupos Parlamentarios que hayan presentado votos particulares y después los demás Grupos Parlamentarios. Todos ellos por 15 minutos, durante los cuales, pueden presentarse enmiendas transaccionales para conseguir un texto de transacción entre el informe y los votos particulares.

Seguidamente se votan lo votos particulares y, por último, el informe que se remite para su publicación en el Boletín Oficial de Cortes Generales junto con los votos particulares mantenidos.

Si la Subcomisión de Interior solicita a la Comisión de Interior que ésta eleve a la Mesa de la Cámara, el debate y votación del Informe en el Pleno, y la Mesa, oída la Junta de Portavoces, así lo acuerda; en el plazo de 48 horas desde la votación en Comisión del Informe y votos particulares, los Grupos Parlamentarios pueden presentar los votos particulares que mantengan para el Pleno.

Por último, el informe (sea aprobado solamente en la Comisión de Interior, o bien, aprobado por el Pleno) se publicaría en publicación en papel y electrónica para su inclusión, si resulta factible en internet y su posible presentación en diferentes foros relacionados con la materia.

II. Comparecencias efectuadas en la Subcomisión para el Estudio de las Redes Sociales.

— Sesión N.º 5, de 26 de junio 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 de INTECO (Instituto Nacional de Tecnología y de Comunicación).

— Sesión N.º 6, de 11 de septiembre de 2013.

D. Eugenio Fontán Oñate, Presidente del Colegio de Ingenieros de Telecomunicaciones.

D.ª Natalia Basterrechea, Directora de Asuntos Públicos de Facebook.

D. Francisco Ruiz Antón, Representante de Google Spain.

D. Antonio Ramos, Presidente de ISACA.

— Sesión N.º 7, de 18 de septiembre de 2013.

D. Sebastián Muriel Herrero, Vicepresidente de Tuenti.

Preguntas y observaciones de los miembros de la Subcomisión a D. Sebastián Muriel, así como respuestas y puntualizaciones.

D. Carlos Represa Estrada, representante del Centro Nacional de Seguridad Escolar.

D. Guillermo Cánovas Gaillemín, Presidente de Protégeles

D. Miguel Comín, Director Fundación Alia2.

D. Marcelino Madrigal García, activista antipornografía infantil en redes y experto en seguridad protección del menor.

cve: BOCG-10-D-643

— Sesión N.º 8, de 25 de septiembre de 2013.

D. Jesús María Sánchez Herrero, Presidente de CEAPA.
D. Ramón Arnó Torrades, coordinador de la comisión de menores de la Asociación Profesional Española de Privacidad (APEP).
D.ª Myriam Fernández Nevado, Vicepresidenta de la Asociación GSIA (Grupo de Sociología de la Infancia y de la Adolescencia).
D.ª Ana Marzo Portera, representante de la organización Padres 2.0.

— Sesión N.º 9, de 12 de febrero de 2014.

D. José Luis Piñar Mañas, Director de la Cátedra Google del CEU.
D. Juan María Martínez Otero, miembro del consejo asesor de iCmedia.
D. Juan Carlos Ortiz Pradilla, profesor de Derecho Procesal de la Universidad de Castilla-La Mancha
D.ª María Concepción Torres Díaz, profesora de Derecho Constitucional de la Uniersidad de Alicante.

— Sesión N.º 10, de 19 de febrero de 2014.

D. Íker Merodio, doctor en Periodismo.
D. Ángel Mario Tascón Ruiz, experto en uso del lenguaje en internet y deontología periodística.
D. Ícaro Moyano Díaz, periodista experto en comunicación empresarial.

— Sesión N.º 11, de 6 de marzo de 2014, por la mañana.

D. Faustino Jiménez Carracedo, CEO de Arsys.
D. Jesús Encinar Rodríguez, fundador de Idealista.
D. Juan Antonio Osaba Arenas, Director General de MASSCOM.

— Sesión N.º 12, de 6 de marzo de 2014, por la tarde.

D. Alfonso Carrascosa Marco, Fundación Legalitas.
D. Jorge Campanillas Ciaurriz, abogado especializado en Derecho Tecnológico.
D. Pablo Fernández Burgueño, abogado especializado en propiedad intelectual, protección de datos y nuevas tecnologías.
D. Alejandro Touriño Pena, despacho de abogados Écija.

— Sesión N.º 13, de 2 de abril de 2014, por la mañana.

D. Jesús Alloza, consejero delegado de COONIC.
D.ª Carlota Navarrete Barreiro, Coalición de Creadores e Industrias de Contenidos.
D. Víctor Domingo Prieto, presidente de la Asociación de Internautas.
D. Miguel Pérez Subías, presidente de la Asociación de Usuarios de internet.
D. Ricard Martínez Martínez, presidente de la Asociación Profesional Española de Privacidad-APEP.
D. Luis Alberto Calvo Campos, director de Sistemas de Seguridad de Indra.

— Sesión N.º 14, de 2 de abril de 2014, por la tarde.

D. Jorge Flores Fernández, director de Pantallas Amigas.
D. Ramón Miralles López, coordinador de auditorías y seguridad de la información en Autoridad Catalana de Protección de Datos.
D. José Manuel Tourné Alegre, director general de la Federación para la Defensa de la Propiedad Intelectual, FAP.
D. David Maeztu Lacalle, experto en seguridad y protección del menor, propiedad intelectual y regulación del entorno laboral en el marco de las redes sociales.

— Sesión N.º 15, de 22 de abril de 2014.

D. Francisco Fernández Marugán, Adjunto Primero a la Defensora del Pueblo.
D. José Luis Rodríguez Álvarez, director de la Agencia Española de Protección de Datos.

cve: BOCG-10-D-643

D.ª Elvira Tejada de la Fuente, Fiscal Delegada para la Lucha contra la Delincuencia Informática. Coordinadora Nacional de Criminalidad Informática.

D. Manel Prat Peláez, Director General de los Mossos d'Esquadra.

D. Marcial Marín Hellín, Consejero de Educación, Cultura y Deportes de Castilla-La Mancha.

— Sesión N.º 16, de 25 de junio de 2014.

D. Francisco Martínez Vázquez. Secretario de Estado de Seguridad.

— Sesión N.º 17, de 3 de septiembre de 2014.

D.ª Sinead McSweeney, directora de política pública EMEA de Twitter.

D.ª Patricia Cartes, directora de seguridad de Twitter

III. Breve resumen de las materias más relevantes suscitadas en cada comparecencia.

D. Víctor Calvo-Sotelo Ibáñez-Martín, Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información. Comparecencia de 26 de junio de 2013.

Las cuestiones más relevantes planteadas por el compareciente se refirieron a los siguientes puntos:

— El objetivo de las Administraciones Públicas es encauzar los importantes cambios incorporados por las tecnologías de la sociedad de la información (61 % de los usuarios consulta diariamente las redes; hay 2.600.000 personas entre 10 y 15 años, lo que equivale a que el 91 % de este tramo de edad en 2012 ha usado la red).

— Necesidad de entender los diferentes elementos positivos y oportunidades que ofrece el uso de las redes sociales (en la información, la cultura, la empresa, etc.).

— Problemas derivados de este uso masivo y creciente de las redes sociales:

• El ciberacoso *(ciberbulling:* acoso entre iguales; y *grooming:* acoso de adulto sobre menor).
• Siendo un fenómeno internacional, requiere reformas internacionales.
• Primacía de la ciber-seguridad: estrategia nacional de Ciber-seguridad de INTECO.
• Adecuación de la tradicional protección al honor a la intimidad personal y familiar y a la propia imagen (Art. 18 CE), a la protección de datos informáticos. Proyecto de Reglamento de la U.E. que aborda el «derecho al olvido».
• La Unión Europea trabaja en varios frentes en esta materia:

◦ Tratar de llegar en este asunto a conseguir una voz única de Europa.
◦ Proyecto de Directiva de Seguridad Europea; Proyecto de Reglamento de Datos y SAFER (Programa de Seguridad en internet).

— En España se está trabajando en la Gestión de programas:

• Caso Protégeles;
• Agenda Digital España, que comprende:

◦ INTECO como centro de excelencia digital.
◦ Contenidos Digitales en itinerario educativo.
◦ Plan para la Confianza Digital.
◦ Convenio Ministerio del Interior: Apoyo Técnico a Unidades Cuerpo nacional de Policía y Guardia Civil.

D. Borja Adsuara Varela, Director General de Red.es. Comparecencia de 26 de junio de 2013.

El compareciente aborda, entre otros temas, lo siguiente:

— Se suelen denominar Redes a todas las plataformas de comunicación electrónica, así la propia internet es una red social, si bien, los contenidos y caracteres son distintos, pues hay contenidos indexados o no, este último sería el caso de Facebook.

cve: BOCG-10-D-643

— Ciberdelincuencia: los delitos no cambian, lo que varía es la metodología delictiva.

— El Código Penal ha de ser la última ratio del ordenamiento jurídico siendo preferibles el recurso a técnicas educativas y preventivas.

— Menores, es diferente hablar en este campo de niños que de adolescentes (por ejemplo, el delito de pornografía infantil podría aplicarse hipotéticamente a un adolescente que manda una fotografía). En esta cuestión hay dificultades en la delimitación de la identidad sujeto y objeto delictivo.

• El 93 % de los adolescentes entre 14 y 17 años están en redes sociales, por este orden: Facebook, Tuenti y Twitter. La preferida por este sector suele ser Tuenti.

• El 92 % de los niños menores de 2 años ya tienen huella digital (fotos de bebés transmitidas a través de redes sociales).

— Administraciones Públicas y Redes sociales: Las Administraciones Públicas deben garantizar los derechos constitucionales de los ciudadanos a través de la red.

— La protección de los ciudadanos de ciberdelitos requiere un análisis a la luz de estas tecnologías de tipos o circunstancias penales clásicos como las amenazas o la inducción a la violencia junto con nuevas circunstancias a considerar potenciadas por las redes como el uso del nickname o la suplantación de identidad.

• Resulta esencial la protección de menores frente a amenazas exteriores como la pederastia o la corrupción de menores o exhibición de pornografía infantil y del menor respecto de otro menor (por ejemplo, la práctica de sexteo *(sexting,* sexo de adolescentes por imitación de mayores en la red).

— Posibles modificaciones legislativas:

• Actualizar la Ley Orgánica 1/982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

• Actualizar la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual.

• Distinguir, en relación con el Proyecto de Código Penal, entre prácticas imprudentes y conductas delictivas.

— Otras medidas en relación con las redes sociales:

• Fomentar la autorregulación sin excesos que encorseten.

• Fomento de la educación en el uso de la red para prevenir delitos y prácticas de riesgo.

— En materia de propiedad intelectual, proteger los nuevos modelos de negocio y gestión a través de la red.

— Estimular el sello de confianza online de seguridad en el comercio electrónico.

D. Manuel Escalante García, Director General de INTECO (Instituto Nacional de Tecnologías de Comunicación). Comparecencia de 26 de junio de 2013.

El compareciente se refiere, entre otras materias, a:

— Cada vez más, la vida personal y profesional y las transacciones comerciales están en el mundo digital.

— El uso de internet y, en general, de las redes sociales, transciende países, en lo positivo, ya citado, y en lo negativo (globalización de la delincuencia).

— Amenazas posibles que se ciernen sobre particulares y empresas:

• Robo de tecnologías.

• Extorsión de empresas.

• Daño a la imagen de corporaciones y administraciones Públicas.

• Fraude electrónico a Internautas (incremento en el fraude).

• Virus *(Wonder)* que pueden determinar que el usuario, sin saberlo, forme parte de una red con su PC.

• Menores: delitos relacionados con pornografía infantil y pederastia (uso de las llamadas «redes de cebolla» que implican sucesivas capas de encriptación que dificultan extraordinariamente la localización).

cve: BOCG-10-D-643

• Ciberespionaje (Red October).
• Complejidad de las redes delictivas (las llamadas «Redes Zombies».
• Ciberterrorismo (virus orientados a la infección masiva, entre otras circunstancias).
• Redes de la llamada «Internet Oscura».
• La revolución de los móviles que lleva por su cercanía al usuario a confundir el plano personal y el profesional.
• Carácter esencial de la garantía del uso responsable de las nuevas tecnologías: potenciar capacidades de protección, en lo público y en lo privado.
• Esencial los intercambios de información entre organismos homólogos y en la rapidez en la respuesta a incidentes (3.900 incidentes en el primer cuatrimestre de 2013), actuar a modo de «bomberos tecnológicos», con ejercicios de pruebas de estrés y, en definitiva, mejorar la cultura de la seguridad.
• Ejemplo del Reino Unido con la estrategia nacional de seguridad con importantes inversiones para garantizar la economía segura.

— Dificultad en los sistemas de certificación por la complejidad, cada vez menos organismos aspiran a certificar. Hay perfiles de protección en software y en hardware.
— Resulta fundamental la acción educativa el «itinerario educativo en nuevas tecnologías».
— Convenio entre Fuerzas y Cuerpos de Seguridad y Seguridad Informática.
— Convenio de Protección de la información sobre infraestructuras críticas.
— Esencial potenciar capacidades de autoprotección y las relaciones de confianza internacional entre organismos supranacionales (caso de Europol C.3, o en Defensa el Mando Unificado de Ciberdefensa).

D. Eugenio Fontán Oñate, Presidente del Colegio de Ingenieros de Telecomunicaciones. Comparecencia de 11 de septiembre de 2013.

El Sr. Fontán se refirió en su comparecencia, entre otras cuestiones, a:

— La velocidad tecnológica del momento actual y a la denominada «web 2.0» propia de la última década del siglo XX. El compareciente destacó que la siguiente generación será de usuario creadores de contenidos, a veces voluntaria o involuntariamente.
— Otro elemento destacado planteado en esta comparecencia es la llamada de atención sobre la democratización de las redes sociales por el abaratamiento de los soportes. Más de 200 millones de Twist diarios suponen un avance imparable y reflejo de la tercera y cuarta generación de smartphones.
— Otro punto a considerar es el denominado internet de las cosas, consistente en conectar objetos a internet lo que permite teleconexiones, por ejemplo, en elementos domésticos como calefacción o medición del grado de humedad de terrenos, etcétera.
— Para 2020 se calcula que habrá 50 millones de dispositivos conectados en red. La era de «big data».
— Hay regulación del hardware pero no hay regulación de internet, por más que existan Comités de expertos trabajando sobre la «gobernanza de internet».
— En todo caso, el compareciente precisa la conveniencia de cambiar de modelo tras un análisis exhaustivo y reflexivo sobre internet.
— La información que circula por internet escapa a las regulaciones nacionales y, paradójicamente, puede darse la circunstancia de que a veces se aplica legislación de otros países desde los que surge este tipo de información electrónica (caso de la primera enmienda de la Constitución de Estados Unidos).
— Un asunto esencial en la regulación de internet y en la agenda digital es la protección de menores, que se vincula a la alfabetización digital. Por lo que atañe a España plantea una serie de cuestiones relacionadas con internet y que sería conveniente estudiar antes de dar un enfoque completo:

• ¿Se cumple la Ley Orgánica de Protección de Datos en materia electrónica?
• ¿Se cumple la seguridad en las Redes Sociales?
• ¿Es posible la portabilidad de redes?
• ¿Es factible el borrado de contenidos y con qué alcance?
• ¿Constituye la gratuidad electrónica un derecho?
• ¿Se puede hablar del derecho al secreto de las comunicaciones electrónicas?

cve: BOCG-10-D-643

— El compareciente concluyó esta primera intervención ante la Subcomisión indicando que de la relevancia de las respuestas da idea el que el 93 % de los españoles se conecta con Redes Sociales.

— En respuestas a Sres. Diputados el compareciente manifiesta que Google más que una red social es un archivo digital.

— Respecto de la normativa aplicable expresa que la mayor parte del tráfico europeo e iberoamericano se cursa a través de Estados Unidos. A nivel europeo, sería conveniente que hubiera una normativa estándar toda vez que los operadores de redes sociales son actores económicos y además, matiza, sería conveniente pensar en un a modo de código de conducta para determinadas cuestiones.

— Asimismo, indica que los contratos de adhesión que existen en determinados ámbitos informáticos deberían cumplir unos requisitos y debería haber procedimientos administrativos sencillos de ámbito europeo en los que prevalezca el concepto de ciudadano.

— El compareciente enfatiza el aspecto económico prevalente en las Redes Sociales que constituye un gran factor democratizador afirmando «en las Redes todos somos más iguales».

D.ª Natalia Basterrechea, Directora de Asuntos Públicos de Facebook. Comparecencia de 11 de septiembre de 2013.

La Sra. Basterrechea en su intervención ante la Subcomisión de Redes Sociales hizo referencia, entre otros elementos, a los siguientes:

— Por lo que se refiere a internet la libertad informática se comprende en el artículo 19 de la Declaración Universal de Derechos Humanos, toda vez que las Redes Sociales no son sino plataformas de comunicación.

— Hay en torno a 1.150.000 millones de usuarios en el mundo de internet, de los que corresponden a España 18 millones. Estos datos reflejan la diversidad de usuarios en la red.

— Facebook supone un enfoque robusto, multifacético y renovador de las Redes Sociales, en el que la seguridad de los usuarios es prioritaria.

— Las medidas para conseguir dicha seguridad consisten en, entre otras, impedir compartir contenidos que inciten al odio, amenazas, acoso, pornografía, violencia y actitudes discriminatorias.

— Los ejes de la política de seguridad de Facebook consisten en: la ayuda para el fácil uso en 24 idiomas, los 365 días del año y 7 días cada semana. En segundo lugar, las interacciones con consejos, guías, etcétera; y en tercer lugar un centro de seguridad para familias.

— La compareciente alude al Instituto de Seguridad Familiar en línea *(Family On Line Safety Institute Centre, FOSIC)* en el que se trabaja sobre un programa de educación para padres, para colectivos «vinculados a otros centros como el teléfono de la esperanza o la denominada Red de samaritanos».

— En cooperación con Google, Facebook trabaja para hacer de internet un lugar mejor para los niños.

— Además, Facebook está conectada con las Fuerzas y Cuerpos de Seguridad del Estado mediante un canal de comunicación de máxima prioridad que permite denunciar cuando se detectan situaciones delincuenciales.

— Mediante una tecnología de fotos DNA (tecnología que dimana contenidos) se pretende contar con colaboradores activos para la identificación del mal trato y la pedofilia, con denuncias al centro de niños desaparecidos de EEUU y de allí a las autoridades.

— En respuesta a preguntas de los Sres. Diputados miembros de la Subcomisión expresa la conveniencia de coordinar responsabilidades mediante la creación de un Comité de expertos.

— Asimismo, la compareciente contestando a Sres. Diputados, expresa que la denuncia social resulta esencial para prevenir casos de abuso de menores.

— En materia de normativa aduce la conveniencia de contar con legislación de ámbito europeo (alude concretamente a la Directiva sobre ciberseguridad).

— En cuanto a la responsabilidad de los usuarios debería tenerse en cuenta la denominada teoría de la responsabilidad de los propios actos, esto es consciencia de que tu pasado, tu historia, resulta muy difícil borrar de las páginas web.

cve: BOCG-10-D-643

D. Francisco Ruiz Antón, Google Spain. Comparecencia de 11 de septiembre de 2013.

El compareciente en su intervención ante la Subcomisión hizo mención de las siguientes cuestiones, entre otras:

— Internet como herramienta maravillosa, que cuenta con 2.400 millones de personas interconectadas, de las que en España hay unos 27 millones, algo por debajo de la media de la OCD. internet ha cambiado mucho, a mejor, pero aún sigue teniendo riesgos, porque, afirma, cualquier avance disruptivo tiene sus riesgos.

