CALIFICACIÓN: Notable 8.

OBSERVACIONES:

Se trata de un trabajo que tiene una enorme actualidad, y tiene el mérito de tener que analizar una realidad social muy cambiante, que va por delante del legislador, y que aún no tiene definidos sus perfiles normativos, doctrinales ni jurisprudenciales. Al mismo tiempo, trasciende las fronteras del ordenamiento estatal e implica necesariamente una visión global.

La autora hace una exposición adecuada del marco jurídico normativo, con referencia al Reglamento comunitario de inminente entrada en vigor, así como a las recomendaciones que realiza la Agencia Española de Protección de Datos. También hace un repaso en torno a los principales problemas que se plantean en nuestra sociedad en torno al uso de redes sociales y los menores, tanto en situaciones en los que son parte pasiva como activa.

Finalmente, tratándose de un trabajo jurídico propio de un Máster de Abogacía, también hace un esfuerzo final por aportar una visión personal razonablemente argumentada sobre el rol del abogado en este contexto.

TRABAJO DE FIN DE MÁSTER

Máster III de Abogacía | Convocatoria de junio

Protección de Datos: Especial incidencia en los menores y el uso de las redes sociales

Autora: Ana Cabrera Rodríguez

Tutor: Vicente Jesús Navarro Marchante. Profesor del área de Derecho Constitucional de la Universidad de La Laguna.

Lunes, 22 de enero de 2018.

"El reto técnico-jurídico es vigilar y ser proclives a medidas que garanticen los derechos de los usuarios. […] Analizada la situación actual, el futuro pasa por encontrar un buen equilibrio entre las funcionalidades de la Red y las garantías de los derechos individuales".

Agustín de Asís[1]

[1] Asís, A. (2010). *'Redes sociales y protección de datos. Redes Sociales e interpretación en Red: una perspectiva técnica-jurídica*', Santander, Universidad de Cantabria.

Introducción

La protección de datos constituye un derecho autónomo con aplicación en casi cualquier ámbito de la vida y de la sociedad. Y tal es su amplitud que intentar abarcar todo lo que este conlleva es prácticamente imposible para un solo estudio. Por ello, el objetivo del presente trabajo es sentar las bases de este derecho y su legislación aplicable, y profundizar algo más en la problemática que este supone para los menores de edad. Jóvenes de entre 13 y 18 años, a veces incluso menos, que prácticamente se han criado con las nuevas tecnologías, y que desde cortas edades aprenden a usar. Este acceso a recursos técnicos es útil cuando son usados como medios de aprendizaje, incluso de ocio, siempre que se haga de forma controlada y prudente. Es necesario poner de relevancia la vital importancia que tiene educar a los niños para un correcto uso de internet y las nuevas tecnologías para que aprovechen todas sus ventajas y eviten todos sus inconvenientes, pero el derecho también tiene cabida en el problema, por cuanto debe proporcionar los medios necesarios para su protección y todo lo pertinente para asegurar que las intromisiones en el derecho a la protección de datos no queden impunes.

Para ello, primero es importante hablar de los conceptos básicos que entrañan la protección de datos, los mismos se pueden localizar fácilmente en la legislación de la materia, que analizaremos a continuación. Para posteriormente centrarnos en los menores, en el uso que estos hacen de las tecnologías y de los problemas y los desafíos que ello implica para la protección de los mismos en el ámbito de internet.

Índice

1.- Antecedentes normativos en el ámbito de protección de datos.

La protección de datos como tal, es un derecho de relativamente nueva configuración, dado que ha obtenido más importancia con el cada vez mayor uso de medios tecnológicos y redes sociales, tanto en el ámbito personal como en el profesional. Aún así, podemos remontarnos a épocas pasadas donde vemos las primeras alusiones a esta protección en el derecho antiguo, con el secreto de confesión eclesiástico[2].

Este derecho, reconocido como fundamental en nuestro país[3], es eminentemente de construcción internacional, debiendo estudiar no sólo las normas españolas, sino las europeas, que sirvieron como base de las normas estatales que hoy tienen gran arraigo en nuestro país, y que siguen en constante evolución y cambio.

