LA PROTECCIÓN DE LA PRIVACIDAD DE LOS MENORES EN INTERNET

TRABAJO FINAL DE GRADO.
CRIMINOLOGÍA Y SEGURIDAD 2017/2018

ALUMNO: **Sandra Porcar Parra**
TUTOR: **Félix Serrano Gallardo**

INDICE:

Abreviaturas

AEPD	Agencia Española de Protección de Datos
ARPA	Advanced Research Projects Agency
CE	Constitución Española
CP	Código Penal
DPO	Data Protection Officer
INCIBE	Instituto Nacional de Ciberseguridad
INE	Instituto Nacional de Estadística
INTECO	Instituto Nacional de Tecnologías de la Comunicación
ISP	Internet Service Provider
LECrim	Ley de Enjuiciamiento Criminal
LSSICE	Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico
ONTSI	Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información
OSI	Oficina de Seguridad del Internauta
PIAs	Privacy impact assessment
RGPD	Reglamento General de Protección de Datos
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea

Extended summary

Since the emergence of new information and communication technologies or also known as ICT, has moved to live in a completely digitized world in which these are the undisputed protagonists. ICT is present in all kinds of areas, in the educational, social, cultural, leisure, professional, etc., providing numerous advantages that have greatly facilitated everyday life for most people, for example, immediate access to information and culture, creation of new professions and markets, cross-border communication.

However, while ICTs have provided many benefits, they also carry great risks if they are not used correctly and responsibly. Risks to which special attention must be paid if it is the children who suffer them.

More and more children are using ICT, according to a survey realized by the National Institute of Statistics in 2016, 95.2% of children between 10 and 15 years use the Internet, 94.9% use computers and 69% '8% have a mobile phone.

New generations live connected daily, to study, play, talk with their friends or look for any type of information. The great presence of minors on the Internet and the continuous rise of new technologies leads to the appearance of malicious people who want to take advantage of them or even the minors themselves use it to harass or extort others. The apparent impunity due to the anonymity provided by the Internet fosters that, actions previously carried out in the physical sphere, now go on to develop in the digital sphere, and as a result, a door opens to new crimes whose essential characteristic is that they are committed through of technological means, which makes the identification of the culprit considerably difficult and sometimes causes more serious consequences for the minor.

Among the most common crimes that occur today on the Internet and that have a child victim are the following:

- Cyberbullying is the harassment of a minor by another minor through technological means. It is a crime with very serious consequences that unfortunately happens more and more frequently. The commission through technological means and the anonymity that these provide, makes that the minors not really aware of the damage it cause and therefore, encourages them to adopt more violent and offensive roles. Many times, cases that, at the beginning, could be classified as bullying, such as bullying, it's transferred to the Internet later and referred to as cyberbullying. The psychological damage caused by this type of crime is really serious, even causing the suicide of many children.

- Sexting consists of sending photos and videos of sexual content through any technological means, usually the mobile phone. This practice is very common among teenagers, who are exchanging photographs or videos of erotic or provocative nature voluntarily with their partners or people they like. The dangerous thing of this fact occurs when for example there is a rupture or a discussion and the receiver of the content blackmails the sender with publishing their videos or images.
- Grooming is also one of the crimes that is occurring more frequently and consists of those behaviours performed by an adult to establish relationships with a child through the Internet with the intention of obtaining material of a sexual nature or even prepare a meeting sexual with him. In this type of behaviour, many times an adult pretends to pose as a child to establish relationships with other minors and, once they has earned his trust, they begin to ask for photographs or any kind of compromised material. The problem occurs when they get this type of material, then they use it to blackmail the child and get sexual encounters with him or to continue to provide more material.

The danger of these and other crimes is that when being committed through the Internet the child is exposed to its consequences constantly, for example, if a child is physically harassed at school by their companions, that child will not be harassed again until the next day when he return to school. However, with cyberbullying being committed through new technologies, these break the space-time barrier and the child is harassed at any time, anywhere and by all kinds of people, which obviously increases, and much, the psychological consequences that the child has to endure.

Being a victim of cyber crimes is not the only risk to which minors are exposed. The use of the Internet can also imply a violation of their fundamental rights, rights such as honour, personal and family privacy and their own image. In general your private life can be available to anyone, unconsciously when browsing for web pages or consciously and voluntarily being themselves who provide all kinds of personal data for example through social networks.

In view of these new developments, the adoption of new strategies and measures to combat them is essential. In the legislative field, it is necessary to bet on a specific protection related to minors and the technological world and, in addition, that is constantly updated. It is true, that every time there are more protection mechanisms against new

technologies, in this sense, we have now the “Nuevo Reglamento General de Protección de Datos” that will be applicable in 2018 and that introduces many new features that are expected to be very beneficial in the near future, such as the figure of “Data Protection Officer” or the famous “Right to be forgotten”.

We must also highlight the role of service providers. There are many minor users of a Social Network, so providers should not depart from the risks that these suppose, but try to establish better privacy and security mechanisms to provide greater protection to its users.

However, the main thing is prevention, and inside this is very important the education. A good education of minors in the correct and responsible use of ICTs and in the risks they may entail is essentials, but also it is vitally important to educate parents, who often ignore these risks or are not aware of the dangers and at the same time educate the teaching staff also, since many of the cases that occur on the Internet have their trigger in the school ambit. There are many the disputes that take place in schools and institutes among children and adolescents who then move to social networks, chats and more. Therefore, it is about providing the minors with a good education and also with the older ones so that they can transmit that knowledge to the little ones.

Resumen: La aparición y evolución de las nuevas tecnologías han traído consigo numerosos beneficios que han posibilitado una vida más cómoda y llena de oportunidades, pero también han conllevado una serie de riesgos. Los menores son los que hacen un mayor uso de las TIC e Internet, lo que unido al hecho de su especial vulnerabilidad, les convierte en víctimas idóneas de ataques a su privacidad y resto de derechos fundamentales a través de ilícitos cometidos a través de aquéllas vías. Por lo tanto, además de establecer mayores garantías y mejor protección para los menores en materia legislativa también es importante la educación para que aprendan a usar responsablemente las TIC y así evitar que sean víctimas de delitos o que sean ellos mismos los que se expongan excesivamente.

Palabras clave: Nuevas tecnologías, menores, TIC, Internet, delitos cibernéticos, educación.

Abstract: The emergence and evolution of new technologies have brought numerous benefits that have made possible a more comfortable life and full of opportunities, but they have entailed a series of risks also. Children are the ones who make the greatest use of

ICT and the Internet, which, together with the fact of their special vulnerability, makes them the ideal victims of attacks on their privacy and other fundamental rights through unlawful acts committed through these means. .Therefore, in addition to establishing greater guarantees and better protection for minors in legislative matters, education is also important so that they learn to use ICTs responsibly and so prevent them from being victims of crimes or that they are themselves those who expose themselves excessively.

Keywords: New technologies, minors, ICT, Internet, cyber crimes, education.

1 Introducción.

Las tecnologías de la información y la comunicación, comúnmente conocidas como las TIC han supuesto un gran avance para las sociedades de hoy en día. Desde su aparición, su evolución ha sido, y sigue siendo, exponencial y están tan inmersas en la vida cotidiana que difícilmente se podría vivir sin ellas. No resultaría arriesgado decir que prácticamente todas las personas –en los países desarrollados- disponen de teléfonos móviles, tablets, ordenadores, etc., a los que están conectados constantemente. Se utilizan para todo tipo de actividades, desde las tareas más básicas como chatear con los amigos, buscar información, ver programas televisivos…, hasta para tareas más complejas como por ejemplo hacer una transacción bancaria.

Uno de los sectores que más uso hace de las TIC es el de los menores[1], los más pequeños nacen ya en un mundo digitalizado en el que las nuevas tecnologías son las protagonistas absolutas, por eso deben aprender a controlarlas y usarlas con responsabilidad desde el primer momento. Las TIC traen consigo numerosos beneficios que facilitan considerablemente la vida diaria, especialmente para los menores, a quienes dota de unas posibilidades que hace años eran inimaginables. Hay que aceptar que las nuevas tecnologías forman parte del presente pero sobre todo del futuro, en el que su presencia será aún mayor.

Aunque las TIC han facilitado, y mucho, la vida a todos en general, no hay que olvidar que éstas también conllevan una serie de riesgos a los que hay que prestar especial atención cuando las personas que sufren las consecuencias de esos riesgos son los menores. En muchos aspectos se podría decir que los menores son más hábiles manejando las nuevas tecnologías que los adultos, prácticamente nacen con ellas por lo

[1] Según el INE el 95’2% de los menores entre 10 y 15 años hacen uso de Internet, la población de entre 16 y 74 años usan Internet un 80’6% y a medida que va avanzando la edad su uso va decreciendo.

que adquieren unas habilidades y una destreza en su manejo desde pequeños que a los adultos les resulta más costoso. Sin embargo, aunque sean mejores manejándolas también hay que tener en cuenta que son menos cautelosos, menos desconfiados, lo que los hace más vulnerables ante cualquier ataque que puedan sufrir a través de las TIC. En muchas ocasiones, no son conscientes de que hay gente malintencionada que pretende hacerles algún daño a través de estos medios, o no son conscientes de que tienen que tomar precauciones en sus actuaciones a través de Internet para no ser ellos mismos los que se expongan a esos ataques.

La realidad demuestra que cada vez son más comunes los ataques cibernéticos que tienen como víctimas a los menores. Delitos como el *ciberbullying* en el que un menor es acosado virtualmente por otro menor, el *grooming* en el que un adulto acosa a un menor a través de medios tecnológicos, el *sexting* o la pornografía infantil, entre otros, están a la orden del día. Además, el único riesgo no es solo ser víctimas de delitos como los mencionados sino que los menores también ven cada vez más como sus derechos fundamentales son vulnerados con gran facilidad. Derechos tan importantes como la privacidad y la intimidad pasan a un segundo plano e incluso dejan de existir en Internet, por eso, hay que enseñarles a los menores que no se trata de derechos renunciables sino que son necesarios para mantener una mínima calidad de vida y que deben usar las nuevas tecnologías de forma responsable para no volcar en Internet toda su información personal. La Oficina de Seguridad del Internauta (OSI) advierte que "todo lo que hacemos en Internet deja un rastro y nuestra información personal es muy valiosa, no solo para nosotros, también para otras personas, empresas e incluso para los ciberdelincuentes"[2].

A medida que van evolucionando las nuevas tecnologías también van apareciendo nuevas formas de criminalidad en la Red, por este motivo, a lo largo del presente trabajo, se analizará la situación actual de los menores en el uso de las TIC, las ventajas y riesgos más comunes a los que se ven expuestos y se atenderá especialmente a las Redes Sociales online que se hayan de plena actualidad y que suponen uno de los medios donde más ataques sufren los menores.

También se irá viendo como la legislación se va adaptando a los avances de las TIC con la aparición del nuevo Reglamento General de Protección de Datos (RGPD). Se trata de un Reglamento que entró en vigor en el año 2016 y que no se aplicará hasta el año

[2] Oficina de Seguridad del Internauta "En Internet cuida tu privacidad" [en línea] < https://www.osi.es/es/tu-informacion-personal > [consulta: 30 de agosto de 2017].

2018, por lo que no se podrán valorar sus consecuencias prácticas pero sí analizar las novedades que ofrece.

Asimismo, se atenderá a algunos mecanismos de protección en materia de privacidad en Internet como el *Data Protection Officer* (DPO) o el derecho al olvido y el papel que desempeñan los proveedores de servicios para garantizar la privacidad de sus usuarios.

Por último, se hará hincapié en la importancia de la educación de los menores en un uso responsable de las TIC como base esencial para evitar gran parte de los riesgos que suponen. Es decir, la educación como medida preventiva de Política Criminal en este ámbito.

2 Los menores y el fenómeno Internet.

2.1. Aparición y evolución de Internet.

Internet apareció dentro del ámbito militar hace ya más de veinticinco años. En el año 1969, en plena guerra fría, el Departamento de Defensa de los Estados Unidos de Norteamérica, decidió buscar nuevas formas de comunicación ya que consideraban que su sistema de comunicación, que se basaba en la comunicación telefónica, era muy vulnerable. Por este motivo, dicho departamento, a través de su Agencia de Proyectos de Investigación Avanzados (*Advanced Research Projects Agency*, ARPA), decidió centrarse en las redes de ordenadores y así surgió la primera red experimental llamada ARPANET[3]. A partir de ese momento su evolución se hizo incontrolable, hasta llegar a la red que hoy en día tenemos y conocemos como INTERNET, que ya no se trata de una simple red de ordenadores sino de miles de redes conectadas entre sí que dan lugar a la llamada "Red de Redes" con millones y millones de usuarios y presente en todos los ámbitos de nuestras sociedades, conformando al mismo tiempo lo que CASTELLS llama "Sociedad Red"[4]. Tanto es así que, actualmente, resulta difícil pensar en un hogar en el que no haya un ordenador, un portátil, una tablet, y qué decir del teléfono móvil, todos ellos obviamente con conexión a Internet.

[3] ARPANET "fue la primera red en la que se puso en uso un protocolo de comunicación por paquetes que no requería de computadoras centrales, si no que era -como lo es la actual Internet- totalmente descentralizada". ALSINA GONZÁLEZ, Guillem: "Definición de ARPANET" [en línea], *Definición ABC*, 2016, < https://www.definicionabc.com/tecnologia/arpanet.php > [consulta: 24 de abril de 2017].

[4] CASTELLS, Manuel, *Internet y la Sociedad Red.* Conferencia *de Presentación del Programa de Doctorado sobre la Sociedad de la Información y el Conocimiento,* 2000. "Internet es ya y será aún más el medio de comunicación y de relación esencial sobre el que se basa una nueva forma de sociedad que ya vivimos, que es lo que yo llamo la sociedad red".

