XX Edición del Premio Protección de Datos Personales de Investigación
de la Agencia Española de Protección de Datos

ACCÉSIT 2016

Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos Breve referencia al fenómeno *Pokémon Go*

Laura Davara Fernández de Marcos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

BOLETÍN OFICIAL DEL ESTADO
MINISTERIO DE LA PRESIDENCIA
Y PARA LAS ADMINISTRACIONES TERRITORIALES

MENORES EN INTERNET Y REDES SOCIALES: DERECHO APLICABLE Y DEBERES DE LOS PADRES Y CENTROS EDUCATIVOS

Breve referencia al fenómeno *Pokémon Go*

MENORES EN INTERNET Y REDES SOCIALES: DERECHO APLICABLE Y DEBERES DE LOS PADRES Y CENTROS EDUCATIVOS

Breve referencia al fenómeno *Pokémon Go*

Laura Davara Fernández de Marcos

Agencia Española de Protección de Datos

Agencia Estatal Boletín Oficial del Estado
Madrid, 2017

http://publicacionesoficiales.boe.es

NIPO: 786-17-043-X
ISBN: 978-84-340-2399-4
Depósito Legal: M-12649-2017

IMPRENTA NACIONAL DE LA AGENCIA ESTATAL
BOLETÍN OFICIAL DEL ESTADO
Avda. de Manoteras, 54. Madrid 28050

Índice

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
APDCM	Agencia de Protección de Datos de la Comunidad de Madrid
BIT	Brigada de Investigación Tecnológica
BOE	Boletín Oficial del Estado
CARU	Children's Advertising Review Unit
CIPA	Children's Internet Protection Act
COPPA	Children Online Privacy Protection Act
CP	Código Penal
DNI	Documento Nacional de Identidad
DOUE	Diario Oficial de la Unión Europea
EEUU	Estados Unidos
FOMO	Fear of missing out
FTC	Federal Trade Commission
GT29	Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE
INCIBE	Instituto Nacional de Ciberseguridad
INTECO	Instituto Nacional de Telecomunicaciones
LCE	Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la Información y de comercio electrónico
LGDCU	Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
LPI	Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual
MMS	Multimedia Message System
OSI	Oficina de Seguridad del Internauta
PxD	Privacidad por defecto
PdD	Privacidad desde el diseño
Pg	Página
RAE	Real Academia Española de la Lengua
RLOPD	Reglamento de desarrollo de la LOPD

SMS	Short Message System
TIC	Tecnologías de la Información y las Comunicaciones
TS	Tribunal Supremo
UCA	Unidad de Conductas Adictivas
UE	Unión Europea
Vid.	Véase

PRÓLOGO

El premio Protección de Datos Personales de Investigación que convoca de forma anual la Agencia Española de Protección de Datos (AEPD) tiene como finalidad fomentar la investigación y reflexión acerca de este derecho fundamental. En esta vigésima edición, el jurado, compuesto por el Consejo Consultivo de la AEPD, ha distinguido la obra «Menores en Internet y Redes Sociales: Derecho aplicable y deberes de los padres y centros educativos. Breve referencia al fenómeno *Pokémon Go*», de Laura Davara Fernández de Marcos, con el accésit en la modalidad de Trabajos originales e inéditos.

Las nuevas tecnologías se han convertido en herramientas de uso prácticamente universal por parte de los menores. Según datos de 2016 del Instituto Nacional de Estadística, el 95% utiliza internet, mientras que el porcentaje de jóvenes que dispone de teléfono móvil se incrementa significativamente a partir de los 10 años hasta alcanzar casi el 94% en la población de 15 años.

Esta obra profundiza en el estudio de las implicaciones que internet y las redes sociales generan en la privacidad de este colectivo desde una perspectiva tanto jurídica como preventiva. La autora aborda el marco jurídico aplicable a las distintas situaciones que se pueden producir en el uso de internet, el Reglamento General de Protección de Datos, de aplicación en mayo de 2018, e incluye referencias a normativa de distintos países. Trata, asimismo, acerca del papel que desempeñan en este ámbito los centros educativos y los padres por su responsabilidad en la educación de los menores, y realiza un análisis específico de las implicaciones que el juego «Pokémon Go» presenta para la privacidad de los usuarios y, en particular, para las personas más jóvenes. Para finalizar, la obra concluye con una serie de recomendaciones dirigidas a reforzar las garantías de los derechos y la seguridad de los menores en el uso de internet.

La espectacular evolución de internet y de los servicios que se ofrecen en ella constituye un fenómeno que afecta a toda la sociedad, pero de manera especial a los menores de edad, de los que se ha llegado a decir que viven en internet. Según todos los estudios, el acceso a

la Red se produce a edades cada vez más tempranas, llegando a ser de uso casi global en la franja de 10 a 15 años.

Teniendo en cuenta que el flujo constante de información de carácter personal del que se nutren las redes sociales puede afectar a su privacidad y a su derecho a la protección de datos, la Agencia Española de Protección de Datos ha incluido en su Plan Estratégico un conjunto de líneas de acción orientadas a proteger y garantizar los derechos de los ciudadanos, en especial de este grupo.

La AEPD cuenta con un canal de atención especializada para tratar estos temas con jóvenes, padres y profesores, y dispone de numerosos materiales didácticos en su página web. Para profundizar en este campo, la Agencia va a realizar varias actuaciones adicionales como nuevos vídeos, talleres y fichas prácticas dirigidas a estos colectivos, además de una guía para centros docentes. Estas iniciativas, a su vez, se complementarán con otras medidas proyectadas dentro del marco global del Plan Estratégico de la Agencia. El objetivo es mejorar la protección de la información personal y la privacidad de un colectivo vulnerable que no siempre es consciente del grado de exposición pública al que se somete cuando realiza determinados usos de la tecnología.

Mar España Martí
Directora de la Agencia Española de Protección de Datos

1. INTRODUCCIÓN

No cabe duda de que las Redes Sociales[1] son un fenómeno que, contando con más de 10 años de edad en algunos casos[2], aún es, en cierto modo, desconocido en lo que a implicaciones jurídicas, pautas, límites y responsabilidades que se derivan de la actuación en las mismas; siendo este desconocimiento e incertidumbre aún mayor cuando los protagonistas —ya sea directa o indirectamente— son menores de edad.

Y es que, si bien en un primer momento las Redes Sociales fueron concebidas para que personas que habían perdido el contacto al finalizar los estudios lo recuperaran a través de esta herramienta[3], con el paso del tiempo, los más pequeños de la casa se alzan como sus principales valedores, comenzando en muchos casos a edades muy tempranas[4] como los 9 o 10 años donde, en más de una ocasión, los hijos manejan mejor[5] que sus progenitores los aparatos

---

1 Aunque nos referimos a Redes Sociales, el presente trabajo de investigación versa sobre Internet en general aunque, dado el papel protagonista que desempeñan los niños y jóvenes en las Redes Sociales, hemos querido hacer alusiones concretas a las mismas.

2 Facebook se creó en 2004 y Twitter en 2006, por poner sólo algunos ejemplos. Aunque en el caso de redes sociales como Whatsapp o Instagram, aún no alcanzan los diez años de edad.

3 Pese a no haber gozado del éxito que se esperaba, la primera Red Social data de 1995 y bajo el nombre «classmates.com» tenían como objetivo que los compañeros de clase que finalizaban los estudios pudieran mantener el contacto una vez dejaran la escuela.

4 Debiéndose tener en cuenta en este punto tal y como indica Ruiz de Huidobro que «(…) el menor de edad se caracteriza por sus condiciones de inmadurez (física, psicológica, social) que le impiden valerse por sí mismo y justifican su protección jurídica, una de cuyas manifestaciones es un régimen de la capacidad de obrar caracterizada por su limitación (…)». *Vid*. RUIZ DE HUIDOBRO DE CARLOS, J. M.: «La regulación legal de la capacidad de obrar del menor, propuestas de Lege Ferenda», en *Jornadas sobre derecho de los menores* (Isabel E. Lázaro González, Ignacio V. Mayoral Narros, coordinadores). Ed. Universidad Pontificia Comillas de Madrid, Madrid, 2003, p. 448.

5 Es por ello que «Los menores de hoy en día son los llamados nativos digitales porque han nacido y crecido con las nuevas tecnologías, cuentan con ellas en sus vidas desde muy pequeños y, de algún modo, llegan a constituirse en su seña de identidad. Sin embargo, muchos padres tienen aún un

tecnológicos y sus posibilidades y funcionalidades, siendo una más las Redes Sociales.

Dada la importancia de este tema, abordaremos el impacto y las implicaciones jurídicas que tiene la actuación del menor teniendo en cuenta las obligaciones de los padres y tutores, de los Centros educativos a los que acuden, tomando como base la normativa existente y algunas cuestiones jurisprudenciales que arrojan cierta luz en esta materia; todo ello en una balanza en la que también tienen peso específico los derechos de los menores, entre los que cabe citar: el derecho de los menores a la protección de sus datos[6] de carácter personal, el derecho a la intimidad o al secreto de sus comunicaciones.

Por último, y dada la actualidad del tema y el impacto que, a todos los niveles ha generado, abordaremos el fenómeno «Pokémon Go» estudiando el propio fenómeno así como las implicaciones jurídicas, las ventajas e inconvenientes para todos los usuarios —haciendo especial hincapié en los menores—.

---

perfil tecnológico bajo, lo que revela la existencia de una brecha digital entre adultos y menores y supone un obstáculo en el objetivo de lograr un uso seguro y responsable». *Vid.* ECHEBURÚA, E y REQUESENS, A.: «Adicción a Redes Sociales y nuevas tecnologías en niños y adolescentes», Pirámide, Madrid, 2012, p. 22.

6 De vital importancia nos resulta lo dispuesto por el Dictamen 2/2009, del GT29, sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas) emitido el 11 de febrero de 2009 (398/09/ES, WP160), en el que se pone de manifiesto que, desde la perspectiva de la protección de datos, Las necesidades de protección de datos de los niños han de tener en cuenta dos aspectos importantes. En primer lugar, los diversos grados de madurez que determinan el momento a partir del cual los niños pueden empezar a ocuparse de sus propios datos y, en segundo lugar, hasta qué punto los representantes tienen derecho a representar a los menores en los casos en que la divulgación de datos personales pueda ser perjudicial para los intereses del niño. A continuación se tratará de determinar cuál es la mejor manera de aplicar las normas existentes de la Directiva, a fin de garantizar una protección adecuada y efectiva de la intimidad de los niños. Disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_es.pdf. Visitado el 25 de septiembre de 2016.

2. EDAD DE ACCESO DE LOS MENORES A REDES SOCIALES

Tal y como hemos comentado, hay que partir de la base de que las Redes Sociales son una herramienta que, en sus inicios, nacieron con la vocación de mantener el contacto con personas que los usuarios habían conocido en el colegio y/o en la universidad y que, al pasar a otra etapa formativa o laboral, se veían abocados a perder el contacto por el distanciamiento. Es por ello que, en un principio, las Redes Sociales no fueron pensadas para niños, ni, por supuesto, su público *target* —su público objetivo— eran los menores de edad. Quizás por eso, en la práctica totalidad de las Redes Sociales, la edad mínima de acceso son los catorce años[7].

Sin embargo, está más que comprobado que, desde los ocho-nueve años, los menores entran en las Redes Sociales y se registran, con o sin el conocimiento de sus padres, poniendo únicamente una fecha de nacimiento anterior a la suya y haciendo el cálculo para que supere la edad mínima exigida por la plataforma. A esta facilidad de acceso, se le tiene que añadir que únicamente se pide un nombre, un apellido, una contraseña y una dirección de correo electrónico —datos que todos los menores pueden proporcionar sin apenas esfuerzo ni dificultad—.

Es por ello que, en todas las Redes Sociales, existen miles —en algunos casos, millones— de perfiles de usuarios que no cuentan con la edad mínima exigida por la red social pero que, por el contrario, se alzan como usuarios activos y con un manejo más que ágil de la red social —nos atrevemos a decir que dicho manejo no suele ser tan ágil en lo que respecta a la configuración de privacidad de las mismas—.

En este sentido, traemos a colación una reunión mantenida entre los dirigentes de Tuenti y el Director de la Agencia Española de Protección de Datos (AEPD) donde la citada red social se comprometió a

---

[7] En el caso de Facebook, Twitter, Instagram y Snapchat la edad se fija en los trece años. En el caso de Tuenti en los catorce y en el caso de Whatsapp en los dieciséis.

depurar los perfiles que aparentasen ser titularidad de un menor de 14 años, instándoles al envío del Documento Nacional de Identidad que acreditase que superaban la edad mínima exigida en un plazo de 92 horas, ya que en caso contrario se procedería a la cancelación de sus cuentas.

Las cifras de este proceso son realmente llamativas y clarificadoras del escaso control de verificación de edad puesto que en la citada reunión los dirigentes de Tuenti indicaron que más de un 90% de los usuarios requeridos por la red social a mostrar un documento que acreditase que fueran mayores de 14 años, no respondieron a la solicitud y, por tanto, sus cuentas fueron bloqueadas, tal y como acordaron Tuenti y la AEPD en una reunión que tuvo lugar en abril de 2009 donde valoraron los riesgos de privacidad de los menores de edad que hacían uso de la red social.

Siguiendo con el caso de Tuenti, queremos llamar la atención sobre su deseo de cumplir con la normativa española en materia de protección de datos en todo momento; desde su concepción, en la que exigía los catorce años como edad mínima de acceso, pasando por la ya citada verificación de edad de sus usuarios a instancia de la AEPD y finalizando por la reciente modificación de la aplicación móvil que permite la descarga de todas las fotografías que el usuario ha compartido en Tuenti, de manera que, una vez descargadas y si el usuario lo desea, pueda darse de baja de la citada red social puesto que, en los últimos años, el número de usuarios activos en Tuenti ha sufrido una gran merma y todo apunta a que los usuarios que siguen teniendo cuenta en Tuenti es por miedo a perder las fotografías que subieron cuando eran usuarios activos de la misma.

Creemos que, en cierto modo, esta posibilidad que ofrece la red social española se puede asemejar al derecho de portabilidad de los datos que contempla el Reglamento Europeo de Protección de Datos[8]

---

[8] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE serie L núm. 119/1, de 4 de mayo. Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES. Visitado el 3 de octubre de 2016.

(en adelante, el Reglamento Europeo de Protección de Datos) al afirmar que «El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado». Hacemos esta llamada de atención puesto que, gracias a este derecho, los usuarios —en este caso de Tuenti pero plenamente aplicable a cualquier red social— podrán ejercer su derecho a la portabilidad y traspasar todo el contenido que han compartido en una red social a otra, sin necesidad de borrar todo de la primera y volver a subirlo a la segunda.

Una vez fijados los límites de edad establecidos por las distintas Redes Sociales, queremos llamar la atención sobre lo dispuesto por la normativa —vigente y «futura»— en este sentido. Por un lado, en lo que respecta a la normativa vigente, acudo a lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[9] y, en particular, en su artículo 13 al señalar que los menores de edad mayores de catorce años podrán prestar el consentimiento para el tratamiento de sus datos de carácter personal.

Al hablar de normativa «futura», nos referimos al Reglamento Europeo sobre protección de datos que si bien entró en vigor el 25 de mayo de 2016, no resultará de plena aplicación hasta el 25 de mayo de 2018. En concreto, el artículo octavo del referido Reglamento Europeo sobre protección de datos señala que «Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la

---

[9] Publicado en el Boletín Oficial del Estado de 19 de enero de 2008 (en adelante, también, «el RLOPD»).

medida en que se dio o autorizó. O, dicho de otra manera, fija la edad para prestar el consentimiento en los dieciséis años[10]».

A día de hoy el problema no es la edad —catorce o dieciséis— sino la manera de verificar que el usuario que se registra tiene la edad que afirma tener. Si bien la solución más eficaz sería la generalización del uso del DNI electrónico —también por parte de los menores, pero con unos atributos más limitados que los de los adultos—, actualmente estamos muy lejos de que el uso generalizado del DNI electrónico sea una realidad.

Sabedor de la dificultad de verificación de edad de acceso a los servicios prestados por vía electrónica, tanto el legislador español como el europeo tratan esta cuestión afirmando, respectivamente que «Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales» (artículo 13.4 del Reglamento de la LOPD) y que «El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible» (artículo 8.2. del Reglamento Europeo de Protección de Datos).

Por todo ello, y pese a que el deber de verificar la edad exigida recae en el responsable del servicio[11], en nuestra opinión es necesario

---

[10] Ha de tenerse presente que el Reglamento Europeo de Protección de Datos es de aplicación a todo el territorio de la Unión Europea. En el caso de Estados Unidos —por ser el país con mayor número de usuarios de Redes Sociales— hemos de atenernos a lo dispuesto por la conocida por sus siglas como COPPA (Children Online Privacy Protection Act) que fija la edad mínima para que los menores presten el consentimiento en los trece años.

[11] Compartimos lo afirmado por Jules Polonetsky, director de «The Future of Privacy Forum», quien en la 31 Conferencia Internacional de Protección de Datos y Privacidad celebrada en Madrid en mayo de 2009, y repasando el estado de la tecnología en lo que se refiere a sistemas de verificación de la edad, indicaba que «la más tradicional son las páginas web que sólo solicitan la edad como único requisito, "con lo que se puede mentir"; pero existen otras técnicas como la invitación en una red social por un igual, el análisis semántico, los códigos de identificación (eID), o los datos biométricos». No sólo compartimos sino que consideramos más que necesario que los

que padres, profesores y demás agentes que traten con menores desarrollen una labor de concienciación y sensibilización sobre un uso adecuado —y cumpliendo las normas— de las Redes Sociales.

responsables de las Redes Sociales implementen medidas y mecanismos para, cuánto menos dificultar, el acceso de menores a sus plataformas. Información disponible en http://www.privacyconference2009.org/media/notas_prensa/common/pdfs/051109_4_proteccion_privacidad_menores.pdf. Visitado el 1 de octubre de 2016.

3. DERECHOS DE LOS MENORES. NORMATIVA APLICABLE

Al hablar de los derechos de los menores, comenzamos con una breve alusión al «marco internacional» a través de dos documentos de gran interés a nivel europeo e internacional que, si bien no mencionan de manera expresa a los menores, ha de entendérseles incluidos en sus disposiciones, a saber: por un lado, la Declaración de Derechos Humanos de las Naciones Unidas[12] que, en su artículo 12, afirma que «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques». Y, de otro, la Carta de los Derechos Fundamentales de la Unión Europea[13] cuyo artículo séptimo prevé que «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones».

Yendo un paso más allá, la Constitución Española, en el apartado cuarto de su artículo 39 establece que «Los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos». Y es por ello que en este apartado queremos hacer un recorrido sobre las principales normas que, a nivel nacional, tienen como objeto proteger a los menores de edad, mediante el establecimiento de determinados derechos para ellos —y consecuentes obligaciones para otros agentes como pudieran ser padres, centros educativos u organismos oficiales—, centrándonos en lo que respecta a los derechos de los menores a la hora de usar Internet en general, con todo lo que ello supone en materia de datos de carácter personal, contenido adecuado, uso ilícito etc.

---

12 La Asamblea General de las Naciones Unidas, reunida en París, mediante Resolución de 10 de diciembre de 1948, aprobó la Declaración de Derechos Humanos sin ningún voto en contra pero con ocho abstenciones. Su texto se puede consultar en http://www.un.org/es/documents/udhr/.

13 Proclamación Solemne publicada en el Diario Oficial de las Comunidades Europeas, serie C, de 18 de diciembre de 2000. Su texto se puede consultar en http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

Entrando de lleno en la normativa nacional vigente aplicable a los menores acudimos en primer lugar a la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor[14].

En el primer artículo fija su ámbito de aplicación en los menores de dieciocho años para continuar en el artículo segundo afirmando que el criterio de «interés superior del menor» ha de ser valorado y considerado «como primordial» en todas las acciones y decisiones que le conciernan —ya sea en el ámbito público como en el ámbito privado—. Este criterio de «interés superior del menor» supone y exige que todas las decisiones y acciones que sean adoptadas de cara a los menores han de ser interpretadas y ejecutadas poniendo en primer lugar el interés del menor y que, tal y como establece el apartado cuarto del citado artículo dos de la Ley de Protección Jurídica del Menor «En caso de concurrir cualquier otro interés legítimo junto al interés superior del menor deberán priorizarse las medidas que, respondiendo a este interés, respeten también los otros intereses legítimos presentes. En caso de que no puedan respetarse todos los intereses legítimos concurrentes, deberá primar el interés superior del menor[15] sobre cualquier otro interés legítimo que pudiera concurrir».

Por su parte, el artículo 4 establece el «derecho al honor, a la intimidad y a la propia imagen» de los menores afirmando que, en caso de que la difusión de información o utilización de imágenes de los menores suponga una intromisión ilegítima en la intimidad, honra o reputación de los menores, el Ministerio Fiscal actuará para protegerles[16]. En

---

14 Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor, de modificación del Código Civil y de la Ley de Enjuiciamiento Civil, publicada en el Boletín Oficial del Estado de 17 de Enero de 1996 (en adelante, también, «la ley de protección jurídica del menor»).

15 Llamar la atención de este principio con el apartado f del artículo sexto del Reglamento Europeo sobre Protección de Datos que afirma, al regular la licitud del tratamiento, que sólo será lícito si dicho tratamiento «es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño».