Así, nos encontramos con la primera referencia normativa clara de nuestra historia más reciente, como es la Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948, que recoge en su artículo 12, lo siguiente: <<*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*>>. Entendiendo este como un primer paso para la protección de los datos personales de los individuos, obviamente en esa época no existían medios tecnológicos por los que los datos personales y privados pudieran verse amenazados.

Es entonces cuando surge en el año 1968 la Resolución 509 del Consejo de Europa, sobre derechos humanos y los nuevos logros científicos y técnicos, en la que se analizan los medios técnicos descubiertos hasta el momento en relación con los riesgos generados para los derechos de las personas, cuya conclusión fue la necesidad de proteger la privacidad de las personas frente a las nuevas tecnologías.

Unos años más adelante, en el año 1973 y posteriormente en 1974, surge en Europa la idea de la realización de Bancos de Datos, como medida de protección ante el

[2] Impuesto en el IV Concilio de Letrán en el año 1215, y que aún hoy está protegido legalmente. Hernández López, J. M, El derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional, Aranzadi, 2013.

[3] Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre de 2000, véase en https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

creciente uso de las nuevas tecnologías, dictando en ese momento el Consejo de Europa recomendaciones a los estados miembros, por un lado para el establecimiento de bancos de datos en el sector privado[4] y posteriormente, para el establecimiento de los mismos en el sector público[5]. Autores como Concepción Conde[6] entienden que los principios en ellas contenidos, adaptados a la evolución tecnológica y social del momento, siguen teniendo plena actualidad y vigencia, estableciendo la autora como puntos fundamentales para esta protección contra abusos, entre otros, el derecho de información y acceso a los datos personales, la máxima seguridad para impedir su difusión no consentida, y que la conducta de las propias personas responsables de dichos datos debe ayudar en la prevención. Este último punto, recuerda al concepto actual de "responsabilidad activa" propuesta en las últimas reformas legislativas, de las cuales hablaremos más adelante, y que nos hace ver cuán aplicables son los principios básicos proclamados hace más de 40 años aun cuando la técnica avanza tan rápido.

Por otro lado, en España, la primera mención en la legislación la encontramos en la Constitución de 1978, en su artículo 18.4, que establece: *"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"*. Enclavado como una parte del derecho a la intimidad, este sirve de base para construir el derecho de protección de datos.

Volviendo a Europa, y siguiendo la línea temporal, en el año 1981, el Consejo de Europa aprueba el Convenio 108, el 28 de enero en Estrasburgo, ratificado por España el 31 de enero de 1984 y entrando en vigor al año siguiente. Un convenio que sigue vivo y actualizándose con los años. Fue ampliado en el año 2001 a través de un nuevo protocolo, y en la actualidad, está siendo revisado para su reforma. Es la primera norma a nivel europeo que establece los conceptos y las normas básicas para la protección de los datos personales, y que servirá como base para las legislaciones internas, en su

[4] Resolución 73 (22) de 26 de septiembre de 1973 del Consejo de Europa, respecto a "la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado".

[5] Resolución 73 (29) de 20 de septiembre de 1974 del Consejo de Europa, respecto a "la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público".

[6] Conde, Ortiz, C. (2006) *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Dykinson, ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/bull-ebooks/detail.action?docID=3170265

artículo 2, por ejemplo, podemos encontrar las definiciones que esta materia ha ido introduciendo en la sociedad y que ayudan a entender mejor el texto normativo, siendo útiles aún en la actualidad. Por otro lado, en su artículo 8 sobre las "*garantías complementarias para la persona concernida"*, se introducen los derechos de una persona a conocer, acceder, rectificar y eliminar sus datos de un fichero automatizado que le concierna, lo que en la Ley Orgánica Española de la que hablaremos a continuación se conoce como los derechos ARCO del usuario. Este Convenio serviría también como base para la creación de la Agencia Española de Protección de Datos –en adelante, la AEPD-, creada en 1992, como establece la información institucional en su página web[7].

En España, para responder a las necesidades surgidas por los nuevos medios técnicos y las normas europeas sobre la materia, surgió la Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), que desarrollaba el derecho del artículo 18.4 de la Constitución y al mismo tiempo, se cumplía con lo establecido en el Convenio 108 de Estrasburgo, en su artículo 4, sobre compromisos de las partes: "*Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo"*, entendiendo como "partes" a los estados firmantes del convenio.