Junto al fenómeno de Internet se deben situar las tecnologías de la información y la comunicación (TIC). Ya desde su aparición, que se sitúa aproximadamente con la invención del telégrafo (1833), éstas han experimentado una evolución descomunal, que aun hoy en día no ha parado. De obligada mención es aquí Gordon E. Moore, cofundador de Intel y autor de la conocida "Ley de Moore"[5]. Publicó esta ley el 19 de abril de 1965 en la revista *Electronics* y venía a decir que cada año aumentaría la complejidad de los circuitos integrados, es decir, cada vez se tendría una tecnología más avanzada y potente, y, a su vez, el coste iría disminuyendo. Esta ley se sigue cumpliendo hoy en día, por ejemplo se observa en los teléfonos móviles, si se compra hoy un móvil se ve como al pasar un año su precio se ha reducido considerablemente y a los dos años pasa a estar desfasado porque ya hay nuevos móviles más potentes.

Como ha quedado patente, Internet y las nuevas tecnologías son algo inherente a la vida humana. Según una encuesta realizada por el Instituto Nacional de Estadística (INE) en 2016[6], el 77'1 % de los hogares españoles disponen de ordenador, el 99'3 % de los hogares tienen teléfono, ya sea móvil o fijo, y el 81'9 % de los hogares tienen conexión a la Red, lo que traducido en cifras supone 13 millones de viviendas familiares con conexión a Internet en España. Observando estas cifras se demuestra la gran importancia de las nuevas tecnologías (TIC) en la sociedad. Su uso, cada vez más generalizado, constituye algo esencial para el desarrollo de la vida diaria, se utilizan en multitud de tareas cotidianas como leer el periódico, hacer la compra, buscar información, hablar con otras personas, realizar una transacción bancaria, etc. Además, su uso no entiende de edades, son utilizadas por personas adultas, ancianas, pero sobre todo, por menores y adolescentes, que constituyen el sector central de este trabajo.

Haciendo especial hincapié en los menores, se entiende por tal en España cualquier persona menor de 18 años[7]. Como es sabido, las tecnologías de la información y la comunicación tienen un impacto muy positivo en el día a día, facilitando multitud de tareas

[5] CHEANG WONG, Juan Carlos, *Ley de Moore, nanotecnología y nanociencias: síntesis y modificación de nanopartículas mediante la implantación de iones*, UNAM. México, 2005, Pág. 3 – 4. "En 1965, Gordon Moore (co-fundador en 1968 de la compañía Intel) afirmó que el número de transistores por centímetro cuadrado en un circuito integrado se duplicaba cada año y que la tendencia continuaría durante las siguientes dos décadas. Más tarde, en 1975, modificó su propia afirmación y predijo que el ritmo bajaría, y que la densidad de transistores se duplicaría aproximadamente cada 18 meses. Esta progresión de crecimiento exponencial de la densidad de transistores, o sea, el duplicar la capacidad de los microprocesadores cada año y medio, es lo que se considera actualmente como la Ley de Moore".

[6] Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, INE, 2016. Disponible en www.ine.es

[7] Según el artículo 315 del Código Civil, "la mayor edad empieza a los dieciocho años cumplidos". Artículo 12 CE, "los españoles son mayores de edad a los dieciocho años".

y ofreciendo nuevas oportunidades, pero, no obstante, también conllevan numerosos riesgos y en especial para los menores, precisamente por su corta edad, lo que los hace más vulnerables en el mundo tecnológico. Como dice LORENTE LÓPEZ[8], "…la generalización del uso de las nuevas tecnologías plantea graves riesgos para la infancia, dado que facilitan (e incluso favorecen) la transgresión de sus derechos fundamentales". Derechos fundamentales como el honor, la intimidad personal y familiar, la propia imagen y otros nuevos que se han ido conformando como el derecho a la protección de datos personales o el llamado derecho al olvido. Éste último, pese a no estar reconocido como tal, cada vez va cobrando más importancia y supone, en resumidas cuentas, la posibilidad de eliminar información personal de cualquier servidor de Internet o bien limitar su acceso.

Frente a estas realidades, se hace imprescindible una regulación específica relativa a los menores, por constituir, como se ha dicho anteriormente, el sector más vulnerable. Además, no solo es necesaria una regulación específica sino también que esa regulación se vaya actualizando y adaptando constantemente a los avances tecnológicos. Sin embargo, hoy en día, esto aun supone un reto ya que debido al ritmo en el que el mundo tecnológico en general avanza, se hace imposible que el ordenamiento jurídico pueda seguirle. Por lo tanto, y lamentablemente, se seguirá contando con una legislación obsoleta y desfasada con grandes lagunas de protección.

2.2. Ventajas.

No se puede negar que se vive completamente inmersos en la *Sociedad de la Información*[9] en la que las nuevas tecnologías ocupan una posición crucial. Ante esta realidad y la constante evolución de las TIC resulta inevitable plantearse cuánto tiene de beneficioso esta presencia excesiva de las tecnologías en las vidas cotidianas, y si son más las ventajas frente a los inconvenientes.

Sin ningún lugar a duda, las TIC son realmente esenciales en el día a día. Si se vuelve la vista atrás, las oportunidades y posibilidades que hoy se tienen son infinitamente

---

[8] LORENTE LÓPEZ, Mª Cristina, *Los derechos al honor, a la intimidad personal y familiar y a la propia imagen del menor*. Aranzadi, Navarra, 2015, pág. 205.

[9] COZ FERNÁNDEZ, Jose Ramón; FOJÓN CHAMORRO, Enrique; HERADIO GIL, Rubén; CERRADA SOMOLINOS, Jose Antonio, *Evaluación de la privacidad de una Red Social Virtual.* Associação Ibérica de Sistemas e Tecnologias de Informacao. 2012. Retrieved from https://search.proquest.com/docview /1027228507?accountid=15297 "El termino sociedad de la información fue acuñado por primera vez en 1962 por Fritz Machlup (1962), pero no es hasta la década de los 70 cuando se generaliza su uso, debido, fundamentalmente, a una evolución en los medios de generación de riquezas, pasando de los sectores industriales a los sectores de la tecnología de la información y las comunicaciones (TIC)".

superiores, lo que ha conllevado un gran aumento de la calidad de vida. Son tantos los ámbitos en los que están presentes que incluso se haría costoso seguir la vida sin ellas.

Las TIC han supuesto un impacto muy positivo en distintos campos como la medicina, con nuevos aparatos capaces de detectar y curar enfermedades; el laboral, con maquinaria que facilita el trabajo, pero sobre todo, a supuesto un gran impacto en el ámbito de la comunicación y la información. Una de las mayores ventajas ha sido romper con la barrera espacio-tiempo, ahora es posible comunicarse con cualquier persona de cualquier parte del mundo en cualquier momento. Se puede acceder a todo tipo de información en cuestión de segundos gracias a Internet, posibilitando un acceso a la cultura a personas que carecen de recursos para ello.

Otro aspecto importante es su incidencia en el entorno escolar, en el que llegan a constituirse como una herramienta imprescindible, tanto para los docentes a los que les facilita con creces multitud de métodos de educación, como para los estudiantes a quienes les otorga grandes facilidades de almacenaje y búsqueda de información, entre otras cosas.

Para poder llegar hasta donde se está hoy en día, las sociedades han tenido que "sufrir" un periodo de adaptación a las nuevas tecnologías, una adaptación que se les hace más costosa a unos que a otros, obviamente. Y, como es lógico, también están quienes no han tenido que pasar por esa adaptación, puesto que precisamente ya han nacido inmersos en esa Sociedad de la Información, los conocidos como *nativos digitales*[10]. No obstante, no hay que olvidar que, como en todo, habrá gente que no esté dispuesta a hacer este cambio o bien no pueden porque no tienen recursos, conformándose así la llamada "brecha digital"[11].

Si ya se puede decir que la tecnología ocupa una posición destacable en la vida de casi todos, para los menores aun más. No es de extrañar ver a un niño de apenas unos meses manejar un teléfono móvil con más destreza que un adulto o niños de pocos años con tablets propias y móviles de última generación. Como todo, si se hace un buen uso de

[10] Este término fue utilizado por primera vez por MARC PRENSKY, autor del libro "*Enseñanza nativos digitales*" y se refiere a aquellas personas que han nacido desde el año 1980 hasta ahora, cuando ya había una tecnología muy desarrollada. Otro término también utilizado por este autor es el de *inmigrantes digitales* que hace referencias a aquellas personas que han vivido el proceso de cambio tecnológico.

[11] El término "brecha digital" se puede definir como "la separación que existe entre las personas (comunidades, estados, países…) que utilizan las Tecnologías de Información y Comunicación (TIC) como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que aunque las tengan no saben como utilizarlas". MARTÍNEZ, Evelio: "Qué es la Brecha Digital" [en línea], 2008 < http://www.labrechadigital.org/labrecha/qu-es-la-brecha-digital17.html > [consulta: 7 de octubre de 2017].

la tecnología puede suponer para los menores grandes ventajas. Les ayuda en el proceso de socialización gracias a los chats, foros, juegos online, etc., mediante los que pueden mantener relaciones sociales con grupos de iguales con los que comparten aficiones e inquietudes. Se les posibilita un acceso a la cultura e información inmediato ayudando en su educación más allá del entorno escolar. Favorecen la toma de decisiones y les dota de mayor independencia fomentando así el desarrollo de su personalidad y, sobre todo, satisfacen con creces sus necesidades de entretenimiento y ocio.

2.3. Inconvenientes.

Aunque las TIC hayan supuesto un gran impacto positivo para la vida de casi todos, no se debe olvidar que también tienen su parte negativa. Todas las personas son susceptibles de los riesgos que comportan las nuevas tecnologías, especialmente los menores. Debido a su corta edad, que los hace más vulnerables, los convierte en potenciales sujetos pasivos, potenciales víctimas de los depredadores que usan las redes y, el aparente anonimato que éstas proporcionan, para aprovecharse de ellos y de su inocencia.

Cada vez preocupa más la protección de los menores ante los riesgos que suponen las TIC, sobre todo ante el incipiente crecimiento del número de delitos cometidos contra los menores en Internet. En este sentido se manifestó ya la Decisión nº 1351/2008/CE, de 16 de diciembre del Parlamento Europeo y del Consejo[12] que establece en su Preámbulo que "la evolución de la tecnología, la transformación de la manera en que niños y adultos utilizan Internet y las demás tecnologías de la comunicación y la modificación de los comportamientos sociales crean nuevos riesgos para los niños".

Los niños y adolescentes, de por sí, son más tendentes a asumir riesgos y en concreto en Internet, posiblemente por el hecho de haber nacido ya sumergidos en el mundo virtual y verlas como algo natural del día a día. Este hecho, unido a la globalidad e inmediatez de la Red, ocasiona perjuicios a los menores de los que en muchas ocasiones no son conscientes. Difundir una imagen en la Red puede suponer que en cuestión de segundos sea visible en cualquier parte del mundo y esté a disposición de todo tipo de personas. En este sentido destacan las Redes Sociales que por su propia dinámica invitan a compartir todo tipo de datos personales poniendo en riesgo la privacidad.

[12] *Decisión nº 1351/2008/CE* del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, por la que se establece un programa comunitario plurianual sobre la protección de los niños en el uso de internet y de otras tecnologías de la comunicación.

Una de las ventajas de las TIC que se ha dicho anteriormente, es que fomentan las relaciones sociales al permitir hablar con personas de todo el mundo en cualquier momento, pero no hay que olvidarse de la otra cara de la moneda, ya que del mismo modo las TIC deterioran considerablemente las relaciones cara a cara. Ahora pocas veces se queda con los amigos para charlar sino que se opta primero por enviarle un *WhatsApp*[13] o hablar a través de chats. Además, se tiene que tener en cuenta que muchas veces ni siquiera se puede saber con total seguridad con quién se está hablando realmente. Hay personas que se dedican a crear perfiles falsos con la intención de obtener un beneficio propio, ya sea suplantando o usurpando la identidad de alguien o creando perfiles de personas que no existen. Por ejemplo, esta práctica es común entre los pedófilos, quienes se hacen pasar por niños para así poder entablar relaciones con otros menores.

No hay que olvidarse tampoco de los problemas físicos que supone su uso excesivo, cansancio visual, posibilidad de sufrir cáncer por las radiaciones que emiten los aparatos, depresión, etc. Además, el mayor riesgo que comportan las nuevas tecnologías e Internet es la gran vulneración de derechos fundamentales en especial los consagrados en el artículo 18.1 de la Constitución Española, es decir, el derecho al honor, la intimidad personal y familiar y la propia imagen. Por eso los esfuerzos del Derecho deben estar orientados a garantizar estos derechos y evitar su vulneración, además de dotar a los menores de una protección integral. De este modo, el apartado 4 del artículo 18 de la CE establece que "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

Asimismo, se cuenta con otras leyes que brindan protección a los más pequeños como por ejemplo, la Ley Orgánica 1/1996 de protección jurídica del menor y la Ley Orgánica 8/2015, de modificación del sistema de protección a la infancia y a la adolescencia.

2.4. Datos relevantes sobe el uso de Internet por los menores.

Según los últimos datos proporcionados por el INE a través de una encuesta realizada en 2016[14], el 77'1% de los hogares españoles, integrados al menos por un miembro de entre 16 y 74 años, cuentan con ordenador en 2016. Si se atiende al teléfono móvil se ve

[13] PÉREZ PORTO, Juan y GARDEY Ana: "Definición de Whatsapp" [en línea], 2016 < https://definicion.de/whatsapp/ > [consulta el 3 de marzo de 2017]. Whatsapp es una "aplicación que permite enviar y recibir mensajes instantáneos a través de un teléfono móvil. El servicio no solo posibilita el intercambio de textos, sino también de audios, videos y fotografías".