16 Y añadiendo el artículo 4.5 de la citada Ley que «los padres o tutores y los poderes públicos respetarán estos derechos y los protegerán frente a posibles ataques e terceros».

el apartado tercero determina lo que se puede considerar como «intromisión ilegítima» y establece que ésta podrá ser «cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales». Al analizar el tenor literal del artículo cuarto, nos viene a la cabeza la tendencia del «oversharing» de los padres y es que, si bien es cierto que en la Sociedad de la Información y del Conocimiento en la que vivimos el gusto por lo social y por compartir todo tipo de información —personal o no— en forma de imagen, vídeo o audio es generalizado, la realidad es que todo ello ha determinado que algunos padres hayan caído en lo que se ha dado en denominar el «oversharing» —palabra inglesa que describe el hecho de compartir todo tipo de información personal, prácticamente sin límite[17].

Ahondando en esta cuestión, lo que queremos destacar es que el fenómeno del oversharing cobra, si cabe, más importancia cuando la información que se comparte está protagonizada por los menores y es que, si bien no cabe duda de la buena intención de los padres al compartir fotografías y vídeos —tiernos[18], graciosos, llamativos u origi-

---

17 En septiembre de 2016, una madre utilizó Facebook para concienciar a todos los padres sobre los peligros del alcohol. Y, lejos de hacerlo escribiendo un post con los riesgos de abusar de esta bebida o a través de estudios científicos que avalan los perjuicios del mismo, decidió subir una fotografía de su hija adolescente en coma en el hospital tras haber abusado del alcohol. No entramos aquí a juzgar sobre la conveniencia o no de concienciar sobre los peligros del alcohol sino simplemente queremos hacer una llamada de atención sobre la permanencia «casi eterna» de lo subido a la Red y de las consecuencias que puede tener esta fotografía en el futuro de la adolescente. Información disponible en http://www.abc.es/sociedad/abci-facebook-publica-facebook-foto-hija-coma-para-concienciar-peligros-alcohol-201609051722_noticia.html. Visitado el 28 de septiembre de 2016.

18 Este es el caso de una joven austriaca de dieciocho años que, tras haber pedido a sus padres que borrasen todas las fotos que habían subido en Facebook a lo largo de su infancia en todo tipo de situaciones —en el baño, desnuda, dormida etc.— y tras negarse estos, decide denunciarles por haber violado su derecho a la intimidad y a la protección de datos de carácter personal. Aún no se conoce el fallo pero lo que está claro es que es necesario una formación mayor sobre todo lo que implica subir una imagen en Internet y las consecuencias que puede tener en un futuro. Disponible en https://es.noticias.yahoo.com/cumple-18-a%C3%B1os-y-demanda-a-sus-padres-por-todas-140417721.html?soc_src=social-sh&soc_trk=fb. Visitado el 6 de octubre de 2016.

nales— de sus hijos, la pregunta que debemos hacernos es ¿vulnera esta actitud el derecho del menor a la intimidad, el honor y la propia imagen? Creemos que no hay una respuesta taxativa en ninguno de los dos sentidos pero sí que creemos, tal y como abordaremos en el apartado destinado a la acción, obligación y responsabilidad de los padres, que es necesario que hayan recibido una formación sobre el impacto de las imágenes subidas a Internet así como la conveniencia de hacer conscientes tanto a los menores como a los adultos de los derechos y deberes —de unos y de otros— respecto al uso de Internet en general y de las Redes Sociales en particular.

Por último, de la Ley de protección jurídica del menor, nos gustaría destacar el «derecho a la información» que prevé el artículo 5 y cuya redacción —dada por la modificación que experimentó esta Ley en julio del año pasado— incluye una referencia a las tecnologías de la información y la comunicación. En concreto, el apartado primero del citado artículo cinco establece que «Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo», añadiendo la importancia de la alfabetización digital y mediática de cara a permitir que el menor actúe en su vida *online* «con seguridad y responsabilidad» y haciendo hincapié en la posibilidad de «identificar situaciones de riesgo derivadas de la utilización de las nuevas tecnologías de la información y la comunicación así como las herramientas y estrategias para afrontar dichos riesgos y protegerse de ellos».

Finalizando con el análisis de la Ley de Protección Jurídica del menor, simplemente destacar que, no cabe duda de que, de entre los derechos de los menores, en la Sociedad de la Información y la Comunicación en la que vivimos, el derecho a una información adecuada y adaptada a sus necesidades así como el derecho a que se les proporcionen los medios adecuados para protegerse y, en caso necesario, defenderse ante un determinado comportamiento o acción ilícita son derechos imprescindibles para la vida cotidiana del menor que, por sus condiciones de inmadurez e inocencia, puede verse inmerso en un problema de cierta índole relacionado con el uso de las TIC y ante el cual, el Derecho, ha de estar preparado y ofrecerle soluciones.

Por lo que se refiere a la normativa vigente en materia de protección de datos de carácter personal, el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento

de desarrollo de la LOPD otorga a los menores de edad —pero mayores de catorce años— la capacidad de prestar el consentimiento[19] para el tratamiento de sus datos de carácter personal, al afirmar que «Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento[20], salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela».

Para que este consentimiento sea válido, el apartado tercero del citado artículo 13 exige que la información sobre el tratamiento de los datos de carácter personal de los menores para el cual estos deben prestar su consentimiento sea expresada «en un lenguaje que sea fácilmente comprensible por aquéllos». En este punto, quiero hacer una llamada de atención sobre el «cumplimiento» —o no— de las condiciones de uso y políticas de privacidad de las Redes Sociales que existen en la actualidad y cuya edad mínima de acceso son los catorce años, a saber: Instagram, Tuenti, Facebook, Snapchat. Tras haberlas revisado y analizado, creemos que podemos afirmar la total falta de adecuación de las políticas de privacidad e información sobre uso y tratamiento de datos de carácter personal a la exigencia de «lenguaje fácilmente comprensible por los menores». Y es en este punto donde hacemos una llamada de atención sobre lo dispuesto en el Reglamento Europeo de Protección de Datos en el que los conceptos «transparencia», «privacidad por defecto», «información adecuada» y «protección de menores» se alzan como protagonistas.

Por último, simplemente llamar la atención sobre el hecho de que, de todo lo anterior se desprende que, en lo que se refiere al consenti-

---

19 Por su parte, la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen establece en su artículo 3 que «el consentimiento de los menores e incapaces deberá presentarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil».

20 Exige el apartado segundo que el consentimiento al que se refiere que pueden prestar los menores de edad no podrá ir, en ningún caso, dirigido a «recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos».

miento para el tratamiento de los datos de carácter personal de los menores de catorce años, estos necesitarán el consentimiento de los padres o tutores.

Por su parte, la Ley 34/2002, de 22 de julio, de servicios de la Sociedad de la Información y de comercio electrónico[21], aborda el derecho a la información de los menores con una única referencia explícita al control de contenidos para menores que figura en la Exposición de Motivos en la que se afirma que «(…) sólo se permite restringir la libre prestación en España de servicios de la sociedad de la información (...) en los supuestos previstos en la Directiva 2000/31/CE[22], que consisten en la producción de un daño o peligro grave contra ciertos valores fundamentales como el orden público, la salud pública o la protección de los menores». No obstante, consideramos de gran interés esta normativa por cuanto al regular la responsabilidad de los prestadores de servicios de información afirma que deberán actuar en el momento en el que tengan conocimiento de que se está produciendo una actuación inadecuada. Es por ello que, especialmente en el tema de los menores, estos han de ser conscientes de que tienen el derecho —y, en cierta medida, la obligación— a comunicar a los prestadores de servicios —esto es, a los responsables de las páginas en Internet y a los responsables de las Redes Sociales— cualquier uso ilícito o que contravenga las normas o las condiciones de uso de las citadas plataformas —pudiendo hacer uso para ello de los servicios de notificación y comunicación de infracciones que ofrecen todas las Redes Sociales— por cuanto están en su derecho a no ver contenido que no sea adecuado para ellos y, por supuesto, están en su derecho a no verse afectados por un uso ilícito, abusivo o violento por parte de otros usuarios.

En otro orden de cosas, queremos citar brevemente lo dispuesto por la Ley 7/2010, de 31 de marzo, General de la Comunicación Au-

---

21 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, publicada en el Boletín Oficial del Estado de 12 de Julio de 2002 (en adelante, también, la «LCE»).

22 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), publicada en el Diario Oficial de la Unión Europea, serie L, de 17 de julio de 2000.

diovisual[23], en concreto en el apartado segundo de su artículo séptimo al afirmar que «está prohibida la emisión en abierto de contenidos audiovisuales que puedan perjudicar[24] seriamente el desarrollo físico, mental o moral de los menores[25], y en particular, programas que incluyan escenas de pornografía o violencia gratuita. El acceso condicional debe posibilitar el control parental». No obstante, conviene tener en cuenta que únicamente quedarán obligados a observar lo dispuesto por esta normativa los prestadores de servicios de la sociedad de la información, en aquellos casos en los que emitieran a través de sus plataformas electrónicas contenidos para adultos en formato audiovisual, pero en ningún caso si éstos se encuentran en formato imagen —fotografías, revistas *online*, etc.— y/o textos.

No podemos dejar pasar este apartado sin hacer una referencia expresa al secreto de las comunicaciones que, con la calidad de derecho fundamental, se encuentra recogido en el apartado 3, del artículo 18 de la Constitución Española, al señalar que «se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

Queremos destacar que este derecho, contemplado en el Título Primero de la Constitución Española («de los derechos y deberes fun-

---

23 Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual, publicada en el Boletín Oficial del Estado de 1 de abril de 2010.

24 Traemos a colación en este punto lo dispuesto por el Decreto 25/2007, de 6 de febrero, por el que se establecen medidas para el fomento, la prevención de riesgos y la seguridad en el uso de Internet y las tecnologías de la información y la comunicación (TIC) por parte de las personas menores de edad, de la Comunidad Autónoma de Andalucía en la que se establece expresamente en su artículo 5 b) que «se consideran contenidos inapropiados e ilícitos los elementos que sean susceptibles de atentar o que induzcan a atentar contra la dignidad humana, la seguridad y los derechos de protección de las personas menores de edad y, especialmente, en relación con los siguientes —entre otros—: b) Los contenidos violentos, degradantes o favorecedores de la corrupción de menores, así como los relativos a la prostitución o la pornografía de personas de cualquier edad».

25 En este mismo sentido se pronuncia la Children's Advertising Review Unit (CARU). Se trata de un Código de buenas prácticas aprobado en 2001 por la Federal Trade Commission americana e impulsado por la industria de la publicidad con el objetivo de proteger a los menores respecto a los contenidos publicitarios a los que puedan estar expuestos.

damentales»), se encuentra elevado a la calidad de «derecho fundamental» con todo lo que lleva consigo este especial tipo de derechos y su protección jurídica.

Respecto al secreto de las comunicaciones, establece la Ley General de Telecomunicaciones[26] que los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución Española.

Queremos finalizar el apartado relativo a la normativa aplicable en España con una normativa que, si bien otorga un plazo de dos años desde el pasado 25 de mayo que entró en vigor para que resulte plenamente aplicable y no es de aplicación exclusivamente española sino de ámbito europeo, por su importancia se merece una reseña en este punto. Como no podía ser de otra manera, nos estamos refiriendo al Reglamento Europeo sobre Protección de datos y que tiene por objeto actualizar la ya obsoleta Directiva 95/46/CE[27] en materia de protección de datos de carácter personal y dotar de seguridad jurídica a cuestiones tan generalizadas actualmente como son el *cloud computing* o las Redes Sociales, destacando las novedades a incorporar en materia de protección de menores.

Antes de entrar en el articulado, consideramos conveniente destacar algunos considerandos del Reglamento Europeo sobre protección de datos, de cuyo contenido se deriva la clara vocación de protección de los menores en lo que respecta al uso de las Tecnologías de la Información y las Comunicaciones así como el aumento de la transparencia, la mejora de la información proporcionada respecto al tratamiento de los datos de carácter personal y el establecimiento de la privacidad por defecto y de la privacidad desde el diseño.

---

26 Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, publicada en el Boletín Oficial del Estado de 10 de mayo de 2014.

27 Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, publicada en el Diario Oficial de la Unión Europea, serie L, número 281, de 23 de noviembre de 1995.

Comenzamos con el Considerando 38 que exige una protección específica de los datos personales de los menores[28], especialmente en lo que se refiere al uso de datos de carácter personal de niños "con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño".

En la misma línea de protección específica se centra el Considerando 58, poniendo el acento en la transparencia y en la necesidad de informar, especialmente a los menores, de una manera fácilmente accesible y fácil de entender, concretando que, en el caso de los niños «cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender».

Entrando ya de lleno en el contenido del tantas veces señalado Reglamento Europeo sobre protección de datos, traemos a colación en primer lugar lo dispuesto por el artículo octavo que lleva por nombre «Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información» y cuyo primer apartado reza así: «Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó». De esta afirmación se desprende que el consentimiento para tener una cuenta en Redes Sociales se situaría en los dieciséis años de edad —y no en los catorce en los que está fijado actualmente por la normativa española—.

En todo caso, hay que esperar a ver cómo reaccionan los Estados Miembros y qué edad establecen por cuanto el Reglamento Europeo de Protección de Datos establece que «Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años» pero, a todas luces, lo que queda claro es que

---

[28] Justificando esta protección «adicional» en que «pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales».

el legislador europeo es consciente de la necesidad de proteger a los menores de los peligros de las Tecnologías de la Información y las Comunicaciones (TIC) y de todas las herramientas y aplicaciones en que se concretan.

En este mismo sentido, y tratando de dar solución a situaciones en las que el menor haya proporcionado datos de carácter personal sin ser consciente del impacto que esa información subida a Internet podía causarle en un futuro, incluye el artículo 17, en concreto en su primer apartado, lo que muchos consideran un nuevo derecho «el derecho a la supresión y al olvido». En concreto, el primer apartado del citado artículo diecisiete afirma[29] que «El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando (…) f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1» o, dicho de otra manera, cuando los datos hayan sido obtenidos de los menores consecuencia de la prestación de un servicio de la sociedad de la información.

Asimismo, el Reglamento Europeo sobre protección de datos incorpora otra serie de novedades que, si bien no están destinadas específicamente a los menores de edad, sí que van a suponer un cambio para ellos. Entre estas, queremos destacar la «privacidad por defecto» y la «privacidad desde el diseño» y es que en el Reglamento Europeo de Protección de Datos se establece la necesidad de que todas las aplicaciones y herramientas TIC tengan configurada por defecto y desde el diseño —sin que el usuario tenga que modificar aspecto alguno de la política de privacidad ni de las condiciones de uso—, a favor de la privacidad del usuario, la herramienta en cuestión. Y decimos que esta novedad, pese a ser aplicable a todas las aplicaciones y herramientas —y no sólo las destinadas a menores—, va a suponer un

---

[29] Llama la atención el cambio de redacción respecto a la Propuesta de Reglamento en la que el citado artículo 17 rezaba: «El responsable del tratamiento tendrá la obligación de suprimir los datos personales sin demora injustificada, especialmente en relación con los datos personales recogidos cuando el interesado era niño, y el interesado tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le conciernan sin demora injustificada».

cambio para los menores ya que ellos no tienen la madurez necesaria para pensar en el valor de sus datos de carácter personal y en el carácter oneroso de los proveedores de las Redes Sociales y de las demás herramientas de Internet y, por tanto, ni se plantean la posibilidad que tienen de cambiar las opciones de privacidad y de compartir datos de carácter personal que vienen «de base», es decir, «por defecto», en la aplicación en cuestión.

De todo ello se desprende, como anticipábamos al comienzo, el deseo, la preocupación y el ánimo del legislador europeo[30] de dotar de la suficiente seguridad jurídica a realidades que hace 20 años —cuando se aprobó la todavía vigente Directiva 95/46/CE sobre protección de datos, ya referida— eran impensables y que, hoy en día, son una realidad generalizada tanto para adultos como para menores, con todo lo que ello conlleva.

---

30 De gran interés resulta conocer el Informe llevado a cabo por la Unión Europea en julio del presente año que bajo el título «Ciberbullying among young people» ofrece una visión y análisis detallado de todas las cuestiones de interés en la materia: definiciones, estadísticas, cifras, medidas legislativas adoptadas en el seno de la UE en este sentido y acciones adoptadas, entre otras. Disponible en http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf. Visitado el 12 de octubre de 2016.

4. NORMATIVA Y DERECHO APLICABLE FUERA DE LA UNIÓN EUROPEA: BREVE RESEÑA

Dada la globalidad de las Tecnologías de la Información y las Comunicaciones, y sin pretender un exhaustivo rigor jurídico, en forma superficial, solamente con el ánimo de «llamada de atención», queremos hacer una breve reseña a algunos aspectos normativos que, fuera de nuestras fronteras, regulan, directa o indirectamente, determinados aspectos relacionados con las TIC y su uso por parte de los menores.

En Estados Unidos, destacamos la aprobación, en 1998, de la Children's Online Privacy Protection Act (COPPA)[31], convirtiéndose en una de las primeras normas a nivel internacional centradas en la protección de los menores en lo que respecta al tratamiento de sus datos de carácter personal[32], en concreto, de los menores de trece años. Para ello, incluye una serie de mecanismos para que los padres puedan controlar la información personal que se recaba de sus hijos así como una serie de medidas para proteger y dotar de seguridad jurídica la presencia de los menores en Internet.

---

31 Texto completo disponible en http://www.ecfr.gov/cgi-bin/text- idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5. Visitado el 10 de octubre de 2016.

32 Esta Ley tiene su origen en el «Web of Deception: Threats to Children from Online Marketing» informe realizado en el año 1996 por la asociación Center for Media Education que tenía por objeto analizar las prácticas de recogida de datos de menores en Internet. Tras conocer los resultados de este informe, la FTC (Federal Trade Commision) llevó a cabo una campaña de supervisión que puso de relieve la existencia de numerosos defectos en el tratamiento de datos personales de menores (entre las que se encontraban la ausencia de políticas de privacidad o la falta de consentimiento parental, entre otras) y que derivó en una petición al Congreso para regular esta materia; petición que se convertiría en la citada COPPA. Disponible en http://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/10.pdf. Visitado el 9 de octubre de 2016.

Más allá de lo dispuesto en la COPPA, consideramos de interés traer a colación que, en lo que se refiere no al tratamiento de datos de los menores sino al acceso por los menores a contenido no adecuado para su edad en Internet, destaca la conocida como CIPA —siglas que responden al nombre completo de la norma: *Children's Internet Protection Act, CIPA*— que, vio la luz en el año 2000 con el objeto de proteger a los menores respecto a la información a la que acceden —o pueden llegar a acceder— en la Red, resultando de aplicación esta normativa tanto a los Centros educativos como a las bibliotecas.

Por otra parte, el Congreso de Taiwán ha aprobado una normativa que permitirá multar a los padres[33] que dejen a sus hijos menores de dieciocho años «usar el móvil en exceso». La multa prevista en caso de incumplir la normativa supera los 1.500 dólares.

Paraguay, por su parte, se encuentra en trámites de aprobación del Proyecto de Ley «De protección de niños, niñas y adolescentes contra contenidos nocivos de internet» que, tras ser objeto de algunas modificaciones por parte del Senado el 5 de mayo del presente año, aún no ha sido aprobada pero que, como su propio nombre indica, tiene como objetivo «establecer una regulación jurídica para la protección de niños, niñas y adolescentes de aquellos contenidos inapropiados para ellos, que son difundidos por internet en lugares de acceso público»[34].

En Colombia hay que acudir a lo dispuesto por la Ley Estatuaria 1581 de 2012 de Protección de Datos Personales[35] que, en su artículo séptimo bajo el título «Derechos de los niños, niñas y adolescentes» reza «Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública» y continua afirmando que «Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los repre-

---

33 No hace falta irnos tan lejos. Y es que, en Inglaterra e Irlanda los tribunales de menores pueden imponer sanciones a padres y tutores si se prueba que una falta deliberada en el cuidado y control del niño ha contribuido a la conducta delictiva del menor.

34 Información obtenida de http://www.senado.gov.py/index.php/noticias/173963-resultados-de-la-sesion-ordinaria-4-2016-05-05-17-24-03. Visitado el 13 de octubre de 2016.

35 Texto completo disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. Visitado el 13 de octubre de 2016.

sentantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás».

En el Salvador, hay que acudir a la Ley de Protección Integral de la Niñez y de la Adolescencia que fue promulgada en el año 2009 y cuyo artículo 46 reza que «se prohíbe, a través de cualquier medio, divulgar, exponer o utilizar la imagen de niñas, niños y adolescentes en contra de su voluntad y sin el conocimiento y aprobación de sus madres, padres, representantes o responsables. Asimismo, se prohíbe exponer o divulgar datos, imágenes o informaciones que lesionen el honor o la reputación de las niñas, niños y adolescentes o que constituyan injerencias arbitrarias o ilegales en su vida privada o intimidad personal y familiar».

Dada la importancia y, por desgracia, presencia cada vez más generalizada, hemos considerado oportuno citar algunas normativas que, específicamente, abordan el tema del *ciberbullying*. Y es que, son muchos los países que, lejos de nuestras fronteras, ya contemplan y regulan el ciberacoso, destacamos las siguientes:

— En Chile, la Ley General de Enseñanza para reglamentar y prevenir la violencia escolar o el *bullying*, fue modificada en septiembre de 2011 con el objeto de «promover la buena convivencia escolar y prevenir toda forma de violencia física o psicológica, agresiones u hostigamientos», incluyendo de manera específica el ciberacoso.