Pocos años después de la aprobación de la LORTAD, surgiría en la Unión Europea la Directiva 95/46/CE, del Parlamento Europeo y del Consejo de la Unión Europea, de 24 de octubre de 1995. Cabe hacer un inciso para mencionar que en el Tratado de Funcionamiento de la Unión Europea, en su actual artículo 16 –de la Versión Consolidada del año 2010-, establece el derecho a proteger los datos personales bajo la siguiente redacción: "*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de*

[7] Historia de la AEPD: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/historia-ides-idphp.php

aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes". Así, respondiendo al apartado segundo del artículo 16, surge la Directiva, la cual va un paso más allá en la protección de datos personales, pues como se puede observar en sus considerandos, en la época estaba cobrando importancia no tanto la existencia de ficheros automatizados con datos personales, que ya venían estableciéndose, sino el flujo transfronterizo de dichos ficheros, derivado del establecimiento del mercado interior europeo y de una cada vez mayor globalización[8]. Así, esta Directiva trata de proteger dicho flujo, así como armonizar y coordinar las legislaciones de los estados parte para favorecer dicha circulación a la vez que se protege[9].

En España, tras la aprobación de la Directiva 95/46/CE, surgió una nueva *Ley Orgánica, la 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal* (LOPD), que adaptaba los cambios introducidos por esta norma europea, y que derogaba a la LORTAD en su totalidad. La LOPD, todavía vigente, ha sufrido varias modificaciones a lo largo de su historia.

Posteriormente, en el año 2008 se publica el *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*. Este serviría de complemento a una norma que llevaba ciertos años en funcionamiento.

Llegaríamos así a la última norma dictada en el ámbito europeo, el nuevo Reglamento General de Protección de Datos -del cual hablaremos extensamente en el siguiente punto.

Sin embargo a lo anterior, debemos hacer mención tanto a las recomendaciones y resoluciones dadas por el Consejo Europeo, así como las directivas y decisiones de la Unión Europea, dictados todos ellos en esta materia para regular sectores específicos como el transporte de pasajeros, empleo, telecomunicaciones, centros educativos, firma electrónica, entre otros. Además de la jurisprudencia del Tribunal de Justicia de la unión Europea, cuyas resoluciones son vinculantes para todos los estados parte. Todos ellos pueden ser consultados en la Página Web de la Agencia General de Protección de Datos.

[8] Considerando Quinto, Directiva 95/46/CE.

[9] Considerando Octavo, Directiva 95/46/CE.

Además de los documentos dictados en ámbito internacional, en España encontramos gran cantidad de leyes que contienen preceptos en la materia dentro de ámbitos específicos –como sanidad, seguro, tributaria, etcétera-, así como normas autonómicas –de las Comunidades de Andalucía, Cataluña y País Vasco[10]-, y por supuesto, las resoluciones e instrucciones de la Agencia Española de Protección de Datos, que son normas de carácter reglamentario, así como la jurisprudencia de los juzgados y tribunales del Estado.

2.- Nueva regulación europea: el Reglamento General de Protección de Datos.

Tras establecer el marco normativo aplicable hasta la fecha, es el momento de hablar del nuevo *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* –en adelante, el Reglamento General.

Como su título indica, es la norma que sucederá a la Directiva 96/46/CE. Publicado el 25 de mayo de 2016, da un plazo de *vacatio legis* de dos años, entrando plenamente en vigor a partir del próximo 25 de mayo de 2018, como se establece en su artículo 99. Llama la atención este inciso, dado que el carácter que se atribuye a los reglamentos europeos en el Tratado de Funcionamiento de la Unión Europea, en su artículo 288, segundo párrafo, es el de *"directamente aplicable en cada Estado miembro"*, sin necesidad de un período de transición o de adaptación de las legislaciones nacionales para su entrada en vigor, lo que sí ocurre con las directivas europeas. Sin embargo a lo anterior, el propio reglamento en el último inciso de su artículo 99: "*El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro*", por lo cual, llegada la fecha de entrada en vigor, si las legislaciones nacionales no han introducido los preceptos contenidos en el reglamento, éste será directamente aplicable.