[14] Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, INE, 2016.

como la presencia es muy superior, con un 96'7%, manteniéndose respecto a los datos de años anteriores al igual que el ordenador. Otros aparatos TIC como el vídeo, el DVD o el mp3 y mp4 van en descenso ya desde los últimos tres años.

Si se observan los hogares que disponen de acceso a Internet, el porcentaje se sitúa en un 81'9%, por lo que actualmente en España hay más de 13 millones de viviendas familiares con acceso a la Red.

Analizando ahora los datos respecto el uso de las TIC por los menores, se ve como la población infantil de entre 10 y 15 años hace un uso muy elevado de estas tecnologías de la información y la comunicación. Prácticamente la totalidad de los menores hacen uso del ordenador (94'9%) y aún más de Internet (95'2%). Por primera vez se produce un sorpaso del uso de Internet respecto al uso del ordenador.

En atención al sexo la diferencia es apenas significativa, los niños hacen un uso ligeramente superior del ordenador e Internet, mientras que las niñas del teléfono móvil.

En cuanto a la edad, el uso del ordenador e Internet va en aumento progresivamente desde los 10 años hasta los 15. Sin embargo, respecto a la disposición de teléfono móvil sí que hay una diferencia abismal de su uso por menores de 10 años (25'4%) respecto a los menores de 15 años (93'9%).

Observando estos datos y viendo que el 90'6% de los menores de 10 años ya hacen uso de Internet, indican que la gran mayoría de los menores se conectan a la Red antes de los 10 años, lo que lleva a plantearse a qué tipo de contenido acceden estos menores y bajo que controles lo hacen.

El dossier de indicadores sobre uso de TIC por menores en España elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información[15] (ONTSI) en diciembre de 2016 proporciona datos respecto al lugar en el que los niños hacen más uso de Internet, entre otros datos. Según este dossier, sobre el porcentaje total de niños que han hecho uso de Internet en los últimos 3 meses que es el 95'2%, la mayoría lo hace desde su vivienda o desde el centro de estudios con un 93'7% y 71'1% respectivamente, quedando el cibercafé en último lugar con un 5'5%. Por lo tanto, analizando estos datos se deduce que un papel fundamental de control lo desempeñan los padres y profesores, ya que es tanto en casa como en la escuela donde los niños

[15] Dossier de indicadores sobre uso de TIC por menores en España elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información disponible en http://www.ontsi.red.es/ontsi/es/content/dossier-de-indicadores-sobre-uso-de-tic-por-menores-en-espa%C3%B1a-diciembre-2016

acceden más a la Red y por consecuencia, donde hay más posibilidades de que sufran ataques a través de las TIC.

Si se atiende ahora a la Memoria de la Fiscalía General del Estado de 2017[16], señala que no se cuenta con una estadística sobre los delitos informáticos cometidos por menores, ya que abarcan una gran variedad de tipos penales, por lo que se mantienen los informes de las Secciones en línea de años anteriores.

Según esta Memoria en el año 2016 se incoaron en todo el territorio nacional 8.035 procedimientos judiciales sobre delitos relativos a la criminalidad informática. Se observa así un llamativo descenso respecto a los 22.575 procedimientos incoados en el año 2015, es decir, un descenso de un 64'40%. Este hecho tiene una explicación, y es que como ya manifestaba la Memoria del año 2016 "la reforma procesal operada por la ley 41/2015 de 5 de octubre, ha determinado que en muchos de los territorios provinciales, los cuerpos policiales desde primeros de diciembre del pasado año, dejaran de remitir a los órganos judiciales, por disposición del nuevo artículo 284.2 LECrim, aquellos atestados en los que no constara autor conocido y no concurriera ninguna de las excepciones previstas en ese mismo artículo"[17].

Por lo tanto, no se puede concluir que haya habido un descenso real de la criminalidad informática respecto a años anteriores, sino que el descenso se atribuye a la falta de remisión de atestados policiales, lo que impide contar con datos objetivos y fiables.

No obstante, la Memoria sí que establece datos respecto a ciertos delitos específicos que se encuentran dentro de las excepciones del artículo 284.2 a) LECrim. De este modo si se atiende a la pornografía infantil se aprecia un ligero descenso de las incoaciones de un 11'21% respecto de los 767 expedientes del año 2015. En cuanto a los delitos de acoso a menores de 16 años no se aprecia variación respecto al año anterior, manteniéndose en un total de 98 causas judiciales.

2.5. Tipos delictivos más comunes en la Red entre o hacia menores.

Como se viene diciendo, las TIC conllevan numerosos riesgos para las personas y especialmente para los menores de edad, uno de ellos es la comisión de delitos contra éstos a través de medios tecnológicos que, desafortunadamente, van en aumento a la par que las nuevas tecnologías se van desarrollando.

[16] Memoria de la Fiscalía General del Estado de 2017 < https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/index.html > [consulta: 26 de octubre de 2017].
[17] Memoria de la Fiscalía General del Estado de 2016 < https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/index.html > [consulta: 26 de octubre de 2017].

2.5.1. *Ciberbullying* o ciberacoso.

Tradicionalmente solo se hablaba de *bullying* o acoso escolar, OLWEUS desarrolló a mediados de los años 80, la definición de acoso escolar y decía que "un estudiante es acosado o victimizado cuando está expuesto de manera repetitiva a acciones negativas por parte de uno o más estudiantes"[18].

Con el paso del tiempo las nuevas tecnologías se han ido desarrollando y han dado paso a una variante del *bullying* llamada *ciberbullying* o ciberacoso. Por *ciberbullying* se entiende "el daño intencional y repetido infligido por parte de un menor o grupo de menores hacía otro menor mediante el uso de medios digitales"[19].

Por lo tanto, para poder hablar de ciberacoso se deben dar una serie de elementos característicos:

- **Situación de acoso**: debe existir una situación de acoso.
- **Persistencia:** esa situación de acoso debe ser prolongada en el tiempo, por tanto, se deben excluir las situaciones de acoso que se dan puntualmente[20]. Lo peligroso de este método de acoso es la globalidad de las nuevas tecnologías que permiten un contacto con la víctima 24 horas al día, esté en el lugar que esté.
- **Entre iguales:** entre las víctimas y los acosadores no debe haber una gran diferencia de edad sino que han de ser de edades similares y normalmente tendrán algún tipo de relación en el mundo físico, por ejemplo, serán compañeros de clase.
- **A través de medios tecnológicos:** las conductas de acoso se realizan a través de medios como Internet haciendo uso de teléfonos móviles, redes sociales, ordenadores, etc. Este elemento es esencial para poder hablar de *ciberbullying* y diferenciarlo del acoso tradicional.

Entre los métodos o medios más comunes para cometer ciberacoso están los insultos y/o amenazas directas a través de las redes sociales o aplicaciones de mensajería

[18] OLWEUS, Dan, *Acoso escolar,"bullying", en las escuelas : hechos e intervenciones*, Noruega, 2017.

[19] Red. es. *Monográgico ciberacoso escolar (ciberbullying).* Pág. 4-5. Disponible en *http://www.chaval.es/chavales/sites/default/files/Monografico%20Ciberbullying%20o%20ciberacoso%20escolar_Red.es.pdf*

[20] Si bien decimos que las conductas de acoso deben ser reiteradas en el tiempo, es cierto que en ocasiones por ejemplo, la publicación de un vídeo difamatorio, por las características del medio en el que se vierte, puede suponer para la víctima unas consecuencias de victimización prolongadas en el tiempo y sin embargo el agresor únicamente ha realizado una conducta. En este caso seguiríamos hablando de ciberacoso.

instantánea como *Whatsapp*; el robo de contraseñas; difundir rumores, vídeos o fotos humillantes y vejatorias, ya sean reales o manipuladas; la creación de perfiles falsos en las redes sociales para amenazar; etc. En suma, un sin fin de conductas negativas que provocan graves consecuencias para los menores víctimas, tanto a nivel físico como psicológico, que en los peores casos ha desembocado en suicidios.

Según el estudio "Riesgos y Seguridad en Internet: Los menores españoles en el contexto europeo"[21], en España alrededor del 16% de los menores de 9 a 16 años afirman haber sufrido acoso tanto online como offline, y si hablamos únicamente de los menores víctimas de *ciberbullying* la media se sitúa en un 5%.

La Convención de Naciones Unidas sobre los Derechos del Niño en su artículo 3.1[22] establece como una consideración primordial el interés superior del niño, a la hora de adoptar cualquier medida referente a los niños por parte de las instituciones púbicas o privadas, los tribunales y demás autoridades administrativas u órganos legislativos. Asimismo, en su artículo 28.2 impone un deber a los Estados Parte para que adopten las medidas necesarias para tratar que la disciplina escolar se administre de forma compatible con la dignidad humana del niño.

En este ámbito escolar se cuenta con la Ley Orgánica 2/2006, de 3 de mayo, de Educación que establece en su artículo 1 k) que uno de los principios en los que deberá basarse el sistema educativo español es en "la educación para la prevención de conflictos y para la resolución pacífica de los mismos, así como la no violencia en todos los ámbitos de la vida personal, familiar y social".

Además, la Fiscalía General del Estado también consideró importante hacer una mención expresa a este fenómeno social dictando la Instrucción 10/2005 de 6 de octubre[23], para establecer unas pautas de actuación penal para los fiscales encargados de estos asuntos.

---

[21] GARMENDIA, Maialen; GARITAONANDIA, Carmelo; MARTÍNEZ, Gemma; CASADO, Miguel Ángel, *Riesgos y seguridad en Internet: Los menores españoles en el contexto europeo.* Universidad del País Vasco/EuskalHerrikoUnibertsitatea, Bilbao, EU Kids Online, 2011.

[22] Convención de Naciones Unidas sobre los Derechos del Niño, de 20 de noviembre de 1989, artículo 3.1 "En todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño*".*

[23] Instrucción 10/2005 de 6 de octubre de la Fiscalía General del Estado "La consecución del objetivo de lograr un ambiente de paz y seguridad en los Centros educativos y en el entorno de los mismos, donde los menores puedan formarse y socializarse adecuadamente debe tornarse en meta irrenunciable, superando la resignada aceptación de la existencia de prácticas de acoso o matonismo entre nuestros menores, como algo inherente a la vida de los centros escolares e institutos".

En atención a la legislación penal, no hay un tipo específico que castigue el *ciberbullying*, ya que éste puede derivar en varias conductas que afectarán por tanto, a distintos bienes jurídicos. No obstante, el tipo penal más próximo en el que se puede encuadrar sería el artículo 197 del Código Penal situado en el Título X "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio" en el que se castigan "conductas consistentes en el uso y difusión de información contenida en soportes informáticos, electrónicos o digitales y por medios tecnológicos, así como la publicación de vídeos y fotografías por los mismos medios"[24].

La reforma del Código Penal de 2015[25], introdujo una modalidad específica de acoso en el artículo 172 ter en el que también podrían tener encaje este tipo de acoso realizado entre los menores.

2.5.2. Sexting.

El término *sexting* es un anglicismo que se compone de dos palabras: "*sex*" (sexo) y "*texting*" (enviar mensajes de texto mediante teléfonos móviles). Consiste en el envío, difusión o publicación de imágenes o vídeos de carácter sexual, producidos o protagonizados por el propio remitente, a través de medios tecnológicos, principalmente el teléfono móvil.

Para poder hablar de *sexting* son necesarias una serie de características:

- **Voluntariedad:** Los vídeos o imágenes difundidas a través de los medios tecnológicos son realizadas por el propio remitente de forma voluntaria. También se puede dar el caso de que no sean realizados por el remitente sino por otra persona, pero con el consentimiento, al menos inicial, del que los protagoniza.
- **Uso de dispositivos tecnológicos:** El envío se realiza a través de toda clase de dispositivos tecnológicos, siendo el teléfono móvil el más utilizado. Este es uno de los grandes problemas del *sexting* puesto que las imágenes y vídeos que se envían pueden difundirse a escala global en cuestión de segundos o minutos, perdiéndose el control sobre ellos al instante.
- **Contenidos de carácter sexual o erótico:** Los contenidos que se envían son de carácter sexual, por ejemplo, imágenes desnudos o semidesnudos, en posiciones

[24] Red.es: *Monográfico ciberacoso escolar (ciberbullying).* Pág. 33.
[25] Reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

sugerentes, etc., normalmente con la intención de provocar sexualmente al receptor.

- **Entre adolescentes:** La práctica del *sexting* es muy común entre adolescentes. "Hoy en día los adolescentes utilizan este método como forma de expresión y desarrollo de su sexualidad"[26] y lo ven como algo absolutamente normal, lo que les hace no ser conscientes de los riesgos que supone enviar este tipo de contenidos. Normalmente se suelen enviar, por ejemplo, entre parejas adolescentes, una persona con la que se está coqueteando o simplemente para llamar la atención de alguien, presumiendo que la imagen o vídeo se va a mantener en el ámbito privado entre esas dos personas. Sin embargo, es muy probable que ese contenido se divulgue, bien de forma consciente, por ejemplo por venganza de una parte de la pareja tras una ruptura, para presumir ante los amigos, etc., o bien de forma involuntaria, por un descuido, por un robo en el que te sustraen el teléfono móvil o porque lo has perdido.

Con la práctica del *sexting* se pueden ver afectados derechos muy importantes como el derecho a la intimidad, a la propia imagen e incluso la dignidad. Los menores, "a pesar de que manejan las nuevas tecnologías con gran soltura, a menudo «desconocen los niveles de privacidad» de sus perfiles, por lo que consideran que una imagen "comprometida" no tiene por qué ser usada de forma fraudulenta, o no imaginan que las fotografías y vídeos de sus móviles puedan salir del mismo olvidando la posibilidad de robo, pérdida o error en el envío"[27].