— El compareciente distingue entre riesgo como potencialidad de daño y daño como mal real, para concluir que las tecnologías tienen riesgo.

— Para Google resulta fundamental la protección de los más vulnerables, por ejemplo los niños, que son destinatarios a quienes se debe enseñar habilidades digitales y a la par los riesgos de internet que, en el caso español, son riesgos de carácter medio.

— Es importante también considerar que por ejemplo en la Unión Europea en 2015 habrá en torno a 17 millones de puestos de trabajo no cubiertos por falta de perfiles adecuados en jóvenes, lo que conduce a la conveniencia de cambiar los diseños curriculares en economía digital.

— Resulta esencial el papel de los Diputados en estas materias toda vez que son quienes transforman las ideas en políticas públicas o normas.

— A continuación el compareciente se refiere a determinados elementos de Google concebidos como técnicas de Seguridad: tales como Google take out para llevarlo a otra plataforma sin perder; Centro de Seguridad Familiar Google; Safe search que es un filtro en Google; herramientas para eliminar contenidos inapropiados (por ejemplo, filtros en smartphones); Centro de recepción permanente de uso indebido; Acuerdos entre Google y Policías contra el abuso de menores en internet (Safe search, Alia2, etcétera); lucha contra la pornografía infantil (por ejemplo, técnica para bloquear imágenes de pornografía infantil); y políticas públicas que involucren a padres y profesores.

— En respuesta a Sres. Diputados indica que al objeto de evitar la comisión de determinados delitos, especialmente sensibles, como por ejemplo la pederastia, se publica en el «Transparency Report for thematical» la identificación del delito y con ello se pretende aplicar elementos disuasorios.

— También en respuesta a Sres. Diputados se refiere a sistemas de seguridad en Estados Unidos que a veces hacen difíciles las respuestas inmediatas a solicitudes de información planteadas desde otros ámbitos.

— Respecto de su Organización alude al programa PRISMA ya que ellos están duplicando la encriptación para hacerla más difícil. Reitera que la «Central de estas cuestiones» se encuentra en Estados Unidos.

— Asimismo, en respuesta a una Sra. Diputada el compareciente se refirió a los protocolos con las Fuerzas y Cuerpos de Seguridad y a la entrega de información solo si proviene de un Juzgado.

— También en respuesta a Diputados, indicó que ellos tienen tecnología de filtros y sistemas de «sanción» como por ejemplo, si detectan que un usuario tiene tres videos inapropiados se le cierra la cuenta; Lo propio sucede cuando se detectan insultos o amenazas.

— Coincide con otros comparecientes en la necesidad y conveniencia de la Directiva de Ciberseguridad y en la «ventanilla única».

— Por último, también en relación con otro Diputado se refiere al «derecho al olvido» en relación con lo cual alude a los robots TXT (sistemas selectivos para que no se indexen determinados contenidos).

— En respuesta a otro Diputado indica que no son los usuarios los que lideran las Redes Sociales sino las empresas de Silicon Valley; Esta «revolución» puede dar lugar a que Europa se quede atrás en la materia.

— En materia de regulaciones se refiere a diferentes niveles de seguridad correspondiendo el máximo, por ejemplo, a los operadores de infraestructuras críticas; el medio a las Redes sociales y el bajo, por ejemplo a las PYMES, etcétera.

cve: BOCG-10-D-643

D. Antonio Ramos, Presidente de ISACA. Comparecencia de 11 de septiembre de 2013.

El compareciente entre otras cuestiones se refiere a los siguientes extremos:

— ISACA es una Asociación Profesional que trabajan en auditorías, gestión de riesgo y gobierno de TIC.

— Para ello resulta esencial el concepto de ciberseguridad que consiste en la aplicación de la seguridad en el entorno cibernético cuya finalidad es obtener un entorno ciberseguro.

— La propuesta de estrategia de ciberseguridad de la UE recomienda sistemas etiquetados para no expertos.

— La realidad es que no hay amenazas nuevas, sino nuevas formas de amenaza, en un entorno en el que los usuarios no son conscientes de las consecuencias de sus actos.

— La estrategia española de seguridad parte de que no hay ciberamenazas, sino amenazas por métodos distintos.

— El compareciente recalca que hay que hacer que los actos inseguros tengan sus consecuencias, porque mejorar la clarificación de las cláusulas de seguridad en las Redes Sociales constituyen una prioridad.

D. Sebastián Muriel, Vicepresidente de Tuenti, acompañado del Responsable de Seguridad. Comparecencia de 18 de septiembre de 2013.

El compareciente en su primera intervención ante la Subcomisión abordó, entre otras, las siguientes cuestiones.

— Compañía tecnológica 100 % española. 250 personas trabajando en España, gente muy joven de los que un 65 % aproximadamente, son ingenieros y expertos en diseño.

— Llama la atención sobre la evolución desde la web a operador móvil plantee fenómenos nuevos.

— Las Redes Sociales como «herramientas técnicas de intermediación» en las que las empresas españolas compiten en desigualdad de condiciones.

— La estrategia y marco de actuación de los últimos años se basa en tres elementos. En primer lugar, autorregulación, dotando a usuarios de herramientas para reportar sobre contenidos inapropiados (Tuenti es un club privado); segundo la vinculación con las Fuerzas y Cuerpos de Seguridad del Estado funciona muy bien; tercero, la educación y prevención con información y concienciación es esencial en esta materia.

— La seguridad en las Redes Sociales, según este compareciente, en representación de Tuenti es resultado del esfuerzo compartido entre industria, administración, educadores y padres, y usuarios.

— Para Tuenti las medidas de privacidad son esenciales y a ese fin alude a las siguientes propuestas:

• No indexar datos en buscadores (por ejemplo, en Tuenti solo lo ven los asociados como amigos).

• Solo se permiten identidades reales (lo que permite eliminar muchos problemas porque, por ejemplo, más del 65 % de los perfiles delictivos eran falsos).

• Encripta toda su información, lo que no sucede en otras plataformas.

• Máximo nivel de privacidad: distinción entre contacto (para chatear) y amigo (intercambio de fotos y contenidos).

• Política de claridad y de simplificación (derecho de identificación).

• Un centro de ayuda y seguridad en la Red (incide en la propuesta de que se informe a la Sociedad para que esta entienda las Redes Sociales y los patrones de uso, desde un planteamiento de fomento de la cultura de privacidad y seguridad en internet).

• Política de colaboración con Instituciones (no hay que reinventar nada puesto que los problemas son comunes en todo el mundo, luego el planteamiento correcto para resolverlos ha de ser a nivel internacional).

• Un problema con el que tropiezan las cuestiones de seguridad en internet y en las Redes es la existencia de leyes nacionales en un mundo global y normativas que a veces son del siglo XIX o del XX para un mundo del siglo XXI.

• Los usuarios son cada vez más sofisticados y la edad cada vez es menor, luego urge una pedagogía en casa, en la escuela y para los usuarios, con asignaturas concretas que expliquen las TIC en los currículum escolares, en los ciclos más tempranos.

• Desde otro punto de vista se refiere el compareciente a la necesidad de que haya compañías españolas o, en su defecto, cada vez habrá menos tejido nacional para defender que las compañías propias sean actores en el mundo de las tecnologías, y se radiquen en España para generar riqueza en este sector; a este fin alude a que ha de haber las mismas reglas de juego para todos.

cve: BOCG-10-D-643

— En respuesta a los Sres. Diputados de la Subcomisión el compareciente se refiere a que hay nicho de negocios a medio y largo plazo en este ámbito.

— En el mismo turno de respuesta a Diputados se refiere a que debería ser un requisito que el perfil para menores fuera de máxima privacidad y que las respuestas a las denuncias se hicieran lo más brevemente posible.

— El compareciente, contestando a otro Diputado, se refiere a la conveniencia de trabajar al menos en el nivel europeo, y requerir a las empresas de fuera la correspondiente contribución vía impuestos que ayude a que mediante una combinación de talento, más inversión, más comercialización se estimule mediante normas la empresa informática europea y española.

— El compareciente reconoce a preguntas de un Diputado la dificultad de resolver la brecha entre hechos y derechos, pero sí expresa su convicción de que la legislación no debe entorpecer el entorno, si bien una Red Social requiere además de tecnología, formación y selección de actitudes.

D. Carlos Represa Estrada, representante del Centro Nacional de Seguridad Escolar. Comparecencia de 18 de septiembre de 2013.

— El CNSE, puntualiza el compareciente, no es un centro público, sino un centro que colabora con la C. A. de Castilla-La Mancha en una iniciativa de seguridad en las aulas.

— El compareciente efectúa una serie de reflexiones sobre la materia que se refieren a los siguientes aspectos, entre otros:

• La seguridad en internet esta relacionada con la educación ética.

• Quién es el responsable y de quién es el «whats up» de los menores.

• Conveniencia de un plan de acción tutorial, un Centro de Asistencia, cursos on line para profesores al alcance de cualquier CC AA, incorporar estos contenidos en el itinerario educativo.

• Registro europeo de protección de datos.

• Por qué no un observatorio sobre seguridad de menores en redes sociales.

• En respuesta a Diputados matiza que lo primero es definir el concepto de seguridad en internet, específicamente para menores y, después, atender a la territorialidad.

• Asimismo en respuesta a la pregunta de un Diputado sobre la multiplicidad de asociaciones o fundaciones en la materia responde que es cierto que nadie ha liderado la coordinación de una manera firme y falta coordinación.

• En la misma línea, precisa a título de ejemplo sobre políticas preventivas, que en alguna embajada de país UE se solicita cuando un trabajador británico va a trabajar con niños, un certificado de que ese trabajador no ha tenido problemas con niños.

• En cuanto a las Apps expresa cuán fácil es el acceso sin consecuencias, cuando debería garantizarse un acceso a través de responsable, para menores de 14 años.

D. Guillermo Cánovas Gaillemín, Presidente de Protégeles. Comparecencia de 18 de septiembre de 2013.

— El compareciente se refiere al programa de seguridad de menores en España, dependiente de la Comisión europea que abarca una línea contra contenidos inapropiados (ellos reciben sobre unas 2500 denuncias/mes, acerca de contenidos inapropiados; otra de ayuda contra el abuso («help plan» de las que España fue el primer país en crearlas); y una tercera de formación de menores en TIC (en Europa se trabaja en el análisis de las consecuencias antropomórficas que pueden acarrear las TIC, incluyendo su posible afectación de las características cerebrales positivas o no, de carácter neuronal etc., ; nuevos fenómenos como la multitarea en el ordenador que se apunta puede suponer una pérdida de tiempo de entre un 30 % a un 40 % ; afectación de las TIC a las relaciones sociales, etcétera.)

— Resulta esencial que los menores reciban formación, pues ello es básico para un enfoque razonable de la cuestión que, sostiene, debería también extenderse al entorno familiar (cuando no se trabajan en familia proliferan los desórdenes adictivos); y a los profesores (se refiere a cómo en los planes de estudio de profesorado solo a veces hay una optativa cuatrimestral sobre estas materias).

— En materia de contenidos el compareciente se muestra partidario de la regulación, entendiendo que no basta la autorregulación. Y cita en su apoyo el caso de Alemania donde se han excluido las páginas contra la prevención de anorexia.

— Se han detectado casos de ciberdelincuencia protagonizada por menores.

cve: BOCG-10-D-643

— En respuesta a un Diputado, el compareciente coincide con las sugerencias referentes al «agente encubierto» y el posible tipo de «apología de la pederastia» y, añade, la conveniencia de dotar con mas medios a las Fuerzas y Cuerpos de Seguridad del Estado.

D. Miguel Comín, Director Fundación Alia2. Comparecencia de 18 de septiembre de 2013.

— El compareciente se muestra favorable a un papel relevante por parte del Observatorio Nacional de Telecomunicaciones a la par que recalca que el ámbito normativo ha de ser de nivel europeo.

— Esta Fundación, precisa, trabaja en tres frentes: la educación (se pretende llegar a unos 8 millones de niños), tecnología (que permita un internet mas seguro), y aunar esfuerzos sectoriales para multiplicar ventajas.

— El compareciente se refiere, entre otras cuestiones, a diferentes propuestas de interés, a su juicio, en la materia, tales como:

• El recurso a una figura que sí está en otros ámbitos como terrorismo o drogas, cual es el «agente encubierto».

• No considera conveniente crear nuevas asignaturas sino una formación transversal que se inicie en la formación universitaria de los propios profesores, con incentivas al reciclaje de los profesores en estas materias.

• La adhesión a iniciativas europeas como la operada en 2007 respecto de CIRCAM para filtrar páginas de pornografía infantil, a cuyo respecto señala que debería haber normas que faciliten bloqueos de contenidos pedófilos, como sucede con el Convenio de Lanzarote del Consejo de Europa de protección de los niños contra la explotación sexual y el abuso infantil, de 25 de octubre de 2007, ratificado por el Reino de España y publicado en el BOE de 12 de noviembre de 2010.

• Considerar en el plano criminológico, la conveniencia de unos «antecedentes penales específicos» tal y como en algunos otros países, caso del Reino Unido; o tipificar la apología de la pederastia.

— En respuesta a un Diputado coincide en que las asociaciones y fundaciones compiten entre sí (incluso, señala, a veces entre privadas y públicas) y no hay una federación de asociaciones o fundaciones para la defensa del menor en las redes.

D. Marcelino Madrigal García, activista antipornografía infantil en redes y experto en seguridad y protección del menor. Comparecencia de 18 de septiembre de 2013.

— El compareciente se define como experto en TIC, con las que trabaja desde 1986, programador y desde hace unos siete años activista en la denuncia de contenidos ilícitos contra menores; amén de padre preocupado por la cuestión.

— El compareciente destaca la difícil identificación de pedófilos sin ayuda del proveedor de servicios que, en algún caso —Brasil, por ejemplo—, es responsable civil subsidiario.

— El compareciente se refiere al funcionamiento desigual de los mecanismos de denuncia de pedofilia en las redes que, a veces, parecen castigar más al mensajero que al autor. En todo caso indica la necesidad de comunicar a las empresas lo sucedido mediante, por ejemplo, un mail y lo propio sería que la empresa, vista la «denuncia» desactive la escena, y, en su caso, la borren, caso este último de la asociación «Missing kids» que, sostiene, recibe subvenciones de algún importante gobierno e incluso de algún gigante informático y que, afirma, en Estados Unidos recibe apoyo investigador del FBI u otras policías estatales, y que tiene acuerdos con algunos países (entre los que no está España), o a través de Interpol.

— En España cabe enviar un correo electrónico al CNP denunciando esta clase de páginas o contenidos.

— En su intervención el compareciente precisa que al objeto de evitar páginas de contenidos inadmisibles, como la propia pedofilia, o xenofobia o racismo, o estímulo a la anorexia y bulimia, sí se pueden hacer cosas y afirma que si bien «las empresas no tienen corazón, sí tienen bolsillo».

— Según criterio del compareciente la educación, esencial en la materia, debe ser transversal u horizontal y no una asignatura específica.

cve: BOCG-10-D-643

— En respuestas a un Diputado el compareciente se refiere al diferente nivel de regulación según distintos países y así señala que en algunos casos es una tarea de *lobby* (caso de la desaparición en Francia de páginas antisemitas que, aduce, ha obedecido a la relevante tarea del *lobby* judío), en otros casos obedece a denuncias a través de los MCS, y en otros a una rigurosa regulación, supuesto de Brasil y Colombia.

D. Jesús M.ª Sánchez Herrero, Presidente de CEAPA. Comparecencia de 25 de septiembre de 2013.

— El compareciente precisa que comparece en su condición de padre y no como experto, e inicia su intervención afirmando que podría decirse que en la actualidad: — «los hijos nacen con un ordenador bajo el brazo» y hacen un uso de las redes sociales que desconcierta a los padres por su suficiencia y versatilidad.

— Desde su condición de padre el compareciente se refiere, entre otros aspectos a lo siguiente:

• Procede partir en esta reflexión del necesario respeto a la intimidad y espacio propio de los hijos y, en paralelo, la obligación de los padres de asesorarles.

• La experiencia indica que es recomendable ubicar el ordenador en zonas comunes de la casa familiar, como una herramienta de contacto interfamiliar que facilite el mensaje de padres a hijos sobre el carácter ético del uso de las herramientas informáticas, en aspectos como la reprobación de conductas de *moving* o el respeto a la propia y ajena privacidad, así como el acercamiento a las redes desde la curiosidad y no desde el miedo.

— Cuando los hijos contacten con amigos en las redes sociales es aconsejable que sepan que no es conveniente acercarse a quienes no conocen (al igual que en la «vida real» se advierte de conductas de extrema confianza sin causa), mantener un uso celoso de la propia privacidad, incluso incorporar contraseñas difíciles de reconocer y que no las recuerde el ordenador, no dar información personal o familiar a través de la red, no copiar contenidos, no poner fotos y menos si son muy personales, y, en suma, que sean conscientes de las consecuencias de no protegerse.

— No tiene sentido, afirma el compareciente, «demonizar» las redes sociales que *per se* son asépticas, lo negativo es el mal uso de éstas.

— A preguntas de los Diputados el compareciente coincide con lo expuesto por alguno de ellos sobre la brecha digital entre padres e hijos, el exceso de materias curriculares y sobre la falta de profesorado cualificado y afirma que en su organización han tratado de crear una escuela 2.0 (CEAPA/APAS) para la formación de padres.

D. Ramón Arnó Torrades, Coordinador de la comisión de menores de la Asociación Profesional Española de Privacidad (APEP). Comparecencia de 25 de septiembre de 2013.

— El compareciente interviene en su doble condición de coordinador de la comisión de menores de APEP y abogado en ejercicio especialista en el entorno jurídico de la información, desde cuya perspectiva plantea en primer lugar la sugerencia de que la Subcomisión amplíe su objeto de estudio de las redes sociales también a los buscadores, sistemas de correo electrónico, y redes *peer to peer,* pues se ha constatado que es mayor el riesgo delictivo en estos entornos.

— De otra parte, y entre otras cuestiones, el compareciente aboga por una posible reforma de la LECRIM que si bien ya contempla en el Art. 282 la función de la policía judicial de recabar y recoger efectos y pruebas del delito, con la finalidad de acomodar las actuaciones de investigación de delitos cometidos a través de las redes sociales, sería conveniente considerar los requerimientos preventivos de bloqueo de información, de forma que la simple denuncia permita bloquear ad cautelam, toda vez que si no se hace así por el complejo procedimiento vigente, desde que se solicita el bloqueo de la información hasta que ésta llega al juzgado de guardia, puede haber desaparecido ya.

— En esta línea se sugiere también, para evitar la dificultad de contactar con prestadores de servicios extranjeros que se designe una persona en España como responsable o contacto para agilizar solicitudes cursadas por la policía judicial.