[10] En nuestro país, se crearon 3 agencias de protección de datos adicionales a la estatal. Actualmente dos de ellas siguen en funcionamiento: la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos, que se encargan de controlar los ficheros de datos creados o gestionados en sus respectivas comunidades y en la Administración Local de su ámbito territorial.

La razón que da la propia AEPD es que ese período de dos años se dispuso para la acomodación de las instituciones públicas tanto estatales como europeas, así como las organizaciones privadas que tratan datos a las nuevas normas contenidas en el reglamento, así como la adopción de normas para permitir o facilitar su aplicación[11].

Lo primero que hay que reseñar, es que en su artículo 4, se establecen los conceptos básicos a tratar en la materia de protección de datos, y que nos ayudarán a tener una mejor comprensión de los preceptos del Reglamento General.

Entre las novedades más importantes que esta ley ofrece, encontramos en primer lugar, la ampliación del ámbito de aplicación territorial de las normas en él contenidas, por cuanto son de aplicación a aquellas empresas que aun cuando no están establecidas físicamente en ningún país de la Unión Europea –en adelante, UE-, tengan acceso y traten ficheros de datos de ciudadanos de la unión. Así lo establece el artículo 3 del Reglamento General, y supone una novedad dado que implica mayores garantías.

Por otro lado, encontramos la regulación del derecho al olvido, que si bien ya estaba reconocido[12], no se recogía en ninguna norma estatal o comunitaria. Este derecho supone que cualquier ciudadano de la unión está facultado para solicitar la eliminación de aquellos datos que le conciernen cuando estos no cumplen los requisitos legales para estar publicados. Según la AEPD *"incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o no tiene relevancia ni interés público, aunque la publicación original sea legítima"*[13].

Además de lo anterior, introduce el concepto de "responsabilidad activa" en el ordenamiento europeo, tomando ésta como la prevención que las empresas y organizaciones que tratan datos personales tendrán que llevar a cabo a partir de la entrada en vigor de la norma. Siendo una obligación que implica establecer un sistema por el cual se cumplan o se intente razonablemente cumplir con los principios básicos y

[11] Gabinete de Prensa de la AGPD, "El Reglamento Europeo de protección de datos en 12 preguntas", nota de prensa, 2016 http://www.agpd.es/portalwebAGPD/gabinete_prensa/notas_prensa/notas_prensa_indice_2016/index-ides-idphp.php

[12] Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014.

[13] "5 puntos clave para ejercer el "derecho al olvido", Página Web Agencia Española de Protección de Datos http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php

normas del Reglamento. Así lo describe la Agencia de Protección de Datos en su página web.

Por último, en cuanto a la obtención del consentimiento del usuario por parte del responsable del tratamiento, ya los considerandos del Reglamento General establecen los principios a seguir para dar y tomar el consentimiento en cuanto a protección de datos. Así, encontramos el considerando 32, en el que expresa qué forma debe revestir el consentimiento del interesado, pudiendo ser por escrito o verbal, y qué se entiende como declaración por escrito, llegando a permitir que sea marcar una casilla. Estableciendo de igual forma lo que no se considera una opción válida para otorgar el consentimiento: la inacción, el silencio o, que por ejemplo, la casilla de aceptación esté ya marcada. Por otro lado, el Considerando 42 del Reglamento General establece que *"debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace"*, atribuyendo la tarea al responsable de demostrar que el interesado ha dado su consentimiento y las garantías de las que ha gozado. De esta forma establece los requisitos para darlo, a través de un modelo de declaración *"con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo"*, requisitos que ya proponía la Directiva 93/13/CEE del Consejo[14] en materia de cláusulas abusivas, y que el ámbito de la protección de datos ha hecho suyo. Se introduce el concepto de conocimiento informado, proponiendo que para que se considere de esta forma, "*el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales"*, lo que da mayores garantías al usuario. De la misma forma, en su considerando 43, el legislativo europeo fija que para que el consentimiento se entienda libre, debe permitir autorizar por separado las distintas operaciones de tratamiento de datos, no valiendo con un solo momento de aceptación para realizar cuantas operaciones se quiera con dichos datos.