En el CP de 1995 inicialmente se protegía el derecho a la intimidad a través del artículo 197.1 en el que se castigaba al que "para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales…", por lo tanto, se castigaba el obtener imágenes sin el consentimiento de la persona y una de las características esenciales del *sexting* es voluntariedad a la hora de enviarlo. De esta manera, las conductas que a día de hoy se califican como *sexting* se puede decir que eran atípicas o se reconducían a otro tipo de delitos como por ejemplo las injurias.

---

[26] COLÁS TURÉGANO, Asunción, *Los delitos de género entre menores en la sociedad tecnológica: rasgos diferenciales*. En Menores y redes sociales. Tirant lo Blanch. 2016.

[27] Red. es. *Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad. Monográfico sexting.* Disponible en http://www.chaval.es/chavales/sites/default/files/Monografico%20Sexting_Red.es.pdf

Tras la reforma de 2015 del CP se ha introducido un nuevo apartado 7 en el artículo 197 para dar cabida a la figura delictiva del *sexting*, propiciado por un caso muy polémico y mediático. En este nuevo apartado 7 se castiga ahora al 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".

En caso de que la víctima fuese menor de 16 años se daría un concurso entre el delito establecido en el artículo 197.7 CP y el delito del artículo 183 ter CP, también introducido en la reforma del Código Penal de 2015 y que hace referencia al contacto con menores a través de Internet.

2.5.3. *Grooming*.

El *grooming* es un tipo de ciberacoso ejercido por un adulto sobre un menor para establecer una relación con éste a fin de conseguir del menor un beneficio de índole sexual.

El término *grooming* se encuentra íntimamente ligado con la pedofilia y la pederastia. Si bien el pedófilo es un adulto que se siente atraído por los menores, un pederasta es quien comete un delito sexual con un menor. Por lo tanto, un pedófilo no busca el contacto físico con el menor mientras que un pederasta sí. De este modo, se establecen dos tipos de *grooming* según exista este contacto o no. Por un lado, estará el *grooming* en el que el adulto tratará de engatusar al menor para que éste le proporcione imágenes y distinto material de contenido sexual y, por otro lado, el *grooming* en el que el adulto, además de querer conseguir ese material, buscará obtener un encuentro físico con el menor.

Así mismo, también se puede diferenciar el *grooming* según exista la fase previa de relación y obtención de confianza. Es decir, habrá adultos que ejerzan el *grooming hackeando* las cuentas de menores para obtener imágenes comprometidas con las que luego poder chantajearles, y los habrá que establezcan una fase previa en la que se intenten ganar la confianza del menor para que sea este quien voluntariamente proporcione el material sexual.

Atendiendo a este último caso en el que se genera una fase previa, que será el más común, se puede establecer una serie de características comunes:

- **Inicio de una relación:** El *groomer* realiza un primer contacto con el menor a través de Internet con la intención de acercar posiciones y ganarse su confianza, muchas veces haciéndose pasar por niños de su misma edad.
- **Inicio de la "amistad":** El *groomer* ya ha conseguido establecer una relación con el menor y ahora lo que pretende es afianzar una supuesta amistad, preocupándose por él, conociendo sus gustos, sus intereses, información personal, etc., de forma que consiga ganarse totalmente su confianza.
- **Componente de índole sexual:** La finalidad última de todo *groomer* es conseguir material o un acercamiento de carácter sexual con el menor. Por ello, una vez el adulto ya se ha ganado totalmente la confianza del menor, comienza a hacerle proposiciones sexuales, como por ejemplo, que se realice fotografías o grabaciones eróticas e incluso en algunos casos se les propone tener un encuentro fuera de Internet con la intención de mantener relaciones sexuales.
- **Chantaje:** "El chantaje es la principal arma con la que cuenta el acosador"[28]. Cuando el acosador ya ha conseguido que el menor le proporcione material sexual o le proporcione información sensible, comenzará a chantajearle y amenazarle con difundir sus intimidades con la intención de obtener así más material o incluso un encuentro físico con el menor.

La práctica del *grooming*, al igual que otras formas de acoso, supone graves consecuencias para los menores víctimas tanto a nivel psicológico como físico, ya sean problemas de sueño, retraimiento y conductas regresivas, ideación suicida, ansiedad, rabia, etc. Por ello, hay que ser capaces de detectar estos síntomas a tiempo para poder combatir este problema que por desgracia cada vez se da con más frecuencia.

En cuanto a la protección legal frente a los delitos de *grooming*, fue en 2010, mediante la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica el Código Penal, cuando se introdujo por primera vez en nuestra legislación la figura del "*child grooming*" en el artículo 183 bis. Posteriormente, tras la Ley Orgánica 1/2015, de 30 de marzo, se vuelve a modificar el Código Penal y se añade el artículo 183 ter que hace referencia a las penas relativas a los delitos de *grooming*.

[28] Red.es: *Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad. Monográfico grooming*. Disponible en http://www.chaval.es/chavales/sites/default/files/Monografico%20Grooming_Red.es.pdf

2.6. Especial referencia a las redes sociales on line.

Las redes sociales tradicionales (la familia, amigos, compañeros de la universidad o del trabajo, ...) han cambiado considerablemente con la aparición de las nuevas tecnologías, pasando a hablar ahora de redes sociales on line. PAULA ORTIZ define de manera amplia las redes sociales on line como "aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de Internet para que estos generen un perfil con sus datos personales, facilitando la creación de redes en base a criterios comunes y permitiendo la conexión e interacción con otros usuarios"[29]. De este modo, las redes sociales on line se constituyen como un claro ejemplo de la Web 2.0[30], en la que los usuarios son consumidores de información y al mismo tiempo creadores de contenido.

Ya en 2011 en el estudio "Menores y redes sociales"[31], BRINGUÉ y SÁBADA determinaron que el 71% de los menores entre 10 y 18 años que participaron en la muestra (9.230 menores) utilizaba redes sociales y que a partir de los 14 años su uso llegaba a superar el 80%, llegando al porcentaje máximo a los 17 años con un 85%. Si se tiene en cuenta que cada vez es mayor la presencia de los menores en las redes sociales es fácil hacerse una idea de la gran cantidad de usuarios menores que hay a día de hoy registrados en una red social y no hay que olvidar que la edad mínima legalmente establecida en España para acceder a una red social es de 14 años[32].

Hace años la red social más utilizada por los menores era Tuenti, que se creó en el año 2006 por un grupo de 5 jóvenes, todos menores de 23 años, en Madrid. Su intención era crear una red social diferente que estuviera compuesta únicamente por conocidos y que no indexase datos personales de los usuarios en los motores de búsqueda. Así, se puede afirmar que Tuenti es "una de las redes sociales más seguras y la que cuenta con la política de privacidad más estricta y rigurosa"[33]. Pese a esto, Tuenti, a día de hoy, ha

[29] RALLO LOMBARTE, Artemi; MARTÍNEZ MARTÍNEZ, Ricard y ALAMILLO DOMINGO, Ignacio, *Derecho y Redes Sociales.* Civitas Thomson Reuters, Cizur Menor (Navarra), 2013, pág. 22.

[30] LOZANO SALINAS, Jose María, *La Web 2.0*. Dialnet, 2008, pág. 2. "En la Web 2.0 los consumidores de información se han convertido en productores de la misma información que ellos mismos consumen".

[31] BRINGUÉ, Xavier y SÁDABA, Charo, *Menores y Redes Sociales*. Foro Generaciones Interactivas. 2011.

[32] El artículo 13 del Reglamento de Protección de Datos, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, establece que los mayores de 14 años podrán prestar su consentimiento para el tratamiento de sus datos y que, en caso de ser menores de 14 años, será necesario el consentimiento de los padres o tutores.

[33] MARTOS DÍAZ, Natalia y CASADO OLIVA, Óscar, *Derecho y redes sociales*. Civitas Thomson Reuters, Cizur Menor (Navarra), 2013, pág. 235.

pasado a un segundo plano como red social estableciéndose ahora como un operador de telefonía y dejando paso a otras redes sociales como *Facebook, Twitter, Youtube*, *Instagram*, etc.

Este fenómeno de las redes sociales unido al rápido y fácil acceso que permiten los *smartphones* dotan a los usuarios de grandes posibilidades, sobretodo de comunicación. No obstante, también supone graves problemas para la privacidad, precisamente porque como se decía anteriormente, la propia dinámica de las redes sociales implica que el usuario comparta grandes cantidades de información personal. Concretamente este aspecto preocupa aún más en relación con los menores. El hecho de verse sumergidos en las tecnologías desde que nacen, hace que estos nativos digitales estén acostumbrados y vean como algo normal y natural, desarrollar su vida social completamente a través de las redes sociales y compartir todo tipo de información íntima bajo una falsa apariencia de seguridad.

Si se profundiza un poco más en la dinámica de las redes sociales se observa como desde el mismo momento en el que uno se registra ya se ve obligado a facilitar información personal, por ejemplo, Facebook exige para poder registrarte el nombre, apellidos, número de teléfono o correo electrónico, fecha de nacimiento, sexo y por supuesto una contraseña.

Además, la mayoría de las redes sociales cuentan con una sección denominada “perfil” en la que sugieren que se aporte otro tipo de datos personales, como el lugar de estudio o de trabajo, aficiones, datos de contacto, familiares, situación sentimental, etc., que muchas veces se dan sin pensar en las consecuencias reales que ello puede suponer. Desafortunadamente, hay personas que se dedican a recabar este tipo de información con la intención de crear perfiles falsos, suplantar la identidad, acosar, etc.

Los nativos digitales nacen ya con otro concepto de privacidad, por lo que aportan con mayor facilidad este tipo de información y pocas veces ponen restricciones. Por este motivo, y porque cada vez son más comunes los delitos entre los menores empleando las nuevas tecnologías, es necesario replantearse la cuestión y establecer cambios que doten de más protección a este sector tan vulnerable.

Sin embargo, la pérdida de privacidad no es el único riesgo al que se ven expuestos los menores ante una red social. El acceso a contenidos inadecuados es quizás el más común, en una red social se comparte todo tipo de información, vídeos, fotos, etc., por personas de distintas edades y que muchas veces no serán los más apropiados para un menor, por eso es importante saber en qué tipo de redes sociales se registran y con que

personas se relacionan. Otro riesgo que cada vez es más preocupante es la posibilidad de ser víctimas de delitos como los mencionados en el apartado anterior, *ciberbullying*, grooming, sexting, *ciberstalking*, pornografía infantil, etc.

Pese a los distintos riesgos que pueden conllevar las redes sociales, la solución no radica en la prohibición del acceso a éstas para los menores, como dice TRONCOSO REIGADA "aislar a un hijo de las redes sociales, prohibírselas, es posiblemente, condenarle al desarraigo. El acceso a Internet es un derecho fundamental de la persona, lo que no quiere decir que no tenga que estar sometido a límites, que requieren de una regulación legal y un control judicial, sin perjuicio de la posible intervención en el ámbito de autoridades administrativas independientes"[34].

Es innegable que las redes sociales y la tecnología en sí son esenciales en el mundo moderno en el que se vive y son los menores, precisamente por haber nacido ya inmersos en el mundo tecnológico, los que deben ser capaces de controlarlas y manejarlas a la perfección para hacer frente al futuro. Por esta razón los esfuerzos deben ir dirigidos a una buena educación de los menores en este ámbito, a concienciarles desde muy temprano de las ventajas y los riesgos que acarrean las redes sociales e Internet para que sean capaces de hacer un uso correcto por sí mismos. Para ello es necesaria una gran implicación de los padres y las instituciones, pero también y fundamentalmente de los proveedores de servicios. Son éstos últimos quienes desempeñan un papel esencial, precisamente por ser los encargados de desarrollar la red social y en consecuencia los que tienen mayores posibilidades de establecer mecanismos de protección para los menores.

Aunque es cierto que cada vez son más las redes sociales que tratan de aplicar mayores controles y protecciones, aun cuentan con pocas restricciones preestablecidas. Por ejemplo, un mecanismo de protección de la privacidad podría ser configurar los perfiles de modo que al registrarse en una red social, éste, por defecto, se estableciera como un perfil privado, de manera que para hacerlo público se tuviera que cambiar la configuración de la cuenta.

Otra cuestión importante es el tema de la edad, como se ha dicho anteriormente en España se puede acceder legalmente a una red social a partir de los 14 años, sin embargo la realidad demuestra que son muchos los usuarios de redes sociales que no alcanzan esa edad. La mayoría de las redes sociales actuales únicamente cuentan con

[34] TRONCOSO REIGADA, Antonio, *La protección de datos personales. En busca del equilibrio.* Valencia, 2010, pág. 1691.

una casilla a la hora de registrarte en la que debes indicar que eres mayor de 14 años con un simple clic, de modo que no se puede asegurar en absoluto que realmente la persona que se registra tiene esa edad o más. O, simplemente es tan fácil como indicar que tienes una edad superior a la que realmente tienes. Son aspectos difíciles de controlar pero que posiblemente con la petición del DNI electrónico podrían solventarse.

En definitiva, se trata de crear un entorno más seguro en Internet que sea capaz de asegurar la privacidad no solo a nivel nacional sino mundial, teniendo siempre en cuenta los distintos ordenamientos jurídicos de cada Estado. Por este motivo, es esencial la coordinación de todos ellos en la medida de lo posible, puesto que Internet es un fenómeno que escapa a cualquier tipo de barrera o frontera.