— En lo atinente al secreto de las comunicaciones, en un mero correo electrónico pueden confluir diferentes derechos: el derecho al secreto de las comunicaciones, el derecho a la protección de datos y el derecho a la intimidad, cada uno con su propia normativa sectorial, ante lo cual el compareciente indica

cve: BOCG-10-D-643

que puede haber casos de contradicciones que no solo generan inseguridad jurídica sino confusiones ya que no está específicamente regulado, aunque, señala, si existe la Circular 1/2013 de la Fiscalía en que se abordan estas complejas cuestiones. En todo caso no está definido cuándo empieza y cuándo termina el secreto y lo propio respecto de la protección de datos. Lo fundamental sería que hubiera criterios claros. A ello se añade un uso judicial restrictivo, a raíz de la Ley 25/2007 de Retención de datos de comunicaciones electrónicas, a otorgar oficios para conocer quien (dirección IP, operador, y a través de qué correo electrónico) puede haber cometido una estafa a través de internet con cantidades menores, circunstancia que de aprobarse el nuevo CP que parece pasaría a dejar de tipificar ciertas infracciones que pasarían a ser delitos menos graves, con ello podrían dejar una parte de infracciones penales sin juzgar. Lo que lleva al compareciente a plantear si no estamos ante un exceso de rigidez al considerar que para cualquier clase de solicitud de información es necesaria la correspondiente autorización judicial porque se entiende que forma parte del secreto de las comunicaciones, dándose la paradoja, indica, de que la AEPD lo solicita al operador y, al parecer, lo obtiene, pero no así la policía judicial.

— Con la finalidad de agilizar estas materias el compareciente plantea la posibilidad de especializar juzgados de instrucción para este tipo de delitos cometidos en relación con la informática.

— A destacar, precisa, que estos delitos a veces escapan de las estadísticas ante la dificultad de definirlos en los programas informáticos que permiten calificar los delitos a la vez que la policía judicial realiza el atestado.

— En cuanto a menores precisa que lo mismo que se enseña a los niños cómo abordar la seguridad vial en el colegio debería hacerse respecto del uso de las tecnologías de comunicación electrónica, y, a este fin, propone que en el tramo entre 6 y 12 años se introduzca una asignatura sobre este asunto que podría partir de lo ya regulado en la Ley del menor de 1996, con enfoques claramente preventivos (cómo establecer contraseña segura, cómo proteger la propiedad intelectual, qué es delito, cómo detectar un entorno peligroso) y formativos a través de profesores y funcionarios de las FF y CC de SS, mediante un sistema grato y amigable (por ejemplo, videojuegos, o juegos de rol etc.)

— Los padres, sostiene el compareciente, no tienen herramientas suficientes para proteger a los hijos en internet, aunque sí responsabilidad civil solidaria por la de los hijos sometidos a patria potestad, derivada de ilícitos.

— En respuesta a las preguntas de Diputados el compareciente señala que la jurisprudencia sobre acceso a direcciones IP es variada pues se accede desde distintas vías jurisdiccionales, civil en materia de derecho al honor, o penal.

— También a preguntas de los Diputados señala que en la LOPD los datos sobre menores no están especialmente protegidos, aunque sí en el CP.

— Cuestión relevante relacionada con la normativa en materia de protección de datos es el ejercicio de la patria potestad en internet.

— En respuesta a un Diputado, con quien expresa su coincidencia, aduce que quizás estamos a una propensión «buenista» a la minusvaloración del problema penal en menores, cuando debería analizarse con rigor el denominado «ciberdelito» y considerar que se ha dado una herramienta poderosísima a los hijos (hay estadísticas que dicen que solo un 20 % de las infracciones penales entre menores se denuncian) y cree que se esta escapando de las manos de padres, educadores y responsables públicos.

D.ª Myriam Fernández Nevado, Vicepresidenta de la Asociación GSIA (Grupo de Sociología de la infancia y la adolescencia). Comparecencia de 25 de septiembre de 2013.

— En representación de un grupo de profesionales de GSIA vinculados a la protección de los derechos de los niños bajo la transversalidad de la CDN de Naciones Unidas (20/11/1989, ratificada por España y publicada en el BOE de 31/12/1990).

— La compareciente expresa, entre otras, las siguientes consideraciones: la necesidad de romper los «clichés» antitecnológicos, no es cuestión de considerar internet como un peligro y elevar la edad de acceso a las TIC, sino de enseñar a los niños a gestionar emociones e información.

— Las redes sociales son para los niños más que un canal de comunicación un medio para relacionarse con iguales y para desarrollar su ocio (Art. 17 CDN: derecho al juego). Se debe buscar como objetivo la autodeterminación digital del usuario, que éste aprenda a autoprotegerse y a habitar en ese entorno singular y evolutivo.

— Una aproximación a esta materia puede hacerse desde las tres pes de la CDN: Provisión (los estudios demuestran que los niños son los usuarios mas activos de las redes sociales); prevención

cve: BOCG-10-D-643

(determinación de riesgo, legislación adecuada de ámbito nacional e internacional, y específicamente un CP y una LECRM al día, y educación en un uso responsable); y participación —a la que la compareciente añade protagonismo responsable, puesto que el promedio de perfiles de un niño suele estar por encima de tres en la misma red, mientras que las niñas suelen diversificar en diferentes redes, lo que conduce a preguntarse sobre si hay permiso familiar para ello.

— La protección de la privacidad entendida como un derecho individual (versión norteamericana) sino como un derecho fundamental (versión europea) requiere coordinar las normas civiles, penales, procesales y las nacionales, supranacionales e internacionales. Si bien, precisa, a preguntas de los Diputados, que en la visión americana del suministro de datos por ley federal los operadores están obligados a informar sobre el tráfico de datos a requerimiento policial o judicial, mientras que según el Art. 15 del Convenio Europeo sobre Ciberdelincuencia (Convenio de Budapest, ratificado por España el 23 de noviembre de 2001 y publicado en el «BOE» el 17 de septiembre de 2010) solo procede en caso de requerimiento judicial. La compareciente aboga por modificaciones en la LECRIM, y por la figura del «agente encubierto» en materia de delitos informáticos, mas el Delegado de Protección de datos.

D.ª Ana Marzo Portera, representante de la organización Padres 2.0. Comparecencia de 25 de septiembre de 2013.

— Representa a la organización Padres.2 y es abogada en ejercicio. Experta en contenidos electrónicos, protección de datos, propiedad intelectual y ciberseguridad.

— La compareciente señala que su principal objetivo es un tratamiento integral de la prevención de riesgos derivados de las TIC especialmente en menores y, por ello, colaboran con Tuenti y con la unidad de investigación de adicciones tecnológicas y juego de la Facultad de Psicología de la Universidad de Valencia.

— La compareciente se refiere, entre otros aspectos, a la rápida obsolescencia de la normativa sobre TIC debido a la rápida evolución de estas técnicas que da lugar a que, cuando una ley es aprobada para hacer frente a una determinada situación tecnológica, ésta ya ha avanzado hacia un nuevo futuro.

— En la propuesta de Programa comunitario plurianual sobre la protección de la infancia en el uso de internet y en la Propuesta de Resolución del Parlamento europeo sobre la protección de los niños en el mundo digital de 2012 se considera que los menores necesitan ayuda para utilizar internet de forma razonable, responsable y segura, lo que apunta a la formación y a la coordinación de sectores implicados. A ello responde la organización de la compareciente con la necesidad de alfabetización en los medios de comunicación digitales para educadores y padres. A este respecto se refiere a la preocupación, manifestada en sede parlamentaria con ocasión de una comparecencia del Director de la AEPD, sobre que los datos personales que tratan colegios e institutos (singularmente los sanitarios) parecen estar al margen de las garantías sobre ficheros informatizados; refiriéndose, a este respecto a un Plan de la AEPD en 2006 que resultó demoledor en la constatación de la falta de cumplimiento de la normativa de protección de datos y privacidad en centros escolares que, añade la compareciente, cabe presumir que aún no se ha mejorado suficientemente, lo que, sostiene, constituye además mal ejemplo para los educandos. En el turno de preguntas de Diputados se expresa por parte de alguno de ellos que los niveles de seguridad han mejorado en centros educativos.

— La compareciente se refiere a la extendida practica entre menores del sexteo *(sexting,* delito contra la integridad moral tipificado actualmente en el 173 CP, con independencia de cual sea el medio para su comisión) y a la generalizada inconsciencia penal de los menores cuando, sin saberlo, incurren en estas conductas que encajarían en el citado tipo penal.

— En materia de derecho a la intimidad se esta manejando conceptos del siglo XX (LOPCDHI LO 1/1982) cuando estamos en el siglo XXI. No obstante una Opinión de la AEPD (la 5/2009) conceptúa como responsable de ficheros a las personas físicas en el transcurso de actividades estrictamente personales y domésticas, lo que nos sitúa ante la paradoja de que un menor cuando configura su perfil social y lo mantiene abierto a usuarios de la red, o permite la indexación de datos, según la AEPD supone que se activan las responsabilidades inherentes a un responsable de fichero de datos. Y, desde Padres.2, se plantean y plantean ante la subcomisión si era la intención de la norma, cuando la primera regulación de este asunto excluía los datos de uso estrictamente personal. Otra aparente paradoja del sistema es la existencia de sentencias judiciales con sanciones civiles a los padres o responsables por conductas ilícitas de menores, cuando estamos en la era en que los nativos digitales son ellos y no —generalmente— los padres. Además los padres se interponen demandas por el uso o divulgación de imágenes u otros datos

cve: BOCG-10-D-643

por menores, a veces desde los propios centros educativos quienes por falta de formación o información no alertan de este mal uso.

— La compareciente señala que la información a centros y profesores hasta ahora ha sido básicamente privada y plantea la conveniencia de que las instituciones publicas tomen cartas en el asunto puesto que estamos ante una realidad legislativa civil obsoleta, una doctrina administrativa en la aplicación de la normativa de privacidad discrecional, e inexistencia de un Plan general que recoja protocolos de actuación y una efectiva coordinación intersectorial.

— Respecto del PLO del CP la compareciente alerta sobre el proyectado artículo 183 bis del PLO que podría contener un concepto jurídico indeterminado; a la par que se refiere como tipos vinculados a estas materias a los artículos 197.4 bis y 270.

— A juicio de la compareciente sí serían convenientes algunos cambios en la LOPD como, por ejemplo la inclusión en el artículo 11 de la LOPD a las FF y CC de SS en el elenco de a quienes se pueden ceder datos sin consentimiento, caso de la existencia de una relación contractual, o a Juzgados y Tribunales o Ministerio Fiscal o Tribunal de Cuentas; toda vez que se constatan cesiones al margen de la normativa, asunto especialmente particular en el ámbito de la videovigilancia y cesiones por empresas de seguridad privada. A este respecto es fundamental la doctrina de la AEPD que, señala, ha tratado de interpretar que si la LOFF Y CC DE SS establece que el tratamiento se puede llevar a cabo, pues la cesión está permitida. Estos factores se unen a cierto crecimiento de las sanciones a personas físicas en la AEPD por responsabilidad paterna ante lo que los menores puedan publicar en redes sociales (por ejemplo publicar un video en Youtube un niño, en el que salen otros niños, sin autorización de los padres, ha sido sancionado por la AEPD), sobre lo que también se debería reflexionar porque son mas bien asuntos civiles (Ley orgánica de protección civil de 1982) y que, no obstante, se están tramitando por vía administrativa.

— La compareciente se refiere a la desventaja competitiva europea en esta materia, porque Europa no puede transferir libremente datos a terceros, según la Directiva Europea de 2003, y otros países sí lo hacen.

— Concluye la compareciente, a preguntas de los Diputados sobre la necesidad de información transversal; de especialización de los juzgados; especialización en la protección educativa y en la propiedad intelectual.

D. José Luis Piñar Mañas, Director de la Cátedra Google del CEU. Comparecencia de 12 de febrero de 2014.

Comparece en su condición de titular de la cátedra Google y, especialmente como catedrático de Derecho Administrativo y exdirector de la AEPD entre 2002 y 2007, refiriéndose, de manera especial, a las siguientes cuestiones:

— Respecto de las medidas de seguridad para los menores en las redes sociales, materia sobre la que dirigió una investigación nacional e internacional entre 2009/2010, hay algunas conclusiones bien ilustrativas como que solo en torno a un 18 % / 20 % se pide DNI u otra identificación a los menores para hacerse usuarios de una red social (datos sobre encuesta citada con un universo de unos 3.000 niños de 14 a 16 años de colegios de toda España, puesto que los de edades inferiores necesitarían en todo caso consentimiento paterno). Consultados estos niños un 97 % eran conscientes de que la información que colgaban era accesible para otros usuarios, mientras que un 80 % contestaba que para ellos era muy importante el nivel de privacidad ; en torno a un 80 % afirmaban tener contactos en la red con menores de 14 años; y sobre un 70 % nunca había ejercido peticiones de cancelación; mientras que alrededor de un 80 % no tenía percepción de amenazas a su privacidad a través de las redes, aunque hasta un 45 % sí afirmaba conocer alguien que si había tenido experiencias contrarias a su privacidad, tal y como se recoge en la «Opinión 5/2009 UE», sobre Redes sociales en línea, del Grupo del Art. 29 (constituido por autoridades de protección de datos de todos los países UE).

— Relevancia de una legislación clara y con determinación de obligaciones para los diferentes agentes en internet.

— La legislación española pasa por ser una de las más garantistas en materia de protección de datos.

— Como recomendación se refiere a la autorregulación que tenga carácter vinculante.

— La gran cuestión en esta materia es la aplicación extraterritorial o no de las normas en una materia que no tiene fronteras, de ahí la relevancia del futuro Reglamento europeo que tropieza con graves

cve: BOCG-10-D-643

problemas, como el denominado «one stop shop» que supone que la autoridad competente para conocer una denuncia será la del país donde figure la matriz de la empresa.

— El compareciente plantea la necesidad de contar con una norma internacional en la materia.

— En respuesta a observaciones de un Diputado expresa que, aun reconociendo la dificultad para trabar un buen acuerdo internacional sobre la materia, eso no quita para instar la necesidad imperiosa de alcanzar un acuerdo internacional sobre ella.

— Así, si el modelo español de protección de datos ha sido ejemplo a imitar por numerosos países en América Latina, República Checa, Croacia etc., España tiene una posición de relativo liderazgo en defensa de la protección de datos que podría servir como pauta para una política internacional de protección de datos.

— En cuanto a la responsabilidad paterna, también ante observaciones de algún Sr. Diputado, aduce que no se puede meter el Derecho sancionador en las relaciones privadas paterno filiales, o regular desde el Derecho Público relaciones exclusivamente privadas.

— El compareciente se refiere a un principio capital cual es el del interés superior del menor.

— Asimismo ante observaciones de Diputados el compareciente se expresa por la existencia de normas concretas, claras y por la responsabilidad de los responsables de tratamientos de datos, así como sobre la falsa gratuidad de los servicios que facilita cierres sin contraprestación, y sin que se garantice el principio de portabilidad de los datos recogido en el proyecto de Reglamento europeo.

— También en relación con reflexiones de algún Sr. Diputado sobre el derecho al olvido, precisa el compareciente que, como se ha hecho en Italia, lo procedente sería exigir a la fuente de información que adopte las medidas necesarias para que esa información no pueda ser indexada o identificada por los buscadores que, por otra parte, hay miles.

D. Juan M.ª Martínez Otero, miembro del Consejo Asesor de iCmedia. Comparecencia de 12 de febrero de 2014.

iCmedia es una federación de asociaciones de consumidores y usuarios de los medios que aúna a 17 asociaciones, además el Sr. Otero es Profesor de Derecho de la Comunicación en el CEU San Pablo de Valencia.

El compareciente, entre otros temas, señala lo siguiente:

Las categorías jurídicas clásicas a veces no sirven para estas materias o para minimizar riesgos como los siguientes:

— El riesgo de conexión permanente a las redes sociales: para cuya prevención es esencial la alfabetización digital a niños/jóvenes, familias, poderes públicos, con la incorporación de contenidos curriculares de formación digital.

— El riesgo, no muy extendido, pero de extrema gravedad cuando se produce, de daños contra la libertad sexual de los menores (el *grooming* ya está incorporado al CP), si bien cabría otras medidas preventivas como escalonar la edad de uso y el numero de conocidos/amigos del usuario menor en la red social (por ejemplo 12 años / 20 amigos, y así escalonadamente, etc.) lo que reduciría el riesgo.

— El *ciberbullying* o acoso escolar a través de las redes sociales, que también esta tipificado, si bien quizás se podría considerar establecer penas de inhabilitación para tener un perfil en una red social; incluso estableciendo cursos para recuperar puntos.

— El sexteo *(sexting)* consistente en enviar imágenes de contenido sexual, producidas en casa, a distintos compañeros y que en la proyectada reforma del CP ya se incluye como delito si bien podría bastar una sanción civil o castigar al que graba y es primer emisor.

— Actualizar la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, contemplando el consentimiento tácito en internet.

— Los riesgos de carácter publicitario: sería de interés limitar anuncios de apuestas, pornografía, «contactos», esoterismo, etcétera, cuando se trata de usuarios menores, estableciendo prohibiciones o cautelas en redes donde están los menores.

— Los riesgos de contenidos audiovisuales que deberían tener en cuenta cuando el usuario es menor, si el prestador de servicios lo sabe. A este respecto coincide con algún Sr. Diputado sobre la diferenciación entre menores por tramos de edad si bien la propia Constitución en el Art. 20.4 habla de «protección de la

cve: BOCG-10-D-643

infancia y la juventud» y determinadas limitaciones planteadas podrían estar en línea con las medidas más o menos extensas de protección de menores.

— Cuestión importante es la responsabilidad paterna pues cabe una culpa in vigilando ya que el menor está bajo su responsabilidad en internet, y, a este fin habrá que explorar formulas desde establecer filtros por los padres, a cursos de formación, o acreditar que el padre ha puesto medidas filtro, de modo que si un padre puede acreditarlo, ello pudiera rebajar su responsabilidad económica proporcionalmente.

— En lo atinente a la respuesta normativa ante estas nuevas y cambiantes circunstancias, en contestación a un Diputado, expresa su coincidencia con el compareciente Piñar sobre la preferencia de normas sencillas y claras con principios básicos y que permitan la interpretación judicial.

D. Juan Carlos Ortiz Pradilla, Profesor de Derecho Procesal de la Universidad de Castilla-La Mancha. Comparecencia de 12 de febrero de 2014.

El compareciente centra su intervención en qué ocurre cuando falla la privacidad en internet y cuando se cometen delitos en internet: qué medidas preventivas y de investigación pueden adoptarse. A cuyo fin aborda cuatro líneas básicas con sus correspondientes propuestas:

— La delimitación del delito grave: partiendo de la base de que internet más que un medio de comunicación es «un lugar de comunicación» donde la gente vive, se conoce, e incluso delinque. La delimitación del delito grave con base en la pena, ha dado paso a otros criterios como la trascendencia social o repercusión social y, mas aún, el TC en Sentencia de 2006 vino a determinar como criterio delimitador para hablar de delito grave a la hora de permitir la interceptación de las comunicaciones, la utilización de las nuevas tecnologías en la comisión del hecho delictivo, para facilitar la impunidad de los delincuentes, aunque no alcanzara determinada pena. La ley 25/2007 transpuso la Directiva de conservación de datos electrónicos cuyo artículo 1 dispone que solo se cederán datos conservados por operadores a los agentes facultados cuando se trate de la investigación de delitos graves tipificados en el CP o leyes penales especiales y los tribunales (algunos, matiza en respuesta a un Sr. Diputado, y de forma ciertamente excepcional) han aplicado de forma literal este artículo y solo lo consideran aplicable cuando se trata de delitos graves en los términos del artículo 33 CP, esto es con pena privativa de libertad con mas de cinco años, lo que excluiría múltiples infracciones penales cuyo tipo común está castigado por debajo de esta pena, pero que son muy comunes en internet, caso del fishing, injurias, calumnias, estafas informáticas etc., ello conduce a que se haya propuesto por la Fiscalía General del Estado una interpretación, bien del propio Art. 1 de la citada ley o del concepto de delito grave del vigente CP, mediante la utilización de agravantes.