Estas son las novedades fundamentales que introduce el Reglamento General, a cuya entrada en vigor deberemos estar bien atentos por cuanto se pondrán a prueba estas nuevas normas y su efectividad.

[14] Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. «DOCE» núm. 95, de 21 de abril de 1993, páginas 29 a 34.

3.- Regulación específica para los menores.

Tras un análisis general de la legislación, tanto sus antecedentes como la actual, cabe analizar específicamente la protección que se da a los datos de los menores de edad, tanto en el ámbito internacional como en el estatal.

3.1.- Estados Unidos: Children's online privacy (COPPA)

Los Estados Unidos de América en el año 1998 fue el primer país en dictar una norma dedicada a la protección de los datos personales de los menores[15], siendo el modelo a seguir por parte de la legislación europea como veremos más adelante. Fue propuesta por *Federal Trade Comission* (Comisión Federal de Comercio, FTC). Tras la misma, se dictaron a su vez normas de desarrollo aprobadas al año siguiente, entrando en vigor en el año 2000,

La ley se enfoca en la protección de los menores de 13 años frente al tratamiento que llevan a cabo operadores de sitios web dirigidos directamente a menores o dirigidos a un público en general pero tenga "conocimiento efectivo"[16] de que tratan datos de menores.

La norma y su desarrollo se basan en unos principios generales, que la profesora Mª Belén Andreu sintetiza en los siguientes:

1º.- Dar publicidad de las políticas o aviso de privacidad sobre el tratamiento de los menores, debiendo estar estas redactadas de forma clara y visibles tanto en la página principal como en cualquiera que se recaben datos.

2º.- Informar y obtener consentimiento paterno o de los representantes legales previo al tratamiento. Es curioso este punto porque establece aquí una obligación para los operadores de realizar "esfuerzos razonables" de comprobación de este permiso "teniendo en cuenta la tecnología disponible", redacción que coincide íntegramente con la usada en la reciente normativa europea de protección de datos, de la que hablaremos en el siguiente subapartado. En cuanto a esta obligación la propia ley propone

[15] Andreu Martínez, Mª B., 2013, *La protección de datos personales de los menores de edad*, Thomson Reuters, Aranzadi.

[16] Entendiendo que este conocimiento efectivo se da desde el momento en que el operador recaba alguna información que o bien determine claramente la edad –como la fecha de nacimiento-, o bien permita conocerla –como los estudios que cursa. Para profundizar más sobre los conceptos se recomienda acudir a la obra de Mª Belén Andreu Martínez, mencionada en la refer. núm 14.

mecanismos por los que los operadores pueden hacerla efectiva, existiendo una clasificación en función de la dificultad de los mecanismos en función del tipo de tratamiento que la página o sitio web haga de los datos de los menores. Si es un uso interno, pueden hacer uso de mecanismos más sencillos, mientras que si esos datos serán comunicados a terceros o incluso publicados, deberán llevar a cabo mecanismos más exigentes y con mayores garantías. Ejemplos de estos mecanismos los veremos más adelante en el presente trabajo.

3º.- Se reconocen los derechos mejor conocidos en España como derechos ARCO, a los progenitores y representantes legales en relación a los datos de los menores;

4º.- Prohibido condicionar la participación de un menor en un juego o actividad a la obtención de más datos de los necesarios para formar parte de los mismos;

5º.- y por último, la adopción de mecanismos de protección de la confidencialidad, seguridad e integridad de los datos.

Estos principios establecen la base respecto de la cual se construirá la protección efectiva de los menores en internet, imponiendo claras obligaciones a los operadores, que en la actualidad conocemos con el concepto más concreto de responsables de tratamiento.

Posteriormente se han realizado revisiones de esta norma y dictado modificaciones, además de nuevos textos, entre ellos guías de conducta en publicidad, y códigos de conducta para empresas encargadas del tratamiento de datos de menores, aunque a efectos del presente trabajo, no interesa entrar a estudiarlas todas[17], la que sí nos interesa es la modificación realizada en el año 2013[18], que actualizó las normas del año ’98 y ’99 para implementar los conceptos que los cambios tecnológicos y más

[17] Para información más en profundidad sobre esta ley o normativa posterior acudir directamente a la norma mediante la página web de la “Federal Trade Comission” https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule; otros recursos de la propia FTC, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy ; o bien a la obra de la Profesora María Belén Andreu Martínez, *“La protección de los menores de edad”*, referenciada anteriormente.