3 La privacidad e intimidad del menor en Internet.

Como se ha venido manteniendo, la aparición y evolución de las TIC ha comportado que, junto a las numerosas ventajas y avances que éstas han supuesto, se desarrollen también a la par gran cantidad de riesgos, en especial para los menores al ser considerados como personas más vulnerables. Tal y como se ha expuesto anteriormente los menores tienen muchas posibilidades de ser víctimas de delitos cibernéticos como el *ciberbullying*, *sexting*, etc., pero otro de los grandes riesgos que presenta el uso descontrolado de Internet y en concreto de las Redes Sociales es la pérdida de privacidad e intimidad.

Privacidad e intimidad son dos términos que van unidos de la mano y del mismo modo que Internet no garantiza uno tampoco lo hace con el otro. Lo cierto es que lo mejor sería que se entendiese cuanto antes que no hay ni privacidad ni intimidad en Internet, y menos aún en las redes sociales. En este sentido, establece PELÁEZ FERNÁNDEZ que "tal y como se entiende en la actualidad el concepto de red social, conlleva la renuncia por parte de los usuarios del derecho a la intimidad"[35].

Cualquier persona que navega por Internet, sin saberlo, va dejando un rastro que los hace fácilmente identificables para terceras personas con tan solo introducir un nombre en un buscador, pero si, además, lo que se utiliza son Redes Sociales como las que hay a día de hoy (*Instagram, Facebook, Twitter*,…) los riesgos son aún mayores, ya que la propia dinámica de estas Redes Sociales consiste en la creación de un perfil con toda clase de datos personales. Es este aspecto el que más preocupa en relación con los

[35] PELÁEZ FERNÁNDEZ, Palmira, *Redes sociales y derecho fundamental a la intimidad en los menores*. UNED, 2015, pág. 1.

menores, puesto que son menos conscientes de los riesgos que supone facilitar tanta información personal y por ello se disponen a crear perfiles con todo tipo de datos personales reales que les coloca en una situación de total vulnerabilidad.

"La privacidad la podemos definir como el ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado, y que debe de mantenerse de forma confidencial"[36]. El problema es que este concepto de privacidad se encuentra en entredicho a día de hoy, por lo menos para los menores que ya manejan una concepción distinta de dicho término. Ahora, lo "normal" es compartir a diario fotografías y vídeos personales, publicar la localización a cada momento, datos personales como fecha de nacimiento, domicilio, lugar de estudios, etc. En suma, publicarlo absolutamente todo sin dejar nada en el ámbito de la vida privada. El problema está en creer realmente que eso es lo normal, que es lo que hay que hacer, que actuar de esa manera homogeneiza al menor con su grupo de adscripción y evita su segregación del mismo. Se han establecido en el mundo digital unas prioridades que no son las correctas, como ser el que más seguidores tiene en las redes sociales, el que más "me gusta" recibe en sus fotos, etc., relegando la privacidad a un segundo plano.

Resultaría absurdo pretender tener la misma privacidad e intimidad en la vida real que cuando se hace uso de Internet. Simplemente con navegar por Internet ya proporcionamos una gran cantidad de datos sin darnos cuenta, ¿qué se debe esperar entonces si son los propios usuarios los que voluntariamente proporcionan toda clase de información y datos personales sin ningún tipo de control?.

Es ahí donde está el error, si de por si digamos que Internet no está dado a proteger la intimidad, no deben ser los propios usuarios quienes faciliten que esa intimidad sea vulnerada. Según una encuesta del INE[37], "tres de cada cuatro usuarios de Internet en los 12 últimos meses (el 73,5%), han suministrado algún tipo de información personal a través de Internet. El 65,7% menciona *datos personales (nombre, fecha de nacimiento, etc.).* Con prácticamente las mismas menciones (el 65,1%) se indica *datos de contacto (dirección, número de teléfono, etc.).* Tras ellas se sitúan los *detalles de pago* (45,2%) y *otra información personal* (31,5%)". El INE, en una de sus encuestas[38], arroja otro dato interesante, "el 62,9% de los usuarios de Internet en los 12 últimos meses (casi 11 puntos

[36] COZ FERNÁNDEZ, Jose Ramón; FOJÓN CHAMORRO, Enrique; HERADIO GIL, Rubén; CERRADA SOMOLINOS, Jose Antonio, *Evaluación de la privacidad…,* cit. Pág. 1.
[37] Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, INE, 2016.
[38] Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, INE, 2016.

más que en 2015) declara conocer que las "*cookies*" son unos ficheros que se pueden utilizar para rastrear los movimientos de las personas en Internet, para hacer un perfil de cada usuario y presentarles anuncios a medida. Sin embargo, tan sólo el 31,0% de los usuarios (siete puntos más que en el año anterior) indica *haber realizado modificaciones en la configuración del navegador para prevenir o limitar las cookies".*

El problema se agudiza cuando se habla de los menores, al haber nacido inmersos en la era digital, no son conscientes del peligro real que entraña un mal uso de Internet ni de los riesgos a los que ellos mismos se exponen. Alrededor de un 70% de menores son usuarios de una Red Social donde publican diariamente toda clase de información, como dónde están en ese momento, qué están haciendo, dónde viven, si tienen pareja, etc., y lo peor, no es solo que publican información personal propia sino que también lo hacen de terceros muchas veces sin su consentimiento, por ejemplo al etiquetar a amigos en una foto. Lo que no saben es que hay mucha gente malintencionada que se dedica a recopilar ese tipo de información para cometer delitos como el acoso o la pornografía infantil entre otros.

Otra cuestión relevante es que cuando hablamos de intimidad al igual que de privacidad, hay que tener en cuenta también el derecho a la libertad de información y a la libertad de expresión. Con carácter general el derecho a la información tendrá un lugar predominante sobre los derechos al honor, a la intimidad y a la propia imagen puesto que "contribuyen a la formación de la opinión pública y con ello al pluralismo político que exige el principio democrático"[39]. Sin embargo, esto no significa que se tenga derecho a ver y decir todo lo que nos plazca en Internet y menos cuando se habla de menores, ya que, como bien dice LORENTE LÓPEZ "la infancia y la juventud gozan de una especial protección constitucional, que establece claros límites a la libertad de información. Informar es libre pero ante los menores esa libertad disminuye, encontrando exigencias y responsabilidades inmediatas"[40].

Nuestra Constitución, en su artículo 18, tutela este conjunto de derechos que se ven íntimamente afectados por las nuevas tecnologías y que, la unión de todos ellos trata de dar protección a la privacidad de una persona, es decir, a la vida personal. En el conjunto de este artículo 18 se pretende garantizar el derecho al honor, la intimidad personal y familiar y a la propia imagen, además del derecho a la inviolabilidad del domicilio, el secreto de las comunicaciones y un nuevo derecho a la protección de datos. Se trata, en

[39] LORENTE LÓPEZ, María Cristina, *Los derechos al honor, la intimidad personal y familiar y a la propia imagen del menor.* Arandazi. Navarra, 2015.
[40] LORENTE LÓPEZ, María Cristina, *Los derechos al honor, la intimidad personal*…, cit. Pág. 85.

definitiva, de una serie de derechos que hay que garantizar para mantener una mínima calidad de vida.

Son derechos que, como bien establece la Constitución en su artículo 53.2, se encuentran especialmente protegidos mediante el recurso de amparo ante el Tribunal Constitucional y mediante la LO 1/1982 de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Asimismo, el artículo 20.4 de la CE recalca la protección especial que reciben los menores al establecer que "Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia".

Del mismo modo, la Sentencia del Tribunal Supremo 311/13, de 8 de mayo, reafirma que los menores necesitan de una protección reforzada y que ésta "ha sido reconocida por la doctrina del TC y la jurisprudencia del TS, en el sentido de que si bien todas las personas tienen derecho a ser respetados en el ámbito de su honor, intimidad y propia imagen, los menores lo tienen de manera especial y cualificada, precisamente por la nota de desvalimiento que les define por tratarse de personas en formación más vulnerables por tanto a los ataques a sus derechos".

También hay que destacar la LO 8/2015, de 22 de julio, de modificación del sistema de protección a la infancia y a la adolescencia y la ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia que han modificado gran cantidad de leyes y pretenden otorgar una mayor protección a este colectivo tan vulnerable que son los menores. Estas reformas han sido desarrolladas en dos leyes por el hecho de que todas las cuestiones que afecten a derechos fundamentales deben ser reguladas mediante Ley Orgánica, mientras que el resto de cuestiones son reguladas mediante Ley Ordinaria.

En definitiva, está claro que la evolución de las TIC no se va a frenar, por lo menos de momento. Por eso, lo importante es que se vaya evolucionando a la par tanto en materia de protección como en materia de educación. No solo se deben dirigir los esfuerzos a establecer leyes y leyes que traten de proteger a los menores, sino de dotarles de una buena educación para con las nuevas tecnologías, enseñarles que son buenas y muy beneficiosas pero que también entrañan unos riesgos y que por ello es esencial hacer un buen uso de ellas y tener claro que la intimidad es necesaria para conservar una calidad de vida y que no es aconsejable volcar esa intimidad en el mundo virtual donde dejará de ser suya para siempre.

3.1. Injerencia de los padres en la intimidad de los menores.

Cuando se hace referencia a la intimidad de los menores y los riesgos que para ésta pueden suponer las nuevas tecnologías, es inevitable preguntarse si los padres tienen derecho a controlar o supervisar la actividad que desarrollan los hijos menores en Internet.

Como es sabido, la intimidad supone un derecho fundamental establecido en el artículo 18 de la Constitución y reconocido a toda persona, sea menor o no. Del mismo modo, este derecho se encuentra también reconocido en el artículo 4.1 de la Ley Orgánica 1/1996 de Protección Jurídica del Menor "Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones". Además, añade esta misma ley en su artículo 4.5 que, "Los padres o tutores y los poderes públicos respetarán estos derechos y los protegerán frente a posibles ataques de terceros".

En esta misma línea, el artículo 16 de la Convención de los Derechos del Niño, de 20 de noviembre de 1989, proclama que "Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".

Por lo tanto, en principio se podría pensar que los menores, al igual que los adultos, disponen de sus derechos fundamentales por el mero hecho de ser persona y que no sería posible una injerencia en ellos por parte de los padres ni de nadie. Sin embargo, hay que destacar aquí la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen que regula el consentimiento de los menores respecto a las intromisiones en sus derechos estableciendo en su artículo 3 que, **"**El consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil. En los restantes casos, el consentimiento habrá de otorgarse mediante escrito por su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el juez".

No hay que olvidarse tampoco de que los padres a su vez, en ejercicio de la patria potestad tienen unos deberes que cumplir. En este sentido, NATALIA GARCÍA dice "la patria potestad habrá de ejercerse con pleno respeto de los derechos que tienen los

menores reconocidos, pero, al tiempo, teniendo en cuenta que también incumbe a sus progenitores la obligación de velar por ellos"[41]. ¿Entra pues, dentro de su obligación de velar por ellos, el controlarles sus actividades con las nuevas tecnologías e Internet?

En este sentido se pronuncia la Sentencia del TS de 10 de diciembre de 2015 dictada por el Magistrado del Tribunal Supremo Antonio del Moral, Ponente de la mencionada Sentencia. En esta Sentencia se consideraron válidas las pruebas obtenidas por una madre al acceder a la cuenta de Facebook de su hija sin su consentimiento por la simple razón de que existían indicios claros de que la menor en cuestión estaba siendo víctima de acoso sexual a través de esta Red Social. Por tanto, lo primero que hay que tener en cuenta es que si no hay nada que demuestre una falta de madurez del menor, no estaría justificada una injerencia en sus derechos. Sin embargo, si hay indicios que hacen prever que el menor está siendo víctima de algún acto ilícito que lo coloque en una situación de vulnerabilidad, la intromisión por parte de los progenitores estaría más que justificada. Como dice la citada Sentencia, "No puede el ordenamiento 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 que las evidencias apuntaban inequívocamente en esa dirección".

Se destacan pues, varias ideas en relación con el derecho de injerencia de los padres en la intimidad de los menores. Lo más importante es concienciar a los menores y darles confianza para que cuando sufran el mínimo ataque a través de las nuevas tecnologías lo comuniquen abiertamente a sus progenitores. Por otro lado, también es esencial establecer un punto medio de control, es decir, los padres no deben controlarlo todo pero tampoco dar una libertad absoluta, sino que en función de cada caso y cada menor se deben establecer unos límites y unas pautas de control adecuadas. Para ello se debe tener en cuenta el grado de madurez de cada menor y velar siempre a favor del interés superior del menor.

Por último, también hay que tener en cuenta la publicación de fotografías de los hijos menores por parte de los padres. En este caso, la Audiencia Provincial de Pontevedra determinó en su Sentencia 208/2015 de 4 de junio, que para colgar fotos de un hijo menor es necesario el consentimiento de los dos progenitores, ya que la representación legal del menor la ostentan ambos por ser titulares de la patria potestad.

[41] GARCÍA GARCÍA, Natalia: "¿Pueden los padres violar realmente la intimidad de los menores?" [en línea], *Sepín*, 2016, < https://blog.sepin.es/2016/09/intimidad-menores-control-parental/ > [consulta: 28 de octubre de 2017].

4 Mecanismos de protección de la privacidad en Internet.

4.1. El nuevo Reglamento General de Protección de Datos de la Unión Europea.

El 4 de mayo de 2016 se publicaba en el Diario Oficial de la Unión Europea el nuevo Reglamento de Protección de Datos (RGDP) denominado, *Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 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*. Este nuevo Reglamento deroga la anterior Directiva 95/46/CE[42], transpuesta en nuestro ordenamiento jurídico mediante la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Entró en vigor el 24 de mayo de 2016, pero no será posible su aplicación hasta que hayan transcurrido dos años, es decir, hasta el 25 de mayo de 2018, por lo que hasta entonces hay que regirse por lo dispuesto en la Directiva. Se establece un periodo tan amplio para su aplicación por dos razones, por un lado, para que las instituciones, entidades y organismos tengan tiempo suficiente para ir adaptándose a lo establecido en el nuevo Reglamento y, por otro lado, para elaborar las normas necesarias que permitan el desarrollo y aplicación del Reglamento.