— En cuanto a los responsables del tratamiento de datos son mayoritariamente empresas privadas que generalmente tienen su domicilio social fuera de España de modo que es de difícil aplicación la normativa española cuando disponen de toda la información posible sobre los usuarios, luego sería de altísimo interés ver cómo estas empresas pueden quedar sujetas a la normativa europea (quizás en el futuro Reglamento europeo) y repensar las formas de colaboración actual entre empresas y FF y CC SS Estado y órganos jurisdiccionales, para evitar tener que recurrir necesariamente a comisiones rogatorias a través de Estados Unidos para solicitar datos de empresas radicadas en un estado norteamericano. Se da, además, la paradoja, indica, de que hemos obligado a empresas a conservar datos y también a que los dejen de conservar, esto debería estudiarse rigurosamente porque es cierto que para algunas empresas la conservación es muy costosa, pero para las que se dedican a «minería de datos» es su fuente de negocio.

— En tercer lugar sobre la obtención de pruebas electrónicas nos encontramos, sostiene el compareciente, con que el cruce de estos datos puede arrojar mucha información e incluso perfiles, pero también es cierto que la prueba electrónica es volátil, fugaz y alterable y puede ser hasta ubicua, lo que desplaza la cuestión de la territorialidad a la accesibilidad y a la internacionalización, a cuyo fin resulta fundamental el Convenio del Consejo de Europa sobre Ciberdelincuencia de 2001, o Convenio de Budapest ratificado por España y publicado en el BOE de 17 de septiembre de 2010, que prevé la obtención transfronteriza de la prueba electrónica, y uno de cuyos artículos que se piensa reformar- el 32- se refiere a la obtención de información en fuentes abiertas. Además, a preguntas de un Diputado, responde el compareciente que el es partidario de legitimar medidas de investigación, pero legitimarlas por ley.

cve: BOCG-10-D-643

— En lo referente a los actos delictivos a través de las redes sociales: amenazas, acosos, etcétera, que, con frecuencia, parten de la suplantación de la personalidad que, como tal delito, no existe, sería de interés la posible evaluación y definición de un tipo penal autónomo dentro de la figura de la coacción. A este respecto, contestando a un Diputado, indica que muchas de las conductas delictivas ya están tipificadas en el CP y, en algunos casos, ha sido la Jurisprudencia la que, de una forma lógica ha interpretado el concepto de documento o medio de pago.

D.ª María Concepción Torres Díaz, Profesora de Derecho Constitucional de la Universidad de Alicante. Comparecencia de 12 de febrero de 2014.

La compareciente parte del punto de vista del Derecho Constitucional para referirse, entre otras, a las siguientes cuestiones:

— Necesidad de ponderar seguridad y derechos, singularmente la privacidad, entendida en sentido amplio (como protección de datos, intimidad y derechos conexos) tal y como se hace en las conclusiones del Abogado General del Tribunal de Justicia de la UE sobre la Directiva 24/2006 y su compatibilidad con la Carta Europea de Derechos fundamentales (Arts. 7 y 8 derecho a la vida e identidad privada).

— Necesidad de partir en cualquier regulación de derechos fundamentales de la normativa constitucional prevista en el Art. 53 CE, en cuanto a requisitos formales y materiales y a su protección reforzada mediante el Amparo constitucional, y con la debida adecuación de las medidas limitativas a los principios de idoneidad, proporcionalidad y necesariedad.

— «Refundamentalidad» de los derechos fundamentales tradicionales (libertad de expresión, información, derecho a la intimidad) y nuevos derechos de cuarta generación como pudieran ser el derecho de acceso universal a internet; a la integridad y confidencialidad de los sistemas tecnológicos; derecho al olvido digital (sobre el que la compareciente se refiere a su carácter no general y a la necesaria aplicación del principio de proporcionalidad y ponderación con otros derechos como el de información o la libertad de expresión); derecho a la tutela en la protección de datos; derecho al anonimato situacional (que puede verse seriamente afectado por la geolocalización que permite establecer perfiles conductuales): esto es, derechos nuevos, bien por su ámbito de ejercicio que es virtual, o concreciones tecnológicas de derechos clásicos que vienen a constituir nuevos derechos autónomos como el derecho a la intimidad en la protección de datos; o la extensión de la intimidad y el derecho al secreto de la correspondencia al ordenador personal o cualquier otro dispositivo electrónico; o el derecho a la integridad y confidencialidad de los sistemas tecnológicos y de información, muy conectado con el derecho a la tutela informativa; protección de datos y secreto de las comunicaciones; a cuyo respecto la compareciente cita ST Constitucional alemán de 27/2/2008 en la que se declara inconstitucional una reforma de la ley de servicios de inteligencia de Renania del Norte Westfalia que permitía el uso de «troyanos» para acceder a ordenadores de personas sospechosas, y se menciona un nuevo derecho a la integridad y confidencialidad de los sistemas tecnológicos y de información .

D. Iker Merodio, Doctor en Periodismo. Comparecencia de 19 de febrero de 2014.

— A destacar las siguientes observaciones, entre otras, de esta comparecencia del periodista Merodio con columnas diarias en dos periódicos y participante en tertulias de radio sobre internet y nuevas tecnologías: el número de usuarios de redes sociales es superior al de conductores y, sin embargo, esta desregulado, o mas bien «incontrolado», cuando mas de la mitad de los españoles utilizan internet a diario, y en el tramo de jóvenes mas del 97 %.

— El anonimato (no el pseudónimo) es una de las grandes perversiones de internet y resulta fundamental para la comisión de delitos.

— Internet facilita también el intrusismo y propicia la dictadura del titular.

— En respuesta a observaciones de los Diputados expresa que más que nueva legislación en materia de seguridad lo esencial es que la actual se cumpla.

— En relación a si se puede pagar por obtener mayor seguridad en internet responde que sí, y un ejemplo de ello son, afirma, los llamados servicios Premium.

cve: BOCG-10-D-643

D. Ángel Mario Tascón Ruiz, experto en uso del lenguaje en internet y deontología periodística. Comparecencia de 19 de febrero de 2014.

— Autor de un libro, junto con Yolanda Quintana, sobre ciberactivismo, destaca en su intervención la modificación del ecosistema mediático, desde los noventa (prensa, radio y TV) a la actualidad (prensa radio, tv, usuarios, redes sociales, móviles, webs etc.,); asimismo destaca como algunas cuestiones procedentes de la «ética *hacker*» se han extendido a la sociedad.

— El compareciente aborda lo que denomina algunas tesis sobre lo que está sucediendo en el mundo de las redes sociales:

• En primer lugar, la tecnología ha estado siempre relacionada con el poder y el control de recursos. Estamos en un momento como fue la revolución industrial en el que aparece un mundo emergente tecnológico con gente que sabe manejar los recursos frente a quienes no saben.

• Han aparecido otras herramientas y, a veces, se legisla sin conocerlas. El uso de estas nuevas herramientas se ha democratizado (por ejemplo, hoy en día no hace falta una concesión administrativa gubernamental para poder transmitir por radio).

• Las herramientas son cada vez más sencillas, velocísimas y omnipresentes. Estas herramientas crean una brecha entre un sistema moribundo y uno neonato que no acaban de sincronizarse. A este fin, la formación es esencial.

• Se ha producido un desplazamiento de las élites (políticos, medios de comunicación, sindicatos tradicionales).

• La sociedad ha hecho propios muchos de los principios correspondientes en origen a los hacker y a los expertos informáticos.

• Cualquier persona puede convertirse en activista a través de las nuevas tecnología y movilizar de manera muy rápida a toda la sociedad «activismo del clic». Habrá en los próximos años batallas que se van a librar por la defensa de los derechos civiles en la red.

— En muchos casos, matiza en respuesta a un Diputado, bastaría con cumplir la legislación vigente.

— El mismo tipo de delito existe en el mundo analógico y en el digital.

— En el caso de Google habría de analizarse la cuestión impositiva.

D. Ícaro Moyano Díaz, Periodista experto en comunicación empresarial. Comparecencia de 19 de febrero de 2014.

El compareciente, entre otras cuestiones, se refiere a los siguientes aspectos:

— En cuanto a la construcción de identidad tradicionalmente se hacía mediante referencias familiares, y oficialmente con el DNI y el pasaporte, en lo que atañe al entorno de confianza es el escenario de los afectos el que nos define; mientras que en el caso de internet, el 80 % de nuestra información lo incorporamos nosotros mismos, lo que significa que cabe manipulación iconográfica.

— Hay dos enfoques diferentes en la consideración de estas materias: la óptica del derecho europeo *(Opt in):* no se puede hacer nada sin autorización del usuario; y la óptica de Estados Unidos basada en el *Opt out.* La consecuencia es que resulta más fácil la generación de empleo y la versatilidad tecnológica en el caso anglosajón, norteamericano, que en el europeo.

— Otra cuestión a considerar es el fenómeno de la verificación de identidad que tiene mucho más que ver con la acción comercial que con el concepto de seguridad en internet que es bastante débil.

— Una posible solución frente a estas circunstancias es la utilización del hardware en seguridad, así, indica el compareciente, determinado gigante de la informática mundial, investiga en anillos.

— En todo caso hay una clara vulnerabilidad en internet y los hackers pueden hacer a veces lo que quieren a la par que se está derrumbando la ética *hacker.*

— Estas circunstancias han dado lugar a un retorno al anonimato basado en el recelo informático y a la aparición de foros como «Secret» en California.

— El compareciente coincide, en respuesta a un diputado, con los demás comparecientes en esta sesión e indica que más que legislar, lo importante es cumplir con la legislación vigente.

— El problema de la legislación europea en materia de empresas tecnológicas es que no se han atrevido a plantarle cara a estas macroempresas, alguna de las cuales paga impuestos en Irlanda, luego

cve: BOCG-10-D-643

no es que no cumplan la legislación europea, sino que conocen perfectamente aquellos lugares más beneficiosos en la aplicación de legislación europea.

— También respecto a lo indicado por algún diputado, se refiere al altísimo nivel de competitividad e investigación tecnológica de algunas empresas en Estados Unidos, por ejemplo, alguna de las cuales contrata cada año seis mil o siete mil programadores indios porque en su cultura se favorece el talento y la creación de empresas. En Europa, y concretamente en España, nos falta educación sobre el valor de las cosas y una pedagogía sobre este asunto en la escuela, la familia y los medios de comunicación social.

— Coincide este compareciente con otros en que efectivamente parece que va a haber internet de dos velocidades.

D. Faustino Jiménez Carracedo, CEO de Arsys. Comparecencia de 6 de marzo de 2014.

El compareciente indica que es Director de Arsys, una empresa que trabaja en paternariado con una empresa alemana sobre industria básica de internet y que gestionan sobre 100 millones de correos electrónicos al día.

— El compareciente expresa que la intimidad en internet no existe; Por otro lado, en materia de denuncias aduce que la inmensa mayoría de los problemas informáticos no están denunciados.

— Indica el Sr. Jiménez que es conveniente regular los derechos y también los delitos a través de internet.

— La legislación en España es muy proteccionista para el usuario y muy inconveniente para las empresas cuando la industria básica de internet es esencial para el desarrollo futuro y Europa carece de industria de internet básica.

— El compareciente se refiere al Libro blanco de las telecomunicaciones en el que se hace especial hincapié en el fomento y la optimización de la sociedad de la información.

— En respuesta a los Diputados indica que es esencial actuar con pragmatismo para afrontar los problemas de las redes sociales y que Europa, que es poco pragmática, tenga una industria tecnológica.

D. Juan Osaba Arenas, Director General de MASSCOM. Comparecencia de 6 de marzo de 2014.

— El compareciente expresa su coincidencia con lo manifestado por quienes comparecen en la misma sesión con él y añade un matiz cual es la necesidad de eliminar las barreras que impiden crear empresas. Se refiere también a conceptos empresariales muy americanos como por ejemplo «el Business angel» o inversores que entran en las Universidades para aportar dinero ante nuevos proyectos. Esto en España no existe y a veces ni siquiera los bancos están por colaborar.

— El compareciente indica que tampoco todo vale, porque si bien los adultos no tienen problema en el mundo de las redes sociales, señala, a título de ejemplo, que si en la vida cotidiana para comprar tabaco le preguntan al cliente si tiene 18 años, en las Apps no hay una que inquiera si el uso es para menores.

— Indica el Sr. Osaba que por primera vez en la historia los nativos digitales son los hijos y los que tienen dificultades para acceso o trabajo en la red los padres. Esto plantea un nuevo paradigma y lleva a considerar que también la formación de la población adulta es esencial.

— El compareciente plantea la posibilidad de que haya una segmentación de las Apps por edades y una simplificación de las reglas de acceso.

— Por último se refiere a la conveniencia de incorporar una asignatura a la ESO sobre estas materias para formación de los niños sobre la seguridad en la red y crear observatorios con integración de profesores, alumnos, padres, Fuerzas y Cuerpos de Seguridad que establezcan normas o límites estrictos y sobre todo, enseñen a mantener la privacidad y la intimidad como un medio para proteger a los más vulnerables.

— En su respuesta a un diputado matiza que la mentalidad americana es cooperativa mientras que aquí somos muy individualistas.

— Quizá debería contemplarse una zona más restringida, una especie de portal que permitiera trabajar de otro modo.

cve: BOCG-10-D-643

D. Jesús Encinar Rodríguez, Fundador de Idealista. Comparecencia de 6 de marzo de 2014.

— El compareciente expresa entre otras cosas que Idealista.com es una empresa con unos 300 empleados que dan servicio en Italia, España y Portugal. El Sr. Encinar indica que España es uno de los lugares donde la complejidad legislativa más dificulta montar una empresa de internet, a título de ejemplo expresa que cuando se lee que el fundador de tal empresa empezó en un garaje, él piensa: — Si yo hubiera empezado en un garaje hubiera venido un inspector de la seguridad social y me hubiera cerrado la empresa.

— En materia de impuestos cabe decir otro tanto porque si hay mega empresas que no pagan impuestos, podría decirse que Idealista paga más impuestos que algunas mega-empresas juntas.

— Conforme a lo indicado su petición sería que se regule lo menos posible y se suprima la regulación que supone impedimentos para que haya más empresas en España y más innovación tecnológica.

— El apoyo económico parte de la filosofía de que alguien da dinero porque espera ganar. La fórmula consiste en que si se pierde se descuenta lo invertido de la plusvalía.

— Insiste el compareciente en la dificultad de obtener una subvención o un *modus operandi* empresarial que no se vuelva contra el impulsor de la empresa.

— Se refiere también al micromecenazgo (*crowdfunding)* supuesto que debería ser favorecido por la legislación y que sin embargo tropieza con enormes dificultades.

— Paradójicamente, donde existe desregulación es en el sector financiero que es precisamente donde debería regularse el apoyo a las empresas emergentes.

— Tampoco las universidades constituyen focos empresariales porque existe una mentalidad de «cadena de favores» que dificulta apoyar a los innovadores y a las mentalidades con criterios empresariales.

D. Alfonso Carrascosa Marco, Fundación Legalitas. Comparecencia de 6 de marzo de 2014.

— Interviene en su condición de Presidente de Legalitas, compañía que, afirma, conoce bien los problemas ciudadanos. Esta empresa que nació hace quince años, cuenta con 250 abogados por toda España para en torno a trescientos mil clientes individuales y ocho millones de clientes de colectivos.

— El compareciente, entre otros, plantea dos problemas vinculados a la materia objeto de la subcomisión: el primero de ellos, el robo de identidad o usurpación de identidad, el delito que más ha crecido y crece en el mundo; en España, afirma, más de cuatro millones de personas han sido afectadas por robo de datos personales.

— El segundo problema que está creciendo es el relativo a la nube puesto que se trata de la prestación transnacional de estos servicios lo que dificulta extraordinariamente el ejercicio de derechos que en España tenemos reconocidos pero que al tratarse de empresas fuera del ámbito de la UE son de difícil realización, dando lugar a un fenómeno cual es que desde el aparato de la justicia se tienda a minimizar la gravedad de las conductas en las que no se evidencia un contacto físico y más cuando existe gran distancia entre agresor y víctima como sucede en los delitos cometidos por internet.

— Otra cuestión en el plano jurídico en relación con las redes en internet son las amenazas o coacciones.

— Otro tema que plantea es el de los problemas de jurisdicción que necesariamente requieren la cooperación internacional o la investigación policial transnacional.

— Por último, el compareciente se refiere también al control parental respecto de los menores.

— En relación con todo esto desde la Fundación Legalitas se sugieren, entre otras, algunas medidas cautelares como:

• Crear un protocolo para los casos de violencia escolar.

• Determinar un procedimiento por el que se pueda solicitar el borrado definitivo e inmediato de las fotos de menores en internet a solicitud de padres o tutores sin que exista una causa penal iniciada.

• Sistema de ayuda psicológica a menores maltratados o violentados.

• Despenalizar ciertas conductas estableciendo como eximente la acción de los padres para controlar los accesos a internet de sus hijos menores de edad.

• Medidas cautelares regulando la facultad del Juez de guardia o Instructor para acordar medidas de protección al menor frente a publicaciones no deseadas que difamen a los menores (por ejemplo, orden de borrado inmediato y definitivo previa custodia judicial de la prueba, o de la típica foto en red social publicada por venganza de expareja despechada, etcétera.

cve: BOCG-10-D-643

• Termina su intervención indicando que los niños menores son los que menos denuncian cuando la realidad, según un estudio de la Comisión europea, el 47 % ha sufrido acoso.

— En respuesta a Diputados el compareciente indica que es menester recurrir a medios internacionales para hechos internacionales.

D. Jorge Campanillas Ciaurriz, abogado especializado en Derecho Tecnológico. Comparecencia de 6 de marzo de 2014.

El compareciente, abogado ejerciente, pertenece a la Asociación *«Derecho en red»,* en su comparecencia plantea las siguientes cuestiones, entre otras:

— En punto al anonimato, seudónimos o suplantación de identidad en las redes indica que hace falta una modificación de la normativa sobre protección de pseudónimos.

— Respecto de la búsqueda de IP los jueces interpretan que solo ha de controlarse en caso de delitos graves, pero esto debería estudiarse.

— El compareciente se muestra a favor de regular en el futuro Código Penal la suplantación de identidad.

— Asimismo, se refiere a la conveniencia de regular un verdadero derecho fundamental a la protección de datos.

— En contestación a un Diputado respecto de la propiedad intelectual en internet precisa que la propia internet está sometida a propiedad intelectual y que, según su criterio, se habría de poner énfasis en la autoría y no en los agregadores.

D. Pablo Fernández Burgueño, Abogado especializado en Propiedad Intelectual, Protección de datos y nuevas tecnologías. Comparecencia de 6 de marzo de 2014.