[18]Children's Online Privacy Protection Rule: Final Rule Amendments To Clarify the Scope of the Rule and Strengthen Its Protections For Children's Personal Information https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf

específicamente el desarrollo de las redes sociales, habían introducido en la materia. Así, por ejemplo, se añadió al concepto de dato personal protegido, los nombres de usuario usados por los menores en estas redes, así otros datos que permitieran identificar el nombre, dirección o datos de contacto directo con el menor, como puedan ser la geolocalización, fotografías, vídeos o audios en los que participe el menor, siendo estos reconocidos por sí mismos como datos personales.

Esta modificación añade también nuevos mecanismos para comprobar el consentimiento parental, aplicando los nuevos avances para facilitar el otorgamiento y reforzar la protección. En cuanto a esto, la FTC propone un procedimiento para que se presenten nuevos métodos de comprobación para ser aprobados por este organismo e incluidos en el catálogo de los ya existentes.

3.2.- Normas comunitarias

3.2.1.- Los grupos de trabajo

En las principales normas europeas sobre protección de datos analizadas en los apartados anteriores, no existen preceptos dirigidos a la protección de los menores, hasta la llegada del nuevo Reglamento General, aplicable a partir de este año, en el que por fin se menciona a los menores como usuarios diferenciados del resto, necesitados de una protección especial, y añadiendo normas específicas como veremos más adelante.

No obstante a lo anterior, sí que han existido estudios por parte de los Estados miembros y sus autoridades de control para poner de relieve la importancia de protección de los menores y protegerlos frente a las nuevas tecnologías. Se crean así los "*grupos de trabajo"*. La página web de la Agencia Española de Protección de Datos nos habla de tres: el WP29, grupo europeo de trabajo del artículo 29; el IWGDPT, grupo de Telecomunicaciones de Berlín; y el WPISP, grupo de trabajo para la seguridad de la información y la privacidad de la OCDE.

Nos centraremos en el trabajo desarrollado por el primero de ellos[19], creado por la Directiva 95/46/CE, se integra por las Autoridades de Protección de Datos de todos los estados miembros, un Supervisor Europeo de PD y la Comisión Europea. Todas sus

[19] Para más información sobre los grupos de trabajo, se recomienda la base de datos de la AEPD: http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/index-ides-idphp.php

recomendaciones y dictámenes los podemos encontrar en la página de la Comisión Europea[20], teniendo mayor importancia a efectos del presente trabajo, el Dictamen 2/2009, de 11 de febrero, sobre la protección de datos personales de los niños[21] y el Dictamen 5/2009, de 12 de junio, sobre las redes sociales[22], aunque este último lo analizaremos más adelante cuando abordemos el tema específico de las redes sociales.

Introduciéndonos pues en el Dictamen 2/2009, y como es de esperar, el principio general por el que se rige es el interés superior del menor[23], estableciendo en su propia introducción en el apartado 1º con el título de *framing* o marco normativo, que el fin del documento es consolidar la protección de datos de forma estructurada, definiendo los principios fundamentales aplicables e ilustrándolos con el ejemplo de la protección de datos personales en el ámbito de los centros escolares[24].

Este documento establece que la protección de los menores, pasa por aplicar las normas generales de protección de datos, teniendo en cuenta las normas especiales sobre menores del resto de normativa y el interés superior del menor como fin último. Y que es tarea tanto de la familia, como de los centros educadores, así como de la sociedad y el Estado, como coordinador de los recursos y autoridad de control del cumplimiento de esos principios y derechos.

Así mismo, en cuanto a la representación que ostentan progenitores y representantes legales, expresa que la misma no debe ser entendida con absoluta prioridad sobre el niño, debiendo esta reflejar en todo momento lo mejor para el menor. Eso implica que no se puede consentir el tratamiento de datos en cualquier

[20]Comisión Europea, Documentación del Grupo del Artículo 29: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec15

[21] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf

[22]Opinion 5/2009 on online social networking: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

[23] Apartado II, A, 1º sobre Principios Fundamentales Generales del Dictamen 2/2009.