— El estado de Illinois en EEUU[36] ha aprobado una ley —que entró en vigor el 1 de enero de 2015— que prevé que las escuelas de dicho estado puedan exigir las contraseñas de las Redes Sociales de los alumnos que rompan la normativa del establecimiento, o que se sospeche que cometen *ciberbullying*.

---

[36] Respecto a la normativa en materia de *cyberbullying* existente en Estados Unidos llamamos la atención sobre un cuadro elaborado por el Cyberbulling Research Centre en el que se pueden consultar en qué Estados de EEUU existen leyes contra el ciberacoso, entre estos estados se encuentran: Alaska, Alabama, California, Arizona, Florida o Delaware, entre otros. Disponible en http://cyberbullying.org/bullying-laws. Visitado el 1 de octubre de 2016.

— En Puerto Rico se modificó la Ley Orgánica del Departamento de Educación de Puerto Rico para incluir penas a los estudiantes que ciberacosaran a otros compañeros. Las penas incluyen días de suspensión de asistencia y multa económica.

— En República Dominicana nos encontramos con la Ley 53/007, de 23 de abril, sobre Crímenes y Delitos de Alta Tecnología. Pese no hablar de manera directa sobre el ciberacoso sí que, en varios de sus artículos —baste uno por todos, en concreto, el artículo 22 que reza «la injuria pública cometida a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones o audiovisuales, se sancionará con la pena de tres meses a un año de prisión y multa de cinco a quinientas veces el salario mínimo»— habla sobre el uso de las TIC con fines fraudulentos, maliciosos o ilegales.

— En Colombia, tenemos que acudir a lo dispuesto por la Ley 1620, de 15 de marzo de 2013, por la cual se crea el Sistema Nacional de Convivencia escolar y formación para el ejercicio de los derechos humanos, la educación para la sexualidad y la prevención y mitigación de la violencia escolar en la que, en su artículo 8, entre las tareas asignadas al Comité Nacional de Convivencia Escolar establece la de «Coordinar la creación de mecanismos de denuncia y seguimiento en Internet, Redes Sociales y demás tecnologías de información a los casos de *ciberbullying*».

— En México DF, la Ley para la promoción de la convivencia libre de violencia en el entorno escolar fue aprobada en 2011 y tiene como objeto luchar contra toda clase de acoso escolar, con independencia de que en el acoso se haga uso de las Tecnologías de la Información y las Comunicaciones o no.

— Por su parte, en Argentina, el Instituto Nacional Contra la Discriminación, la Xenofobia y el Racismo (INADI) ha creado un Observatorio de Redes Sociales para poder «detectar, denunciar y combatir el ciberacoso».

No queremos hacer aquí un barrido y análisis pormenorizado de todas las normas que versan sobre el uso de las TIC por los menores en todo el mundo sino simplemente hacer una llamada de atención sobre el uso generalizado, sin limitación geográfica, de este tipo de herramientas y la necesidad de proteger a los menores en todo momento y lugar.

5. ASPECTOS PENALES

Hemos querido dedicar un apartado específico a la regulación de aspectos penales de conductas en Redes Sociales para dejar a un lado la falsa concepción de «Impunidad» de lo que acontece en Internet en general y en las Redes Sociales en particular. Por ello, traigo a colación en este punto las cuestiones que, de manera específica, están previstas en el Código Penal español[37] —teniendo como referencia la reforma acontecida en marzo del pasado año 2015—.

En primer lugar, destacamos el caso del conocido como «grooming», esto es, aquella conducta en la que un adulto, normalmente haciéndose pasar por un niño, contacta con un menor de edad para obtener de él favores de carácter sexual y/o pornográfico. Desgraciadamente, en los últimos años este tipo de delitos ha proliferado en nuestro país y el legislador no ha dudado en incorporarlo al Código Penal de manera que se trata de un delito tipificado, en concreto, en el artículo 183 bis del Código Penal.

Si bien no está definido como delito de «grooming» lo cierto es que el artículo 183 bis establece que «El que, con fines sexuales, determine a un menor de dieciséis años a participar en un comportamiento de naturaleza sexual, o le haga presenciar actos de carácter sexual, aunque el autor no participe en ellos, será castigado con una pena de prisión de seis meses a dos años. Si le hubiera hecho presenciar abusos sexuales, aunque el autor no hubiera participado en ellos, se impondrá una pena de prisión de uno a tres años». Además, la reforma señalada del Código Penal, del año 2015, incorpora un artículo 183 ter, con el siguiente contenido: «1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la co-

---

[37] El Código Penal español (en adelante, también, «el Código Penal»), se encuentra recogido en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicada en el Boletín Oficial del Estado de 24 de noviembre, modificada por la Ley Orgánica 1/2015, de 30 de marzo, publicada en el Boletín Oficial del Estado de 31 de marzo.

municación[38] contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño. 2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años».

Otra de las conductas que, desgraciadamente, también están teniendo lugar en y a través de las Redes Sociales es la llamada «sextorsión», esto es, el uso de imágenes de contenido erótico o sexual para chantajear a la persona fotografiada. En este sentido, la ya citada reforma del Código Penal operada por la Ley 1/2015, incluye una referencia a este tipo de situaciones al afirmar, en el apartado séptimo del artículo 197 que «Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa».

---

[38] Llamamos la atención en este punto sobre el caso de Suecia en este sentido que, tras varios años de debate, tiene previsto penar «los abusos sexuales online con hasta diez años de cárcel». Así lo ha puesto de manifiesto el ministro de justicia que prevé que esta normativa entre en vigor en 2018. Disponible en http://www.elmundo.es/sociedad/2016/10/05/57f53d0ee2704e79678b45b0.html. Visitado el 7 de octubre de 2016.

Por último, en lo que respecta a la suplantación de identidad, partimos de la base de que en el ordenamiento jurídico español la suplantación de identidad está tipificada como delito, si bien no de manera expresa. En este sentido, traemos a colación en este punto los dos artículos del Código Penal español que versan sobre suplantación de identidad aunque, en mi opinión, resultan insuficientes para hacer frente a una actividad, por desgracia tan extendida, como es la propia suplantación de identidad en red[39] por los propios menores que falsean su edad para poder acceder a las Redes Sociales, todo ello sumándole la falta de responsabilidad penal de los menores de catorce años según nuestro ordenamiento jurídico. Planteado el problema y la obsolescencia de nuestra norma que no se adapta a este tipo de faltas y delitos TIC cometidos por y entre menores, baste traer a colación lo dispuesto en el artículo 401 del Código Penal[40].

En todo caso, es necesario partir de la base de que no existe un delito ni una falta tipificada en el Código Penal como «suplantación de identidad» sino que hemos de realizar la analogía con el tipo de «suplantación del estado civil» previsto en el artículo 401, donde se dispone que «El que usurpare el estado civil de otro será castigado

---

39 Prueba de la importancia y desgraciado aumento en la presencia de conductas de suplantación de identidad, es que la propia Fiscalía General del Estado propone tipificar el delito de suplantación de identidad en Internet. Esta propuesta la ha plasmado en la Memoria que el Fiscal General presentó a mediados de septiembre de 2014 en la Apertura del Año Judicial ante el Rey Felipe VI. Afirma la Fiscalía la necesidad de tipificar estos comportamientos dada la potencialidad que ofrece Internet (entre los que cita las Redes Sociales de manera expresa) para difundir información a una pluralidad de personas en cualquier lugar del mundo —pudiendo, con ello, lesionar gravemente los derechos de los afectados—. En este sentido, propone que el Código Penal castigue con una pena de seis meses a dos años de prisión o multa de seis a veinticuatro meses «a quien suplante la identidad de una persona física realmente existente utilizando sus datos identificativos a través de Internet, medio electrónico o sistema informático en línea, de tal modo que genere error sobre la intervención en esos medios de la persona suplantada». Disponible en http://noticias.lainformacion.com/policia-y-justicia/arbitraje/las-claves-del-informe-de-la-fiscalia-general-del-estado-mas-delitos-economicos-mas-corrupcion-menos-violencia_58IK406floslVPhuP0Q9o5/. Visitado el 10 septiembre de 2016.

40 Artículo que indica que «el que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años».

con la pena de prisión de seis meses a tres años». Puesto que este no es el objeto del presente trabajo, simplemente destacar que, además de que la norma no pone énfasis ninguno en la necesidad de que esta usurpación se lleve a cabo haciendo o no uso de medios electrónicos (o, dicho con otras palabras, de manera *offline* u *online)* es necesario que se den varias notas para poder hablar del tipo previsto en el artículo 401 del Código Penal, bastando para ello traer a colación el Fundamento de derecho segundo de la Sentencia de la Sala Segunda del Tribunal Supremo de 15 de junio de 2009 que afirma que «Usurpar el estado civil de otro lleva siempre consigo el uso del nombre y apellidos de ese otro, pero evidentemente requiere algo más, sin que sea bastante la continuidad o la repetición en el tiempo de ese uso indebido para integrar la mencionada usurpación (...)».

Por tanto, «para usurpar no basta con usar un nombre y apellidos de otra persona, sino que es necesario hacer algo que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden; como puede ser el obrar como si uno fuera otro para cobrar un dinero que es de este, o actuar en una reclamación judicial haciéndose pasar por otra persona, o simular ser la viuda de alguien para ejercitar un derecho en tal condición, o por aproximarnos al caso presente, hacerse pasar por un determinado periodista para publicar algún artículo o intervenir en un medio de comunicación». De todo ello, podemos concluir afirmando que resulta muy difícil que un menor incurra en la comisión de un delito de usurpación por el mero uso del nombre y la fotografía de otro menor en una red social.

Sin embargo, consideramos particularmente interesante la reflexión ofrecida por Hurtado Bueno quien, en un artículo publicado en el sitio web de INTECO[41], afirma que «si bien el crackeo de una cuenta de Facebook o Twitter, por ejemplo, por sí misma no es una suplantación de identidad constitutiva del delito de usurpación del estado civil, sí podría ser constitutiva de un delito de descubrimiento

---

41 Información extraída del artículo «Suplantación de identidad en Internet: aspectos penales» escrito por Alonso Hurtado Bueno el 7 de diciembre de 2011 y disponible en http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Post_suplantacion. Visitado el 13 de septiembre de 2016.

y revelación de secretos, regulado expresamente en los artículos 197 y siguientes del Código Penal o incluso un delito de daños en "redes, soportes o sistemas informáticos" expresamente reconocido en el artículo 264.2 del Código Penal».

Destacamos, asimismo, el artículo 172 ter del Código Penal que reza así:

«Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.»

No se trata de un acoso «tipo», de hecho, precisamente por sus especiales requisitos, se le conoce por el anglicismo «stalking»[42].

Si bien no se trata de un delito vinculado únicamente a las Redes Sociales, ni siquiera a Internet en general, sí que hemos considerado conveniente incluirlo en este punto por cuanto el objeto del delito —el acoso reiterado— sí que puede llevarse a cabo haciendo uso de las Tecnologías de la Información y las Comunicaciones. Y, de hecho, en muchas ocasiones, la cuasi-omnipresencia de las TIC en la vida de

---

[42] *Stalking* es una voz anglosajona que significa acecho y que describe un cuadro psicológico conocido como síndrome del acoso apremiante. El afectado, que puede ser hombre o mujer, persigue de forma obsesiva a la víctima: la espía, la sigue por la calle, la llama por teléfono constantemente, la envía regalos, la manda cartas y sms, escribe su nombre en lugares públicos y, en casos extremos, llega a amenazarla y a cometer actos violentos contra ella. Disponible en http://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-el-stalking. Visitado el 11 de octubre de 2016.

todos los ciudadanos —mayores o menores de edad[43]— puede convertirse, en este caso, en un arma de doble filo en el que, lejos de suponer una ventaja y una mejora en su calidad de vida, se convierta en una de las principales causas de su tristeza, agobio, angustia o ansiedad.

Este artículo fue introducido por la reforma del Código Penal del año 2015 y viene, en nuestra opinión, este artículo a dar cabida a todas aquellas actuaciones —molestas y altamente dañinas— que, sin duda, causan un menoscabo en la víctima —menor o mayor de edad—, tanto en lo que respecta a su propia libertad como a su dignidad y seguridad. Y es que, tal y como establece el propio artículo, las acciones llevadas a cabo con objeto de acosar incesantemente llevan aparejada la alteración grave del desarrollo de su vida cotidiana.

Por último, simplemente tener en cuenta que, puesto que se trata de una figura «exnova», habrá que esperar a ver en qué sentido se pronuncian nuestros Tribunales para conocer qué ha de entenderse por lo que, a nuestro juicio, a día de hoy se antojan como «conceptos jurídicos indeterminados» como: «acoso incesante y reiterado» y «alteración grave de la vida cotidiana».

En conclusión, ha de quedar claro que las acciones delictivas que se cometen en, a través o haciendo uso de Internet y las Redes Sociales no quedan impunes; hay una normativa que hay que cumplir y unos derechos que hay que respetar y, en caso de no hacerlo, el Código Penal prevé, en algunos casos de manera específica y en otros tangencialmente, multas y penas de cárcel para aquellos que cometan alguno de los actos delictivos tipificados.

En nuestra opinión, con la ya tantas veces referida reforma operada en el Código Penal en marzo de 2015 se dio un gran paso para avanzar en la posición del Derecho respecto al uso de las TIC pero aún queda camino por recorrer y es necesario dotar de una mayor seguridad jurídica a todos los usuarios de Internet en general y de las Redes Sociales en particular, ya sean adultos o menores de edad; si

---

43 Si bien no se trata de una conducta relacionada exclusivamente con menores, el propio artículo 172 ter hace una referencia a la edad de la víctima al afirmar que «Si se trata de una persona especialmente vulnerable por razón de su edad,enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años».

bien es cierto que, en el caso de los menores de edad, por su situación de inmadurez e indefensión, la urgencia de protección y seguridad jurídica es, si cabe, aún mayor.

5.1. RESPONSABILIDAD PENAL DE LOS MENORES

Hablando de la actuación de los menores en Internet y de la posibilidad de cometer acciones que vulneren la normativa vigente —independientemente o no de que hayan sido tipificados como delitos en el Código Penal— es necesario hacer una alusión a la responsabilidad penal de los menores de edad. Y es que, dependiendo del país en el que nos encontremos, el menor autor de un delito, habrá de ser considerado o no responsable penal de sus actos.

En el caso de España, hay que atender a lo dispuesto tanto por el Código Penal como por la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores[44] que fija su ámbito de aplicación en los «mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas[45] en el Código Penal»[46]. Y es que, el Código Penal, en su artículo 19 lo único que dispone referente a los menores de edad es que «Los menores de dieciocho años no serán responsables criminalmente con arreglo a este Código. Cuando un menor de dicha edad cometa un hecho delictivo podrá ser responsable con arreglo a lo dispuesto en la ley que regule la responsabilidad penal del menor».

---

44 Publicada en el BOE núm. 11, de 13 de enero de 2000.

45 Téngase en cuenta que la reforma de 2015 del Código Penal ha suprimido las faltas y ha incluido los llamados «delitos menores».

46 Llama la atención ver cómo, cuando se aprobó el vigente Código Penal —en 1995— no existía una ley sobre responsabilidad penal del menor y el legislador, mediante la inclusión de la Disposición Transitoria Duodécima estableció que: «Hasta la aprobación de la ley que regule la responsabilidad penal del menor, en los procedimientos que se sustancien por razón de un delito o falta presuntamente cometido por un menor de dieciocho años, el Juez o Tribunal competente requerirá a los equipos técnicos que están al servicio de los Jueces de Menores, la elaboración de un informe sobre la situación psicológica, educativa y familiar del menor, así como sobre su entorno social y, en general, sobre cualquier otra circunstancia que pueda haber influido en el hecho que se le imputa».

Combinando lo dispuesto en ambas normas, cabe concluir que los menores de catorce años no serán responsables penalmente de los delitos que cometan. Hacemos una llamada de atención en este sentido puesto que, en el caso de los delitos cometidos en y/o a través de Redes Sociales, no son infrecuentes los casos en los que las acciones que vulneran las normas sean cometidas por personas menores de catorce años[47]. Consideramos necesario que se haga un mayor hincapié en la necesidad de formación de los menores para prevenir y erradicar la comisión de estos delitos puesto que, en nuestra opinión, en muchos casos son cometidos con total ignorancia del autor sobre la comisión de un delito.

No obstante, el que no sean responsables penalmente y, en el caso de España, no puedan ir a la cárcel, no es óbice para que la ley de responsabilidad penal del menor establezca una serie de medidas para los menores de edad que son autores de conductas delictivas. En todo caso, ha de quedar claro que el objetivo de esta norma es lograr la reinserción del menor en la sociedad y, por ello, se habla de medidas y acciones encaminadas a lograr dicho objetivo.

Por último, en lo que respecta a la responsabilidad penal de menores de edad —siempre que sean mayores de catorce años— haremos una alusión a las medidas y acciones que se contemplan y regulan en el artículo 7 de la Ley de responsabilidad penal del menor y entre las que cabe destacar, las previstas en las letras a) a ñ), a saber: Internamiento en régimen cerrado; Internamiento en régimen semiabierto; Internamiento en régimen abierto; Internamiento terapéutico en régimen cerrado; Tratamiento ambulatorio; Asistencia a un centro de día; Permanencia de fin de semana; Libertad vigilada; La prohibición de aproximarse o comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el Juez; Convivencia con otra persona, familia o grupo educativo; Prestaciones en beneficio de la comunidad; Realización de tareas socio-educativas; Amonestación;

---

47 Conviene tener en cuenta que, según lo dispuesto por el artículo 3 de la Ley de responsabilidad penal del menor cuando el autor de los delitos sea menor de catorce años «no se le exigirá responsabilidad con arreglo a la presente Ley, sino que se le aplicará lo dispuesto en las normas sobre protección de menores previstas en el Código Civil y demás disposiciones vigentes».

Privación del permiso de conducir ciclomotores y vehículos a motor, o del derecho a obtenerlo y, por último, la inhabilitación absoluta.

Reza el apartado tercero del citado artículo séptimo que «Para la elección de la medida o medidas adecuadas se deberá atender de modo flexible, no sólo a la prueba y valoración jurídica de los hechos, sino especialmente a la edad, las circunstancias familiares y sociales, la personalidad y el interés del menor, puestos de manifiesto los dos últimos en los informes de los equipos técnicos y de las entidades públicas de protección y reforma de menores cuando éstas hubieran tenido conocimiento del menor por haber ejecutado una medida cautelar o definitiva con anterioridad, conforme a lo dispuesto en el artículo 27 de la presente Ley». Por último, y como no podía ser de otra manera, se hace hincapié en el deber del juez de explicar motivadamente en la sentencias las razonas «por las que aplica una determinada medida, así como el plazo de duración de la misma, a los efectos de la valoración del mencionado interés del menor».

Por último, y puesto que el objetivo de este apartado no es hacer un estudio exhaustivo y detallado sobre la responsabilidad penal del menor sino hacer una breve alusión en la que queden claras sus implicaciones y diferencias según en el territorio en el que nos encontremos, hacemos un breve recorrido por la regulación de la edad del menor para poder ser considerado «responsable penal» de sus acciones, tanto en la Unión Europea como en Estados unidos.

En nuestro país vecino —Francia— la edad penal para que los menores sean responsables ha quedado fijada en los trece años. Aunque, lo que más llama la atención, es que no existe una normativa específica para menores sino que, en el caso de la comisión de un delito, a estos les resultan de aplicación las mismas penas que si aquél hubiese sido cometido por un adulto, eso sí, con la correspondiente atenuación de la pena teniendo en cuenta las especiales características del menor.

Bien distinto es lo que sucede en Holanda donde si el delito es cometido por un menor de doce años se desestima automáticamente. Y es que en los países bajos se considera un niño menor de 12 años no tiene capacidad para cometer un delito y, en caso de encontrarse en esta situación, se produce una derivación automática del caso a la entidad u organismo protector de menores que corresponda, a saber:

servicios sociales, Consejo para la Protección de la Infancia o servicios médicos, por poner tan solo unos ejemplos.

En la otra cara de la moneda, nos encontramos con Suiza donde se considera penalmente responsable a los menores que hayan cumplido los siete años de edad aunque, en nuestra opinión con acierto, establece un régimen sancionador diferente para niños con edades comprendidas entre los siete y los catorce y otro para los menores que han cumplido los catorce pero no llegan a alcanzar la mayoría de edad.

Por su parte, Italia y Alemania tienen un régimen parecido entre ellas y que, a su vez, nos recuerda a lo dispuesto por la normativa española ya que los catorce años son la edad clave en cuestión de responsabilidad penal. En concreto, el código penal italiano establece que los menores de catorce años son inimputables. Mientras que, en el caso alemán, se establecen tres categorías de responsabilidad penal bien diferenciadas en función de la edad, a saber: los menores de catorce años —considerados incapaces de culpa—; los menores de edad que ya han alcanzado los catorce años y que, por tanto, comienzan a ser responsables penales de sus actos, eso sí, quedando fijada la diferencia entre los menores cuyas edades oscilan entre los 14 y los 17 y los considerados como «semi-adultos», o dicho de otra manera, los que tienen edades que oscilan entre los 18 y los 20 años.