— El compareciente Pablo FB usuario habitual de las redes sociales inicia su intervención con referencia a los *bitcoins.* A continuación se refiere al derecho al olvido que, según él, no se puede aplicar y a los criptocontratos que generan normativas de ejecución automática.

— Según el compareciente las leyes nacionales son ineficaces fuera de las fronteras en un mundo como es el digital en el que todo es transnacional.

— Aconseja el compareciente la participación de España en los lugares de creación de las normas, normas privadas de eficiencia internacional.

— Propone no que se hagan más leyes o más severas en España sino que se cuente con normativa real, eficaz y eficiente en el mundo, que España participe en esos Congresos donde están los prestadores de servicios en la determinación de normas internacionales. El compareciente reitera la conveniencia de hacer las normas con los dueños de internet, los prestadores de servicios.

— Asimismo, se refiere a que la normativa de 1982 (Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen) está desfasada. También es menester poner al día la Ley de propiedad intelectual, la Ley Orgánica de Protección de datos y la Ley de venta a distancia que ha quedado claramente desfasada.

— Asimismo, en respuesta a un Diputado manifiesta el compareciente que si se usa con lucro internet debería pagarse por ello, mientras que el uso libre sin ánimo de lucro habría de estar permitido.

— En cuanto a menores y también en respuesta a varios Diputados, resultaría esencial saber si una persona es mayor de edad e incorporar un botón de denuncia en las redes sociales (tal y como la Guardia Civil tiene un programa para móviles): — ¿por qué no crear un plug-in para el navegador por ejemplo internet Explorer que permita cuando se ve algo ilícito en internet simplemente pulsar y que se registre la página y se envía a la Guardia Civil, grupo de delitos telemáticos, de modo que se pudiera generar una acción inmediata?

— Por último, también en respuesta a Diputados habría que actualizar la formación en tecnologías del personal de la oficina judicial para evitar situaciones absurdas. Los propios jueces deberían tener un conocimiento informático en una sociedad en la que a veces incluso los medios de prueba dependen de la informática.

cve: BOCG-10-D-643

D. Alejandro Touriño Pena, Despacho de abogados Ecija. Comparecencia de 6 de marzo de 2014.

— El compareciente es socio de un despacho de abogados focalizado en las nuevas tecnologías y, entre otras cuestiones, inicia su intervención señalando que internet crea problemas pero también es un campo excelente de comunicación y de negocio y oportunidades. Según el criterio de este compareciente muchas de las normas no creadas para internet son perfectamente útiles y aplicables, porque la sobrerregulación, afirma, es errónea, a su juicio.

— Dos tipos de problemas «de camino»: los mismos problemas que se cometen en la calle se cometen en internet, pero nos encontramos con una norma que permite a determinados operadores que la identificación de un usuario no se pueda lograr más allá de los supuestos en los que nos encontramos con delitos graves.

— Otro de los problemas que se podría denominar «de destino» es la habitualidad de la suplantación de identidad en internet.

— Por último, hay también otro problema cual es, el ejercicio de los derechos de la personalidad en internet.

— El compareciente, a instancia de los Diputados, precisa que es mejor legislar principios que no una legislación muy exhaustiva y que quede pronto desfasada.

— Añade también en contestación a Diputados, que si el legislador no regula acabarán haciéndolo los operadores.

D. Jesús Alloza, Consejero delegado de COONIC. Comparecencia de 2 de abril de 2014.

— Este compareciente se refiere en su intervención fundamentalmente al cambio de paradigma de la comunicación y a la reputación on line de las marcas aludiendo, entre otras circunstancias, a: la fragmentación de audiencias, la democratización de los usuarios, la comunicación bidireccional y la grandísima proliferación de marcas.

— Los rasgos de este nuevo paradigma serían: la mayor exposición crítica, solo un rumor puede generar graves crisis de ahí la relevancia de la reputación on line, la tendencia a dar mayor importancia a los directores de comunicación; en suma la conveniencia de crear un protocolo de actuación en relación con las crisis de reputación.

— En respuestas a un Diputado se refiere a la protección del consumidor en internet porque vivimos un momento de intoxicación por exceso de información.

— Asimismo, en contestación a un Diputado el compareciente habla del «anonimato responsable» porque los usuarios avanzados pueden entrar y utilizar cualquier mecanismo a través del cual nadie se entere por medio de que IP se va a entrar. A este respecto, resalta el compareciente, que pareciera que has de cometer un delito para que el Juez pida la dirección IP.

— En respuesta a un Diputado manifiesta que la gratuidad no puede existir y no puede estar dominando el mercado de internet. El modelo de negocio existe desde que se utilizan contenidos en beneficio propio.

D.ª Carlota Navarrete Barreiro, Coalición de creadores e Industrias de contenidos. Comparecencia de 2 de abril de 2014.

— La compareciente lleva a cabo una primera parte expositiva en la que, entre otras cuestiones, se refiere a la perspectiva del menor, muy importante para una empresa de contenidos. Desde las industrias culturales, afirma, valoran muy positivamente las medidas para la protección del menor.

— Algunos datos llamativos que expone la compareciente son: que el 84 % de los contenidos en España son piratas (ello supone menos de 27.000 empleos y falta de ingresos vía IRPF e IVA) el valor de lo pirateado superó los 16.000 millones de euros en 2013.

— El 30 % de los menores utiliza internet y ha facilitado su número de teléfono en alguna ocasión; mientras que el 54 % de los menores no ha recibido información alguna sobre normas básicas de seguridad en internet. Se produce una clara vulneración de los derechos de propiedad intelectual a través de internet.

— Reitera lo dicho en contestación a Diputados sobre la necesidad de que cualquier trabajo tenga una remuneración porque a veces en internet se tiene la falsa percepción de que todo está puesto a disposición de los usuarios.

— Se muestra partidaria, en contestación a un Diputado, del valor de campañas estatales para divulgar unas reglas de uso adecuado en internet, en materia de propiedad intelectual.

— La coalición a la que representa se ha manifestado por la creación de una fiscalía especializada en propiedad intelectual.

cve: BOCG-10-D-643

D. Víctor Domingo Prieto, Presidente de la Asociación de Internautas. Comparecencia de 2 de abril de 2014.

— Coincide con otros comparecientes en que estamos asistiendo a una nueva era digital que redefine todos nuestros conceptos e incluso nuestra manera de vivir, razón por la cual considera que la intervención del legislador es muy importante, como así expresa con relación al Proyecto de Ley de propiedad intelectual o el Proyecto de Ley del Código Penal objeto de debate parlamentario en la fecha de la comparecencia. En relación con propiedad intelectual aduce que, a su juicio, no se puede hacer pagar al contribuyente por copia privada; en relación con la denominada «tasa Google» ellos entienden que los medios de comunicación social deberían de pagar a los agregadores.

— Por último se refiere al *copyleft* (cesión de derechos) que el proyecto de ley de propiedad intelectual no recoge puesto que solo se refiere al *copyright.*

— Con respecto al Código Penal expresa su preocupación por la «criminalización del enlace» pero el enlace, precisa, por sí mismo no es un ilícito, lo que es ilícito son los contenidos a los que apunta; la Ley de la sociedad de la información de 2012 dice que los responsables de contenidos son los autores de los mismos o los que los albergan en un sitio pero no los que enlazan, criminalizar el enlace puede generar una inseguridad jurídica importante para la industria, las compañías y el propio usuario.

— En cuanto a la seguridad en internet, el acoso, la suplantación de identidades, la intromisión, el fraude y la protección de menores: su asociación lleva haciendo campaña de seguridad on line desde hace tiempo porque entienden que educación y formación son esenciales a estos efectos, si bien, a este respecto, hay una notoria brecha entre generaciones, porque la generación más joven vive en la «cultura del clic» mientras que los adultos tienen una especie de complejo de inferioridad en el manejo de las nuevas tecnologías.

— Otro punto es la propuesta relativa a la creación de juzgados especializados en el mundo digital. Ya hay fiscalías especializadas pero los jueces, precisa, han de entrar en la sociedad de la información.

— El compareciente en contestación a un Diputado indica que según su criterio quien debe decir lo que es apto o no es un Juez, más que una Comisión.

— También, en contestación a un Diputado, matiza que el acceso a la banda ancha debería ser un derecho y que en España se han implementado medios electrónicos de gran utilidad en internet como el DNI electrónico.

D. Miguel Pérez Subías, Presidente de la Asociación de usuarios de internet. Comparecencia de 2 de abril de 2014.

— Se refiere entre otras cuestiones a la interoperabilidad de las redes sociales, la intimidad, menores, la seguridad de la identidad digital, cuestiones todas ellas sobre las que, señala, el legislador puede hacer mucho.

— El compareciente expresa que echa en falta en las redes sociales una distinción de niveles en aras de mayor intimidad.

— Indica que a los menores les falta claramente información y llevan a cabo acciones cuyo alcance desconocen.

— Expresa que la media de permanencia en una pantalla de ordenador o un smart u otro dispositivo electrónico es de 7 horas, lo que genera un claro problema de «sobreexposición» digital.

— Otra cuestión que plantea es si alguien podría ponerle un «sobre» a los correos electrónicos.

— La gestión de la identidad y la seguridad, los temas biométricos constituyen también otro elemento a considerar.

— ¿Dónde está el verdadero gobierno de internet?: ¿Quién lo controla?

— No hay que resistirse a intervenir sino hacerlo con conocimiento.

— En contestación a un Diputado responde que la interoperabilidad es técnicamente sencilla y es la mejor defensa del usuario.

— En cuanto al anonimato según su opinión el derecho al anónimo se puede dar tanto en la vida digital como fuera de ella.

cve: BOCG-10-D-643

D. Ricard Martínez Martínez, Presidente de Asociación Profesional Española de Privacidad-APEP. Comparecencia de 2 de abril de 2014.

— En su comparecencia aborda, entre otros asuntos, la incapacidad para ejercer un control en el mundo digital.

— Coincide con el compareciente anterior en que hay un exceso de exhibición de los menores en las redes sociales y en la necesidad de que los menores, los niños, aprendan a usar internet.

— La Agencia Española de Protección de Datos acordó con Tuenti tener un modelo de control a posteriori y con Facebook se estableció aplicar la edad legal en España a los 14 años.

— El compareciente ante las observaciones de Diputados indica que el solicitaría que las conclusiones de esta Subcomisión se eleven al Gobierno porque en estos momentos se entra en la fase de negociación en materia del Reglamento de protección de datos de la Unión Europea y Directiva específica que regulará el tratamiento de datos en el ámbito policial y que están en tramitación en el marco europeo, razón por la cual, para ilustrar la posición española sería relevante poner en valor lo que se ha dicho ante la Subcomisión.

— A este fin y teniendo en cuenta la paradoja del anonimato y la protección de la identidad en internet, el compareciente se refiere a la función tuitiva del Estado, como ya se hizo con ocasión de la Ley 25/2007 que generó un debate sobre si la IP era un dato personal o no, concluyéndose que era parte del protocolo de las comunicaciones; pues bien, precisa el compareciente, aplíquese a este respecto la regulación del secreto a las comunicaciones que decida un Juez, aunque se retengan con carácter preventivo los datos.

— Resulta fundamental también a este respecto la denominada «platform for privacy preferences» cuya idea básica era impulsar el desarrollo de tecnologías capaces de negociar en automático la privacidad, esto es impulsar un software con un perfil de privacidad definido, materia que sería de indudable interés.

— El compareciente también en respuestas a Diputados se refiere a la portabilidad de los datos, al derecho al olvido y a la *privacy by design* que están en el borrador de Reglamento europeo y que resultan de interés. La etiqueta «yo soy confiable para los menores» sería de gran utilidad y también la filosofía «yo ofrezco mercado si ustedes me dan seguridad».

D. Luis Alberto Calvo Campos, Director de Sistemas de Seguridad de Indra. Comparecencia de 2 de abril de 2014.

— En su intervención parte de la necesidad de proteger a las personas más vulnerables y en la protección de los derechos fundamentales en el mundo de las redes sociales en el que éstas son asépticas y dependen del uso que se las dé.

— El compareciente define la red social como un servicio que alguien presta a través de internet que permite relacionarnos con terceros y que normalmente nos obligan a que hagamos nuestro perfil.

— Además de ello, las redes crean ciber vínculos que buscan información para hacer mil usos de ellas y es cierto que banalizan los riesgos.

— Indica el compareciente que faltaría un control de registros de usuarios que deberían estar asociados a un DNI.

— Una cuestión que se plantea es que los perfiles sean correctos aunque el sistema se presta a la utilización de múltiples perfiles.

— Existe tecnología respecto al derecho al olvido y también para la importación de datos.

— Indica el compareciente que debería regularse el derecho de acceso y de rectificación a través de internet porque si hay tecnología para manejar el «Big data», saber dónde estás (localización), también para preguntar quién ha cedido mis datos. Asimismo, indica que las redes deberían estar etiquetadas según su nivel de seguridad.

— En respuesta a Diputados expresa que hay tecnología que permite hallar la identificación biométrica en terminales, después está en cómo lo implemento en el iphone y el precio de consumo en mercado y más aún que pasa con esa huella, o mi cara, o mi iris, a dónde va a ir. Sin duda, se podría legislar sobre esta cuestión, y el tema es que no hay garantía de hasta dónde va a llegar esa información.

— Hay medidas sobre protección poniendo difíciles las cosas a quienes intentan vulnerar la seguridad.

— En respuestas a otro Diputado expresa que hay tecnología para borrar (derecho de rectificación) pero que no es fácil y además el derecho al olvido no implica borrar todo lo que existe.

cve: BOCG-10-D-643

D. Jorge Flores Fernández, Director de Pantallas Amigas. Comparecencia de 2 de abril de 2014.

— El objetivo de su asociación, según expresa en el inicio de su comparecencia es prevenir los problemas de menores en internet y en ese sentido ejemplifica con la primera guía de ciberbulliing en 2006 o un video en Youtube sobre sexteo *(sexting)* etcétera. En suma, prestación de iniciativas para prevenir los riesgos de internet para los jóvenes.

— Concretamente, en materia de prevención de menores ellos son partidarios de estimular el concepto de ciudadanía digital, potenciar la cultura de la privacidad, cultura de autoprotección, sistemas de control parental con software de apoyo, proporcionar conocimiento suficiente a menores y adultos sobre la legalidad o ilegalidad de algunas acciones (guía e-legales presentada en la Asamblea de Madrid); difundir medios de las herramientas en internet, pensamiento crítico y autocrítico, gestión de las emociones, incluir estas habilidades en la enseñanza escolar, crear indicadores objetivos de riesgo, primar actuaciones empresariales que favorezcan la información, en suma enseñar alertas sobre cómo afrontar los problemas y autoprotección.

— En respuesta a un Diputado sobre la posibilidad de un «botón mágico» para denunciar acosos, etc., indica que ello es bastante complicado porque se puede pedir socorro pero cuestión distinta es la operatividad.

— Respecto de la autorregulación, también en respuesta a un Diputado, indica que es importante fijar indicadores y que los menores sean conscientes de lo que se puede y no se puede hacer en cada red social que, por otra parte, son diversas en su aproximación en estas cuestiones.

— En contestación a una Diputada, precisa que hay que intentar la aplicación de la norma aunque sea en este complejo mundo de intereses internacionales. Hay dos presiones distintas, los poderes económicos, la demanda de los usuarios y lo que estamos o no dispuestos a pagar por la privacidad.

— En cuanto al anonimato, indica en respuesta a otro Diputado, hay que distinguir atendiendo al interés superior del menor, circunstancia en la que resulta conveniente identificar a las personas que interactúan preferentemente con ellos o en espacios para menores, fuera de eso va a ser imposible, y aun así hay que tener en cuenta que hay casos de usurpación de identidad.

— En respuesta a una Diputada sobre la edad en que se debe empezar a controlar estas cuestiones responde que a los 8 años empiezan actualmente con internet y es desde ahí desde donde sería menester una tutorización aunque parezca muy prematuro, tanto desde casa como desde la escuela.

D. Ramón Miralles López, Coordinador de auditorías y seguridad de la Información en Autoridad Catalana de Protección de Datos. Comparecencia de 2 de abril de 2014.

— Inicia su intervención refiriéndose a las causas que favorecen los riesgos de amenazas y que son básicamente tres: La falta de mecanismos eficaces y sencillos de identificación electrónica; la falta de transparencia de la mayoría de los operadores presentes en la red; y cierta falta de información en la materia y de los mecanismos de protección (especialmente en el muy mayoritario sector de los «huérfanos digitales»).

— Para afrontar estos problemas propone entre otras las siguientes acciones: acciones educativas en las aulas a partir de los seis años según recomiendan las instituciones europeas; Fomentar el apoyo entre iguales en los centros escolares; promover que la industria evolucione en encontrar mecanismos sencillos y seguros de autentificación en la red; control de acceso a determinados sitios para menores (igual que sucede con el alcohol, el tabaco, etcétera); promover el uso de códigos de autorregulación; la adopción de buenas prácticas por la industria; transparencia y más medios para etiquetar (como sucede con la trazabilidad de los alimentos para el etiquetado de lugares para los usuarios); articular sistemas de queja o denuncia sencillos y contextuales; catalogación de las diferentes quejas conforme a estándares, por ejemplo, protección de datos, acoso sexual, vejaciones, xenofobia, maltrato psicológico, etcétera.

— En respuestas a un Diputado, se refiere a las experiencias de mediación y a un proyecto piloto en centros escolares en Cataluña en el que han intervenido los propios alumnos en casos de acoso escolar *(ciberbullying),* (que ha empezado en febrero de 2014) y que en el tiempo de su funcionamiento ha resultado muy positivo.

— En cuanto a otro Diputado matiza que efectivamente cada vez será más un valor competitivo ofrecer prestaciones con mayor privacidad.

cve: BOCG-10-D-643

— En materia de autorregulación responde a un Diputado que entiende que la positiva es la autorregulación pactada o dirigida por el poder público.

— En lo atinente a la edad de los niños él cree que ya desde los seis años conviene explicar con cuentos (por ejemplo, caperucita roja cibernética) qué es la suplantación de identidad.

— Sugiere, en respuestas a un Diputado, incorporar al concepto de autoprotección el de auto responsabilidad.

— En cuanto a la identificación y autenticación, responde a otro Diputado, como se trata de aportar seguridad pero requiere sencillez y se debe hacer compatible la navegación anónima con la identidad digital.

D. José Manuel Tourné Alegre, Director General de la Federación para la Defensa de la Propiedad Intelectual, FAP. Comparecencia de 2 de abril de 2014.

— Según expresa el objetivo de su Federación es que internet sea un espacio seguro, un «barrio limpio» donde los integrantes de esta Federación (productores cinematográficos, audiovisuales, distribuidores, etc.) puedan realizar su trabajo y llevarlo adelante, porque la propiedad intelectual es generadora de riqueza y empleo.

— Expresa que a la Federación que representa les preocupa también y mucho los menores y cuando van a editar una película o estrenarla solicitan la correspondiente calificación, y por eso les preocupa el contenido que se cuela a través de páginas de descarga de películas o incluso casas de apuestas u otro tipo de espacios de internet no recomendable para menores.

— El artículo 10 del la Ley de Servicios de la Sociedad de la información que dispone que haya una identificación del titular de la página que tiene contenidos para el Publico no se cumple. Ha habido más de 230 denuncias y solo 2 expediente sancionadores. Las sanciones deben ser para el que busca organizar un negocio pirateando, no para los usuarios a quienes se debe educar e informar sobre este tipo de conductas inadecuadas.