Tal y como se establece en el Considerando 14[43] del RGPD, la protección que en él se contempla se aplicará a las personas físicas siempre en relación con el tratamiento de sus datos personales y no al tratamiento de datos personales relativos a personas jurídicas. Asimismo, en el Considerando 38 se hace especial mención a la protección de los niños, estableciendo literalmente que "los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de sus datos".

Uno de los problemas que hasta ahora se venían dando era el hecho de encontrar entre los Estados miembros significativas diferencias en los niveles de protección que, junto al auge de las tecnologías de la información y la comunicación (TIC), que facilitan una comunicación instantánea y transfronteriza, han hecho necesaria una actualización profunda del marco legislativo para poder hacer frente a dichos problemas. Por este motivo, aparece el nuevo RGPD que, como bien dice EFRÉN DÍAZ, "su objetivo será

[42] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[43] "La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto".

superar la fragmentación normativa existente y modernizar los principios de privacidad en la Unión Europea"[44].

Dentro de esa actualización del marco legislativo, uno de los aspectos más relevantes ha sido ampliar el ámbito de aplicación de las normas que regulan la protección de datos. Ahora, el nuevo RGPD no sólo se aplica en los Estados miembros sino que se amplía a los responsables/empresas que no se encuentran en el territorio de la Unión pero que ofrecen algún tipo de servicio o producto dentro de ella. Esto se debe a que, tal y como establece el Considerando 116 del RGPD "cuando los datos personales circulan a través de las fronteras hacia el exterior de la unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información".

No obstante, esta no es la única novedad que ofrece el nuevo RGPD sino que son muchas más, entre las que se encuentran, por ejemplo, la introducción de la figura del Delegado de Protección de Datos o *Data Protection Officer* (DPO) que será de suma importancia en el futuro y la incorporación del derecho al olvido.

Una de las novedades más interesantes es establecer la protección de datos desde el diseño y por defecto[45]. Desde el diseño supone que cuando se pretenda sacar un nuevo servicio o producto se debe, previamente, analizar los riesgos que pueda suponer para la privacidad de los interesados y tomar medidas de antemano. Además, SUSANA RODRÍGUEZ y MARÍA VIDAL, sugieren una idea muy acertada al decir que "siendo prácticos, resultaría más complicado y costoso adecuar la aplicación a *posteriori* por lo que el cumplimiento de este nuevo principio va en beneficio de aquellos que traten datos de carácter personal"[46].

Por otro lado, la protección de datos por defecto implica que el responsable del servicio o producto proteja de manera predeterminada los datos personales de los interesados, sin que éstos tengan que hacerlo. Así, por ejemplo, si se atiende a la Red Social de *Instagram*, se observa como esta aplicación dispone de una serie de mecanismos de protección de la privacidad como sería el poner la cuenta como privada, no permitir que todos los usuarios puedan ver tus fotos y comentarios, etc. Bien, pues en este caso, establecer la privacidad por defecto supondría que al crearte una cuenta ya accedieses

[44] DÍAZ DÍAZ, Efrén, *El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*. Aranzadi, 2016, pág. 1.
[45] Artículo 25 del RGPD relativo a la "Protección de datos desde el diseño y por defecto".
[46] RODRÍGUEZ BALLANO, Susana y VIDAL, María, *Habemus nuevo Reglamento General de Protección de Datos*. Aranzadi, 2016, pág. 1.

con toda esta seguridad establecida, y que fuese decisión del usuario si quiere limitar esa seguridad o incluso eliminarla.

Se introduce, también, en el artículo 33 del RGPD la obligación de informar a la autoridad de control, en nuestro caso a la Agencia Española de Protección de Datos (AEPD), de los fallos de seguridad que pudieran darse y que supongan un riesgo para las personas físicas sin dilación indebida y, a ser posible, en un plazo máximo de 72 horas. Lo mismo se establece en el artículo 34 del RGPD para informar a los interesados.

Otra cuestión novedosa es el gran hincapié que se hace en exigir el consentimiento del interesado a la hora de tratar sus datos personales. El RGPD establece en su Considerando 32 que "el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen" y asimismo, "el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento".

En relación con el consentimiento se debe hacer especial referencia al consentimiento otorgado por menores, ya que el ámbito de los menores es considerado delicado de por sí, pero aún lo es más si se atiende a la protección de datos. En este sentido, se encuentra el artículo 8[47] del RGPD, que viene a decir que cuando se trate de una oferta directa a niños de servicios de la sociedad de la información, el tratamiento de sus datos personales únicamente será lícito cuando el menor tenga como mínimo 16 años y preste su consentimiento. En el caso de que el menor tenga menos de 16 años, este tratamiento solo será considerado lícito si el consentimiento es dado o autorizado por el titular de la patria potestad o tutela del niño. No obstante, los Estados miembros pueden establecer legalmente una edad inferior, siempre que no sea inferior a 13 años. El problema que se encuentra en este punto es la verificación de la edad, ya que en muchas ocasiones esto se consigue con la simple marcación de una casilla en la que aseguras que eres mayor de edad, por lo que resulta sumamente sencillo mentir en este aspecto. Por este motivo, "el RGPD obliga al responsable del tratamiento a llevar a cabo esfuerzos razonables para verificar que el consentimiento ha sido dado o autorizado por el titular de la autoridad parental sobre el niño"[48].

Junto al consentimiento se halla íntimamente ligado el principio de transparencia, que exige aportar más información a los interesados con anterioridad a la recogida de sus

[47] Artículo 8 del RGPD relativo a las "*Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información*".
[48] DÍAZ DÍAZ, Efrén, *El nuevo Reglamento General de Protección de Datos…* cit., pág. 20.

datos personales y que, además, toda la información y comunicación relativa al tratamiento de datos de carácter personal sea accesible y fácil de entender, y que se emplee para ello un lenguaje claro y sencillo. Lo mismo se establece en relación con los menores al exigirse que dicha información les sea fácil de entender.

La última novedad a citar, aunque como se ha dicho hay muchas otras, es la evaluación de impacto relativa a la protección de datos[49], también conocida como "*PIAs*" ("*Privacy impact assessment*"). Esta nueva figura supone que cuando se prevea como probable que un tratamiento de datos de carácter personal, en especial mediante nuevas tecnologías, pueda suponer un riesgo para los derechos y libertades de las personas físicas, el responsable de ese tratamiento deberá llevar a cabo una evaluación de su impacto en la protección de datos personales.

En definitiva, el nuevo Reglamento de Protección de Datos se presenta como un mecanismo totalmente actualizado y dispuesto a hacer frente a los problemas que hasta ahora se han encontrado en el ámbito de la protección de datos. Establece, como se ha visto, cuestiones muy novedosas que auguran un buen futuro tras su aplicación, pero al mismo tiempo, se presenta con muchas dudas ya que aún cuesta imaginar cómo se van a llevar a cabo estos grandes cambios y como van a influir en todo el sector.

4.2. El derecho al olvido.

Con la aparición de la Web 2.0, la cantidad de información de una persona en Internet, haya sido publicada por el propio titular o por terceros, ha aumentado considerablemente, lo que está ocasionando cada vez más problemas en la vida personal, por no hablar de la nueva Web 3.0 que no solo permite la comunicación multidireccional entre los usuarios sino que, además, permite "la creación de grandes bases de datos sobre las preferencias de los usuarios configuradas a partir de la información guardada de sus búsquedas personalizadas"[50].

Uno de los ámbitos donde más problemas están surgiendo es en el laboral. Cada vez son más los casos en los que las empresas han despedido a sus trabajadores por ciertas informaciones que han sido publicadas en las Redes, o incluso antes de contratar a alguien rastrean a la persona para obtener datos sobre ella. Por este y otros muchos motivos, es cada vez más habitual que la gente demande cierto control y protección en lo relativo a la información personal que les concierne y se halla en Internet a disposición de

[49] Artículo 35 del RGPD "*Evaluación de impacto relativa a la protección de datos*".
[50] LÓPEZ PORTAS, María Begoña, *La configuración jurídica del derecho al olvido en el derecho español a tenor de la doctrina del TJUE*. UNED. Madrid, 2015, pág. 2.

todo el mundo, pues, "todo ciudadano ha de tener el control y disposición sobre sus propios datos personales"[51]. Y es que lo preocupante no es solo la información que la gente publica en Internet sin darse cuenta gracias a las Redes Sociales actuales (*Instagram, Twitter, Facebook,…)* que invitan a compartir cualquier aspecto de la vida por íntimo que sea, sino que también preocupa y mucho la información que es publicada por terceros y que está al alcance de cualquiera con tan solo poner un nombre en un buscador.

Se habla así del polémico derecho al olvido, tan discutido incluso a día de hoy. Se trata de un derecho que carecía de ningún tipo de regulación hasta la aparición del nuevo Reglamento General de Protección de Datos, pero la Agencia Española de Protección de Datos (AEPD) ya hace tiempo que viene reivindicando su importancia al destacar que ningún ciudadano que no goce de la condición de personaje público, ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a que sus datos de carácter personal circulen por la Red sin poder corregir la inclusión de los mismos en un sistema de comunicación universal como Internet.

El derecho al olvido es definido por M. BEGOÑA LÓPEZ como "la facultad que tiene el titular de un dato personal a eliminar o bloquear información personal que se considera obsoleta por el paso del tiempo o que vulnera sus derechos fundamentales"[52]. Por lo tanto, se debe entender este derecho al olvido como un derecho de cancelación, rectificación o supresión de información personal[53]. Se observa pues, como el derecho al olvido se encuentra muy relacionado con el derecho a la protección de datos, de ahí la importancia de establecer una regulación que de cabida a este derecho ya que hasta el momento no se tenía reconocido legalmente este derecho como tal.

Tras la aprobación del Reglamento, éste, ya reconoce expresamente el derecho al olvido, estableciendo en su Considerando 65 que "los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un derecho al olvido si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no

[51] HERNÁNDEZ RAMOS, Mario, *Cuaderno Red de Cátedras Telefónica. El derecho al olvido digital en la web 2.0*. 2013, pág. 25.
[52] LÓPEZ PORTAS, María Begoña, *La configuración jurídica del derecho al olvido…,* cit. Pág. 1.
[53] ZÁRATE ROJAS, Sebastián, *La problemática entre el derecho al olvido y la libertad de prensa.* Derecom. 2013. Pág. 3."El derecho al olvido debe entenderse como una pretensión a olvidar o ser olvidado respecto de cierta información de carácter personal, que en sentido estricto se trataría de un derecho subjetivo a la cancelación, rectificación u oposición de dicha información".

son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que le conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento". Particularmente, en relación con el consentimiento menciona este mismo Considerando que, el ejercicio de este derecho también debe ser posible incluso cuando el consentimiento se dio siendo niño, ya que se es menos consciente de los riesgos que puede suponer el tratamiento de tales datos.

El nuevo RGPD, además, regula específicamente el derecho al olvido en su artículo 17 estableciéndolo como un derecho de supresión, distinto de los llamados derechos ARCO (acceso, rectificación, cancelación y oposición) que ya estaban reconocidos, al que tendrán opción de acudir todos los interesados cuando se den una serie de circunstancias que se encuentran recogidas en el mencionado artículo. Para dotar de mayores garantías a este derecho el Reglamento también establece en su Considerando 66 que "el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos".

Al hablar del derecho al olvido, de obligada mención es la famosa sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, que hace referencia al caso Google vs. AEPD en el que la empresa Google se negaba a cumplir la normativa española y europea referente a la protección de datos. Se trata de una sentencia muy importante en el ámbito del derecho al olvido y en ella se esclarecen diversas cuestiones relacionadas con dicho derecho.

Lo primero y más importante que establece la sentencia del TJUE es que la actividad que realizan los motores de búsqueda suponen un tratamiento de datos personales y por lo tanto, Google, que se trata de un motor de búsqueda, está sujeto a la normativa de protección de datos europea ya que ha creado un establecimiento en uno de los Estados miembros, lo que le obliga en consecuencia a respetar los derechos de cancelación y oposición que se les reconoce a todos los ciudadanos.

De este modo, las personas tendrán derecho a solicitar a los motores de búsqueda la eliminación de información o datos personales, cuando ello pueda suponer una lesión de sus derechos y el tratamiento no esté justificado. El problema que esto supone es que la eliminación de estos datos se hace únicamente del motor de búsqueda, es decir, lo que

se conseguirá es que al poner un determinado nombre en el buscador, éste no te redirija a las páginas donde se encuentre información de esa persona, pero, sin embargo, la página en sí que contiene dicha información podrá seguir intacta lo que hará posible que se pueda acceder a ella por otros medios o introduciendo otros términos que no sean el nombre de la persona afectada.

Otra cuestión que establece la sentencia del TJUE de 13 de mayo de 2014 es que debido a la gran influencia que tienen los buscadores sobre los derechos de privacidad y protección de datos, hay que destacar que los derechos de las personas deberán prevalecer por encima de los posibles intereses económicos de estos motores de búsqueda e incluso sobre los propios intereses de los internautas en disponer de esa información. Sin embargo, será necesario ponderar cada caso, ya que si se trata de información con gran interés para el público por afectar por ejemplo a un personaje público, esa información no será bloqueada y no se podrá reconocer el derecho al olvido.

En definitiva, esta sentencia supuso "un paso adelante en el derecho al olvido de los ciudadanos[54]" hoy reconocido en el nuevo RGPD, pero aún así habrá que seguir luchando para lograr mayores garantías en lo concerniente a la protección de datos de carácter personal como por ejemplo, eliminar la información de la página de origen para que de este modo se evite poder acceder a ella por otros medios que no sean los buscadores.