Por su parte, Suecia considera que un menor es responsable penal de sus actos cuando ha cumplido los quince años. Bien distinto es el caso de Bélgica que, si bien establece que los menores de dieciocho años no pueden ser considerados responsables penales de sus actos, sí que prevé —para el caso de comisión de delitos por parte de mayores de doce años pero que no han alcanzado la mayoría de edad— regímenes de internamiento cerrado.

Antes de aludir a lo dispuesto por la normativa estadounidense, llamamos la atención sobre lo dispuesto en la normativa inglesa que, si bien establece el comienzo de la «edad penal», es decir, la edad a la que se comienza a ser responsable de los hechos cometidos, en los diez años, diferencia claramente tres categorías de edad y en función del rango en el que se encuentre su autor, habrá que atenerse a unas u otras medidas. En concreto, la normativa inglesa habla de: menores con edades comprendidas entre los diez y los catorce años (niños); menores con edades comprendidas entre los quince y los dieciséis (jó-

venes) y los llamados «semi-adultos» con edades comprendidas entre los diecisiete y los veinte años de edad.

Finalizamos este apartado con una breve alusión a la realidad estadounidense en este sentido. Y es que, en el caso del país norteamericano, la normativa deja a discreción de cada Estado la fijación de la edad del menor para ser considerado responsable penal. El caso de Estados Unidos es uno de los más llamativos puesto que la «libre elección» de cada Estado para fijar la edad de responsabilidad penal de los menores ha derivado en que, en la práctica, más de treinta Estados[48] no hayan establecido una edad mínima lo que supone —al menos, en un planteamiento teórico— que cualquier persona menor de dieciocho años —tenga la edad que tenga— autora de un delito pueda ser sancionada con penas privativas de libertad, esto es, con penas de cárcel.

Como se desprende de este breve barrido tanto a nivel nacional como internacional de la regulación de la responsabilidad penal de los menores, a día de hoy es de lo más variopinta. Y queremos dejar aquí un interrogante en el aire relacionada con la conveniencia —o no— de la fijación «universal» de la edad a partir de la cual los menores han de ser considerados responsables penales de sus hechos al menos en lo que respecta a sus actuaciones y actitudes relacionadas con las TIC, dada la globalidad y omnipresencia de las TIC para favorecer y garantizar, en la medida de lo posible, la protección del menor víctima de estos delitos, independientemente de la localización geográfica en la que se encuentre.

---

48 Por poner sólo un ejemplo, el Estado de Carolina del norte sí que ha fijado la edad mínima para que los menores de edad puedan ser considerados responsables penales de sus hechos, fijando esta edad en los siete años.

6. MENOR, ¿VÍCTIMA Y/O VERDUGO CON SU PRESENCIA EN REDES SOCIALES?

Para responder a la pregunta que da título a este apartado, haremos un breve recorrido sobre los diferentes problemas que pueden derivarse del uso de las Redes Sociales, anticipando ya que el menor, en función del uso que haga de las Redes Sociales, podrá erigirse en verdugo o, por el contrario y en función de la actitud de otros, convertirse en víctima.

En todo caso, nos referimos a los principales riesgos y problemas a los que, *grosso modo,* se exponen[49] los menores cuando entran a formar parte de Internet en general, mediante una presencia activa, y de una red social de manera particular —sin el debido conocimiento y/o control y asesoramiento por parte de sus padres, tutores o profesores—.

Los principales riesgos son:

• *Cyberbullying*, esto es, ser víctimas de acosos y persecuciones[50] por parte de otros menores. Ésta es la práctica más habi-

---

49 Tal y como indica Ramos Gil de la Haza «Los menores de edad han pasado de comunicarse a través del popular Messenger, que ofrece comunicaciones sincronizadas y privadas entre sus usuarios, a entablar conversaciones asíncronas y públicas o semipúblicas a través del tablón de Tuenti o de Facebook, sin darse cuenta de que en ocasiones están revelando información que podría poner en peligro su integridad física o moral». *Vid.* RAMOS GIL DE LA HAZA, A.: «Sobre tendencias, marketing y las nuevas tecnologías», 2008. Disponible en http://www.dosdoce.com/articulo/opinion/2855/redes-sociales-hacia-la-perdida-de- privacidad-del-individuo/. Visitado el 12 de septiembre de 2016.

50 Llamamos la atención sobre la conveniencia de incluir en la definición de *cyberbullying* la palabra maltrato por cuanto Molina Blázquez indica que «(…) dentro del término maltrato pueden recogerse todos los comportamientos que suponen un ataque directo a la integridad física o salud —tanto física como psíquica— y libertad/indemnidad sexual del menor (…)». *Vid.* MOLINA BLÁZQUEZ, C.: «Protección penal de los menores: los menores víctimas de delito», en *Jornadas sobre derecho de los menores* (Isabel E.

tual[51], dentro de los usos maliciosos que se llevan a cabo en la red de redes entre y por menores, de la que estos son tanto víctimas como verdugos. Y es que, en concreto, se trata de aquella práctica —punible— que consiste en, haciendo uso de medios electrónicos y telemáticos un abuso de un menor a otro. Es necesario destacar que, para que podamos hablar de *cyberbullying* tanto el atacante como el atacado tienen que tener la misma edad o, al menos, el mismo rango de edad, de manera que el objetivo consista en un acoso psicológico «entre iguales». Precisamente por la naturaleza de esta práctica, el *cyberbullying* suele tener lugar en entornos escolares —colegios, institutos, escuelas de formación profesional— y deja una huella psicológica en la víctima que, en muchos casos, no acude a pedir ayudar a sus padres o profesores, por miedo o por vergüenza. En esta situación, hay un menor que actúa como víctima y uno —o varios— menores que actúan como verdugos.

• *Grooming:* término anglosajón con el que se designa el hecho de «ser víctima de un acoso por parte de un adulto con mediación de las TIC». Para hablar de *grooming* se tienen que dar dos notas características: a) que el acosador sea una persona adulta y la víctima un menor y b) que el objeto del acoso sea de carácter sexual, ya sea, conseguir favores sexuales por parte del menor de manera explícita, ya sea la obtención de imágenes de contenido erótico del menor que el acosador subirá a páginas de Internet o intercambiará o venderá a cambio de remuneración económica en foros de pornografía infantil

---

Lázaro González, Ignacio V. Mayoral Narros, coordinadores). Ed. Universidad Pontificia Comillas de Madrid, 2003, p. 286.

51 Por desgracia, esta práctica es mucho más habitual de lo que pudiéramos pensar en un principio y los expertos apuntan a una tendencia al alza en el número de casos de ciberacoso. En este sentido, es necesario que las Autoridades se pongan manos a la obra para frenar esta tendencia de uso malintencionado de las TIC para causar un daño a otros menores. Así lo avalan numerosos estudios, baste como ejemplo el realizado por la aseguradora alemana ARAG en mayo de este año en el que bajo el título «Encuesta sobre riesgos digitales» situaba a España, junto a Italia y Polonia, en las peores posiciones en prevención del ciberacoso tanto en los colegios como en internet. Disponible en http://www.larazon.es/sociedad/espana-a-la-cola-en-proteccion-contra-el-ciberacoso-a-menores-FC12767310?sky=Sky-Octubre-2016#Ttt1Fjj5bCFM09vd. Visitado el 8 de octubre de 2016.

o de pederastia. Sobra decir que, en este tipo de conductas, el menor es siempre la víctima.

• *Sexting:* está compuesta por la unión de dos palabras inglesas que aluden a sus dos elementos principales: de un lado, «Sex» que significa sexo y, de otro, «Texting» gerundio cuya traducción al español es envío de mensajes de texto vía SMS desde teléfonos móviles. Por tanto, el *sexting* consiste en el envío, a través del teléfono móvil, de imágenes fotográficas[52] y vídeos de contenido sexual, realizados generalmente, por el propio usuario. Este es precisamente uno de los mayores riesgos y es que, en un primer momento, no existe ningún tipo de coacción para realizarse la imagen y enviarla sino que se ve como un «regalo», por ejemplo, del usuario a su pareja, su grupo de amigos o a una persona que quiere conquistar o, simplemente, como una manera de «ser socialmente aceptados»[53]. El problema viene cuando «lo que comenzó como un juego» —argumento que arguyen muchos usuarios cuándo se les pregunta el motivo de intercambio de mensajes con contenido erótico— se convierte en una verdadera pesadilla, esto es, cuando, fruto de esa superación de la barrera del «ambiente de confianza» del que hablábamos, el contenido del *sexting* aparece en los dispositivos móviles de decenas, cientos —o miles y millones[54] si se llega a subir a Internet a través de Redes Sociales tan conocidas como Facebook o YouTube—. En este caso, hay un menor

---

52 Aunque el sentido original se limitase al envío de textos, con el desarrollo y la mejora de la tecnología aplicada a los teléfonos móviles —y con mayor motivo con la proliferación de los *smartphones*— actualmente el contenido del *sexting* suele venir protagonizado por imágenes, vídeos y todo tipo de contenido multimedia. Recalcamos aquí también que, quizás la alusión al SMS en la definición del *sexting,* si bien es fiel al significado de «texting», al igual que ocurre con la evolución del texto a la fotografía, la aparición de los MMS en primer lugar y de las aplicaciones como Whatsapp o Line, permiten el envío y la difusión prácticamente instantánea de fotografías, vídeos etc, que, al tratarse de *sexting,* tienen contenido sexual o erótico.

53 En este punto traemos a colación el conocido como síndrome «FOMO» —siglas que responden a las palabras «Fear of missing out» o, lo que es lo mismo, miedo a «quedarse fuera», a que le aíslen, a no quedar integrado.

54 Los motivos por los que esa barrera se ve superada pueden ser de lo más diverso: desde un «desliz» por parte del receptor o emisor del mensaje (pulsar enviar cuando se está sobre un contacto que no es el deseado) hasta un envío intencionado por el receptor.

que es víctima y otro menor protagonista que es verdugo y que, en la mayoría de las ocasiones, al difundir el mensaje hace que otros menores se conviertan, también, en verdugos.

• «Sex-casting»: se trata de una versión del «sexting» puesto que su principal característica y única diferencia respecto al *sexting* es el uso de la webcam para la grabación de contenidos sexuales —y su posterior envío y/o acceso, en principio, a alguien de su confianza o interés—. Sin embargo, al igual que en el *sexting*, en multitud de ocasiones, esos contenidos acaban siendo fruto de difusión generalizada y masiva a través de correo electrónico, Redes Sociales o aplicaciones de mensajería instantánea. Como no podía ser de otra manera, y al igual que ocurría en el caso del *sexting*, hay un menor que es víctima y otro menor que se alza como «verdugo principal» y que suele contar con la colaboración de otros menores que actúan como verdugos.

• Sextorsión: al igual que ocurría en el caso anterior, se trata de una palabra que conjuga las dos que la integran y le dan sentido, a saber: *sex* (de sexo) y «extorsión» que, según la Real Academia Española de la Lengua, es la «presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido». Y es que se trata de una práctica estrechamente relacionada con el *sexting* por cuanto no cabe duda de que las fotografías o vídeos de contenido sexual en poder de la persona inadecuada se alza como una herramienta idónea para extorsionar o, dicho de manera coloquial, chantajear a la persona que los protagoniza. En este sentido, la persona que extorsiona es el verdugo y el menor extorsionado la víctima.

• Ver suplantada su identidad. Se trata de una situación, cada vez más común, entre compañeros de colegio o instituto. El procedimiento es sencillo: se abren un perfil en una red social con algunos datos personales de la víctima: nombre, apellidos y fotografía y, tras añadir a numerosos contactos que, fruto del engaño consideran estar entablando amistad con la víctima y no con la persona que hay detrás rellenan su perfil con informaciones falsas sobre el supuesto titular de la cuenta, añadiendo comentarios en los que critican a otros compañeros, subiendo fotografías que dejan en ridículo y avergüenzan a la víctima y demás acciones encaminadas a crear una mala reputación *online* que, en la mayoría de los casos, suele ser muy difícil de lavar de manera definitiva debido, una vez más, a la rapidez con la que se expande y difunde la información en Internet, muchas veces sin comprobar antes la veraci-

dad de la misma. En este caso, la persona que suplanta la identidad es el verdugo y la que ve suplantada su identidad es la víctima.

• Adicción a las Redes Sociales, con la consecuente pérdida de sociabilidad personal y de contacto con familiares y amigos en el día a día. Aunque en un principio pudiera resultar desorbitada la calificación de «adicción»[55] a lo que muchos llaman «mero gusto» por las Redes Sociales, lo cierto es que, en el caso de los menores, se puede llegar a generar una verdadera adicción[56] a este tipo de plataformas si no se llevan a cabo las medidas adecuadas por parte de padres y profesores. Por lo que se refiere a los síntomas[57] que pueden denotar una

---

55 Queremos hacer una breve reflexión en este punto sobre el concepto de «adicción» y es que, si bien la Unidad de Conductas Adictivas de Elda (UCA) la define como «una dependencia psicológica respecto a una cosa en específico que llega a convertirse en algo "central" para la persona que la padece y que termina desorganizando su personalidad», la Real Academia Española de la Lengua ofrece la siguiente definición: «hábito de quien se deja dominar por el uso de alguna o algunas drogas tóxicas, o por la afición desmedida a ciertos juegos». Nos ha resultado llamativo el distinto lugar donde pone el acento una y otra definición y es que, si bien en la primera el énfasis está puesto en la dependencia psicológica, en el segundo caso, la RAE considera que es el sujeto quien «se deja dominar». Consideramos más conveniente en este contexto la definición ofrecida por la UCA puesto que de la ofrecida por la Real Academia Española de la Lengua extraemos dos consideraciones: de un lado, que es el sujeto quien activamente y de manera consciente y deliberada «se deja dominar» y, de otro, que se trata de una actitud vinculada a drogas tóxicas o a juegos, cuestiones ambas que no creemos que quepan en la definición de red social y, como hemos dicho, consideramos que es indudable que se puede hablar de adicción a las Redes Sociales.

56 Traemos a colación en este punto la información aportada por la Unidad de Conductas Adictivas de Elda (UCA) que, en 2012, trató a dos jóvenes cuyo diagnóstico fue «adicción a las Redes Sociales». Fueron los padres de las jóvenes quienes acudieron a la UCA puesto que constataron que ambas pasaban encerradas en sus habitaciones frente al ordenador más de ocho horas al día. Tras analizar el caso, la UCA sometió a las dos jóvenes a una terapia psicoterapéutica con el final de eliminar la adicción y, finalmente, tras cuatro meses de terapia, las jóvenes lograron recuperarse. Disponible en http://www.diarioinformacion.com/elda/2012/07/08/uca-trata-primeros-adolescentes-adictos-redes-sociales/1272674.html. Visitado el 21 de septiembre de 2016.

57 Información basada en el monográfico disponible en http://www.monografias.com/trabajos93/adiccion-a-redes-sociales/adiccion-a-redes-sociales.shtml#ixzz2Kp69Sz1m. Visitado el 10 de octubre de 2016.

adicción a las Redes Sociales se encuentran, entre otros: a) conexión continua a estas plataformas, b) actualización constante del perfil mediante la subida de contenidos gráficos, textuales o audiovisuales, c) sometimiento de sus acciones a la aprobación por parte del resto de la comunidad de la red social mediante la generación de preguntas en la red social, d) sustitución de horas de sueño por horas de conexión a la red social, e) verificación constante, a través del ordenador o del teléfono móvil, de los estados, actualizaciones y contenidos subidos por otros miembros de la red social, f) rechazo a dedicar tiempo extra en actividades fuera de la red social y g) irritabilidad manifiesta al ser interrumpido por personas o circunstancias de la vida real mientras navega por las Redes Sociales.

Por último, simplemente traer a colación algunos de los efectos —tanto en el sujeto que sufre la adicción como en su entorno— que se generan como consecuencia de la adicción a las Redes Sociales, a saber: pérdida y reducción de las habilidades cognitivas del sujeto, deterioro de la salud de la persona adicta por la falta de sueño y la evitación del contacto personal, entre otros. Aunque pueda resultar muy difícil identificar en este punto los sujetos que actúan como víctima y verdugo, en mi opinión caben dos posibilidades: de un lado, que la víctima sea el menor adicto y el «verdugo» sea la «sociedad», el grupo, las relaciones, el miedo al qué dirán etc que le hacen estar en una búsqueda constante por el agrado y el refuerzo de los demás a través del uso incesante de las herramientas TIC en general y de las Redes Sociales en particular y, de otro, que víctima y verdugo converjan en un único sujeto: el menor.

De todo lo anterior, cabe concluir afirmando que, tal y como anticipábamos al comienzo del apartado, en algunas ocasiones el menor es verdugo de otros por un uso inadecuado o abusivo de las Redes Sociales y, en otros, el menor es víctima de la actuación de otros —menores o no— en Redes Sociales.

Sea como fuere, es necesario que el Derecho no permanezca ajeno a esta realidad y que, en todo caso, las personas, organismos, organizaciones y entidades que estén en contacto directo con los menores tengan conocimiento de esta realidad y prevean mecanismos de actuación para implementarlos en caso de que sea necesario.

7. ¿DEBER DE LEGISLAR? ¿CONTROL? ACTUACIÓN DEL PODER LEGISLATIVO Y EJECUTIVO

En cuestión de Derecho y «Nuevas» Tecnologías, siempre se ha dicho y se asume como cierto que el Derecho va por detrás de la tecnología, dada la rapidez con la que todo tipo de herramientas relacionadas con las tecnologías de la información y las comunicaciones salen a la luz. Y es que, si bien es cierto que, en cierta medida, hay que asumir esa realidad debida a la diferente velocidad de actuación y creación entre «tecnología» y «derecho», también es cierto que el Derecho no puede permanecer ajeno a esta realidad y, mucho menos, cuando hay menores afectados.

En este sentido, si bien no queremos volver a traer a colación la normativa aplicable en lo que se refiere a los derechos de los menores ya analizada en un apartado específico del presente trabajo, sí que consideramos necesario traer a colación, de un lado, la normativa que aboga por la actuación tanto del Poder legislativo como del Poder ejecutivo así como algunas actividades, acciones, convenios, propuestas y documentos que, desde distintos ámbitos y organismos, se han publicado en los últimos años para arrojar luz y dotar de una mayor seguridad jurídica al más que complicado binomio compuesto por menores y Redes Sociales.

En un primer momento abordaremos las cuestiones normativas que abogan por una intervención, en uno u otro sentido, de la Administración —entendiendo Administración en un sentido amplio—; para pasar, a continuación, a enumerar y reseñar brevemente en qué han consistido diversas iniciativas, acciones y proyectos que, bien a nivel europeo bien a nivel nacional, se han puesto en marcha de cara a promover una cultura TIC en los menores y a lograr una mayor y mejor defensa y protección de estos en su inmersión en el mundo de las Tecnologías de la Información y las Comunicaciones.

Comenzamos aludiendo a lo dispuesto por el Dictamen 2/2009 del Grupo de Trabajo del artículo 29[58] en el que muestra su deseo y ánimo por defender y proteger los intereses del menor mediante «la formulación de acuerdos entre las autoridades responsables de protección de datos, los Ministerios de Educación y otros organismos competentes, que definan unas condiciones claras y prácticas de cooperación mutua en esta materia para difundir la idea de que la protección de datos es un derecho fundamental».

Por otro lado, en la propia Ley de protección jurídica del menor, ya citada, en concreto en el apartado tercero del artículo 5 se afirma que «Las Administraciones Públicas incentivarán la producción y difusión de materiales informativos y otros destinados a los menores, que respeten los criterios enunciados, al mismo tiempo que facilitarán el acceso de los menores a los servicios de información, documentación, bibliotecas y demás servicios culturales incluyendo una adecuada sensibilización sobre la oferta legal de ocio y cultura en Internet y sobre la defensa de los derechos de propiedad intelectual».

Si bien no se trata de una normativa, sí que nos parece interesante traer a colación que el 24 de abril de 2015, fue aprobado por el Congreso de los Diputados el Informe elaborado por la subcomisión para el estudio sobre Redes Sociales[59] constituida en la Comisión de Interior. En el citado Informe se incluyen una serie recomendaciones de carácter educativo, regulatorio, policial y sectorial, elaboradas a partir de las aportaciones realizadas por 48 expertos en la materia en diversas intervenciones. El informe resume las aportaciones de los comparecientes, resaltando la necesidad de coordinación de todas las instituciones públicas, tanto de la Administración General del Estado como con las comunidades autónomas, la importancia de la colabo-

---

[58] Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas), emitido el 11 de febrero de 2009. Su texto se puede consultar en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_es.pdf. El denominado Grupo de trabajo del artículo 29 fue creado en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un órgano europeo consultivo en materia de protección de datos y privacidad.

[59] El texto del Informe puede ser consultado en http://www.congreso.es/public_oficiales/L10/CONG/BOCG/D/BOCG-10-D-643.PDF. Visitado el 23 de septiembre de 2016.

ración, el intercambio de información y la rapidez en las respuestas entre todos los agentes concernidos; y la importancia de la cooperación internacional, tanto en el nivel de decisión política como en el nivel operacional. Asimismo, propone la adopción de medidas educativas, divulgativas y preventivas, junto con las medidas normativas o policiales; el fomento de la autorregulación y la especial atención a la protección de la infancia y la juventud, distinguiendo tramos de edad y diferentes usos.