— El compareciente en contestación a intervenciones de los Diputados coincide en que se han captado muy bien los temas y se refiere a unas pautas dadas en su momento solicitando a la Sala de gobierno del TS un juzgado especial que se designó en la Audiencia Nacional e instruyó un sumario especial sobre falsificación de películas y venta, que, de algún modo, se vio desbordado por la evolución del uso de esos instrumentos. El ejemplo sirve para que no se inicie la persecución de ilícitos contra la propiedad intelectual persiguiendo al usuario. Cita como ejemplo la política de Sarkozy de persecución de la piratería y los beneficiarios de la piratería cultural y, asimismo, ejemplifica con la política de tráfico en la que el sistema de sanciones ha servido para establecer un nuevo paradigma.

— En materia de edad de menores él conoce a niños de 3 años que ya están con una revista como si estuvieran llevando a cabo una utilización digital.

— Por último, coincide en la conveniencia de que, en vez de sancionar al usuario, se sancione a la empresa que piratea.

D. David Maeztu Lacalle, experto en seguridad y protección del menor, Propiedad Intelectual y Regulación del entorno laboral en el marco de las Redes Sociales. Comparecencia de 2 de abril de 2014.

— Indica que la mejora de la situación a veces pasa por la modificación de algún precepto como sucedió el 28 de marzo del 2014 con una modificación sobre consumidores y usuarios.

— El compareciente sugiere, como algo sencillo, obligar a ciertas empresas que se destinan al mercado español a cumplir con la normativa de arbitraje en España. En lo tocante al acceso a determinados términos y condiciones de las redes sociales habla de la página web www.terminosycondiciones.es que desde 2014 lleva casi un millar de servicios en internet vigilando las condiciones de las compañías y de los usuarios, muy concretamente los cambios en las más importantes redes sociales que pueden afectar a sus usuarios.

— Llama la atención el compareciente sobre actividades que no tienen publicidad en cuyo caso, plantea por qué se les debe aplicar el mismo régimen que a una empresa. Asimismo, alude a los conceptos jurídicos indeterminados y a la indefinición de determinados servicios.

cve: BOCG-10-D-643

— En lo atinente a la usurpación de identidad en las redes sociales hay un problema de tipicidad porque la conducta no está perfectamente descrita en el Código Penal; hasta ahora los Tribunales lo manejaban mediante la «falsedad en documento mercantil», pero quizás fuera interesante introducir un artículo 401 bis nuevo en el Código Penal porque resolvería muchos problemas de internet.

— Si es importante el CP, el compareciente indica que aún es más relevante la actualización del procedimiento penal en la LECRIM porque no hay marco legal adecuado para las pruebas o evidencias digitales.

— La realidad es que se está funcionando mediante jurisprudencia en estas cuestiones procesales penales.

— El Tribunal de justicia de la Unión Europea (TJUE) ha dicho que los datos asociados a nuestras conexiones se están recopilando queramos o no y se ha planteado una cuestión prejudicial en la que el Abogado General informa negativamente porque esto vulnera la Carta Europea de Derechos humanos. Esto habría de tenerse en cuenta a efectos de la normativa española que, en todo caso, haría mejor en ser una regulación por principios, que no una regulación exhaustiva y que quedara desfasada prematuramente.

— En respuestas a un Diputado indica que el ámbito de la Directiva Europea de Protección de Datos se localiza en el lugar en que se tratan los datos y en consecuencia, los mecanismos de identificación por capas.

— También en contestación a otro Diputado alega que si alguien no cumple la legislación española que no venga a radicarse en España o a no cumplir la normativa española.

D. Francisco Fernández Marugán, Adjunto Primero a la Defensora del Pueblo. Comparecencia de 22 de abril de 2014.

— El compareciente inicia su intervención ante la Subcomisión con una referencia a la materia objeto de la Subcomisión que, afirma, trata con derechos primarios de la gente en un momento en que estos tienen, señala, bastantes cortapisas, como se desprende de la información con que cuentan en el excelente observatorio que es el Defensor del Pueblo.

— El Sr. Fernández Marugán alude al desarrollo tecnológico y a las mutaciones cualitativas que ha provocado (de televisión a internet y redes sociales) todo lo cual ha cambiado la forma de percibir el mundo y el modo de hacer política, en tanto acerca lo lejano y convierte en próximo lo exótico.

— El Adjunto Primero al Defensor del Pueblo aporta un libro de la colección Informes, Estudios y Documentos que recoge un estudio del Defensor elaborado con una encuesta amplísima a jóvenes sobre estas materias.

— A continuación, entre otras cuestiones y partiendo de la afirmación de que: «para educar a un niño hace falta toda la tribu», plantea una serie de interrogantes sobre: ¿cómo perciben los jóvenes internet; son conscientes de los riesgos que existen; saben qué hacer si se sienten agredidos, sirve internet para sus estudios?; preguntas todas ellas que se plantearon a los 3000 encuestados en la publicación del año 2010 pero, como ejemplo de la rápida mutabilidad de las tecnologías electrónicas, en dicha encuesta elaborada en el año 2009 no se recogía las relaciones a través de telefonía móvil, porque por aquel entonces, no existía de manera generalizada.

— En relación con el acceso de los jóvenes a las tecnologías indica al compareciente que está mucho más extendido en los núcleos urbanos que en los rurales; de la encuesta citada se infiere también que el uso que hacen los jóvenes de las redes lo realizan desde sus propias habitaciones; y un tercio manifiesta tener sistemas de control; si bien, en lo atinente al control este se basa más en el tiempo de uso que en los contenidos.

— Por parte del compareciente se hace hincapié en la necesidad de líneas de protección, en primer lugar en la familia y después los educadores, destacando las relevancias de los centros educativos y también la conveniencia de no eludir las obligaciones del poder.

— Como elementos de utilidad en la reflexión sobre esta materia, el compareciente se refiere, entre otros, a la brecha generacional, la necesidad de identificar los riesgos para el usuario mediante guías más sencillas, restaurar los códigos de conducta como mecanismos de autorregulación, disponer de algún sistema de alerta y la enseñanza y aprendizaje de este tipo de cuestiones.

cve: BOCG-10-D-643

— El compareciente constata que desde el análisis del DP se infiere que los jóvenes no cuentan con información suficiente para valorar la privacidad y desconocen los riesgos de no preservar su privacidad; asimismo, hay que llevar a cabo una pedagogía sobre uso adecuado de redes sociales, y, sería conveniente, añade, controlar la edad de acceso.

— Debería prohibirse el anonimato y por último, reflexionar sobre la conveniencia de algún sistema de alerta temprano, con una denuncia rápida y arbitrar un procedimiento de colaboración con las Fuerzas de Seguridad.

— En respuesta a intervenciones de Sres. Diputados sobre el papel de los proveedores de servicios en la red indica que el predominio de estos es el predominio del mercado sobre la política y estos asuntos solo pueden resolverse en el ámbito regional internacional.

— Asimismo, en respuesta a los parlamentarios, se refiere a que la forma de actuar para incidir en políticas de menores, etcétera, es hacerlo sobre el regulador, tratando de llegar a acuerdos puesto que el servidor de una red debería tener también interés en evitar las controversias.

D. José Luis Rodríguez Álvarez, Director de la Agencia Española de Protección de Datos. Comparecencia de 22 de abril de 2014.

— En su intervención, entre otras materias, también aborda la evolución tecnológica que supone grandes ventajas pero también tensiones notorias para la vida privada. A título de ejemplo se refiere al papel de los drones, *smarts, big data, weareable technologies,* geolocalización, etcétera, todo lo cual incide en el ámbito de los derechos (por ejemplo, el derecho al olvido es una extensión en el tiempo del derecho a la intimidad, y como tal no es absoluto y acotado a las normas legales de publicidad, no es pues un derecho absoluto sino que tiene que convivir con el resto de los derechos como la libertad de expresión, el derecho de información; y en la colisión entre varios derechos, siempre prevalecerá, como dijo el Tribunal Constitucional, la libertad de expresión e información, luego el derecho al olvido queda acotado a aquellas informaciones de carácter personal que no tienen interés público o relevancia pública).

— Lo evidente es que en esta cuestión hay tres responsables: autor, difusor y distribuidor, cada cual con su propia responsabilidad, por más que por algún distribuidor se produzca un rechazo contumaz a asumir su responsabilidad, por entender que no está sometida ni al Derecho español ni al europeo. Esta es la causa del planteamiento de la cuestión prejudicial por la Audiencia Nacional ante la Unión Europea que plantea tres cuestiones: si se aplica o no el Derecho europeo a la empresa responsable de los motores de búsqueda, si se aplica un tratamiento de datos, y si el afectado que alega su derecho al olvido ha de dirigirse al editor o al buscador.

— Internet, afirma, afecta especialmente en cuanto nuevo paradigma de la comunicación, a los derechos contemplados en el artículo 18 de la Constitución española y además, configura una «biografía digital» que empieza a ser más relevante que la biografía real.

— El compareciente también se refiere al carácter global o mundial de internet y a la resistencia de algunas corporaciones a someterse al Derecho europeo, lo que ejemplifica con referencias a diferentes compañías como F***, con sede europea en Irlanda debido a las ventajas que supone la radicación en ese país; M*** que reconoce su sometimiento al derecho europeo con sede en Luxemburgo; G*** que lleva varios años en un estado de no reconocimiento del Derecho europeo y que en 2012 unificaron sus políticas de privacidad, algunos de cuyos productos están bajo esa política de privacidad unificada y respecto de los que hay algunos casos en los que se han solicitado (por los directores de las Agencias Europeas de Protección de datos) cambios.

— En todo caso, resalta el compareciente, la gravísima amenaza para la intimidad que supone la relación de datos como modelo de negocio, aparentemente gratuito, de algunas empresas, que en realidad se financian con cargo a publicidad y obtienen lo que se denomina «behaviour advertising» materia sobre la que no hay accesibilidad advertida.

— En 2009 la normativa europea instituyó el *Opt out* por *Opt in* o situación de consentimiento previo que encontró dificultades.

— Otra cuestión que plantea el compareciente es la de los problemas que generan otras tecnologías alternativas caso de algunas modalidades de la huella digital que pueden requerir en el futuro nuevas normas.

cve: BOCG-10-D-643

— En cualquier caso el nuevo Reglamento Europeo sobre esta cuestión será muy relevante para abordar estos problemas y habría de partir de la base de que las Corporaciones que actúen en Europa se han de someter al Derecho Europeo.

— En respuesta a observaciones y preguntas de los Diputados de la Subcomisión sobre el alcance del borrado de información se refiere a la indexación de la página y a las posibilidades técnicas para el borrado a través de un robot XT.

— Asimismo, en respuesta a otro Diputado indica el compareciente que sería necesario replantear el principio de publicidad y así el BOE ya trabaja en un escalonamiento de lo público de modo que en los tablones edictales se puede acceder a la información, es pública, pero lleva un protocolo de no indexación.

— En otro orden de cosas y también en contestación a los Sres. Diputados, si bien afirma que hay una base legal muy débil, si una persona es de relevancia pública, no se concedería el derecho al olvido.

D.ª Elvira Tejada de la Fuente, Fiscal Delegada para la lucha contra la delincuencia informática. Coordinadora Nacional de Criminalidad Informática. Comparecencia de 22 de abril de 2014.

— La compareciente inicia su intervención con una referencia a las competencias legales del Ministerio Fiscal: la defensa de la legalidad, de los derechos de todos los ciudadanos y del interés general, a cuyo fin, precisa son principios de actuación: la legalidad, la imparcialidad, la unidad de actuación y la dependencia jerárquica.

— El área de especialización en criminalidad informática del Ministerio Fiscal español se integra con una unidad central radicada en Madrid y una red de fiscales de criminalidad informática distribuidos por todas las provincias españolas.

— La compareciente se refiere, entre otras materias, a los problemas de la investigación, persecución y sanción de la cibercriminalidad:

• Los ciberdelitos no son una categoría concreta de delitos sino una forma de cometer delitos muy distintos y de diferente naturaleza cuyo común denominador es la especial vulnerabilidad de los ciudadanos ante este hecho criminológico, en plataformas preparadas para fomentar la conectividad (el usuario no solo consume contenidos sino que los aporta), plataformas no preparadas para proteger suficientemente la privacidad. Como resultado, un importante monto de información personal de millones de ciudadanos se encuentra almacenada en grandes repositorios sin las debidas garantías de confidencialidad.

• Otra característica es la proyección territorial de las conductas en varios sitios a la vez simultánea o sucesivamente, en diferentes países y con diferente legislación. Solución: armonización normativa. Normas mínimas básicas comunes para todos los Estados.

• La evolución vertiginosa de las tecnologías que plantea situaciones nuevas en cuestión de meses, mientras que el legislador tiene «tempus» más lentos.

— La lucha contra la criminalidad informática descansa sobre la legislación penal sustantiva y mediante la adaptación de la normativa procesal siempre con respeto a los derechos y libertades de los ciudadanos.

— Tipos ilícitos más comunes en las redes sociales: defraudación y estafas en general; actividad ilícita relacionada con la pornografía infantil, acoso a menores en las redes sociales (que crece de una manera llamativa) con finalidades de carácter sexual; difusión de mensajes que incitan al odio, la violencia y la discriminación respecto a los diferentes; utilización de las redes sociales con finalidad terrorista (hay varias sentencias de la Audiencia Nacional por hechos relacionados con este tipo de actividades); y una categoría de delitos relacionados con las redes sociales, son aquellos relativos a atentados a la intimidad, libertad, honor, integridad moral que se canalizan dentro de delitos de amenazas o delitos contra la integridad moral o descubrimiento y revelación de secretos.

— Para evitar que se produzcan impunidades ante hechos criminológicos la compareciente se refiere a la conveniencia de reflexionar sobre la tipificación de la suplantación de identidad en la red, fenómeno muy frecuente, que si bien en función de los resultados de la acción se pueden derivar a amenazas, coacciones, injurias, etcétera, en otras no es posible hacerlo por la inaplicación con carácter extensivo de la normativa penal. Por ello en la Memoria de la Fiscalía de 2011 ya se solicitaba la tipificación de este tipo que en Francia por ejemplo sí está tipificado, así como, en Costa Rica, Perú y Argentina.

cve: BOCG-10-D-643

— La compareciente se refiere en materia de investigación criminológica a la Convención de Budapest que apuesta por la armonización normativa en materia sustantiva y procesal penal.

— Asimismo, destaca la carencia de herramientas procesales (conservación de evidencias electrónicas tanto de tráfico como de contenidos, interceptación de datos de tráfico en tiempo real, e incluso la medida prevista en el articulo 16 de la Convención de Budapest de que por parte de una autoridad —no necesariamente judicial, pues puede ser policial o fiscal— se ordene a cualquier persona física o jurídica que tenga datos informáticos almacenados la conservación de estos datos durante 90 días para poder acceder a ellos previa autorización judicial en el curso de concretas investigaciones tal y como contempla la legislación portuguesa.

— Otra sugerencia se refiere a la posibilidad de hacer algunas adaptaciones en la figura del «agente encubierto» (técnica policial de investigación prevista en el Art. 282 bis de la LECRIM) si bien con referencia al mundo físico y para determinadas actividades delictivas vinculadas a la delincuencia organizada para poder utilizarlo con ocasión de investigaciones tecnológicas, pero que no permitiría su uso, por ejemplo, en el acoso particular a un menor en la red. Lo procedente sería, conservando los parámetros esenciales de la figura (autorización judicial o fiscal dando cuenta inmediata al juez, control de uso basado en la necesidad y proporcionalidad), que se pudiera utilizar también para la investigación en tecnologías de la información y la comunicación.

— En respuesta a un Sr. Diputado señala que los medios personales de la Fiscalía especializada y los medios informáticos son muy deficientes y no hay posibilidad de modificarlos por la crisis económica, si bien los fiscales jefes provinciales están reforzando los servicios.

— Asimismo, en respuestas a otro Diputado, se refiere a los cursos de especialización que, con todas las dificultades, siguen preparando.

— En respuesta a un Diputado sobre la suplantación de identidad matiza que se refiere al uso de la identidad de otra persona que realmente existe de forma deliberada, conduciendo a error efectivo y que, salvo que se traduzca en un daño moral o injuria o amenaza o coacción no es un comportamiento típico.

— La compareciente también en respuesta a un Sr. Diputado alude a la Directiva Europea de agosto de 2013 sobre ataques a sistemas informáticos, figura nueva que no está incorporada al Proyecto de Reforma del Código Penal si bien, parece que hay un anteproyecto de transposición para septiembre de 2015. A este respecto se podría aprovechar la tramitación del Código Penal para la incorporación del tipo referente a daños informáticos.

— En respuesta a otro Diputado precisa que la conservación de datos no tiene por qué poner en peligro ni la intimidad, ni la protección de datos ni el secreto de las comunicaciones, porque, si la conservación ciertamente es estricta, la disponibilidad de datos solo puede hacerse mediante autorización judicial. La clave está en encontrar un punto en el que sin lesionar derechos ciudadanos seamos más eficaces, afirma.

— Termina su intervención ejemplificando la actuación de un posible agente encubierto en esta materia que no es equivalente a la navegación libre por la web y debería autorizarse, en su caso, para investigaciones concretas.

— Por último, y también respecto de las reflexiones de un Diputado, se refiere a la colaboración institucional con el ámbito empresarial, por ejemplo protocolo de colaboración con el CCI (Centro de Coordinación Interbancaria y su grupo de seguridad informática) para facilitar intercambio de información sobre tendencias criminales en líneas generales, envío de denuncias a la fiscalía con la documentación completa y formación.

D. Manel Prat Peláez, Director General de los Mossos d'Esquadra. Comparecencia de 22 de abril de 2014.

El compareciente alude al importante papel de la policía de la Generalitat en la prevención de delitos tecnológicos y se refiere entre otros, a los siguientes asuntos en relación con estas materias

— Necesidad de incrementar la lucha contra la ciberdelincuencia.
— Intensificar la protección de colectivos más vulnerables como los menores.
— Incrementar los vínculos con empresas, personas jurídicas, etcétera.
— Planteamiento internacional en asuntos de ciber delincuencia.
— Necesidad de conocimiento tecnológico actualizado.
— Dificultades de la investigación por la internacionalización de estas conductas.

cve: BOCG-10-D-643

— Incrementar medidas de seguridad y aportaciones tecnológicas en empresas.
— Los afectados no están obligados a facilitar las direcciones IP.
— No hay normas que obliguen a los operadores a cumplir nuestra legislación.
— Agilizar las comisiones rogatorias para la cooperación internacional.
— Reforzar mecanismos de cooperación creando una comisión científica en materia de ciber delincuencia.
— Estudiar la posibilidad de un registro estatal de agresores sexuales.
— Facilitar la investigación de la difusión sin consentimiento de imágenes contra el honor en internet.
— En matización respecto de un Diputado se refiere a las grandes dificultades en materia de prevención por la resistencia de las empresas que a veces ni siquiera dan respuesta a requerimientos judiciales sobre listas de contactos. Es más, precisa, en algún caso, se ha notificado al interesado que la Policía ha preguntado sobre él.
— El compareciente también en respuesta a un Diputado reclama mayor coordinación entre diferentes cuerpos policiales y finaliza su intervención en respuesta a los Diputados refiriéndose a los programas de sensibilización y pedagogía que desde 2008 a 2013 han tenido, en el espacio de su competencia, un número en torno a medio millón de destinatarios.