4.3. El Data Protection Officer (DPO).

El *Data Protection Officer* (DPO) o Delegado de Protección de Datos es otra de las novedades introducidas por el nuevo Reglamento de Protección de Datos. Se trata de una novedad en nuestro país y algunos otros Estados miembros de la Unión Europea, pero no lo es para otros países en los que esta figura ya existía. El DPO surgió por primera vez en Alemania en 1977, con la Ley Federal de Protección de Datos.

Si se atiende a la normativa europea, esta figura ya aparecía en la Directiva 95/46/CE[55] en el apartado 2 de su artículo 18 "…responsable del tratamiento designe, con arreglo, al Derecho nacional al que está sujeto, a un encargado de protección de los datos personales que tenga por cometido…".

Antes de que el Reglamento se aprobara definitivamente, mucho se había discutido acerca de si se debía establecer esta figura como obligatoria o no. En algunos países sí

[54] GUASCH PORTAS, Vicente, *El derecho al olvido en Internet.* UNED, 2015, pág. 8.
[55] 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 estos datos.

es obligatoria, pero en España se ha optado por establecer el DPO como voluntario con carácter general. No obstante, el Reglamento dota de una especial importancia a la figura del DPO, al asignarle una sección propia, la sección 3 del Reglamento compuesta por tres extensos artículos y en uno de ellos ha establecido una serie de supuestos concretos en los que dicha figura será obligatoria en todo caso, que son los siguientes[56]:

- Cuando el tratamiento de datos personales sea llevado a cabo por una autoridad u organismo público, a excepción de los tribunales de justicia que actúen en el ejercicio de su función jurisdiccional.
- Cuando la actividad principal de una entidad, institución u organismo sea la realización de operaciones de tratamiento de datos personales a gran escala.
- Cuando estas entidades, instituciones u organismos tengan como actividad principal el tratamiento a gran escala de datos personales especialmente protegidos que se encuentran regulados en el artículo 9 del RGPD, así como a los datos relativos a condenas e infracciones penales recogidos en el artículo 10 del Reglamento.

En cuanto al cometido del DPO, el RGPD establece en su artículo 39 una serie de funciones propias que son:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales de las obligaciones que les incumben en virtud del Reglamento y otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) supervisar el cumplimiento de lo dispuesto en el Reglamento, en otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
c) ofrecer el asesoramiento que se le pida acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización;
d) cooperar con la autoridad de control;

[56] Casos establecidos en el artículo 37 del RGPD relativo a la "designación del delegado de protección de datos".

e) actuar como punto de contacto de la autoridad de control para las cuestiones relacionadas con el tratamiento de datos personales incluida la consulta previa, y consultar en su caso, sobre cualquier otro asunto.

Como bien dice el Grupo de trabajo de protección de datos del artículo 29 esta lista es abierta y las citadas funciones son las que tiene que tener como mínimo un DPO pero "tanto el responsable como el encargado del tratamiento pueden asignarle otras"[57].

En suma se trata de una figura muy importante y necesaria. Aunque, como se ha visto, el Reglamento solo establezca unos pocos casos en los que esta figura sea obligatoria, igualmente las entidades pueden decidir incluir en su plantilla un DPO cuando lo consideren oportuno siempre que se cumplan los requisitos necesarios. Lo interesante sería que todas optaran por esta opción pero, el hecho de no ser obligatoria en todo caso, puede suponer que las empresas que no se encuentren en uno de los supuestos citados prescindan de ella, pero claro eso solo el tiempo lo dirá.

4.4. El papel de los proveedores de servicios.

Los proveedores de servicios de Internet o ISP (*Internet service provider*) son empresas y organizaciones que proporcionan a sus clientes el acceso a Internet y a otros servicios relacionados, normalmente a cambio de pagar una cuota económica. A día de hoy, la mayoría de las empresas telefónicas que conocemos como Movistar, Vodafone, Orange, Yoigo, etc., funcionan también como proveedores de acceso a Internet.

La Ley de Servicios de la Sociedad de la Información y de Comercio electrónico[58] (LSSICE) establece la responsabilidad de los distintos tipos de prestadores de servicios. En su artículo 13 establece la responsabilidad de todo prestador de servicios de Internet, según el cual, "Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley. Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes".

Por lo tanto, se deduce que "la regla general será la exoneración de la responsabilidad, y las excepciones se darán o bien cuando se trate de contenidos propios, o bien en casos

[57] RECIO GAYO, Miguel, *Directrices del GT29 sobre el delegado de protección de datos: figura clave para la responsabilidad (<<accountability>>)*. Wolters Kluwer, 2017, pág. 12.
[58] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

de falta de diligencia con conocimiento efectivo, tratándose en estos casos de supuestos de responsabilidad por hecho ajeno"[59], es decir, los ISP solo serán responsables de los contenidos que ellos mismos hayan elaborado o se hayan elaborado por cuenta suya.

De este modo, se tratará de analizar ahora que medidas adoptan algunos de los Servicios de la Sociedad de la Información más utilizados en materia de privacidad, es decir, que mecanismos pone cada uno de los Servicios para que sus usuarios configuren la privacidad de su perfil. En este sentido, la AEPD dispone en su página web[60] de una serie de vídeos muy ilustrativos y útiles para conocer la configuración de privacidad con la que cuentan algunas de las Redes Sociales y aplicaciones de mensajería instantánea más conocidas.

Facebook es una Red Social fundada en el año 2004 en la universidad de Harvard y, a día de hoy, es de las más utilizadas. Para poder utilizar *Facebook* hay que crearse un perfil y la foto y el nombre que se establezcan siempre serán públicos, por eso es aconsejable no poner el nombre real. Asimismo, *Facebook* permite configurar distintos niveles de privacidad según las preferencias de cada persona. De forma predeterminada, esta Red Social configura la privacidad de los perfiles de manera que solo pueden ver tus cosas las personas que tienes como amigos, pero no obstante, todos pueden ponerse en contacto contigo y buscarte a través de la Red Social. Otra cuestión importante de *Facebook*, es que cuenta con una casilla, marcada por defecto, que permite que los motores de búsqueda fuera de *Facebook* indexen tu perfil, de manera que cualquier persona puede encontrarte con tan sólo poner tu nombre en un buscador.

Si se atiende ahora a *Instagram*, también se trata de una Red Social que surgió en el año 2010 y que está destinada a compartir fotos y vídeos. Cuando se crea un perfil, esta Red Social, de forma predeterminada, permite que todo lo publicado en él sea visto por cualquier persona, de manera que, para evitarlo, hay que dirigirse a opciones y activar la opción de cuenta privada. De este modo, lo publicado en el perfil solo podrá ser visto por los contactos aceptados. Además, al igual que en prácticamente todas las Redes Sociales y aplicaciones de mensajería instantánea, cuenta con la opción de bloqueo mediante la que puedes evitar que determinadas personas puedan ver tu perfil o ponerse en contacto

[59] HERNÁNDEZ FERNÁNDEZ, Asunción, *Enlaces, búsqueda, propiedad intelectual y responsabilidad: Case State 2010-2013*. Dialnet, 2013, pág. 3.

[60] http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/protegetuprivacidad/index-ides-idphp.php

contigo, lo cual resulta muy útil para evitar acosos o ataques de personas malintencionadas.

Whatsapp es una aplicación de mensajería instantánea en la que se pueden intercambiar mensajes de texto y audio, todo tipo de material multimedia e incluso realizar llamadas y videollamadas. Esta aplicación cuenta también con distintos niveles de privacidad, accediendo a configuración se puede establecer que nadie, solo los contactos o todos puedan ver la información que se comparte como la foto de perfil, el estado, la última conexión, etc. Una de las novedades que ha presentado recientemente esta aplicación es el cifrado de extremo a extremo que se activa por defecto, lo que permite una mayor seguridad en las conversaciones. Según explica la propia aplicación los mensajes y llamadas "están protegidos con cifrado de extremo a extremo, lo que significa que ni *Whatsapp* ni terceros pueden leerlos ni escucharlos". Pese a toda esta seguridad que ha implantado la aplicación, la AEPD advierte que hay que tener cuidado con las Redes *Wifi* a las que se accede, ya que si esta es pública, cualquier persona malintencionada y con experiencia podría capturar tus conversaciones.

Snapchat es también una aplicación de mensajería instantánea de las más utilizadas por los adolescentes y que está destinada a enviar mensajes multimedia. Esta aplicación presenta una particularidad y es que el mensaje desaparece entre 1 y 10 segundos después de publicarlo, lo que provoca una falsa creencia generalizada de que los mensajes son seguros y que no es posible guardar información de *Snapchat*. El problema está en que por culpa de esta creencia, sobretodo los más jóvenes, tal vez por su ingenuidad, se arriesgan a publicar contenido más comprometedor y no son conscientes de que un simple segundo es suficiente para hacer una captura de pantalla y guardar esa imagen para siempre. Como el resto de aplicaciones también se puede configurar la privacidad del perfil para restringir las personas que pueden ver las publicaciones y ponerse en contacto con el usuario. Además, *Snapchat*, al igual que otras aplicaciones, cuenta con la verificación de inicio de sesión lo cual resulta muy útil si alguien consigue las claves de acceso de un perfil, ya que consiste en que cuando se inicie sesión en otro dispositivo se tenga que volver a introducir la contraseña y además, poner un código que llega mediante *SMS* al número de teléfono móvil.

Otra de las opciones con la que cuentan prácticamente todas las aplicaciones y Redes Sociales mencionadas es la de denunciar. Hay ocasiones en las que personas malintencionadas se dedican a crear perfiles falsos sobre otras personas, publican imágenes no adecuadas de alguien, ponen comentarios desagradables, etc., por lo que

las aplicaciones establecen cada una en su respectivo lugar una opción mediante la que se puede denunciar ese contenido inadecuado o dañino para que la aplicación lo elimine.

En definitiva, se observa como los distintos proveedores de servicios cada vez abogan más por establecer mecanismos de protección de la privacidad de sus usuarios, pero aun así, se echa en falta una configuración de los perfiles que sea más restrictiva por defecto, es decir, que tenga establecido de forma predeterminada el mayor nivel de privacidad del que disponga la aplicación. Este hecho resultaría muy útil para los menores que utilizan estas aplicaciones y Redes Sociales, ya que son menos conscientes de los riesgos que éstas suponen y por lo tanto son menos propensos a cambiar la configuración respecto a su privacidad por sí mismos. Además, se aconseja a todos los usuarios en general la lectura de las condiciones de uso y las políticas de privacidad de las distintas aplicaciones, para conocer de antemano a qué se exponen y que tipo de tratamiento de la información hace la aplicación.

5 Importancia de la educación como forma de prevención.

Como se ha dicho ya en varias ocasiones en el presente trabajo, las nuevas tecnologías no son malas sino todo lo contrario, son muy beneficiosas y aportan muchas ventajas en el día a día. No obstante, como todo, tiene su parte peligrosa y es que si se hace un mal uso de ellas pueden entrañar unos riesgos con graves consecuencias para nuestros derechos y, en general, puede suponer una pérdida de calidad de vida, especialmente si se habla de los menores.

Se insiste en que la prohibición resulta totalmente impensable, los menores han nacido ya en la era digital con las tecnologías como protagonistas y resultaría absurdo tratar de prohibírselas, ya que a parte de ser necesarias, tienen acceso a ellas fácilmente en cualquier lugar. Por este motivo, es importante destacar el papel de la educación como forma de prevención ante posibles delitos u otras consecuencias negativas en Internet.

Se trata de recabar esfuerzos para educar a los menores en un uso lícito y responsable de las nuevas tecnologías para que aprendan a extraer todos los beneficios que éstas aportan y saber reaccionar ante posibles amenazas. Es aquí donde resulta totalmente esencial la labor de padres, madres, tutores y educadores, quienes deben formarse e informarse en la prevención de riesgos en este ámbito para después transmitir sus conocimientos a sus hijos y alumnos.

Según el INE a medida que avanza la edad desciende el uso de Internet tanto en hombres como en mujeres, siendo el porcentaje más bajo el comprendido en la edad de

65 a 74 años (40'6% de hombres y 29'4% de mujeres). Por lo tanto, observamos que cuanto más mayores menos probabilidades de que utilicen Internet y dentro de este grupo de personas mayores se encuentran obviamente la mayoría de los padres. Es decir, habrá una gran cantidad de padres y madres que o bien no utilicen Internet o bien lo conozcan mínimamente. Por este motivo, antes de poder educar correctamente a los menores en un uso responsable de las TIC deben ser los adultos quienes se esfuercen en conocerlas y aprender a manejarlas para así poder transmitir una buena educación y saber reaccionar ante cualquier peligro.

"La alfabetización digital, incluida la prevención de riesgos de mal uso, debe comenzar a abordarse desde los primeros contactos con las redes por parte de los menores, ya que es en este contexto donde más oportunidades podremos encontrar para inculcar buenas prácticas y estrategias de prevención y sensibilización"[61]. Lo primero y más importante, es diseñar cursos, charlas, guías, recomendaciones, etc., dirigidos a la formación de padres, madres, tutores y educadores en el uso de las TIC, ya que al haber nacido en un mundo sin la presencia de nuevas tecnologías, para ellos supone un cambio muy grande y en ocasiones les resulta demasiado complejo poder adaptarse a ellas. En este sentido, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) ha hecho grandes esfuerzos y ha elaborado guías muy recomendables para padres y madres. Una vez que éstos tienen ya una base, se trata de poner en práctica esos conocimientos con los hijos y alumnos.