En el mismo sentido que la anterior, nos parece interesante resaltar, en ámbito nacional, la labor desarrollada por la ya extinta Agencia de Protección de Datos de la Comunidad de Madrid (APDCM)[60] que, además de convocar tres jornadas en las que se impartió una charla sobre «Protección de datos y Redes Sociales» en los 404 centros educativos públicos de la Comunidad de Madrid con motivo de la celebración del Día europeo de la protección de datos el 28 de enero de los años 2009, 2010 y 2011, publicó una «Declaración en defensa de la privacidad de los menores en Internet»[61] en la que proponía seis puntos para proteger la privacidad de los menores en Internet y de los que destacamos dos que, en nuestra opinión, están tan estrechamente conectados que podrían haber sido unificados, a saber: «Que la Administración educativa debe impulsar y fomentar la formación de los menores, padres, madres y educadores en el uso adecuado de las tecnologías de la información» y «Que el uso responsable de las tecnologías de la información depende en gran medida de la

---

60 Aunque el órgano fue suprimido con la entrada en vigor el 1 de enero de 2013 de la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas, traemos a colación esta iniciativa de la APDCM y hacemos hincapié en la importante labor formativa, informativa y de difusión que ha desempeñado este organismo a la hora de defender y garantizar el derecho fundamental a la protección de datos desde su creación. Artículo 61 de la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas. Publicada en el Boletín Oficial de la Comunidad de Madrid núm. 310, el 29 de diciembre de 2012 y cuya entrada en vigor se produjo el 1 de enero de 2013.

61 Texto completo de la Declaración disponible en el sitio web de la Agencia de Protección de Datos de la Comunidad de Madrid y, en concreto, disponible en http://www.madrid.org/cs/Satellite?c=PAPDGenericoFA&cid=1142677571004&language=es&pageid=12472205326&pagename=PortalAPDCM%2FPADP_Generico_FA%2FAPD_fichaNoticia&vest=124722053263. Visitado el 24 de septiembre de 2016.

formación del usuario, de ahí que la educación y la concienciación sean un elemento esencial para la consecución de dicho fin». Destacamos estos dos porque, a nuestro modo de ver, cualquier cuestión, acción, proyecto o medida cuyo objetivo sea garantizar la seguridad de los menores en Internet en general y en las Redes Sociales en particular ha de pasar, necesariamente, por una adecuada formación en la materia.

Por otro lado, citamos el Reglamento Europeo sobre protección de datos, ya referida, que, en su artículo 57 b), sitúa, entre las tareas de las autoridades de control territoriales el «promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento» haciendo hincapié en que «las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención».

También queremos señalar, en lo que a la labor de la Unión Europea respecto al uso de Internet y de las Redes Sociales por parte de los menores se refiere, destacamos una estrategia publicada en mayo de 2012, a favor del diseño de una red más adecuada para los menores. En concreto, se trata de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las Regiones: Estrategia europea en favor de una Internet más adecuada para los niños[62].

De la estrategia publicada en 2012, se destacan cuatro líneas de acción que han de ser protagonizadas por los Estados Miembros de la Unión así como por los integrantes de la industria del sector TIC, a saber:

La primera línea de actuación ha de ir encaminada a estimular la producción de contenidos creativos y educativos en línea para niños de manera que redunde en mejores experiencias en línea por parte de los más pequeños. Como segunda cuestión se alza la necesidad de aumentar la sensibilización y la capacitación de todos los agentes con presencia en la web 2.0 que pasa por una necesaria alfabetización digital y mediática, haciéndose hincapié en la enseñanza de la seguridad en línea desde los centros educativos en los que los jóvenes sean

---

62 COM/2012/0196 final. Su texto se puede consultar en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012DC0196.

los verdaderos protagonistas. En tercer lugar, la Comisión pone el acento en la necesidad de crear un entorno en línea seguro para los niños, concretando este objetivo mediante la adopción de parámetros de confidencialidad ajustados a la edad de los menores así como aumentando el uso del control parental de los contenidos y de los sistemas de clasificación y acceso en función de edades y contenidos. Finalmente, como cuarto aspecto se erige la lucha contra los abusos sexuales y la explotación sexual de los niños. En este punto se hace necesaria la instalación de mecanismos que permitan tanto la identificación sistemática y más rápida de la pornografía infantil difundida a través de diversos canales en línea como la denuncia y retirada de los mismos, al tiempo que se aboga por la cooperación y acción conjunta de la Unión Europea con socios internacionales para luchar contra los abusos sexuales y la explotación sexual de los niños.

Por último, a nivel autonómico español, destacamos el Decreto 25/2007, de 6 de febrero, por el que se establecen medidas para el fomento, la prevención de riesgos y la seguridad en el uso de Internet y las tecnologías de la información y la comunicación (TIC) por parte de las personas menores de edad[63], de la Comunidad Autónoma de Andalucía que prevé en su Capítulo III bajo la rúbrica de «medidas de prevención y seguridad en el uso de Internet y de las TIC por parte de personas menores de edad» una serie de medidas destinadas a la protección de los menores en el uso de las TIC, poniendo de manifiesto en el artículo 16 que «La Consejería competente en materia de TIC establecerá un sistema de información y orientación sobre el uso de Internet y las TIC por personas menores de edad».

De todos ellos se desprende la necesidad de que la Administración tome cartas en el asunto y ofrezca a los centros docentes, a padres, profesores y a los propios menores información y herramientas para tener una presencia segura en Internet y, en caso de sufrir algún problema, el conocimiento y los mecanismos necesarios para saber cómo acudir, a quién y qué hacer. Es en este punto donde pasamos a repasar las medidas, proyectos y acciones más llamativos, importantes y/o de mayor calado que, a nivel nacional, han visto la luz en los últimos años.

---

63 Publicado en el Boletín Oficial de la Junta de Andalucía del 22 de febrero de 2007.

El primer proyecto que queremos traer a colación y que ha nacido como fruto de la colaboración de organismos públicos y entidades privadas de cara a proteger a los menores en las Redes Sociales ha sido el denominado como «Te veo ¿me ves?». Es necesario destacar que, si bien cuenta con la colaboración del Ayuntamiento de Madrid y de las Fuerzas y Cuerpos de Seguridad del Estado[64] que apoyan con su «know-how» sobre el *modus operandi* de los delincuentes en Internet y los llamados delitos informáticos o delitos cibernéticos, lo cierto es que se trata de un proyecto de voluntariado corporativo[65] y

---

64 El 24 de enero de 2012, el que fuera alcalde de Madrid, Alberto Ruiz Gallardón, anunció la suscripción, por parte del Ayuntamiento de Madrid, de varios convenios en el marco del proyecto «Te veo ¿me ves?» con objeto de proteger a los menores de los posibles riesgos de un uso inconsciente de Internet y de las Redes Sociales. Así, el alcalde no dudó en mostrar el más firme compromiso de la ciudad de Madrid en colaborar tanto con las empresas líderes en el ámbito de las nuevas tecnologías como con las Fuerzas y Cuerpos de Seguridad y la Asociación Protégeles de manera que se «promueva la colaboración entre estas instituciones con el objetivo de informar a padres y adolescentes para que naveguen de manera segura por Internet y que padres e hijos utilicen la red de manera conjunta y que la intimidad de los más pequeños esté a salvo». Por último, simplemente traer a colación las cifras aportadas por el alcalde de la ciudad de Madrid para avalar la necesidad y urgencia en la adopción de esta medida y es que, tal y como declaró en rueda de prensa: «El 70% de los internautas ya es usuario de alguna red social. Y también el 70% de los niños y adolescentes españoles de entre 6 y 18 años cuentan con algún perfil en las Redes Sociales e, incluso, la mitad de ellos con más de uno. Al mismo tiempo, un 70% reconoce que usa Internet para sus estudios, pero el 40% de ellos también admite que la red afecta negativamente al tiempo que dedican a la familia». Concluimos mostrando nuestra máxima conformidad a la conclusión ofrecida por el alcalde «Las Administraciones y la sociedad civil no podemos permanecer ajenos a este problema, ya que un estudio reciente revela que el 85% de los menores navega en Internet sin la compañía de un mayor, o que el 44% de ellos tiene conocimiento de algún caso de ciberacoso entre sus amigos». Disponible en http://www.madrid.es/portales/munimadrid/es/Inicio/El-Ayuntamiento/Medios-de-Comunicacion/Notas-de-prensa/%22Te-veo--me-ves%22?vgnextfmt=default&vgnextoid=aafa409541e2e210VgnVCM2000000c205a0aRCRD&vgnextchannel=6091317d3d2a7010VgnVCM100000dc0ca8c0RCRD. Visitado el 8 de octubre de 2016.

65 Se entiende por tal aquel en el que todas las personas que imparten las charlas son profesionales de las empresas e instituciones colaboradoras y participan sin ánimo de lucro.

se enmarca dentro de la labor de formación en cuestión de seguridad TIC que, desde el año 2009 están llevando a cabo la Fundación Voluntarios por Madrid junto a la Fundación BT mediante conferencias, charlas y encuentros dirigidos principalmente a adolescentes en riesgo de exclusión social y a padres de las Escuelas de Padres del Ayuntamiento de Madrid. Por lo que se refiere a las características básicas del Proyecto[66], hay que tener en cuenta que, respecto a la duración del mismo, se prevé, como frecuencia media, una periodicidad de dos charlas mensuales, con un total de treinta charlas anuales impartidas, en los centros designados por el Ayuntamiento de Madrid, variando las edades en los menores destinatarios de la sesión de formación. Y, en cuanto a contenido y objetivos en función de los destinatarios, por lo que se refiere a los destinatarios que no alcanzan la mayoría de edad, podríamos resumir el objetivo como la provisión de la información necesaria para que puedan comenzar a navegar por la Red y a hacer uso de las Redes Sociales de manera autónoma, consciente y responsable. Y, en el caso de las charlas dirigidas a padres y tutores, el objetivo va más allá de ofrecer pautas para que ellos naveguen de manera segura, haciéndose hincapié en la proporción y comunicación de patrones básicos que han de adoptarse en el hogar para facilitar una navegación segura en la Red así como la propuesta de herramientas —y modelos para su uso— que favorezcan el control de contenidos en la Red, la restricción del acceso a páginas no adecuadas para el menor o que protejan al menor frente a posibles ataques fruto de su navegación por la web.

Destacamos también el llamado «simulador de privacidad» como herramienta destinada a los usuarios de Redes Sociales —especialmente a los de menor edad y los adolescentes— para que, de manera práctica, puedan comprobar qué supone el hecho de subir una fotografía a una red social y no dar importancia a la configuración de privacidad de su perfil en la misma. Se trata de una iniciativa que ha contado con la participación de la red social española Tuenti y de la

---

66 Toda la información sobre el proyecto y maneras de colaborar disponible en htttp://www.voluntariospormadrid.org/voluntariadocorporativo_Voluntariado_corporativo_Charlas_internet/seccion=61&idioma=es_ES&id=201012174390001&activo=6.do. Visitado el 18 de septiembre de 2016.

iniciativa europea EUKids Online[67]. La herramienta ha sido lanzada coincidiendo con la celebración en toda Europa del Día europeo de la privacidad el 28 de enero de 2013 y, en palabras de sus propios creadores, el proyecto «pretende estimular el cuidado de los datos personales, propios y ajenos, en especial cuando están ligados a las fotografías en las Redes Sociales».

Más recientemente, en octubre de 2015, la Agencia Española de Protección de Datos y el Ministerio de Educación, Cultura y Deporte han firmado un convenio cuyo objeto es «establecer un marco estable de colaboración para realizar proyectos y acciones de carácter educativo en la formación y sensibilización de los menores de edad en materia de privacidad y protección de datos, sobre todo en el ámbito de internet»[68]. La firma de este convenio supone la puesta en práctica de diversas acciones encaminadas a la formación de menores —y de profesores y demás personal que trabaje con ellos— en materia TIC a través de, entre otras cuestiones, el desarrollo y difusión de materiales de interés en este sentido así como de juegos, concursos y dinámicas que hagan más atractiva las cuestiones de privacidad y seguridad TIC para los menores[69].

---

67 EU Kids Online es un grupo de investigación referente en el estudio de menores de edad y nuevos medios de comunicación. Forma parte de una red multinacional de investigación con más de 70 expertos y expertas que estimulan y coordinan la investigación sobre las oportunidades, los riesgos y la seguridad en Internet de los niños y niñas en Europa. Esta red ha sido financiada por el Safer Internet Programme de la Comisión Europea. Información obtenida de http://www.ehu.eus/es/web/eukidsonline/aurkezpena.

68 Su texto se puede consultar en https://www.agpd.es/portalwebAGPD/LaAgencia/gestion_economica/convenios/common/Convenio_Convivencia_MECD_AEPD_13.10.2015.pdf.

69 En esta página web http://www.tudecideseninternet.es/agpd1/ se puede acceder a los contenidos que ha creado la AEPD para fomentar el conocimiento y concienciación del derecho fundamental a la protección de datos por parte de los menores, especialmente en lo que respecta a su actividad en Internet. Asimismo, conviene destacar en este punto que, en junio de este año, la Agencia Española de Protección de Datos y Clan, el canal infantil de RTVE, colaboraron en «una campaña de educación digital para difundir un uso responsable de internet y las Redes Sociales entre los más jóvenes» a través de vídeos protagonizados por los personajes de la serie de ficción «Big Band Clan». Disponible en http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_06_15-ides-idphp.php. Visitado el 5 de octubre de 2016.

Ahondando más en la labor de la Agencia Española de Protección de Datos —sin duda uno de los organismos que, en los últimos años, más está abogando en nuestro país por fomentar un uso seguro de las TIC por parte de todos los ciudadanos, haciendo especial hincapié en el papel de los menores de edad por su mayor vulnerabilidad— traemos a colación la reciente aprobación —en colaboración con el Instituto Nacional de Ciberseguridad[70] (INCIBE)[71]— de la «Guía sobre Privacidad y Seguridad en Internet». La Guía está integrada por dieciocho fichas[72] de carácter eminentemente práctico en las que se da respuesta a cuestiones de importancia en materia de seguridad y protección de datos entre las que cabe destacar, entre muchos otros: la protección de redes WiFi, cómo realizar copias de seguridad, las distintas opciones de configuración de privacidad de las Redes Sociales o cómo proteger los dispositivos portátiles —*smartphones, tablets,* portátiles etc.— en los que, día a día, compartimos y guardamos nuestros datos de carácter personal.

Destacamos, por último, dos entidades que consideramos que son clave en la defensa y protección de los menores en las TIC, a saber: de un lado, la Brigada de Investigación Tecnológica de la Policía Nacional[73] y, de otro, la sección de menores de la Oficina de Seguridad del Internauta del INCIBE.

---

70 El Instituto Nacional de Ciberseguridad de España (INCIBE) es una sociedad dependiente del Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información; es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

71 Y habiendo contado con la colaboración de la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) del Ministerio de Sanidad, Servicios Sociales e Igualdad, Policía, Guardia Civil y Telefónica.

72 Además de las fichas, tanto en el sitio web de la Agencia Española de Protección de Datos como en el de la Oficina de Seguridad del Internauta de INCIBE se ofrecen algunos vídeos y contenidos de interés que son referenciados en la citada ficha.

73 Entre las funciones de la Brigada de Investigación Tecnológica de la Policía Nacional está la de velar por la seguridad de los internautas y de los ciudadanos en general.

Por lo que respecta a la primera de ellas, la Brigada de Investigación Tecnológica (BIT) es la Unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia que han aparecido por el desarrollo y expansión generalizada de las Tecnologías de la Información y las Comunicaciones, a saber: Pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería, ciberacoso o *grooming*, entre otros.

De otro lado, formando parte de la segunda —INCIBE— se encuentra la denominada *Menores OSI* que es una iniciativa que se inscribe dentro de la labor desarrollada por la Oficina de Seguridad del Internauta puesta en marcha por el Instituto Nacional de Ciberseguridad del Ministerio de Industria, Energía y Turismo, cuya principal misión es «promover el uso seguro y responsable de Internet y las nuevas tecnologías entre los menores». Dentro de Menores OSI nos encontramos tres secciones diferenciadas a las que se acudirá en función de lo que se necesite, a saber: —Hogar Ciberseguro: sección a la que podrán acudir los padres con escaso o nulo conocimiento de los principios básicos de una buena educación TIC; —Escuela Cibersegura: en esta sección, tanto los padres como los profesores y los propios menores podrán encontrar recursos educativos de interés relacionados con el uso seguro y responsable de las TIC; y, por último, en la sección de Cibercooperantes podrán acceder todos aquellos que, de manera voluntaria, quieran ayudar impartiendo charlas y talleres sobre el buen uso de las TIC.

No hemos querido incluir en este punto las múltiples organizaciones privadas —con y sin ánimo de lucro— que ofrecen diversas medidas y acciones, bien formativas, bien preventivas, bien de carácter práctico y dinámico, enfocado a mejorar la protección de los menores en Internet en general y en las Redes Sociales en particular sino que, queremos hacer ver con esta pequeña muestra, que es mucho el camino por hacer y que ni la propia Administración, ni el legislador, ni los jueces llegado el caso ni por supuesto los padres, profesores y los propios menores pueden permanecer ajenos a esta realidad que supone el cumplimiento de unas normas.

8. CENTROS EDUCATIVOS Y ACTUACIÓN DE MENORES EN REDES SOCIALES, ¿QUÉ PAPEL DESEMPEÑAN?

Para responder a esta pregunta debemos partir, una vez más, de los derechos de los menores: derecho a la intimidad, derecho a prestar el consentimiento para el tratamiento de datos de carácter personal, derecho al secreto de las comunicaciones o el derecho a recibir información adecuada, entre otros. Teniendo en cuenta todos estos derechos, ha de ponerse en la balanza el papel de los Centros educativos, qué obligaciones tienen, qué responsabilidad y hasta dónde pueden intervenir en caso de que se produzca un conflicto fruto de la actuación en Redes Sociales de uno o varios de los menores que están a su cargo, tomando como base la normativa vigente aplicable en este sentido.

En primer lugar, acudimos a lo dispuesto por la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia[74] que, en su artículo 1.4 afirma que «A través del sistema educativo se implantará el conocimiento que los menores deben tener de sus derechos y deberes como ciudadanos, incluyendo entre los mismos aquellos que se generen como consecuencia de la utilización en el entorno docente de las Tecnologías de la Información y Comunicación». De esta primera normativa, se desprende el deber de los Centros educativos de formar sobre el uso de las Tecnologías de la Información y las Comunicaciones.

Se expresa en esta misma línea de formación en TIC la Ley Orgánica de Educación[75] en varios artículos. Por un lado, el artículo 14.5 afirma que «Corresponde a las Administraciones educativas (…) fomentar una primera aproximación en las tecnologías de la informa-

---

74 Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, publicada en el Boletín Oficial del Estado de 29 de julio de 2015.

75 Ley Orgánica 2/2006, de 3 de mayo, de Educación, publicada en el Boletín Oficial del Estado de 4 de mayo de 2006.

ción y la comunicación (…). Por otro, su artículo 17 incluye, en el apartado i) como objetivo de la educación primaria «Iniciarse en la utilización, para el aprendizaje, de las tecnologías de la información y la comunicación desarrollando un espíritu crítico ante los mensajes que reciben y elaboran».

En esta misma línea se reafirma el artículo 23 al hablar de los objetivos de la educación secundaria obligatoria al mencionar como capacidad a adquirir por parte de los alumnos el «Desarrollar destrezas básicas en la utilización de las fuentes de información para, con sentido crítico, adquirir nuevos conocimientos. Adquirir una preparación básica en el campo de las tecnologías, especialmente las de la información y la comunicación». Por último, el artículo 33 trata de los objetivos de la etapa de Bachillerato y afirma que está enfocado a desarrollar en los alumnos capacidades que les permitan (…) «g) Utilizar con solvencia y responsabilidad las tecnologías de la información y la comunicación».

Más allá del deber de formación e información en cuestiones TIC a los menores, acudimos a otras normas para valorar el deber de actuación en caso de conocimiento de un conflicto en Redes Sociales en el que se haya visto afectado, en condición de víctima o de agresor, uno o varios de los alumnos de los que es responsable el Centro educativo.

En primer lugar, acudimos a lo dispuesto por el Código Civil, en concreto, en su artículo 1903 que reza así «Las personas o entidades que sean titulares de un Centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del Centro, desarrollando actividades escolares o extraescolares y complementarias». De este extremo se deriva la necesidad de que el Centro adopte medidas en caso de que detecte conductas ilícitas en Redes Sociales por uno o varios de sus alumnos en el tiempo en el que estos se encuentren bajo su control.

Por otra parte, en los Decretos autonómicos de convivencia en general se establece que el Centro pueda sancionar hechos ocurridos fuera del centro si tienen su origen en la actividad escolar o afectan a miembros de la comunidad educativa.