D. Marcial Marín Hellín, Consejero de Educación, Cultura y Deportes de Castilla-La Mancha. Comparecencia de 22 de abril de 2014.

El compareciente desde su experiencia indica como cuestiones más relevantes con relación a estos asuntos las siguientes:

— Potenciar la confianza en las nuevas tecnologías de todos los implicados en el ámbito escolar. Castilla-La Mancha ha sido elegida por el MEC (Ministerio de Educación y Ciencia) como centro pionero para el programa la mochila digital para la descarga de libros para los estudiantes.
— Acciones formativas de más de 26.000 docentes en materia de espacio virtual.
— Formar inspectores en la materia.
— Seminarios para profesores.
— Normas de uso de internet.
— Recoger en »el espacio virtual» advertencias sobre el riesgo de las descargas.
— El cuidado de la privacidad.
— Consejos útiles para usuarios.
— Uso seguro de las redes sociales.
— Guías SOS ante el *Grooming*.
— Guía de uso de cookies.
— En respuesta a observaciones de los Diputados se refiere a programas transversales Consejería de Educación, otras Administraciones Públicas y usuarios.
— Teléfono de urgencias para caso de acoso escolar que activen los centros de seguridad más cercanos al Centro Educativo.
— En contestación a Diputados, se refiere al asesoramiento jurídico al profesor y a formación técnica en estas materias.
— Aplicación de un protocolo de seguridad informática en los centros con un responsable de seguridad que puede ser el profesor de tecnologías.
— Creación de centros regionales de formación y apoyo virtual.
— En matización a las observaciones de algunos Diputados alude a la magnífica oportunidad para incorporar la pedagogía virtual en el futuro Estatuto del Personal Docente no Universitario y la formación especializada de los futuros docentes.
— Por último, el compareciente sugiere el estudio y realización de un Libro Blanco sobre tecnologías y escuela.

D. Francisco Martínez Vázquez, Secretario de Estado de Seguridad. Comparecencia de 25 de junio de 2014.

— El Secretario de Estado de Seguridad inicia su intervención felicitando a los Diputados por la creación de esta Subcomisión que ha venido desarrollando un trabajo de alto interés, con intervenciones muy cualificadas.

cve: BOCG-10-D-643

— El Secretario de Estado se refiere al potencial de las redes sociales tanto para proyectos encomiables y ambiciosos como para los más lamentables y, en relación con ello, alude a la importancia de la educación activa en la creación de hábitos saludables en las redes sociales que son grandes generadoras de corriente de opinión, nuevas formas de pensamiento y de movilización social, que participan de un fuerte sentimiento de solidaridad e intervención ciudadana, lo que no impide que haya también usos tenebrosos en numerosos casos delictivos en las redes sociales.

— El compareciente se refiere a que el Gobierno ha abierto también la transparencia en la gestión pública mediante las nuevas tecnologías y específicamente el Ministerio del Interior en campañas de seguridad en el hogar, turismo seguro, o las redes en las que participa la Policía Nacional, la Guardia Civil o el propio Ministerio; concretamente, indica, la Policía Nacional es la Institución española líder en número de usuarios en sus plataformas de redes sociales. La Policía Nacional y la Guardia Civil han puesto conjuntamente en una red el «Plan Contigo» extensión en internet del «Plan Director» para concienciar a los más jóvenes o la «Twitt redada» que sirvió para la lucha contra el narcotráfico.

— El Secretario de Estado se refiere también a aspectos menos positivos de las redes sociales como son: las redes sociales y el terrorismo (Operación A*** de lucha contra el terrorismo yihadista), aspecto este sobre el que llama la atención a la Subcomisión sobre el incremento del uso de internet a través de páginas web o foros no sólo como instrumentos de difusión informativa de yihadistas, sino también como centros de comunicación, propaganda y reclutamiento (Operación A***, etcétera).

— Otro asunto también a destacar en esta faceta negativa de las redes sociales es el cibercrimen (ataques contra sistemas informáticos, robo y manipulación de datos, usurpación de identidad, actividades relacionadas con pedofilia, estafas comerciales y bancarias y delitos de odio).

— Las Fuerzas y Cuerpos de Seguridad, afirma, han incrementado las operaciones para prevenir o atajar este tipo de delitos.

— Es evidente que internet no puede ser un escenario ajeno a las leyes y al margen de la sanción penal de determinadas conductas. En el año 2013 se registraron 42.437 delitos cometidos a través de las nuevas tecnologías de los cuales 26.664 fueron de fraude informático y 9.064 amenazas y coacciones. Si bien, a este respecto, la política criminológica parece que no debería enfocarse hacia la creación de nuevos tipos penales, sino hacia la intensificación de los instrumentos de investigación criminal evitando que su comisión en un medio telemático ampare una cierta impunidad o un cierto anonimato, permaneciendo el Derecho penal como última ratio.

— Parece procedente reflexionar sobre cómo arbitrar una educación especializada en el uso de internet y redes sociales especialmente para niños, jóvenes, adolescentes, padres y educadores aunque solo sea, y no es lo único, porque, por ejemplo, en un estudio llevado a cabo en Estados Unidos se refleja que el 20 % de las entrevistas de trabajo fracasan por la información que de sí mismo ha hecho pública en redes sociales el candidato. En este sentido, señala, desde la Secretaría de Estado de Seguridad se colabora con diferentes actores públicos y privados (Alia2, Protégeles, Centro Internacional para niños desparecidos y explotados), en la detección de las amenazas a menores a través de internet. A ese fin la primera tarea del Ministerio es un estudio demoscópico sobre jóvenes en internet y posteriormente poner en marcha un *«think thank»* que reúna a agentes en la defensa de la seguridad de los menores en internet y facilite la retirada de materiales contra privacidad o intimidad de menores, foros que promuevan la anorexia o bulimia, pro-suicidio, etcétera; tratando de contar siempre con la complicidad de los propios menores.

— Termina el compareciente agradeciendo la tarea de la Subcomisión y haciendo un llamamiento a esa colaboración e interrelación Parlamento-Gobierno.

— En respuesta a un Diputado, el Secretario de Estado incide en la necesidad de cooperación padres, educadores y niños; precisando que para evitar los casos de acoso y abuso de menores es fundamental partir de una dimensión sociológica (análisis de las circunstancias en que se producen estos fenómenos) y otra psíquico patológica, que si bien desborda el ámbito de las Fuerzas y Cuerpos de Seguridad, plantea también la necesidad de averiguar por qué se producen determinados hechos.

— Asimismo, en respuesta a otro Diputado indica que no hay tolerancia alguna con las web de extrema derecha y se refiere a la presentación en el Senado del mapa de la discriminación por motivos de odio.

— Coincide con los Sres. Diputados en que sería muy conveniente un código deontológico en la red.

cve: BOCG-10-D-643

— En respuesta a otro Diputado manifiesta que hay reuniones con empresas prestadoras de datos para plantear que no resulte tan difícil la obtención de información.

— También en respuesta a otro Diputado se refiere al CNPIC.

— En cuanto a la suplantación de identidad indica que ciertamente es un problema y que, en todo caso, se requiere denuncia para la prevención policial. Asimismo, indica que el acoso a menores tiene más alcance en las redes sociales que en la realidad.

D.ª Sinéad McSweeney, Directora Política Pública EMEA de Twitter. Comparecencia de 3 de septiembre de 2014.

— En su intervención indica que está acompañada de su equipo de seguridad y concretamente de Patricia Cartes, Directora de Seguridad global en Twitter.

— La compareciente se refiere a Twitter como plataforma abierta para que la gente comparta información, empresa pequeña pero de prestaciones muy amplias sobre cuya seguridad intervendrá a continuación la Sra. Cartes.

— La Sra. Cartes indica que ella trabaja en el campo del *Safety* más amplio que el concepto de seguridad diseñando las funciones de seguridad y los equipos para atender los problemas de los usuarios.

— La compareciente indica que ellos trabajan con asociaciones como Alia2, como Pantallas Amigas, o como Protégeles.

— La compareciente da cuenta del origen de la empresa Twitter en 2006 y del importante desarrollo en los últimos tres años de esta enorme Plataforma que tiene el 23 % de los usuarios en Estados Unidos y el 77 % en el resto del mundo, lo que da idea de las diferencias culturales entre usuarios.

— Twitter es una empresa con sede en San Francisco pero con oficinas en Dublín. En materia de seguridad, como es sabido, cuenta con un límite de uso de 140 caracteres, red a la que acceden un 25 % de usuarios a través de ordenador y un 75 % a través de dispositivos móviles. La cifra de usuarios es de 400 millones de visitantes únicos al mes. Mil millones de Twitts cada dos días, en un sitio disponible en 35 idiomas con 2.000 empleados a nivel mundial.

— Tienen dos equipos que se encargan de la protección del usuario: Trust & Safety compuesto por especialistas que son quienes orientan sobre el tipo de problema y otro equipo de propiedad intelectual e identidad que se encarga de examinar suplantación de identidad, derechos de autor, usurpación de marcas, protección de menores, etc. y su relación con las leyes en cada país. En España, afirma, trabajan en estrecha conexión con la Guardia Civil, la Policía Nacional y las Fuerzas de seguridad regionales. Hay equipos especializados en «spam», e incluso el equipo de seguridad del usuario que se encarga de mirar cualquier denuncia de abuso, acoso, amenazas, incitación al odio, suicidio, etc. Por ejemplo, en España trabajan mucho con el teléfono de la Esperanza.

— El mecanismo primario de denuncias de infracciones y el más rápido está en los botones de más y recoge la opción de bloquear o recortar contenido. Después existen opciones para describir el tipo de abuso y generar una denuncia vía e-mail al equipo de seguridad de usuarios.

— Las denuncias de abuso y acoso son, señala, una violación de nuestras reglas y cuando recibimos denuncias de este tipo siempre miramos cuál es la intención de la cuenta, se suele advertir al usuario de que ese tipo de comportamiento no es el más acertado y puede, en la mayoría de los casos, producirse una modificación de la conducta. Cuando se comprueba el acoso suspenden de forma temporal la cuenta y lo mismo cuando reciben denuncias y amenazas.

— La explotación infantil es otro asunto en el que son proactivos (la tecnología para la búsqueda de este tipo de contenidos Photodna es la desarrollada por Microsoft que mediante la afinidad de «hashes», parecidos a los píxeles, capta las imágenes de explotación del menor y automáticamente suspende la cuenta y remiten datos al NCMEN *(National Center for Missing and Exploiting Children)* creado por el Congreso de Estados Unidos y que disemina la información de usuarios a las Fuerzas de Seguridad de diferentes países.

— Otro punto en el que son bastantes rigurosos es en la propiedad intelectual e identidad pues no permiten la suplantación de identidad en Twitter aunque sí las «cuentas parodia». En los casos de suplantación de identidad suspenden de forma permanente la cuenta.

— Ellos colaboran con el mundo de la seguridad a nivel europeo en las redes INSAFE e INHOPE, la primera sobre temas de explotación del menor y la segunda sobre denuncias de contenidos en las plataformas. Asimismo, trabajan con asociaciones y organizaciones en España.

cve: BOCG-10-D-643

— En respuesta a Diputados sobre el uso de la red para amenazas terroristas responden las comparecientes que no se permite en la plataforma las fotos con violencia y si las detectan suspenden rápidamente las cuentas.

— Asimismo, en contestación a los Diputados se refieren a la delicada línea entre propaganda e información.

— En contestación a las preguntas de otro Diputado indican que trabajan en algunos proyectos de contra narrativa terrorista para contrarrestar grupos extremistas con las mismas facilidades y capacidades que se utilizan perversamente para la propaganda terrorista.

— También responde a Diputados indicando que su legislación es la de Estados Unidos y que la información se almacena en servidores norteamericanos sujetos a su legislación; ahora bien, en materia de privacidad tienen que cumplir también las leyes de la Unión Europea, y, a ese fin, ejemplifica con la supresión de contenidos antisemitas en Francia, pues son de carácter ilegal, mientras no es así en Estados Unidos.

— Igualmente en respuesta a Diputados matizan que una vez se borra una Twitt se mantiene en periodo de gracia de 30 días para garantizar si efectivamente se desea borrar la cuenta o no. Y en materia de retención de datos tienen una política de privacidad de retención de 12 o 15 meses, pero no retienen las IP tanto pues sería demasiado volumen de información.

— En respuestas a otro Diputado, indican que trabajan cercanamente con los departamentos de delitos informáticos y tratan de responder a cualquier tipo de petición legal que reciban.

— Las comparecientes hacen alusión a un segundo departamento de seguridad informática que es *«Homeland Security»* que también puede trasladar información sobre usuarios a fuerzas de seguridad.

— En cuanto a abusos de identidad las cuentas parodia son cuentas sanas y se mantiene en tanto en cuanto es una parodia. Si no es así hay suspensión temporal y petición de rectificación.

— Desde esta empresa no se permiten cuentas múltiples de modo que cuando se suspende la cuenta de alguien de forma permanente no se permite la creación de cuentas nuevas.

— Contestando a otro Diputado, las comparecientes se refieren al Centro de protección del menor, con un formulario específico para la denuncia de abuso al menor que trabaja veinticuatro horas al día, siete días a la semana, con un tiempo de respuesta muy rápido de minutos.

— También en relación con las denuncias sobre propaganda terrorista intentan dar una respuesta rápida si bien no lo es tanto como la correspondiente a los abusos de menores.

— En el caso de la propaganda de autolesiones y suicidio también priorizan de forma muy rigurosa la identificación de palabras vinculadas a desórdenes alimenticios. El *«spam out»* o terminología de los adolescentes a la hora de referirse a lesiones y desórdenes alimenticios, que vienen a actuar como el *«slang»* y que dan pistas sobre autolesiones y suicidios.

— También contestando a una Diputada indica que en el Reino Unido trabajan con un grupo denominado Paladín que son expertos en aconsejar a las víctimas cómo twittear de forma segura. De manera similar trabajan con la Secretaria de Estado de Asuntos sociales en España.

— En cuanto a la denuncia de abuso en móvil (de hecho la denuncia a nivel de Twit fue diseñada para móvil no para ordenador) debería poder hacerse clicando en «más» y «denunciar». En todo caso, se está trabajando en el sistema y consideran esencial el diseño de guías para perfeccionar la utilización de estos mecanismos.

— También en respuesta a la petición de una Diputada sobre eliminación de imágenes en España en particular, afirma: - si yo aparezco en la imagen y no quiero que esté en Twitter tengo un mecanismo de denuncia y puedo solicitar la eliminación.

— Sobre la minoría de edad ellos no preguntan nombre real, lugar, ni edad; sin embargo, la edad mínima para acceder a Twitter es de 13 años con base en la Ley COPPA, que es la Ley americana que establece que no se pueden procesar datos personales sin el consentimiento de los padres para menores de 13 años. En el caso español, 14. Ahora bien, son conscientes de que no es fácil verificar la edad real de alguien.

— Por último, las comparecientes en respuesta a Diputados indican que Twitter garantiza la máxima seguridad con independencia de la edad, raza o circunstancias personales de cada persona, si bien no se puede decir rotundamente Twitter es absolutamente seguro, pero ellos participan de la idea de aprendizaje continuo.

cve: BOCG-10-D-643

IV. Relación de Documentación aportada a la Subcomisión por los comparecientes.

D. Antonio Ramos, Presidente de ISACA. Comparecencia de 11 de septiembre de 2013.

— «Responding to targeted cyber attacks».
— «Transforming Cyber security using COBIT5».
— «Advanced Persistent Threat Awareness. Study Results».
— «Privacy management on social media sites».

D.ª Natalia Basterrechea, Directora de Asuntos Públicos de Facebook. Comparecencia de 11 de septiembre de 2013.

— Portal prevención acoso.

D. Carlos Represa Estrada, representante del Centro Nacional de Seguridad Escolar. Comparecencia de 18 de septiembre de 2013.

— Enlaces a noticias de prensa JCCM con radio.
— Zero to eight – 19 aug. Young Children and their internet Use.
— Nota de prensa menores. Asociación Nacional de tasadores y peritos judiciales informáticos.
— Resultado de estudio GDI UNIR. «Retos ético-pedagógicos en entornos virtuales. Análisis de la realidad y propuestas educativas».

D. Guillermo Cánovas Gaillemín, Presidente de Protégeles. Comparecencia de 18 de septiembre de 2013.

— Dosier informativo Protégeles.

D. José Luis Piñar Mañas, Director de la Cátedra Google del CEU. Comparecencia de 12 de febrero de 2014.

— Dosier «Redes Sociales y privacidad del menor». Percepción que tienen los menores sobre la utilización y seguridad de los datos que vuelcan en las redes sociales.

D.ª Carlota Navarrete Barreiro, Coalición de creadores e Industrias de contenidos. Comparecencia de 2 de abril de 2014.

— Observatorio de piratería y hábitos de consumo de contenidos digitales 2013.

D. Jorge Flores Fernández, Director de Pantallas Amigas. Comparecencia de 2 de abril de 2014.

— Dosier Pantallas Amigas. Para un uso seguro y saludable de las TIC. Por una ciudadanía digital responsable.

D. Francisco Fernández Marugán, Adjunto Primero a la Defensora del Pueblo. Comparecencia de 22 de abril de 2014.

— Libro «Programación y contenidos de la televisión e internet: La opinión de los menores sobre la protección de sus derechos».

D. Manel Prat Peláez, Director General de los Mossos d'Esquadra. Comparecencia de 22 de abril de 2014.

— EPA Position paper on cyber bullying and social networks.

cve: BOCG-10-D-643

PARTE DISPOSITIVA

V. Informe aprobado por la Subcomisión. Conclusiones de la Subcomisión de estudio sobre Redes Sociales constituida en la Comisión de Interior del Congreso de los Diputados

I. INTRODUCCIÓN

1. Estructura

Las presentes conclusiones son una síntesis de los trabajos de la Subcomisión para el estudio de las Redes Sociales, constituida en el seno de la Comisión de Interior del Congreso de los Diputados. Y, en especial, de las 48 comparecencias celebradas en ella, a lo largo de 13 sesiones, entre el día 26 de junio de 2013 y el 3 de septiembre de 2014.

No es fácil sintetizar en unas conclusiones todo el conocimiento acumulado en casi dos años de actividad (desde la aprobación, por la Comisión de Interior, de esta Subcomisión de estudio, el 27 de febrero de 2013), pero se ha intentado, ordenándolas en dos grandes bloques: consideraciones o principios generales y recomendaciones de medidas concretas; y, dentro de éstas, en cinco apartados:

1. Medidas organizativas
2. Medidas educativas
3. Medidas regulatorias
4. Medidas policiales
5. Medidas sectoriales

2. Las Recomendaciones de la Ponencia de Estudio del Senado

Por otra parte, se han tenido muy en cuenta las recomendaciones de 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, Educación y Deporte, e Industria, Energía y Turismo del Senado (que se publicaron en el BOCG núm. 410, del 3 de octubre de 2014).