En el ámbito doméstico sería aconsejable establecer una serie de pautas para prevenir los riesgos en las TIC, como por ejemplo:

- Establecer una buena comunicación intrafamiliar para que el niño se sienta cómodo en hablar con sus padres si tiene algún problema.
- Educarles en empatía y sensibilidad, enseñarles a ponerse en el lugar de la víctima y sobretodo respeto hacia todas las personas.
- Enseñarles a tener un pensamiento crítico, es decir, enseñarles a que todo lo que vean en Internet no tiene porque ser verdad.
- Ayudarles a adquirir competencias en el uso de las TIC, enseñarles los riesgos que éstas pueden suponer, enseñarles a hacer un buen uso y establecer mecanismos de protección como por ejemplo la adopción de contraseñas.

[61] Red. es. *Monográgico ciberacoso escolar (ciberbullying)*. Pág. 20.

- Imponer unos horarios, para evitar que los hijos estén todo el día conectados a Internet.
- Situar el ordenador o el dispositivo a través del que se conecte a Internet, en una estancia de uso común para poder controlar a que páginas accede y evitar así el acceso a contenido inadecuado para su edad.

Por su parte, el centro educativo debe coordinarse con los padres, madres y tutores para poder detectar cualquier problema y dar una respuesta lo más rápida posible. Del mismo modo, en el ámbito escolar también sería aconsejable adoptar una serie de pautas en materia de seguridad TIC como por ejemplo:

- Impartir charlas educativas, las cuales se van dando ya cada vez con más frecuencia, sobretodo por parte de las Fuerzas y Cuerpos de Seguridad.
- Introducir en el temario que se imparte en clase la educación en las nuevas tecnologías.
- Enseñarles a responder ante una situación de abuso y hacerles entender que contar los problemas no es ser un "chivato" y que pedir ayuda no es de cobardes.
- Insertar en el centro una persona o grupo de personas expertas en la materia, como por ejemplo un criminólogo ya que tiene mucha formación en esta materia.

En definitiva, estas son algunas de las muchas pautas que se aconseja llevar a cabo en materia de prevención de riesgos en el uso de las TIC. Como bien dice PELÁEZ FERNÁNDEZ "prevención y concienciación serán fundamentales para evitar que incluso, en determinados casos, el propio entorno de los jóvenes sea el que lleve a cabo acciones denigrantes hacia sus iguales, aprovechando las redes sociales para vejar a los propios compañeros"[62]. Otra cuestión a destacar es el lanzamiento por parte del INCIBE de un teléfono de ayuda para aconsejar sobre los riesgos que Internet supone para los menores. Este número es el 900 116 117 y en él se tratará de resolver todas las dudas que se puedan suscitar por parte de los niños y adolescentes respecto a la privacidad, el *sexting*, o cualquier otro uso inapropiado de las redes.

[62] PELÁEZ FERNÁNDEZ, Palmira, *Redes sociales y derecho fundamental…*cit., pág. 12.

6. Conclusiones.

PRIMERA: El incesante avance de las nuevas tecnologías es un hecho real y necesario, por lo que se debe aceptar y aprender a convivir con ellas. Si se hace un buen uso de ellas pueden aportar grandes beneficios y nuevas oportunidades con las que antes no se contaba. No obstante, también conllevan una serie de riesgos, especialmente para los menores por ser considerados como más vulnerables, a la par que son quienes más uso hacen de las nuevas tecnologías. Pueden ser víctimas de delitos cibernéticos contra sus derechos fundamentales, tales como el ciberbullying, sexting, grooming, pornografía infantil, etc…

SEGUNDA: La privacidad en general, pero más concretamente la de los menores, se constituye como uno de los ámbitos más afectados por las nuevas tecnologías. El uso indiscriminado de Internet y en especial las Redes Sociales han propiciado una pérdida de privacidad muy alarmante que, unido a la falta de concienciación de los menores –tanto como víctimas como agresores- los coloca en una situación de máxima vulnerabilidad. Por otra parte, en el uso de las tecnologías de la información y comunicación resulta difícil el equilibrio entre la injerencia de los padres o tutores para cumplir con su deber de proteger al menor y el derecho a la privacidad de éste. La solución puede venir en el sentido expuesto por la STS de 10 de diciembre de 2015, Del Moral García, Antonio, de ponderar en cada caso el peligro objetivo que se cierne sobre el menor y la intensidad de la injerencia, sin que la falta de madurez del menor abra el camino a un control absoluto y desproporcionado.

TERCERA: En adhesión a las opiniones de diversos autores, de lege ferenda se considera necesaria una normativa especial para menores en relación con las nuevas tecnologías, con fundamento en su especial vulnerabilidad. Una regulación específica que, además, se fuese adaptando constantemente a los avances tecnológicos, lo cual supone un reto por el vertiginoso ritmo al que las TIC avanzan, pero resulta esencial para poder proporcionar a los más pequeños una buena protección en el mundo digital.

CUARTA: El nuevo Reglamento General de Protección de Datos (RGPD) se impone en la UE como un gran mecanismo totalmente actualizado en materia de protección de datos de carácter personal, dispuesto a dar una respuesta unificada y solventar los problemas

que hasta ahora se venían dando en este ámbito. No obstante, se plantean ciertas incógnitas respecto a si las personas jurídicas públicas y privadas van a ser capaces de adaptarse a todas las novedades y cómo lo van a hacer antes de su aplicación en mayo de 2018. En el caso de las Administraciones Públicas, para implementar este RGPD, los presupuestos generales ya deberían incluir las partidas necesarias para 2018.

QUINTA: El derecho al olvido, reconocido por el nuevo RGPD, se establece como una figura muy importante en materia de protección de datos posibilitando la eliminación o el bloqueo de información personal obsoleta o que vulnera derechos fundamentales. Sin embargo, no será suficiente para garantizar una protección completa, por lo que habrá que seguir trabajando en este ámbito como por ejemplo mejorando las herramientas para exigir la eliminación de la información de las páginas principales que la contienen y no sólo de los buscadores.

SEXTA: La figura del Data Protection Officer (DPO) es otra de las figuras introducidas por el RGPD como responsable del tratamiento de datos de carácter personal que realizan las empresas y Administraciones Públicas. Esta figura únicamente se establece como obligatoria en determinados casos y supone de vital importancia para posibilitar el cumplimiento del RGPD por parte de las empresas. El DPO se presenta como una profesión de futuro.

SÉPTIMA: Los proveedores de servicios juegan un papel fundamental en la protección de la privacidad de sus usuarios. Aunque es cierto que cada vez están estableciendo más mecanismos de protección de la privacidad en los servicios que ofrecen, se echa en falta el establecimiento de medidas más efectivas como por ejemplo, que el perfil privado sea el que siempre se configure por defecto.

OCTAVA: La educación de los menores en un uso correcto y responsable de las TIC se establece como una tarea primordial que deben asumir padres, madres, tutores y educadores para concienciarles de los riesgos que las nuevas tecnologías pueden suponer y dotarles de los mecanismos necesarios para que sean capaces de detectarlos y así prevenir que sean víctimas de ataques a través de las TIC. En tal sentido son medidas de Política Criminal de carácter preventivo las charlas por profesionales en ámbito docente dirigidas no solo a menores, sino también a padres (AMPAS) y

profesores, e iniciativas como el teléfono gratuito del Instituto Nacional de Ciberdelincuencia (INCIBE).

7. Referencias.

7.1. Bibliografía.

BRINGUÉ, Xavier y SÁDABA, Charo, *Menores y Redes Sociales*. Foro Generaciones Interactivas. 2011.

CASTELLS, Manuel, *Internet y la Sociedad Red.* Conferencia *de Presentación del Programa de Doctorado sobre la Sociedad de la Información y el Conocimiento,* 2000.

CHEANG WONG, Juan Carlos, *Ley de Moore, nanotecnología y nanociencias: síntesis y modificación de nanopartículas mediante la implantación de iones*, UNAM, México, 2005.

COLÁS TURÉGANO, Asunción, *Los delitos de género entre menores en la sociedad tecnológica: rasgos diferenciales*. En Menores y redes sociales. Tirant lo Blanch, 2016.

COZ FERNÁNDEZ, Jose Ramón; FOJÓN CHAMORRO, Enrique; HERADIO GIL, Rubén; CERRADA SOMOLINOS, Jose Antonio, *Evaluación de la privacidad de una Red Social Virtual.* Associação Ibérica de Sistemas e Tecnologias de Informacao. 2012. Retrieved from https://search.proquest.com/docview/1027228507?accountid=15297

DÍAZ DÍAZ, Efrén, *El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*. Aranzadi, 2016.

Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, INE, 2016.

GARMENDIA, Maialen; GARITAONANDIA, Carmelo; MARTÍNEZ, Gemma; CASADO, Miguel Ángel, *Riesgos y seguridad en Internet: Los menores españoles en el contexto europeo.* Universidad del País Vasco/EuskalHerrikoUnibertsitatea, Bilbao: EU Kids Online, 2011.

GUASCH PORTAS, Vicente, *El derecho al olvido en Internet.* UNED, 2015.

HERNÁNDEZ FERNÁNDEZ, Asunción, *Enlaces, búsqueda, propiedad intelectual y responsabilidad: Case State 2010-2013*. Dialnet, 2013.

HERNÁNDEZ RAMOS, Mario, *Cuaderno Red de Cátedras Telefónica. El derecho al olvido digital en la web 2.0.* 2013.

LÓPEZ PORTAS, María Begoña, *La configuración jurídica del derecho al olvido en el derecho español a tenor de la doctrina del TJUE*. UNED. Madrid, 2015.

LORENTE LÓPEZ, Mª Cristina, *Los derechos al honor, a la intimidad personal y familiar y a la propia imagen del menor*. Aranzadi, Navarra, 2015.

LOZANO SALINAS, José María, *La Web 2.0*. Dialnet, 2008.

MARTOS DÍAZ, Natalia y CASADO OLIVA, Óscar, *Derecho y redes sociales*. Civitas Thomson Reuters, Cizur Menor (Navarra), 2013.

OLWEUS, Dan, *Acoso escolar,"bullying", en las escuelas : hechos e intervenciones*. Noruega, 2017.

PELÁEZ FERNÁNDEZ, Palmira, *Redes sociales y derecho fundamental a la intimidad en los menores*. UNED, 2015.

RALLO LOMBARTE, Artemi; MARTÍNEZ MARTÍNEZ, Ricard y ALAMILLO DOMINGO, Ignacio, *Derecho y Redes Sociales.* Civitas Thomson Reuters, Cizur Menor (Navarra), 2013.

RECIO GAYO, Miguel, *Directrices del GT29 sobre el delegado de protección de datos: figura clave para la responsabilidad (<<accountability>>).* Wolters Kluwer, 2017.

RODRÍGUEZ BALLANO, Susana y VIDAL, María, *Habemus nuevo Reglamento General de Protección de Datos*. Aranzadi, 2016.

TRONCOSO REIGADA, Antonio, *La protección de los datos personales. En busca del equilibrio.* Tirant Lo Blanch, Valencia, 2010.

ZÁRATE ROJAS, Sebastián, *La problemática entre el derecho al olvido y la libertad de prensa.* Derecom, 2013.

7.2. Webgrafía.

ALSINA GONZÁLEZ, Guillem: "Definición de ARPANET" [en línea], *Definición ABC*, 2016, < https://www.definicionabc.com/tecnologia/arpanet.php > [consulta: 24 de abril de 2017].

Dossier de indicadores sobre uso de TIC por menores en España elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información. Disponible en http://www.ontsi.red.es/ontsi/es/content/dossier-de-indicadores-sobre-uso-de-tic-por-menores-en-espa%C3%B1a-diciembre-2016

GARCÍA GARCÍA, Natalia: "¿Pueden los padres violar realmente la intimidad de los menores?" [en línea], *Sepín*, 2016, < https://blog.sepin.es/2016/09/intimidad-menores-control-parental/ > [consulta: 28 de octubre de 2017].

http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/protegetuprivacidad/index-ides-idphp.php

http://www.chaval.es

MARTÍNEZ, Evelio: "Qué es la Brecha Digital" [en línea], 2008 < http://www.labrechadigital.org/labrecha/qu-es-la-brecha-digital17.html > [consulta: 7 de octubre de 2017].

Memoria de la Fiscalía General del Estado de 2016 < https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/index.html > [consulta: 26 de octubre de 2017].

Memoria de la Fiscalía General del Estado de 2017 < https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/index.html > [consulta: 26 de octubre de 2017].

Oficina de Seguridad del Internauta "En Internet cuida tu privacidad" [en línea] < https://www.osi.es/es/tu-informacion-personal > [consulta: 30 de agosto de 2017].

PÉREZ PORTO, Juan y GARDEY Ana: "Definición de Whatsapp" [en línea], 2016 < https://definicion.de/whatsapp/ > [consulta: 3 de marzo de 2017].

Red. es. *Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad. Monográfico sexting. Disponible en http://www.chaval.es/chavales/sites/default/files/Monografico%20Sexting_Red.es.pdf*

Red. es. *Monográgico ciberacoso escolar (ciberbullying).* Disponible en *http://www.chaval.es/chavales/sites/default/files/Monografico%20Ciberbullying%20o%20ciberacoso%20escolar_Red.es.pdf*

Red.es: *Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad. Monográfico grooming*. Disponible en http://www.chaval.es/chavales/sites/default/files/Monografico%20Grooming_Red.es.pdf

www.ine.es

7.3. Jurisprudencia.

Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 referente al caso Google vs. AEPD.

Sentencia del Tribunal Supremo 311/13, de 8 de mayo referente a la protección del derecho a la propia imagen de los menores.

Sentencia del Tribunal Supremo 864/15, de 10 de diciembre de 2015 referente a la injerencia de una madre en los derechos de su hija menor de edad.

Sentencia de la Audiencia Provincial de Pontevedra 208/2015 de 4 de junio referente a la necesidad de consentimiento por parte de los dos progenitores para publicar en redes sociales fotos de los hijos menores.