Por último, queremos traer a colación algunas cuestiones que, en materia de responsabilidad penal, se han de tener en cuenta a la hora

del deber de actuar por parte de los Centros educativos, a saber: de un lado, lo previsto en el artículo 13 de la Ley Orgánica de Protección Jurídica del Menor, ya referida, que afirma que «toda persona o autoridad, y especialmente aquellos que por su función detecten una situación de riesgo, deben comunicarlo a la autoridad, sin perjuicio de prestarle el auxilio que soliciten». De otro, el artículo 262 de la Ley de Enjuiciamiento Criminal reza así «los que por razón de su cargo tengan conocimiento de un delito, están obligados a denunciarlo inmediatamente».

Si bien en ninguna de las normas anteriores se habla específicamente del uso de Internet y Redes Sociales, no cabe duda de que es plenamente aplicable el deber, como mínimo, de notificar el conocimiento de una conducta delictiva y, en función del caso, adoptar las medidas que correspondan.

Por tanto, para responder a la cuestión que da título a este apartado, los modos en los que, teniendo en cuenta la normativa vigente, el Centro educativo debe actuar, son:

— Formar en el uso de las Tecnologías de la Información y las Comunicaciones. Si bien no hay un modelo que contenga el contenido y forma idóneo de esta formación, en mi opinión esta formación ha de ser impartida por personas expertas en la materia, adaptando el lenguaje a la edad de los menores a las que se destine y enfocada a que sea una formación en valores, práctica, realista con el uso diario que hacen los jóvenes de estas herramientas y orientada no sólo a prevenir[76] los riesgos y amenazas que puede suponer un uso descontrolado sino también a formar en el buen uso y máximo aprovechamiento de estas herramientas.

— Establecer protocolos de actuación para implementarlos en caso de una situación de ciberacoso, suplantación de identidad, *sexting* o *sexcasting* en el que algún alumno del Centro haya sido partícipe. Una vez establecidos esos protocolos, debe el Centro notificar la existencia de los mismos tanto a los padres como a los alumnos y, por

---

[76] De interés en este sentido, resulta el sitio web http://www.mecd.gob.es/educacion-mecd/mc/convivencia-escolar/inicio.html del Ministerio de Educación, cultura y deporte donde se ofrecen recursos de interés en materia de uso de las TIC por parte de los menores, lucha contra el ciberacoso y otras amenazas.

supuesto, a todo el personal del Centro; de manera que todos sepan cómo actuar y cuál va a ser el protocolo cuya máxima será, en todo momento, proteger al menor y ser eficaces, sinceros y transparentes.

— Llevar a cabo un análisis detenido de la realidad del día a día de los alumnos de manera que se pueda identificar, cuanto antes, si un alumno está siendo víctima de algún acto ilícito en Redes Sociales e implementar las medidas que sean necesarias acorde a la gravedad del acto, al conocimiento que tenga el Centro y al impacto que haya causado en el Colegio y en los alumnos, padres y profesores afectados.

Por tanto, el Centro debe ser consciente de que, en pleno siglo XXI, las Tecnologías de la Información y las Comunicaciones son una herramienta más que presente en el día a día de los menores, de los padres y de los profesores y que la educación que debe proporcionar el Centro debe ir «más allá» de la explicación e impartición de materias básicas y tradicionales como pudieran ser Lengua, Matemáticas, Inglés o Historia y, por tanto, debe contar con personal cualificado y, en caso de ser necesario, proceder a la formación de su propio personal en el uso de las TIC por parte de menores.

En este sentido, creemos que independientemente y más allá del papel protagonista de las diversas instituciones educativas en la elaboración y difusión de la campaña informativa, una cuestión fundamental —y , en cierto modo, previa a la campaña de información profunda y detallada— es la implantación en todos los Centros Educativos de Educación Primaria[77], Secundaria y Superior de una asignatura que, con carácter obligatorio e impartido por un experto en la materia, forme a los niños en el uso de Internet en general y de las redes sociales en particular, haciéndoles conscientes no sólo de los riesgos y amenazas que puede suponer un uso inconsciente y descontrolado de la red de redes para ellos y para su familia y amigos, sino también abriéndoles la mirada hacia las infinitas posibilidades que les ofrece Internet y que les puede reportar un beneficio para su vida:

---

[77] Consideramos que sería adecuado incluirlo en el tercer Ciclo de Educación Primaria que corresponde a 5.º y 6.º con alumnos de edades comprendidas entre los 10 y 11 años y que, si no tienen ya cuenta en una red social, sí que son usuarios de Internet o están a punto de serlo. Son los denominados «digital boys».

desde la búsqueda de información hasta la descarga de contenidos pasando por la puesta en contacto con familiares y amigos.

No obstante, y además de abogar por la inclusión de una asignatura en esta materia en todos los niveles educativos[78], en lo que se refiere a la participación de las instituciones educativas en la elaboración y difusión de la campaña informativa sobre las redes sociales diremos que, en nuestra opinión, la participación de todos los centros educativos —públicos y privados— en la misma ha de ser total, tanto en el proceso de diseño y elaboración de la campaña, aportando aquí sus experiencias y vivencias en torno a problemas reales experimentados por sus alumnos en las redes sociales, como en la difusión de la campaña, tanto de cara a los alumnos como a los padres, profesores y demás integrantes del claustro por cuanto resulta imprescindible que todos actúen en una misma línea y conozcan toda la información necesaria.

---

[78] Quedando incluida aquí la etapa universitaria y es que, con Fernández de Buján, opinamos que «(...) deben las aulas universitarias ser portadoras de saberes que tiendan a conseguir una formación plena del alumno universitario(...)». Formación plena que, en nuestra opinión, debe incluir una profunda formación técnica, jurídica, sociológica y ética en todo lo que se refiere a las Tecnologías de la Información y las Comunicaciones. *Vid.* FERNÁNDEZ DE BUJÁN, F.: «La reforma de los estudios de derecho, el nuevo plan de estudios: su valoración y análisis histórico y comparado», Dykinson, Madrid, 1992, p. 26.

9. PADRES ¿DÓNDE ESTÁ EL LÍMITE? ¿CORRESPONSABLES, COAUTORES O MEROS ESPECTADORES?

No cabe duda de que, en la Sociedad de la Información y las Comunicaciones en la que vivimos, el rol de los padres ha, en cierto modo, cambiado. Y es que, en la sociedad actual es común que ambos progenitores trabajen hasta tarde y que, en cierta medida, gran parte del tiempo de ocio de los menores vaya asociado al uso de una *tablet,* un ordenador o un *smartphone* con distintas aplicaciones, tanto las Redes Sociales propiamente dichas como aplicaciones de juegos, entretenimiento y ocio en general. Es por ello que en este apartado quiero intentar dar respuesta, con la Ley en la mano, a la pregunta que le da nombre ¿dónde está el límite de actuación de los padres respecto al uso que hacen sus hijos de las Redes Sociales?

Para ello, en primer lugar, traeremos a colación la normativa que fija obligaciones a los progenitores y, a continuación, trataré de concretar en la práctica el contenido de dichas obligaciones.

En primer lugar, acudimos a lo dispuesto por el Código Civil que, en su artículo 154, reza: «La patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad, y con respeto a su integridad física y psicológica. Esta potestad comprende los siguientes deberes y facultades: 1. Velar por ellos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral. 2. Representarlos y administrar sus bienes». Pese a que cuando se promulgó el Código Civil, nada hacía prever la aparición de las Redes Sociales, sí que considero que, en pleno siglo XXI, al hablar de «formación integral» ha de entenderse, también, «formación TIC».

En segundo lugar, la Ley de Protección jurídica del menor, citada, en el apartado quinto de su artículo 4 (Derecho al honor, a la intimidad y a la propia imagen) señala que «los padres o tutores y los pode-

res públicos respetarán estos derechos y los protegerán[79] frente a posibles ataques de terceros».

De ambas normas se desprende que los padres tienen un deber de formación e información a sus hijos y, de otro, un deber de actuación y protección en caso de ataques por parte de terceros. Por tanto, podríamos hablar de un deber preventivo (formación) y un deber reactivo (actuación en caso de ataques por parte de terceros). Ambos deberes han de estar en el justo equilibro en la balanza con los derechos de los menores de protección de datos, intimidad, propia imagen y capacidad de obrar, teniendo en cuenta siempre los límites de edad y criterios de madurez que fija la normativa[80].

En este punto traemos a colación la sentencia de la sala segunda del Tribunal Supremo[81] en la que, ponderándose el peso del derecho del menor —la menor, en este caso— a la intimidad, secreto de las comunicaciones y propia imagen junto con el deber de custodia y protección de la madre respecto a la hija, la sentencia concluye afirmando que, en este caso concreto, habida cuenta de la sospecha cierta de que la menor podía estar inmersa en una situación de ciberacoso, el derecho de la menor cede a favor del deber de la madre. Concretándose esta afirmación en el derecho de la madre de vulnerar el derecho

---

79 Y es que, si bien en determinados casos el menor actúa con libertad en el uso de las Redes Sociales, hay que tener en cuenta, con Álvarez Vélez cómo aunque «(…) en determinados casos se establezca la titularidad del derecho, carece de capacidad para su defensa». Ahondando en esta cuestión, resulta incluso obvio decir que, en caso de ser necesario, han de ser los padres y tutores quienes adopten las medidas pertinentes de cara a un proceso judicial por violación de derechos del menor. Vid. ÁLVAREZ VÉLEZ, M. I.: «La protección de los derechos del niño. En el marco de las Naciones Unidas y en el Derecho Constitucional Español». Facultad de Derecho-ICADE. Universidad Pontificia Comillas-Madrid. 1994, p. 169.

80 En este sentido, De Couto Gálvez trae a colación cómo «(…) el artículo 154 del Código Civil determina el deber de obediencia a sus padres y representantes, por lo que la autonomía del menor está limitada al criterio de estos, que deben actuar siempre para beneficiar al menor (…)». Vid. ALCÓN YUSTAS, M. F. y DE COUTO GÁLVEZ, R. M.: «Lecciones de Derecho Constitucional y de Derecho Civil (Derecho de la persona)», Parte segunda *Lecciones de Derecho Civil (Derecho de la persona),* Dykinson, Madrid, 1997, p. 167.

81 Sentencia de la Sala Segunda del Tribunal Supremo número 864/2015, de 10 de diciembre.

a la intimidad y al secreto de las comunicaciones de su hija menor al acceder a su cuenta de Facebook para ver y poder aportar en el juicio los mensajes que el acosador le llevaba mandando durante los últimos meses.

Añade que la acción de la madre fue lícita por ser «titular de la patria potestad concebida no como poder sino como función tuitiva», es decir, de guarda y amparo, «respecto de la menor». Por último, en lo que respecta a esta sentencia, queremos llamar la atención sobre cómo el Tribunal Supremo enfatiza que no puede el ordenamiento legal «hacer descansar en los padres unas obligaciones de velar por sus hijos menores y al mismo tiempo desposeerles de toda capacidad de controlar en casos como el presente». En todo caso, ha de tenerse en cuenta que, el *modus operandi* habitual de los padres de menores de edad mayores de catorce años no puede ser acceder indiscriminadamente y sin motivo alguno a las cuentas y perfiles de sus hijos en Redes Sociales por cuanto, como venimos analizando, el menor es titular de unos derechos que, salvo excepciones en las que entren en juego otros derechos fundamentales y/o deberes de los padres, deben ser respetados.

Antes de entrar a abordar la actitud que, a nuestro entender y tras analizar la normativa aplicable, han de adoptar los padres en relación con el uso de las TIC en general y de las Redes Sociales en particular por parte de sus hijos, queremos hacer hincapié en que cuando hablamos de los consejos que han de dar los padres a sus hijos menores nos estamos refiriendo a los menores que se encuentran en la adolescencia donde los padres no pueden imponer su criterio sino que han de dar una cierta libertad e independencia a su hijo. Y decimos esto por cuanto no es el objetivo del presente apartado el abordar y analizar las Redes Sociales para los más pequeños de la casa[82] o los mecanismos de control parental de contenidos no aptos para la infancia, por cuanto en estos casos de los más pequeños de la casa el deber de protección de los padres no se enfrenta a la libertad o a los derechos propios de un niño más mayor por la falta de madurez .

En primer lugar, es necesario que los padres asuman como propia la labor de «formación en TIC» de sus hijos. Partiendo de esto, el primer consejo a poner en práctica es que eviten hacer de sus hijos

---

[82] Baste citar en este sentido las Redes Sociales Fanlala, Club Penguin o Fantage.

«huérfanos digitales». Con esta expresión nos referimos a aquellos «nativos digitales» que no cuentan con el apoyo de sus padres[83]. Y es que, si bien es cierto que, en muchas ocasiones, los hijos manejan con mayor soltura que sus progenitores las herramientas tecnológicas, también lo es que los menores no cuentan con una «cultura digital[84]» suficiente para conocer los riesgos de estas herramientas y es ahí donde los padres juegan un papel fundamental para que su hijo no sea un «huérfano digital» sino un «nativo digital consciente[85] y formado», haciendo hincapié en este sentido en que no se trata sólo de ofrecerle formación sobre los riesgos, amenazas y peligros que supone el uso de las TIC sino también de las innumerables ventajas y beneficios que le puede reportar un uso correcto de estas herramientas, no quedándose limitado a los usos más generalizados de búsqueda de información, puesta en contacto o juego *online* con otros usuarios.

En íntima conexión con lo anterior, recomendamos que el padre transmita a sus hijos la importancia del respeto como principio básí-

---

83 En este mismo sentido se pronuncia la AEPD, en su procedimiento sancionador PS-00468-2009 al afirmar que «Se debe navegar con los menores, ayudarles a distinguir los riesgos, asegurarse de que los niños no accedan a Internet a través de entornos no confiables o de que no intercambien datos personales ni fotografías con desconocidos».

84 En esta cultura digital que sugerimos que los padres creen en el menor han de quedar integrados dos conceptos: de un lado, la terminología básica en Tecnologías de la Información y las Comunicaciones, de manera que el menor se familiarice con términos como antivirus, SPAM, cookies o privacidad. En este sentido, recomendamos que los propios progenitores sean quienes elaboren este «diccionario TIC» adecuado a las edades de sus hijos, sus conocimientos y aptitudes; y, de otro, las cuestiones de carácter práctico y de utilidad para el menor cuando navegue por Internet. En este sentido, recomendamos que se instruya al menor sobre la importancia de los servicios antivirus, la necesidad de mantenerlos actualizados así como la necesidad de estar al día tanto sobre las nuevas aplicaciones y funcionalidades que ofrecen las Redes Sociales como sobre los riesgos y peligros que entrañan.

85 En este punto, y si bien resulta indudable que la educación de un hijo no es baladí, una cuestión que nos parece oportuna traer a colación a la hora de los criterios para formar al menor en el uso de las TIC es el de, más allá de formarle sobre la forma de usarla y los aspectos más prácticos, hacer hincapié en crear en el menor una capacidad crítica suficiente y unos valores fuertes de cara a que el propio menor sea capaz de someter Internet en general y las Redes Sociales en particular a ese filtro de «criticidad».

co de comportamiento —tanto a uno mismo como a los demás— ya sea en el ámbito *offline* como en el *online*, pudiéndose seguir en este punto la máxima de «Tratar a los demás como te gustaría que te trataran a ti» y, trasladado al mundo digital y para ofrecer un punto de vista eminentemente práctico, que los padres inviertan todo el tiempo que sea necesario en poner ejemplos reales a los hijos de, por ejemplo, fotografías u otro contenido audiovisual que no debería ser compartido en Redes Sociales porque falta al respeto —bien al propio, bien al ajeno—, haciendo hincapié en este último punto en que no importa si «los ajenos» son amigos, enemigos o desconocidos.

En la misma línea de convertirse en un ejemplo para sus hijos seguimos al instar a los padres a registrarse en la misma red social que su hijo de manera que conozcan de primera mano las funcionalidades de la red y el potencial de la plataforma así como las opciones de configuración de privacidad de cara a poder explicarle al menor cómo ha de actuar para limitar el acceso a sus contactos a los contenidos subidos a la web[86]. Y, lo que es más, planteamos la conveniencia de que los padres hagan uso de las Redes Sociales no únicamente como «mecanismo de control» sino como herramienta —tanto para su tiempo de ocio como para cuestiones laborales— y lo muestren así a sus hijos, erigiéndose como «usuario modelo» ya que, entre otras cuestiones, respeta las normas de la red social, sube contenido únicamente sobre el que tiene derecho o para el que ha solicitado el consentimiento de terceros, hace uso de los controles de privacidad de la red social y lo utiliza como complemento de las relaciones personales.

Y, por último, queremos hacer hincapié en una actitud que, a nuestro entender, han de tener los progenitores respecto al uso que hacen

---

[86] Y precisamente sobre la importancia del contenido subido a la web trata el llamado «TMI», siglas que responden a la expresión en inglés «too much information». Y es que, tal y como se alude en la Guía elaborada por la empresa de seguridad informática McAfee es importante que los padres hagan caer en la cuenta a los hijos de la importancia de no proporcionar más datos de los estrictamente necesarios o, mejor dicho, de ser conscientes de que proporcionar datos —información personal, vídeos, fotografías etc.— sobre uno mismo puede repercutir negativamente en su futuro, tanto laboral como personal. *Vid.* «Guía para padres sobre sitios Web de Redes Sociales Cinco lecciones para mantener la seguridad de sus hijos cuando socializan en Internet», p. 68.

sus hijos de Internet en general y de las Redes Sociales en particular y no nos estamos refiriendo a otra que la proactividad[87]. Y es que, resulta fundamental que los padres adopten medidas encaminadas a la formación del menor en TIC y a la prevención de que puedan ser víctimas de ciberataques o de otros inconvenientes del uso de las Redes Sociales ya abordados en el presente trabajo[88].

En este sentido, y como medida básica, consideramos necesario que los padres se creen un perfil en las Redes Sociales en las que esté presente su hijo y, en segundo lugar, que hagan uso de sus conocimientos en Tecnologías de la Información y las Comunicaciones para llevar a cabo un seguimiento, entre otras cuestiones y por poner algunos ejemplos concretos, de las páginas y sitios web de Internet donde aparece el nombre de su hijo o la localización de fotografías del menor en sitios inapropiados para, desde el conocimiento, adoptar las medidas pertinentes y, en todo caso, hacer consciente al menor del efecto divulgador de la Red en cuanto a los contenidos que se suben en ella.

Un buen ejemplo de la proactividad de los padres respecto a las experiencias de sus hijos en Internet ha sido la iniciativa llevada a

---

87 Ha de tenerse presente que, para poder informar al menor de todo ello, los padres deben ser los primeros en haberse formado e informado al respecto de todos los riesgos —no limitándose a la instalación de un antivirus y a la configuración del perfil en la red social como «privado»— como, por ejemplo, el «Morphing». Este anglicismo alude a la técnica desarrollada por algunos individuos que, tras descargar una fotografía de la Red, haciendo uso de software de edición y tratamiento de imágenes, realizan un montaje con otra fotografía pornográfica, obteniendo así una nueva fotografía en la que aparece un adulto o un niño protagonizando una imagen de alto contenido sexual.

88 Por citar tan sólo algunos, para prevenir el *sexting*, resulta necesaria una educación conjunta en materia de afectividad, sexualidad y viralidad y descontrol de las TIC en general, y de Internet en particular, puesto que es un desorden y un cierto desconocimiento por parte de los usuarios de estas cuatro cuestiones lo que genera situaciones de *sexting*.

Para prevenir la suplantación de identidad, resulta fundamental la labor de los padres, tutores y profesores que han de concienciar a los menores de la importancia de gestionar correctamente la identidad en Internet, de practicar el «egosurfing» (buscarse a sí mismo en la Red) y de que, entre otras cuestiones, suplantar la identidad de otra persona en la Red, en el ordenamiento jurídico español, está tipificado como delito.

cabo por Santiago Depares —el padre de un menor afectado por rumores falsos vertidos a través de la aplicación «Gossip»— que ha decidido crear la plataforma «Afectadosgossip.es» que, durante su primera semana de vida, superó las 250 personas inscritas. Más allá del número de miembros adheridos —entre los que se encuentran tanto menores afectados o potencialmente víctimas de esta aplicación que permite la inclusión de comentarios anónimos sobre lo que ocurre en los colegios, institutos y universidades como padres con hijos expuestos a esta realidad— lo que llama la atención de esta iniciativa es la vocación con la que surge que no es ni más ni menos que la de «intentar unir fuerzas para desactivar la aplicación, defendiendo a los menores afectados, dando cobertura legal a los padres y haciendo llegar a los creadores de las aplicaciones la necesidad de poner herramientas para evitar el acoso y el anonimato».

Una vez explicado el deber de formación —deber que, en nuestra humilde opinión, es el más importante y el que, seguramente, lleve más esfuerzo hacer y por lo que he destinado más espacio a su desarrollo—, abordo el segundo deber —el que hemos denominado «reactivo»— de manera mucho más breve, haciendo hincapié en que el buen desempeño de este deber también pasa por la exigencia de una previa formación de los padres sobre los mecanismos de denuncia[89] de las Redes Sociales así como sobre la existencia de organizaciones —públicas, privadas y sin ánimo de lucro— que ofrecen ayuda a los menores que han sido víctimas de alguno de las conductas ilícitas que hemos nombrado en el presente trabajo.

---

[89] De gran interés es este artículo elaborado por la OSI de INCIBE en el que se muestran las distintas opciones de denuncia de las principales redes sociales así como otras cuestiones de interés en este sentido. Disponible en https://www.osi.es/es/redes-sociales. Visitado el 15 de octubre de 2016.