En ellas se recoge una síntesis de las conclusiones de las 53 comparecencias, celebradas en un total de 19 sesiones, entre el 9 de mayo de 2013 y el 5 de mayo de 2014, estructuradas en nueve apartados:

1. Alianzas público-privadas.
2. Cooperación internacional.
3. Estrategia, coordinación y coherencia.
4. Alfabetización digital y sensibilización general.
5. Seguridad de internet.
6. Parámetros de edad y privacidad y herramientas de denuncia en las redes sociales.
7. Seguridad de la Red en relación al juego *online* y a la publicidad *online*.
8. Sistema normativo y de aplicación de la Ley de respuesta eficaz frente a los contenidos y conductas ilícitas en la Red.
9. Capacidades operativas en la lucha contra el abuso sexual y la pornografía infantil (o, como sostienen algunos expertos internacionales, abusos a menores).

3. Especialización

Dado que se ha producido un cierto solapamiento, tanto temporal como temático, con la Ponencia de estudio del Senado, enfocada en los riesgos derivados del uso de la Red por parte de los menores, la Subcomisión del Congreso acordó en su sesión de constitución, el día 18 de abril de 2013, tender a una especialización en el análisis de la seguridad de las redes sociales, con carácter general.

Quiere esto decir que tanto los trabajos de la Subcomisión como las presentes conclusiones no se refieren sólo a la seguridad de los menores en el uso de las redes sociales, si bien es cierto que la creación de la Subcomisión trae causa de una Proposición No de Ley del Grupo Parlamentario Popular (de 13 de marzo de 2012) sobre la prevención del ciberacoso a menores en las redes sociales.

Asimismo, en los últimos meses han surgido y se han desarrollado rápidamente en las redes sociales fenómenos nuevos, que no se habían previsto en el origen de la Subcomisión de estudio del Congreso y

cve: BOCG-10-D-643

a los que tampoco le pudieron dedicar mucha atención los comparecientes, como son los llamados «delitos de odio» y, especialmente, la propaganda y proselitismo del terrorismo yihadista; o, en otro orden de cosas, desde la incidencia en problemas como la anorexia o la bulimia a través de páginas o redes sociales, hasta la reflexión sobre la identidad digital, todo lo cual evidencia la necesidad de continuar trabajando sobre estas cuestiones de gran incidencia social.

4. Medidas en marcha

Las recomendaciones de medidas concretas no pretenden ser «originales», sino más bien una recopilación y ordenación de medidas «razonables», en las que han coincidido muchos de los comparecientes, y algunas de las cuales ya estaban previstas en los planes de los diferentes organismos competentes en la materia, e, inclusive, se han ido poniendo en marcha en los últimos meses.

Por eso, no debe extrañar que, entre ellas, se recojan algunas medidas que se anunciaron en su día por los comparecientes, especialmente los representantes ministeriales, y que en los casi dos años de trabajo de la Subcomisión de Estudio, se han puesto en marcha o están en vías de hacerlo; especialmente, las medidas regulatorias vinculadas a proyectos legislativos actualmente en tramitación.

En este sentido, cabe destacar, entre las medidas regulatorias:

— Proyecto de Ley Orgánica de reforma del Código Penal.
— Anteproyecto de reforma de la Ley de Enjuiciamiento Criminal.
— Anteproyecto de Ley de modificación del sistema de protección a la infancia y a la adolescencia .
— La Proposición de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo, publicada en el BOCG de 4 de febrero de 2015.
— Real Decreto de modificación del currículo educativo de primaria.
— Proyecto de Reglamento europeo de Protección de Datos.

Y, entre las medidas operativas:

— Plan Director del Ministerio del Interior en centros educativos.
— Convenios de colaboración de Red.es (con Educación, Interior y Sanidad).
— Estrategia Nacional de Ciberseguridad y Plan Nacional de Ciberseguridad.
— Plan derivado de Cultura de la Ciberseguridad.
— Plan derivado contra la Ciberdelincuencia y el Ciberterrorismo.
— Plan derivado de impulso al desarrollo industrial, capacitación de los profesionales y refuerzo de la I+D+i en materia de ciberseguridad.

5. Concepto de redes sociales

En primer lugar, la Subcomisión abordó la delimitación de su objeto de estudio, intentando definir, a través de las opiniones de los expertos, qué se entiende por redes sociales; así como identificando plataformas o sistemas de comunicación (como, por ejemplo, los de mensajería instantánea), que no se suelen identificar como redes sociales, pero que presentan características y problemas similares.

En este sentido, es oportuna la distinción entre las redes sociales de una persona y las plataformas de tecnologías de la información y la comunicación o servicios de la Sociedad de la Información dirigidos a poner en contacto a sus miembros, que pueden servir para construirlas, mantenerlas o ampliarlas, pero también para modificarlas, reducirlas o, incluso, destruirlas, según el uso que se haga de ellas.

También es pertinente la distinción entre plataformas y servicios tecnológicos de redes sociales y plataformas y servicios tecnológicos de mensajería instantánea, aunque muchas veces los límites no están claros, y las redes sociales incluyen sistemas de mensajería instantánea y los sistemas de mensajería instantánea permiten crear y gestionar grupos, como verdaderas redes sociales.

Por último, aunque, en rigor, no se trata de plataformas o servicios tecnológicos de redes sociales ni de mensajería instantánea, cada vez están cobrando mayor auge las plataformas que prestan un determinado servicio a un usuario individual (como, por ejemplo, Spotify), pero permite comunicarse o compartir contenidos con otros usuarios.

cve: BOCG-10-D-643

Desde el punto de vista de la seguridad, especialmente de los menores de edad, ha supuesto un nuevo riesgo la generalización de los juegos en línea, a medida que se han ido extendiendo las conexiones de alta capacidad. Pues, aparte de permitir jugar con desconocidos de cualquier parte del mundo, suele incluir algún canal de comunicación (mensajería, chat o web-cam) entre los jugadores.

6. Tipos de redes sociales

Hay muchos tipos de redes sociales y, también, muchas posibles clasificaciones de éstas, según el criterio que utilicemos. Aquí nos centramos en los que tienen alguna trascendencia desde el punto de vista de la seguridad:

Un primer criterio de distinción, con consecuencias importantes desde el punto de vista de la seguridad, es si se trata de redes sociales abiertas o públicas, con indexación de sus contenidos en los buscadores, o si se trata de redes privadas o cerradas, ya sean corporativas o personales, sin visibilidad de sus contenidos en los buscadores (clubes privados, como Tuenti).

Desde el punto de vista de la actividad o finalidad, podemos distinguir entre unas redes sociales generalistas, en las que priman los mensajes entre sus miembros, aunque también se pueden compartir contenidos (Facebook, Twitter o Google+), y otras, especializadas, en las que prima bien una finalidad profesional (Linkedin) o bien la compartición de ciertos contenidos (YouTube, Instagram o Pinterest).

7. Situación actual de las redes sociales en España

Según el VI Estudio Redes Sociales de IAB Spain, publicado en enero de 2015:

• Un 82 % de los internautas mayores de edad (entre 18 y 55 años) utilizan las redes sociales, lo que representa más de 14 millones usuarios (sobre un total de 17,6 Millones de internautas, que representa el 71 % de la población).

• Las redes sociales más utilizadas/visitadas en España, son: Facebook (96 %), YouTube (66 %), Twitter (56 %), Google+ (34 %), Linkedin (31 %), Instagram (26 %), Spotify (24 %), Tuenti (12 %), Pinterest (9 %) y Flickr (8 %).

• El uso principal de las redes sociales continúa siendo «social» (ver que hacen tus contactos, enviar mensajes, postear, chatear). Sube mucho ver Videos y Música, debido a la fuerza de YouTube y Spotify.

• Los dispositivos más usados para acceder a las redes sociales siguen siendo los ordenadores (99 %), pero sube el uso de móviles (75 %) y tablets (28 %) y aumentan los accesos desde TV conectada (7 %) y consolas (6 %).

• En cuanto a los adolescentes (entre 14-17 años), el uso de las redes sociales se eleva al 97 %, utilizando menos Facebook (78 %), y más: YouTube (70 %), Twitter (61 %), Instagram (60 %) y Tuenti (54 %).

En cuanto a los riesgos en el uso de las redes sociales por los menores de edad, un reciente estudio de la Universidad Miguel Hernández, dice:

• El 50 % de los jóvenes sufren alguna vez alguna de las formas de ciberacoso: coacciones, amenazas, insultos, publicación de fotografías o vídeos sin consentimiento, emisión de rumores…

• El 5,9 de los ciberacosos son de carácter sexual.

• Cerca del 18 % han sido víctimas de control por parte de parejas o exparejas

8. Situación en países de nuestro entorno

Algunos datos sobre la situación de las redes sociales en Europa:

• Europa tiene 293 millones de usuarios activos en redes sociales (el 40 % de la población), media superada ampliamente por España.

• El 70 % de los adolescentes y jóvenes europeos emplean la mayor parte de su tiempo «online» en redes sociales, pero la mitad lo hace sin ningún tipo de supervisión o control parental.

• Casi un 15 % de los menores internautas entre 10 y 17 años recibe alguna propuesta sexual y el 34 % de ellos se encuentra con material sexual que no ha buscado.

cve: BOCG-10-D-643

9. Debate

Las consideraciones generales y las medidas concretas de estas «conclusiones» están expresadas, intencionadamente, de forma concisa, como se corresponde con el lenguaje utilizado en las redes sociales, porque, por un lado, sólo se trata de resumir y ordenar las propuestas de los expertos y los grupos parlamentarios y, por otro lado, no se pretende «cerrar», sino «abrir» un debate sobre las mismas.

La Subcomisión de Estudio considera que este «informe de conclusiones» no es, en modo alguno, un punto final, sino un punto de partida para el necesario debate que debe continuar en sede parlamentaria, en las administraciones afectadas, en el sector TIC, en foros profesionales, en ONGs, en Universidades, en medios de comunicación y, también, en las propias redes sociales.

10. Publicación

Para ello, sería muy conveniente que, junto con estas conclusiones, se publicase (tanto en papel, como —sobre todo— en digital) todo el material que ha conocido la Subcomisión de Estudio y, especialmente, un resumen de las comparecencias de los expertos que han pasado por ella, así como toda la documentación que han aportado.

La Subcomisión de Estudio considera que todo este material es un conocimiento muy valioso que, con las debidas autorizaciones, debería ser accesible al público y enriquecer los repositorios y portales que se puedan crear sobre esta materia, en colaboración público-privada, como punto de referencia para los estudiosos del fenómeno de las redes sociales y de su futura evolución.

II. CONCLUSIONES PROPUESTAS POR LOS GRUPOS PARLAMENTARIOS PARA EL INFORME DE LA SUBCOMISIÓN SOBRE REDES SOCIALES DE LA COMISIÓN DE INTERIOR DEL CONGRESO DE LOS DIPUTADOS

A) CONSIDERACIONES Y PRINCIPIOS GENERALES

a) Valoración

1. Valoración positiva de las redes sociales, porque permiten la comunicación, el ocio y el ejercicio de derechos ciudadanos.

b) Coordinación

2. Necesaria coordinación de todas las instituciones públicas, tanto de la AGE como con las CCAA.

3. Importancia de la colaboración, el intercambio de información y la rapidez en las respuestas entre todos los agentes concernidos.

4. Importancia de la cooperación internacional, tanto en el nivel de decisión política como en el nivel operacional.

c) Medidas

5. Adopción de medidas educativas, divulgativas y preventivas, juntamente con las medidas normativas o policiales.

6. Fomento de la autorregulación: la existencia de códigos de conducta eficaces es preferible a la imposición de corsés legales o técnicos.

7. Especial atención a la protección de la infancia y la juventud, distinguiendo tramos de edad y diferentes usos.

d) Regulación

8. Atención a los peligros de la sobrerregulación. No todo se soluciona con más leyes específicas. Conductas ya previstas por las leyes generales.

9. Mejor regulaciones de principios generales, salvo en el ámbito penal, que regulaciones muy detalladas, que se vuelven obsoletas en pocos meses.

10. Intentar llegar a soluciones normativas transnacionales, puesto que las redes sociales suelen ser transnacionales.

cve: BOCG-10-D-643

III. RECOMENDACIONES / MEDIDAS CONCRETAS

A) ORGANIZATIVAS: COORDINACIÓN, COOPERACIÓN, COLABORACIÓN

a) Coordinación de las Administraciones Públicas

1. Coordinación de los distintos organismos afectados de la AGE y de las CCAA a través de la SE de Telecomunicaciones y de la Sociedad de la Información.

b) Autorganización de las empresas y organizaciones privadas

2. Fomento de un sistema de autorregulación, autocontrol sectorial y arbitraje de las empresas que operen en España, con independencia de su sede.

3. Fomento de la coordinación de entidades sin ánimo de lucro, dedicadas a los menores: mediante la coordinación en una plataforma.

c) Colaboración Público-Privada

4. Impulso del Foro de Colaboración Público-Privado sobre menores e internet con participación de administraciones, empresas, ongs y universidades.

d) Participación ciudadana

5. Impulsar y simplificar sistemas de denuncia por los usuarios de contenidos y situaciones de riesgo, con respeto de los derechos fundamentales.

e) Cooperación internacional

6. Armonización de los marcos estadísticos nacionales, para medir de forma consistente acceso, uso y riesgos de internet en los menores.

7. Mejorar la cooperación transfronteriza de las autoridades policiales y judiciales en la persecución y lucha contra el delito.

8. Apoyar a las redes internacionales de líneas de ayuda y constituir en España un «Centro de Seguridad en internet» de la red INSAFE-INHOPE.

9. Promover y participar en iniciativas internacionales de concienciación y sensibilización.

10. Apoyar activamente iniciativas que promueven estándares internacionales para interoperabilidad (de etiquetado, control parental,…).

B) EDUCATIVAS: FORMACIÓN, DIVULGACIÓN, PREVENCIÓN

a) Educación de menores

1. Elaboración coordinada de contenidos de formación y sensibilización por las autoridades educativas competentes.

2. Capacitación de los menores en competencias digitales con un contenido que no se limite a seguridad digital, sino orientada a «ciudadanía digital».

3. Necesidad de educar en la escuela en el uso apropiado de las redes sociales, basado en valores: responsabilidad de los propios actos.

4. Lecciones, en el primer ciclo de primaria, sobre los usos y riesgos de la red, con ejemplos de webs y conductas peligrosas para su intimidad.

5. Acciones formativas en centros escolares para prevenir el sexteo *(sexting),* así como cualquier tipo de acoso (acoso escolar —*bulliyng*—, *grooming*…) a través de las TIC.

b) Formación de mayores

6. Formación de maestros y profesores; fomento de la revisión de los planes de estudio, para capacitarse y adaptarse a la evolución tecnológica.

7. Formación de padres que, como en otras actividades que comportan riesgos, deben acompañar a sus hijos en su aprendizaje.

cve: BOCG-10-D-643

8. Formación específica para Jueces, Fiscales y personal de la Administración de Justicia, Fuerzas y Cuerpos de Seguridad y personal socio-sanitario.

c) Divulgación

9. Campañas públicas sobre el uso responsable de redes sociales para prevenir la justificación de la violencia: terrorista, de género, etc.

d) Prevención

10. Programa de prevención de adicciones tecnológicas, desde la adolescencia, basado información, sensibilización y pautas prácticas de acción.

C) REGULATORIAS

a) Penales

1. Apoyar la incorporación en el Código Penal de una definición de «pornografía infantil».
2. Apoyar la tipificación como delito del acceso en línea a archivos con pornografía infantil y el visionado en «streaming».
3. Apoyar la regulación del «agente encubierto» con autorización judicial previa y sólo para la investigación de delitos graves y especialmente complejos.
4. Apoyar la prohibición de uso de troyanos por la policía sin autorización judicial para acceder a ordenadores de personas meramente sospechosas.
5. Estudiar la tipificación penal de la suplantación de la identidad en el entorno digital, sin perjuicio de la responsabilidad por otros delitos conexos.

b) Civiles:

6. Adaptar al entorno digital la Ley Orgánica de Protección Civil del Derecho al Honor, a la Intimidad personal y familiar y a la propia Imagen, con especial atención a la notoriedad y vulnerabilidad de las personas ofendidas.

c) Otras leyes

7. Apoyar medidas cautelares de los Jueces para ordenar la retirada o bloqueo del acceso a contenidos ilícitos, penales o civiles.
8. Regulación sectorial de la seguridad y privacidad por defecto o «por diseño» de los productos y servicios TIC y de la Sociedad de la Información.
9. Apoyar el reconocimiento del «derecho al olvido», particularmente si los datos se hubieran dado cuando los titulares eran menores.
10. Otras modificaciones (administrativas) para mejorar la protección integral de los menores y su educación en la utilización de las redes sociales.

D) POLICIALES

a) Pornografía infantil

1. Reforzar los recursos policiales (medios humanos y tecnológicos) destinados a la lucha contra la pornografía infantil en internet.
2. Intensificar colaboración de las empresas en la detección, información rápida a las fuerzas policiales y retirada de la pornografía infantil.
3. Reforzar la cooperación con cuerpos policiales y con empresas proveedoras de servicios TIC y las líneas de denuncia de organizaciones privadas.
4. Incrementar la cooperación internacional para la lucha contra el abuso sexual y pornografía infantil.

cve: BOCG-10-D-643

b) En general

5. Implantar canales de comunicación de máxima prioridad entre las empresas gestoras de redes sociales y las Fuerzas y Cuerpos de Seguridad.
6. Garantizar que la información que retienen las empresas solo se entrega a terceros mediante orden judicial expresa y previa.
7. Mecanismo para asegurar que determinados datos no se destruyan, mientras se recaba una autorización judicial.
8. Permitir la cesión de datos de tráfico solo mediante previa autorización judicial específica (no de contenidos de comunicaciones) por operadores a agentes facultados en la investigación de delitos.
9. Implantar sistemas de relación de instancias nacionales judiciales y policiales y compañías extranjeras que eviten comisiones rogatorias.

c) Coordinación

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

E) SECTORIALES

a) Contenidos nocivos

1. Impulsar un sistema de etiquetado inteligente de contenidos digitales, basado en tecnología semántica y reentrenable por los usuarios.
2. Clasificación o recomendación por edades de las Aplicaciones (apps), en el mismo sentido que el sistema PEGI para los videojuegos.
3. Promoción de medidas técnicas de control parental que preserven a los menores frente al riesgo de exposición a contenidos nocivos.
4. Estudiar la viabilidad de los diferentes modelos de filtrado de contenidos por los operadores, para bloquear el acceso a contenidos nocivos para los menores.
5. Recomendar mecanismos de verificación de la edad para restringir el acceso de los menores a sitios web que ofrezcan contenidos para adultos.

b) Protección de menores en general

6. Estudiar mecanismos eficaces que permitan a los padres solicitar el borrado de contenidos o imágenes que afecten a sus hijos menores de edad, sin perjuicio de su conservación si afectan a derechos o responsabilidades de otras personas.
7. Control de la publicidad y del acceso desde las redes sociales a plataformas de juego on-line, especialmente por parte de menores.
8. Creación de premios o «sellos» de responsabilidad social específicos, por la contribución de empresas a la protección de los menores en internet.

c) Seguridad en general

9. Establecer protocolos de seguridad de redes wifi accesibles al público, para que no se pueda violar la intimidad de los ciudadanos que se conecten.
10. Implantación de sistemas para la identificación segura en webs que requieran el uso de datos bancarios o tarjetas de crédito y, en todo caso, del DNI-e 3.0.

Palacio del Congreso de los Diputados, 24 de marzo de 2015.

cve: BOCG-10-D-643