10. *POKÉMON GO*, ¿JUEGO, RIESGO O FALTA DE INFORMACIÓN?

En el presente trabajo de investigación en el que hemos querido abordar la presencia de los menores en Internet en general y en Redes Sociales en particular, por el impacto que supone, no podíamos dejar de analizar —pese a que, en los último meses, hemos podido comprobar que no se trata de una cuestión exclusiva de menores— el éxito del fenómeno «Pokémon Go» entre los más pequeños de la casa y, en la medida de lo posible, analizar y responder a la pregunta que da título al apartado ¿se trata de un simple juego, es un riesgo en sí mismo o nos falta información?. Y es que, tal y como veremos a lo largo del presente apartado, no se trata de una aplicación más a la que «regalamos» nuestros datos de carácter personal a cambio de un rato de diversión sino que las implicaciones jurídicas que tiene —o puede tener— son mayores.

Comenzamos acudiendo al origen: 7 de julio de 2016, lanzamiento de *Pokémon Go* en Estados Unidos, el éxito no se hace esperar y se cuentan por miles los ciudadanos que salen a la calle guiados por la aplicación en cuestión. Tan solo ocho días después se produce el lanzamiento oficial en nuestro país y fue, sin duda, un éxito total —al menos, si basamos el éxito en el número de usuarios. Y es que, en nuestra opinión cabe afirmar que el verano de 2016 no va a ser recordado por la canción del verano, por el calor o por el destino turístico más elegido por los españoles. En esta ocasión y dada la «cuasi-omnipresencia» de esta aplicación, el verano de 2016[90] va a ser recordado, a nivel mundial, por unos pequeños seres virtuales conocidos como «Pokémon», para los expertos —niños y no tan niños— conocidos por sus nombres propios: Charmander, Squirtle o Pidgey, por citar sólo algunos. Y es que raro es el sitio en el que no hubiese una llama-

---

[90] Baste como muestra del éxito alcanzado por la citada aplicación, además de la cifras ofrecidas en el presente artículo, la reciente inclusión de «Cazar Pokémon», por parte de Google Maps. Disponible en http://as.com/betech/2016/09/05/portada/1473080557_539161.html?id_externo_rsoc=CM_ES_FB_Mo_1 7_30. Visitado el 13 de septiembre de 2016.

da de atención sobre una «Pokeparada» o en el que no se vieran numerosas personas pegados a un *smartphone*… pero de una manera particular[91].

Y es que, antes de la aparición de «Pokémon Go», eran varios los millones de usuarios —menores y mayores de edad— que utilizaban el *smartphone* como una consola en la que descargarse todo tipo de juegos[92]. Todos estos juegos están en constante evolución y raro es el día que no aparece un juego nuevo en la tienda de Apple o de Android, tanto de carácter gratuito[93]como a cambio de una pequeña contraprestación económica. Tomando esta base como cierta, pudiera parecer que, a priori, *Pokémon Go* no se trata de nada novedoso ni especialmente relevante. Sin embargo, y tal y como veremos a lo largo del

---

91 No cabe duda de que la «nomofobia», esto es, el miedo a salir de casa sin el teléfono móvil es una de las enfermedades más comunes de nuestro tiempo, pero en esta ocasión creemos que se puede afirmar que ha ido un paso más allá porque el teléfono móvil ha pasado de ser la herramienta con la que nos comunicamos —tanto por vía telefónica en sentido estricto como por mensajería instantánea, SMS o *email*—, buscamos información, nos relacionamos, nos orientamos y jugamos para convertirse en algo que va más allá de un juego.

92 De hecho, a los usuarios que, lejos de ser meros jugadores eventuales en sus ratos libres, se convierten en completos adictos a los videojuegos se les conoce como «gameholics». Algunos datos que muestran el nivel de adicción en nuestro país son: 1 de cada 10 *gamers* ha admitido estar delante de la pantalla entre 12 y 24 horas sin parar de jugar y el 6% ha afirmado haberse mantenido pegados a las pantallas jugando durante más de 24 horas. Información disponible en http://www.centroadiccionesbarcelona.com/sabes-quienes-son-los-gameholics-te-descubrimos-como-funciona-su-cerebro/. Visitado el 7 de octubre de 2016.

93 La realidad es que el «pago» de esas aplicaciones se hace a través de los datos de carácter personal del usuario que se lo descarga. En este sentido, resulta de gran interés un estudio elaborado para la Asociación Mexicana de Internet A.C. (AMIPCI), y la Secretaría de Economía (Estudio completo disponible en http://aimsi.org/wp-content/uploads/2016/06/valor_eco_Datospersonales_FINAL.pdf. Visitado el 6 de octubre de 2016) recientemente publicado sobre el valor económico de los datos de carácter personal así como la «calculadora» que lanzó el Financial Times para que los usuarios conociéramos cuánto valían nuestros datos en términos monetarios. La calculadora se puede consultar en el siguiente enlace: http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4MCrxHQ00. Visitado el 6 de octubre de 2016.

presente apartado: sí lo es y, al menos, hay que conocerlo y ser consciente de lo que supone la descarga de esta aplicación en nuestros dispositivos móviles o en el de nuestros hijos, amigos, sobrinos o nietos.

En un primer momento, debemos conocer en qué consiste *Pokémon Go* así como su funcionamiento y características principales para saber cómo actuar. Remontándonos al origen de la aplicación, *Pokémon Go* ha sido desarrollada por la empresa Niantic[94] y está disponible de manera gratuita (aunque, evidentemente, ofrece algunos servicios y funcionalidades adicionales a cambio de una contraprestación económica) tanto para dispositivos móviles IOS como Android, permitiendo al usuario acceder un juego de realidad aumentada cuyos principales protagonistas son los llamados «Pokémon».

Lo primero que ha de quedar claro es qué es un «Pokémon» puesto que, especialmente para los nacidos en los años ochenta, podemos pensar en que se trata de una serie de dibujos o de una colección de cromos de cuando éramos pequeños. Si ese pensamiento viene a nuestra mente, no andamos muy desencaminados puesto que la primera vez que estos personajes[95] aparecieron en nuestras vidas fue en los años noventa gracias a la —por aquél entonces tan de moda— «Game Boy». Años después, esas figuras se convirtieron en una serie de televisión, en juegos de mesa, peluches y hasta en una colección de cromos, dado el fervor que causaba entre los más pequeños de la casa.

Pero, como es de suponer, no nos estamos refiriendo en este punto a aquella serie de dibujos animados sino de la «reconversión» de esos pequeños seres en un juego de realidad aumentada en el que se podría decir que «Invaden físicamente» el dispositivo móvil de la persona que se lo descarga, o mejor dicho, aparece en determinados lugares cercanos a la persona que lo utiliza, siempre y cuando sean visibles por la cámara del *smartphone*.

Como todas las aplicaciones, el juego tiene unas normas y unos objetivos que cumplir —dotando al jugador de algunas herramientas para mejorar su nivel de juego y aumentar sus funcionalidades—. En este sentido, el juego consiste en lo siguiente: el jugador se descarga la

---

94 Y, en concreto, a través de John Hanke, nacido en Texas en 1967 y considerado la «mente pensante» principal de esta aplicación.

95 El término Pokémon viene de la contracción de la palabra japonesa «Poketto Monsutā», que significa monstruo de bolsillo.

aplicación y se registra con una cuenta de Google, debiendo permitir el uso de la geolocalización, el acceso a la cámara y el uso de datos móviles —en caso de que se encuentre en un lugar en el que no haya wifi— para poder comenzar la «partida».

Ponemos partida entre comillas porque no se trata de una partida con un comienzo y un final sino que, al tratarse de un juego de realidad aumentada en el que el jugador podrá capturar «Pokémon» en cualquier lugar[96] y momento en el que se encuentre —siempre que la empresa desarrolladora de la aplicación haya considerado dicho lugar como adecuado[97]para situar un «Pokémon»[98]—. En ese momento, el jugador deberá activar la cámara de su *smartphone* y, haciendo uso de las pókebolas[99], atrapar a la criatura en cuestión —criatura que, en todo momento, se verá superpuesta[100]a la realidad que rodea

---

96 Es esta una de las principales novedades y aparentes «causas del enorme éxito y furor» que ha causado el juego. Y es que los *Pokémon* han saltado de la pantalla del ordenador o la videoconsola al sofá del vecino o al restaurante en el que estamos celebrando una comida familiar, o dicho con otras palabras, *Pokémon* y yo compartimos espacio: el mundo real.

97 Dadas las quejas de algunos usuarios acerca de la necesidad de estar conectado en todo momento al juego —con el consecuente gasto de batería y datos móviles— para conocer la existencia de un *Pokémon,* la compañía no ha dudado en lanzar una nueva herramienta al efecto: «Pokémon Go Plus» que, según lo dispuesto por la propia página web de la aplicación, será lanzado el 16 de septiembre y, gracias al *bluetooth,* «cuando pases por una Poképarada, el dispositivo Pokémon GO Plus se encenderá y vibrará para alertarte de la ubicación». Disponible en http://www.Pokémongo.com/es-es/news/Pokémon-go-plus-estara-disponible-el-16-de-septiembre/. Visitado el 14 de septiembre de 2016.

98 Conviene hacer hincapié en este punto por cuanto no es el jugador el que decide sino la empresa desarrolladora la que actúa de «guía» para llevar al jugador hasta los lugares donde ha situado una criatura virtual.

99 La pokebola es un elemento que el entrenador pokémon utiliza para capturar pokémon. Es necesario lanzar y «acertar» en el Pokémon para que éste sea capturado. Información obtenida de un glosario de términos de «Pokémon Go» disponible en https://www.cnet.com/es/noticias/pokebolas-pokestops-y-huevos-un-glosario-completo-de-Pokémon-go/. Visitado el 5 de octubre de 2016.

100 Y es esta «superposición» uno de los mayores atractivos de la aplicación por cuanto el usuario siente que comparte tiempo y espacio con la criatura virtual que, gracias a la realidad aumentada, se hace, en cierta manera, «real», incorporándose al contexto del jugador.

al usuario— ya sea su casa, su lugar de vacaciones, su coche, un restaurante o un parque.

En un segundo momento, y una vez el usuario haya capturado a las criaturas, puede hacer uso de otras funcionalidades del juego como son las llamadas «pokeparadas» o los gimnasios donde, respectivamente, puede mejorar las capacidades de sus *Pokémons* y enfrentarse a los *Pokémons* de otros usuarios.

Centrados ya los aspectos prácticos del *modus operandi* del juego, entramos ya de lleno tanto en las implicaciones jurídicas del mismo, analizando la normativa aplicable, las condiciones de uso de la aplicación y los riesgos a los que nos exponemos al convertirnos en jugadores. Todo este estudio no obsta para que también hagamos un repaso y analicemos las ventajas de esta aplicación que ha causado verdadero furor tanto en nuestro país como a nivel mundial.

Por lo que se refiere a los aspectos jurídicos de *Pokémon Go*, queremos comenzar partiendo de la base de que, a día de hoy[101]no existe ninguna normativa cuyo ámbito de aplicación sea «Pokémon Go», ni siquiera, que aborde de manera directa los juegos de realidad aumentada y sus implicaciones en materia de privacidad, entre otras cosas, para el usuario. No obstante, eso no quiere decir que *Pokémon Go* sea un «territorio sin Ley», de hecho, ha de someterse a la normativa vigente y en sus condiciones de uso y su política de privacidad[102] así lo pone de manifiesto pero, seguramente no nos equivoquemos al

---

101 Aunque, dado el enorme impacto de la aplicación y los numerosos problemas que han surgido relacionados con la propiedad privada y la situación «indiscriminada» de las pókeparadas, traemos a colación a Kelly Cassidy, legisladora en el estado de Illinois (Estados Unidos), que a principios del pasado mes de agosto lanzó una propuesta de ley —que, bajo el nombre de Ley Pidgey— supondría la obligación de eliminar todas las pókeparadas situadas en negocios privados o en lugares protegidos. Disponible en http://www.antena3.com/defconplay/noticias/legisladora-illinois-propone-ley-pidgey-acabar-Pokémon_2016082600769.html. Visitado el 9 de septiembre de 2016.

102 Queremos destacar en este aspecto el hecho de que La Federación Alemana de Asociaciones de Consumidores de Usuarios (VZBV) ha advertido de la existencia de hasta 15 cláusulas abusivas en las condiciones de uso y la política de privacidad de la aplicación «Pokémon Go». El artículo en alemán está disponible aquí: http://www.vzbv.de/pressemitteilung/vzbv-mahnt-entwickler-von-Pokémon-go-ab.

afirmar que un altísimo porcentaje de los usuarios que se han descargado la aplicación ha obviado la lectura de estos términos[103].

Pues bien, en un primer momento, haremos alusión a los aspectos que, a nuestro juicio, resultan ser más relevantes en este sentido. En primer lugar, la política privacidad de *Pokémon Go* informa sobre los datos recabados[104] de la cuenta de Google y/o de Facebook del usuario que se da de alta indicando que se trata de los datos «a la que nos permita acceder la configuración de privacidad de su cuenta de Google o Facebook», o dicho con otras palabras, si el usuario no ha configurado de manera restringida las opciones de privacidad en sus cuentas de Google y Facebook, al descargarse la aplicación les estará otorgando —seguramente de manera inconsciente e ignorante— acceso a toda la información que comparte en dichos sitios (gustos, aficiones, lugares visitados, fotografías y un largo etcétera.)

Ahondando en la política de privacidad, cabe destacar que se prohíbe el uso de *Pokémon Go* a los menores de trece años, debiendo de ser sus padres quienes se registren. Conviene recordar, en este punto, que la normativa española sitúa la edad para que los menores puedan prestar el consentimiento para el tratamiento de sus datos de carácter personal en los catorce años[105].

---

103 Llamamos la atención en este punto sobre el hecho de que la Federación Alemana de Asociaciones de Consumidores de Usuarios (VZBV) ha advertido de la existencia de hasta 15 cláusulas abusivas en las condiciones de uso y la política de privacidad de la aplicación «Pokémon Go». El artículo en alemán está disponible aquí: http://www.vzbv.de/pressemitteilung/vzbv-mahnt-entwickler-von-Pokémon-go-ab.

104 De la política de privacidad se deriva que estos datos son: el nombre de usuario o nombre real, los mensajes enviados a otros usuarios, el país, la ubicación del usuario, la localización de los *Pokémon* que pretender capturar —GPS, triangulación WIFI o torres de telefonía, entre otros—, idioma elegido por el usuario, datos obtenidos vía cookies y balizas (entre otros, el tráfico web y uso agregado), la dirección IP, el agente de usuario, el navegador y sistema operativo usados, página web de origen, términos de búsqueda, tiempo dedicado, enlaces clicados, etc.

105 Así lo establece el apartado primero del artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal al afirmar que «Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela». BOE núm. 17, de 19 de enero de 2008.

Por otra parte, se informa de la cesión de los datos de carácter personal a los que la aplicación tiene acceso a terceros con el objetivo de prestar un mejor servicio y hacer un seguimiento del uso de la aplicación así como con fines de seguridad. Por último, en lo que a cuestión de protección de datos se refiere, planteamos aquí la posibilidad de que, con el uso de la aplicación en conjunción con las Redes Sociales se esté vulnerando el derecho fundamental a la protección de datos de terceras personas que, estando en el mismo escenario que un *Pokémon,* son fotografiados y compartidos en las citadas Redes Sociales sin muchas veces saberlo y, por ende, sin haber prestado su consentimiento para ello, tal y como exige la normativa vigente en la materia.

En este punto queremos volver a hacer hincapié en lo dispuesto por el Reglamento Europeo de Protección de Datos y que en su artículo 8 bajo la rúbrica «Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información» sitúa la edad mínima para que los menores puedan prestar su consentimiento en lo que se refiera a la «oferta directa de servicios de la sociedad de la información» en los dieciséis años; afirmando que, en caso de ser menor de dieciséis, «tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó». No obstante, el segundo párrafo del primer apartado matiza que «los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años».

En nuestra opinión, independientemente y con carácter autónomo de las implicaciones que *Pokémon Go* tiene o puede potencialmente tener en materia de privacidad y protección de datos[106], abogamos en este punto por la creación, a corto plazo, de una normativa aplicable a la realidad aumentada, teniendo en cuenta todos los ámbitos de aplicación y los agentes implicados. Consideramos conveniente insistir en este punto en la necesidad de que el legislador se ponga manos a la obra en esta cuestión puesto que, en nuestra opinión, la realidad aumentada tiene implicaciones de tal calado en los derechos de las

---

106 En sentido contrario se pronuncia Andrés Guadamuz que aboga por ampliar la legislación sobre protección de datos a los espacios virtuales. Disponible en http://tecnologia.elpais.com/tecnologia/2016/07/27/actualidad/1469635300_993692.html. Visitado el 15 de octubre de 2016.

personas que requiere, por sus particularidades, una normativa al efecto.

Más allá de la normativa aplicable en materia de protección de datos y privacidad, únicamente citamos a continuación algunos aspectos normativos que, en nuestra opinión, han de tenerse en cuenta respecto a *Pokémon Go:*

• Normativa en materia de tráfico. Y es que, si bien cuando descargas la aplicación el mensaje de «no captures *Pokémon* mientras conduces» aparece en tu pantalla, lo cierto es que el Juego te permite hacer uso de la aplicación marcando en una casilla que no eres tú el conductor del vehículo. En este sentido, baste traer a colación que, el apartado g) del artículo 76 de la Ley General de Tráfico[107] establece como infracción grave el hecho de «Conducir utilizando manualmente dispositivos de telefonía móvil, navegadores o cualquier otro medio o sistema de comunicación (…)». Traemos a colación en este punto si el hecho de conducir jugando a *Pokémon* exige una concentración mayor y, por tanto, una distracción total de la conducción por lo que podríamos hablar de «conducción temeraria» —previsto en el artículo 77 de la Ley General de Tráfico como infracción muy grave.

• Normativa en materia de propiedad intelectual. Y es que «Pokémon Go» no viene sino a demostrar la necesidad de armonizar e incluir una regulación específica de los videojuegos por cuanto, a día de hoy, esta aplicación cabría encajarla en tres posibles figuras contempladas por la Ley de Propiedad Intelectual[108], a saber: obra audiovisual, obra multimedia o programa de ordenador. En nuestra opinión, y sin ánimo de extendernos más en esta cuestión, lo ideal sería crear una protección *ad hoc.*

• Normativa en materia de defensa a los consumidores y usuarios. Y es que la normativa exige que el proveedor de servicios los ofrezca con todas las garantías necesarias. En concreto, en nuestro

---

107 Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial publicado en el BOE núm. 261, de 31 de octubre.

108 Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. Publicado en el BOE el 22 de abril de 1996.

país debemos acudir a lo dispuesto por Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias[109] (en adelante, LGDCU) que, en su artículo 12, establece la obligación para los empresarios —en el caso de *Pokémon Go*, de la empresa Niantic— de poner «en conocimiento previo del consumidor y usuario, por medios apropiados, los riesgos susceptibles de provenir de una utilización previsible de los bienes y servicios, habida cuenta de su naturaleza, características, duración y de las personas a las que van destinados».

En nuestra opinión, en términos de *Pokémon Go,* las obligaciones previstas en la LGDCU se traducirían en que la empresa desarrolladora debe establecer los cauces para asegurarse de que únicamente situará *Pokémon* en lugares seguros, que no sean propiedades privadas y que no pongan en peligro la integridad física del jugador —debiendo evitar, por ejemplo, situarlos en lugares de difícil acceso que pongan en riesgo al usuario (montañas, barrancos, etc.).

• Normativa en materia de derecho de reunión. Y es que, hay que estudiar la posibilidad de que las póke-quedadas[110] puedan ser integradas en el concepto de reunión que prevé la citada normativa y, por tanto, deban cumplir con las exigencias establecidas por la misma. En concreto, en nuestro país hay que acudir a lo dispuesto por la Ley Orgánica 9/1983, de 15 de julio, reguladora del derecho de reunión[111] que, en su Capítulo IV, bajo el epígrafe «De las reuniones en lugares de tránsito público y manifestaciones» exige en su artículo octavo que las reuniones que vayan a ser celebradas en lugares de tránsito público —como es el caso de las póke-quedadas— deberán ser «comunicadas por escrito a la autoridad gubernativa correspondiente por los organizadores o promotores de aquéllas, con una antelación de diez días naturales, como mínimo y treinta como máximo».

---

109 Publicado en BOE núm. 287 de 30 de noviembre de 2007.

110 De momento, la que cuenta con el mayor número de usuarios congregados es la poke-quedada celebrada en Madrid el pasado 29 de julio. Disponible en https://guiaPokémon-go.com/2016/07/31/pokequedada-Pokémon-go-madrid-batio-records/. Visitado el 14 de septiembre de 2016.

111 Publicado en el BOE de 18 de julio de 1983, datando la última modificación de la Ley de marzo de 2015.

Continúa el apartado octavo matizando que «Si se tratare de personas jurídicas la comunicación deberá hacerse por su representante». Por lo que, haciendo una interpretación analógica y aplicable al fenómeno *Pokémon Go,* deberá ser el representante jurídico de *Pokémon Go* quien informe a las autoridades correspondientes de nuestro país sobre la convocatoria de las póke-quedadas.

Ahondando en esta cuestión, la información que ha de comunicarse a la autoridad correspondiente respecto a la reunión que se va a mantener viene regulada en el artículo nueve de la citada Ley y está integrada por:

«a) Nombre, apellidos, domicilio y documento oficial de identificación del organizador u organizadores o de su representante, caso de personas jurídicas, consignando también la denominación, naturaleza y domicilio de éstas.

b) Lugar, fecha, hora y duración prevista.

c) Objeto de la misma.

d) Itinerario proyectado, cuando se prevea la circulación por las vías públicas.

e) Medidas de seguridad previstas por los organizadores o que se soliciten de la autoridad gubernativa».

Por último, en lo que al derecho de reunión se refiere, traemos a colación lo dispuesto por el artículo 10 de la Ley reguladora del mismo que establece que «Si la autoridad gubernativa considerase que existen razones fundadas de que puedan producirse alteraciones del orden público, con peligro para personas o bienes, podrá prohibir la reunión o manifestación o, en su caso, proponer la modificación de la fecha, lugar, duración o itinerario de la reunión o manifestación», debiendo tratarse de una resolución motivada y debiendo ser notificada «en el plazo máximo de setenta y dos horas desde la comunicación prevista en el artículo 8».

• Código Penal. En él están previstos algunos delitos en los que pueden incurrir los jugadores de *Pokémon Go* al «hacer todo lo posible» por capturar un *Pokémon* en el lugar en el que le indique la aplicación. Estos son el delito de allanamiento de morada o el de acceder a recintos públicos fuera de las horas de apertura.

En concreto, el artículo 202 del Código Penal reza así: «El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador, será castigado con la pena de prisión de seis meses a dos años». Mientras que, por su parte, el artículo 203 regula el acceso tanto a sitios públicos fuera de las horas de apertura como a los domicilios de personas jurídicas públicas o privadas al afirmar que «1. Será castigado con las penas de prisión de seis meses a un año y multa de seis a diez meses el que entrare[112] contra la voluntad de su titular en el domicilio de una persona jurídica pública o privada, despacho profesional u oficina, o en establecimiento mercantil o local abierto al público fuera de las horas de apertura». En nuestra opinión, cabe la interpretación analógica de sendos preceptos del Código Penal en lo que respecta a los casos que se están dando en algunos jugadores empedernidos de *Pokémon Go* que, hacen lo que sea, por capturar una de esas criaturas.

Baste como ejemplo uno de los casos que más representación ha tenido en prensa[113]: el de Boon Sheridan. Este diseñador tiene su residencia en una antigua Iglesia del Estado de Massachusetts en Estados Unidos, y, hasta este pasado verano, vivía tranquilo y sin sobresaltos. Sin embargo, y haciendo uso de un juego de palabras, el éxito de *Pokémon Go* ha causado un fracaso en la vida de este diseñador al integrar un «gimnasio» en su casa. Y, sí, como venimos diciendo, lo ha hecho sin pedirle permiso y sin siquiera informarle, generando que, de un día para otro, la casa de este famoso diseñador se haya visto «invadida»[114] por cientos de jugadores en búsqueda de *Pokémon*.

---

112 Distingue el Código Penal entre «entrar» y «mantenerse» al indicar en el segundo apartado del artículo 202 que «Será castigado con la pena de multa de uno a tres meses el que se mantuviere contra la voluntad de su titular, fuera de las horas de apertura, en el domicilio de una persona jurídica pública o privada, despacho profesional u oficina, o en establecimiento mercantil o local abierto al público».

113 Valga por todas ellas: http://tecnologia.elpais.com/tecnologia/2016/07/27/actualidad/1469635300_993692.html. Visitado el 16 de octubre de 2016.

114 El malestar que le causa esta situación llegó hasta tal punto que hasta el proio Sheridan, haciendo uso de su cuenta de Twitter, puso de manifiesto lo que, a nuestro entender, puede ser considerado como un «grito de auxilio». En concreto, el tweet rezaba así: «¿Tengo algún derecho respecto a la localización virtual que me ha venido impuesta? Las empresas tienen expectativas, pero esta es mi casa».

• Normativa en materia de Redes Sociales. Si bien no existe a día de hoy una normativa cuyo ámbito de aplicación esté integrado de manera expresa por las Redes Sociales sino que son varias las normas que han de tenerse en cuenta a la hora de subir contenido a las Redes Sociales —LOPD, LPI etc.— , sí que hemos querido incluir esta referencia por cuanto el fenómeno de *Pokémon Go* tiene un gran impacto en las Redes Sociales puesto que los usuarios comparten sus éxitos —en forma de fotografías y vídeos que inmortalizan los momentos en los que capturan a los *Pokémon*— en aquellas y, en multitud de ocasiones, junto a los jugadores aparecen otras personas —familiares y amigos— que están compartiendo ese momento con los jugadores y a los que habrá de pedir el consentimiento para subir la citada fotografía a la Red Social.

Dejando a un lado las implicaciones jurídicas —y sin entrar a valorar si el uso de los datos de carácter personal del usuario ha de ser considerado como inconveniente de la aplicación o como mera consecuencia necesaria de su uso— no cabe duda de que, como toda funcionalidad relacionada con las TIC —y en, nuestra opinión, las aplicaciones no son más que funcionalidades TIC— tiene sus ventajas y sus inconvenientes y antes —o, después, si ya es demasiado tarde—, de sumarnos a los millones de usuarios que la descargan en su dispositivo móvil, es conveniente conocer unas y otros.

Empezando por las ventajas —más allá de la propia diversión y entretenimiento del usuario—, citaremos las siguientes:

— Fomenta el ejercicio físico. En medio de una sociedad eminentemente sedentaria que pasa horas y horas delante del ordenador, la *tablet* o el *smartphone, Pokémon Go* hace que los usuarios se levanten de la silla y se dirijan a los lugares, tanto guiados por su *smartphone* como incitados por otros usuarios o por la propia aplicación que promueve poke-paradas en distintas localizaciones gracias a las que podrán capturar un mayor número de *Pokémon*.

— Genera interacción con otros usuarios. Al igual que muchos otros juegos y aplicaciones *online,* insta a los usuarios a competir con otros jugadores, en esta ocasión, en los llamados «gimnasios».

— Ayuda a aumentar y mejorar la capacidad de orientación de los usuarios así como el conocimiento de la ciudad en la que se juega.

— Insta a conocer nuevos lugares. El hecho de que el jugador no pueda elegir las zonas en las que capturar los *Pokémon* hace que los usuarios acudan a las póke-paradas y conozcan zonas de la ciudad en la que se encuentran que probablemente, de no ser por el juego, no se encontrarían entre sus destinos, teniendo, también, el beneficio de conocer otras zonas de la ciudad y hacer turismo, al tiempo que cazando *Pokémon*.

— Ayuda a superar determinadas fobias relacionadas con la incapacidad de relacionarse y de tener vínculos con el exterior[115].

— Supone una oportunidad de negocio para las empresas que pueden hacer convenios para incluir una poke-parada en su establecimiento o, como ya he visto este mismo verano en Nueva York, ofrecer descuentos en una tienda de ropa a los usuarios de *Pokémon Go*.

— Mejora la situación de los usuarios con depresión y ansiedad. Así lo afirma el psicólogo John M. Grohol, quien, a través de la web PsychCentral, ha asegurado que «los usuarios del juego han experimentado una mejora inesperada en trastornos como la depresión y la ansiedad»[116].

En el otro lado de la moneda, nos encontramos con los inconvenientes:

— Genera adicción. Este es un inconveniente común a gran parte de los juegos y aplicaciones pero, en el caso de *Pokémon Go*, el hecho de que la «partida» no finalice en ningún momento porque cuando uno menos se lo espera aparece un *Pokémon* en su comida —por poner un ejemplo— es, sin duda, un añadido para aumentar el nivel de adicción de la citada aplicación.

---

115 Son varias las investigaciones que afirman el valor de la realidad aumentada para curar este tipo de fobias. Información disponible en http://www.tuexperto.com/2016/07/06/investigadores-usan-la-realidad-virtual-para-curar-miedos-y-fobias/. Visitado el 2 de octubre de 2016.

116 En concreto, los expertos afirman que «El hecho de enfrentarse a sus miedos con el objetivo de capturar *Pokémon* y verse doblemente recompensados con las recompensas del videojuego y la gran aceptación global entre "entrenadores", está convirtiendo el juego en una herramienta muy poderosa para superar o atenuar estas dificultades». Disponible en https://psicologiaymente.net/clinica/Pokémon-go-combatir-trastornos-mentales#!. Visitado el 5 de octubre de 2016.

— Refuerza «el patrón aislacionista del jugador, produciendo riesgo de desconexión social en sus usuarios»[117].

— Un uso indiscriminado, y en cierta medida irracional o inconsciente, puede devenir en la infracción de la normativa vigente, ya sea en materia de protección de datos, por temas de seguridad, de tráfico o de allanamiento de morada, por citar solo algunos.

— Riesgo de ser víctima de *malware*. En los pocos meses que esta aplicación ha visto la luz, ya han sido varias las aplicaciones y páginas web[118] que, simulando ser servicios y funcionalidades adicionales de *Pokémon Go*[119], infectan los dispositivos móviles de los usuarios.

— Riesgo de ser víctima de hurtos y robos. Y es que, al conocer las pókeparadas y dado la gran cantidad de gente que se concentra en un mismo punto con el único objetivo de cazar *Pokémon*, personas con malas intenciones pueden acudir a dichos lugares para sustraer objetos de valor de los usuarios sin que, en muchas ocasiones, se den cuenta al estar centrados únicamente en la captura del *Pokémon* en cuestión.

— Distracción del resto de tareas. Y vamos un paso más allá al no referirnos en este punto únicamente al aislamiento social sino a la distracción en horario escolar y/o laboral[120].

---

117 Así lo afirma el análisis de los efectos psicológicos y sociales del juego que ha realizado Coaching Club, organización que presta ayuda a empresas y particulares. Disponible en http://www.abc.es/tecnologia/moviles/aplicaciones/abci-Pokémon-juego-causa-sindrome-peter-pan-201608031525_noticia.html. Visitado el 12 de septiembre de 2016.

118 En el Informe ESET se puede consultar el listado de aplicaciones maliciosas que se «disfrazan» de vinculadas con *Pokémon Go*. Disponible en http://www.welivesecurity.com/2016/07/15/Pokémon-go-hype-first-lockscreen-tries-catch-trend/. Visitado el 13 de septiembre de 2016.

119 Yendo un paso más allá, ya ha habido varios casos en los que, en países en los que la aplicación no se había lanzado de manera oficial, está disponible y al alcance de todos los usuarios una versión pirata de la misma que introduce un «software espía» conocido como DroidJack que permite obtener datos de la cámara, ubicación del dispositivo, interceptación de mensajes de texto, entre otros. Disponible en http://ayudaleyprotecciondatos.es/2016/07/18/Pokémon-go-privacidad/. Visitado el 13 de octubre de 2016.

120 Es por ello que ya son varias las empresas que han prohibido el uso de *Pokémon Go* en horario laboral. Baste citar como ejemplo: Volkswagen, Airbus y Boeing. Disponible en http://www.elmundo.es/economia/2016/08/19/57b602e1468aeb01738b457b.html. Visitado el 12 de septiembre de 2016.

Como vemos, son muchas las ventajas e inconvenientes de la aplicación y todos los jugadores —tanto los adultos como los menores— deben ser conscientes de ellas, debiendo los padres, en este sentido, desarrollar una labor formativa e informativa dada la falta de madurez de sus hijos que, en muchas ocasiones, actuarán de manera errónea por desconocimiento e ignorancia de los peligros y los riesgos a los que se exponen.

Por último, y tratando de responder a la pregunta que da título al presente apartado, concluiremos afirmando que la respuesta es «todas son correctas», es decir, *Pokémon Go* es un juego —y, dado el éxito, cabe afirmar que proporciona diversión y entretenimiento sin fin—; también es un riesgo —y es que, como hemos visto, el uso de la aplicación conlleva una serie de riesgos y peligros tanto para el propio usuario como para su dispositivo móvil— y, por último, es innegable que, respecto a este fenómeno aún nos falta mucha información.

11. CONCLUSIONES

No nos resulta sencillo hacer unas conclusiones a este trabajo debido a lo fácil que es elucubrar hacia postulados teóricos y, en algunos casos, utópicos.

Señalar que tanto los padres o tutores, como los centros educativos y las personas encargadas, directa o indirectamente, de la formación de los menores en general, deben preocuparse y ocuparse del uso responsable de Internet y, en particular, de la participación en Redes Sociales de aquéllos en forma responsable, es una manera de llamar la atención sin sentido práctico y, como decíamos, con marcados tintes utópicos y poco cercano a la realidad, resultando, no solamente enunciados genéricos que no encuentran demasiado acomodo en la realidad diaria, sino excesivamente sencillos y hasta pobres en su contenido.

Es por ello que, con humildad, pero con el firme convencimiento de lo que planteamos, queremos presentar unas conclusiones, de sentido práctico, que puedan orientar en la mejor forma de apoyar desde todos los ámbitos, el acercamiento al menor a un uso responsable, útil y socialmente positivo de las Redes Sociales.

De esta forma, queremos presentar como conclusiones que sean fiel reflejo de lo expresado en este trabajo y, a ser posible, puedan ser aprovechadas en la realidad del asesoramiento al menor en la utilización de las Redes Sociales, estas cinco llamadas de atención:

Primera. Edad de acceso a las Redes Sociales.

Independientemente de que, por quien corresponda, se señale en los correspondientes textos, preferentemente normativos, la mínima edad de acceso a una red social, ya sea catorce años como parece ser la tendencia más seguida en la actualidad o dieciséis años como señala el Reglamento europeo sobre protección de datos, independientemente de ello, repetimos, es necesario que se legisle y se pongan los medios para obligar a los responsables de servicios de la sociedad de la información y, en particular, a los responsables de las Redes Sociales a que se verifique y se cumpla este requisito mínimo de edad de acceso a una red social, con propuesta de duras sanciones a quien

permita a una persona con edad menor a la mínima exigida, inscribirse o ser titular de una cuenta o registro en la red social.

Hay quien opina que esto es imposible de comprobar pero, en el ámbito europeo y, en particular, en el español, es una cuestión muy sencilla. Recordemos, a estos efectos, que el Documento Nacional de Identidad electrónico tiene dos certificados asociados: uno un certificado de firma y otro un certificado de identificación. Estando claro que en el caso de menores de edad el certificado de firma no puede estar activado ya que no se encuentran en pleno ejercicio de sus derechos civiles, nada impide que esté activado el certificado de identificación que, de manera inequívoca identifica a la persona y la edad que tiene. Es cuestión de exigir normativamente a los prestadores de servicios de las Redes Sociales que comprueben mediante el certificado de identificación la edad correspondiente de mayor de catorce o dieciséis años en el momento de permitir la inscripción a su red.

Segunda. Derecho a la información del menor.

Como ya hemos señalado a lo largo de este trabajo, los derechos de los menores, en la Sociedad de la Información y la Comunicación en la que vivimos, el derecho a una información adecuada y adaptada a sus necesidades así como el derecho a que se les proporcionen los medios adecuados para protegerse y, en caso necesario, defenderse ante un determinado comportamiento o acción ilícita son derechos imprescindibles para la vida cotidiana del menor que, por sus condiciones de inmadurez e inocencia, puede verse inmerso en un problema de cierta índole relacionado con el uso de las TIC y ante el cual, el Derecho, ha de estar preparado y ofrecerle soluciones.

Esta formación e información no puede venir nada más que de la mano de los agentes implicados en el desarrollo cultural y humano del menor que están obligados a proporcionar los medios, insistimos que formativos e informativos, para que el menor pueda adaptarse y avanzar en su formación con la triple seguridad exigible en el ámbito de las tecnologías de la información y las comunicaciones, a saber: seguridad física en la utilización de las herramienta electrónicas, seguridad lógico-informática en la orientación de su utilización y manejo y, cómo no en forma imprescindible, seguridad jurídica que garantice que puedan ejercer la libertad en su ámbito de desarrollo con la protección de la normativa adecuada que sancione aquéllas posturas

o comportamientos de terceros que eviten la marcha normal de su actividad formativa.

Naturalmente que estos agentes, cada uno en su entorno y con su grado de responsabilidad, son los padres o tutores y los profesores y responsables de su formación en los centros educativos. Pero también los son los encargados de legislar, diseñar y proponer currículos formativos y/o de ocio. No olvidemos en este aspecto a los abuelos y otras personas cercanas a los menores que se ocupan, en muchas ocasiones, no solamente de su cuidado y compañía, sino también de su orientación en múltiples aspectos.

Tercera. Transparencia, privacidad desde el diseño y por defecto y derecho al olvido.

La información va unida a la transparencia de forma que están claros los principios y comportamientos que deben acompañar al menor en las Redes Sociales. A esto se añade, además, las dos figuras que presenta normativamente el Reglamento europeo sobre protección de datos y que se conocen como la «privacidad por defecto (P×D)» y la «privacidad desde el diseño (PdD).»

Señala en este sentido el Reglamento europeo sobre protección de datos que el responsable del tratamiento implementará, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento garantice la protección de los derechos del interesado y, añadimos nosotros, existan desde el propio diseño medidas de control y protección a los menores en la utilización de las Redes Sociales.

De otra parte, el responsable del tratamiento implementará mecanismos con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento y, especialmente, que no se recojan ni conserven más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación. En concreto, estos mecanismos garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas. Cuestión que, a nuestro modo de ver, podría garantizar el derecho al olvido de los datos del menor en las Redes Sociales cuando éste

lo solicitara y de todo aquello que, añadido y utilizado en momentos de inmadurez o desconocimiento del menor, éste no quiera que permanezcan en la Red Internet ni puedan ser conocidos o utilizados por nadie.

Cuarta. Formación de los menores, padres, madres y educadores en el uso adecuado de las TIC.

Como ya hemos señalado a lo largo de este trabajo, la Administración educativa debe impulsar y fomentar la formación de los menores, padres, madres y educadores en el uso adecuado de las tecnologías de la información ya que el uso responsable de las TIC depende en gran medida de la formación del usuario, de ahí que la educación y la concienciación sean un elemento esencial para la consecución de dicho fin.

Es así que se debe estructurar de forma clara, concreta y vinculante la formación en el uso de las TIC en general y de las Redes Sociales, en particular, a los padres, madres, tutores, educadores y, en general, todos aquellos que intervienen en la formación y acompañamiento educacional y de desarrollo del menor.

En este mismo sentido, se debe promover la sensibilización y la comprensión de todos los agentes implicados acerca de los riesgos, normas, garantías y derechos relativos a la utilización de las Redes Sociales, haciendo hincapié en que las actividades dirigidas específicamente a los menores de edad deberán ser objeto de especial atención.

Quinta. *Pokémon Go:* mayores garantías jurídicas en el uso de servicios basados en realidad aumentada.

En nuestra opinión, *Pokémon Go* no es sino el principio de lo que se avecina en lo que a realidad aumentada se refiere. Y es que, a día de hoy, esta funcionalidad apenas ha sido explotada y, visto el éxito, creemos poder afirmar con posibilidades de acierto que no tardarán en aparecer numerosas aplicaciones y dispositivos en los que la realidad aumentada sea el reclamo para la prestación de un determinado servicio o para la venta de un determinado producto. Es normal. Estamos en la Sociedad de la Información y las Comunicaciones, una Sociedad que, en pleno siglo XXI, se ha de guiar por las TIC y en las que la globalización y la inexistencia de barreras físicas y geográficas

es una realidad y en la que todo avanza a una velocidad muchísimo mayor a la que la Ley puede hacerlo. Pero eso no puede hacer que el legislador se quede de brazos cruzados.

La Ley debe estar al servicio de los ciudadanos y, en el entorno TIC, esta afirmación, como no podía ser de otra manera, resulta plenamente aplicable. Por todo ello, el uso de *Pokémon Go* —especialmente en lo que respecta a este por parte de menores— debe mejorar en lo que a las garantías jurídicas que, a día de hoy, ofrece por cuanto, en nuestra opinión, resultan insuficientes.

Una vez presentadas estas cinco conclusiones, con el ánimo de apoyar y colaborar en la mejor formación e información del menor en el uso de las Redes Sociales terminemos señalando que el desarrollo tecnológico, la Red Internet y la utilización de las herramientas a ellos asociados, constituyen una realidad social, económica, cultural y, sin ninguna duda, con altos contenidos éticos en el campo de los menores de edad que el derecho no puede desconocer.

Es una realidad incontestable que las nuevas tecnologías se han integrado en el día a día de los menores españoles.

Partiendo de la asunción de esta coyuntura, la obra de Laura Davara Fernández de Marcos profundiza en el estudio de las implicaciones que de ello se deriva, así como en el impacto que internet y las redes sociales generan en la privacidad de este colectivo. Para ello aborda el marco jurídico nacional aplicable a las distintas situaciones que se pueden producir en el uso de internet, con referencias a normativa de distintos países. Examina, asimismo, el papel que deberían asumir en este ámbito los centros educativos y los padres por su responsabilidad en la educación de los menores y, finalmente, realiza un análisis específico de las implicaciones que el juego «Pokémon Go» ha provocado en la privacidad de sus usuarios y, en particular, en las personas más jóvenes. La obra concluye con una serie de recomendaciones dirigidas a reforzar las garantías, los derechos y la seguridad de los menores en el uso de internet.

ISBN 978-84-340-2399-4