[24] Este dictamen entiende en el apartado I que el ámbito escolar es el más relevante en cuanto a la protección de los menores puesto que es una de las partes más importantes de la vida de los menores, y pasan allí una significativa porción de sus días. Por lo tanto, los encargados de tratar sus datos desde su inscripción son los centros escolares, incluyendo en este concepto a los profesores y autoridades escolares.

circunstancia, por más que se otorgue legalmente, sobre todo cuando puede ser lesivo para el interés del menor. Debiendo incluso consultar con el menor, cuando se entienda que tiene edad suficiente para razonar y elegir lo mejor para él mismo.

En general, esta recomendación trata de establecer las bases para ordenar la protección de datos de los menores teniendo en cuenta siempre su interés, y voluntad, dentro de las capacidades que la edad y la madurez le otorguen en cada caso. Encomendando su protección a todo el que esté directamente involucrado en su educación y crecimiento, y por supuesto al Estado para que garantice esa protección.

3.2.2.- Reglamento General de Protección de Datos: Consideraciones iniciales y cuestión de la edad de consentimiento.

En cuanto a la regulación del Reglamento General, encontramos en el Considerando 38 una reflexión sobre la necesidad de protección de los menores de forma específica, dado que *<<pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales",* convirtiéndoles en sujetos especialmente vulnerables, como ya venía reconociendo el legislativo. Además, especifica en qué debe aplicarse dicha protección, entendiendo que *"la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño"* son los procesos en los que se requiere para los menores una defensa superior. Por otro lado, el Considerando 58 que habla sobre el principio de transparencia en cuanto a la información que los responsables dirigen a los interesados, dedica su último párrafo a hablar de los menores añadiendo que si esa información va dirigida directamente a ellos, "*debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender"*.

Pero sin duda, la cuestión más importante en cuanto a los menores introducida por el Reglamento General, es la regulada en el artículo 8 sobre las condiciones del consentimiento otorgado por el niño. Para que el consentimiento de un menor sea válido debe tener los 16 años de edad, y si no es así, debe ser otorgado o autorizado por quien asuma la patria potestad o tutela del menor, para que el consentimiento sea lícito. En cuanto a la edad de consentimiento, el Reglamento permite que cada país establezca en sus normas internas una edad inferior hasta el límite máximo de los 13 años. En España,

actualmente, a falta de una reforma legal que adapte la LOPD al nuevo Reglamento General, ese límite está en los 14 años. Ahora bien, en el *Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal*[25], en su artículo 7 se determina la edad para otorgar el consentimiento en 13 años, el límite máximo que permite el Reglamento Europeo.

Además de lo anterior, el artículo 8 impone al responsable del tratamiento el cometido de verificar que el consentimiento está otorgado legalmente, y que haga "esfuerzos razonables" para asegurarse de ellos "teniendo en cuenta la tecnología disponible", como veíamos en el apartado anterior, esta configuración se basa en la norma estadounidense COPPA, que ya se venía aplicando casi 20 años atrás. Estos últimos conceptos llaman la atención por ser totalmente indeterminados, sin que el Reglamento añada ningún mecanismo por el cual deba hacerse efectiva dicha obligación, como sí hiciera la norma COPPA en su momento, quien proponía como opciones, por ejemplo, el enviar un e-mail a los progenitores solicitando el consentimiento, o realizar una llamada telefónica al teléfono personal del progenitor mediante grabación o locución automática, ampliándose esta con la posibilidad de realizar una videoconferencia con las modificaciones de la norma de 2013; hasta llegar a mayor nivel de seguridad como enviar el formulario de consentimiento por correo ordinario o fax, añadiéndose en el año 2013 el envío del documento escaneado; utilización de una tarjeta de crédito, y a partir del 2013, documentos de identidad, o mediante llamada del progenitor para ser atendido por personal para que verifiquen su identidad. Queda claro que algunas de ellas, en específico esta última, conlleva un esfuerzo quizás desmesurado para los operadores, como el tener contratado personal para atender llamadas de los progenitores, aunque sería bastante efectivo. Pese a ello, lo cierto es que ninguno de estos está previsto en la norma europea, por lo que habrá que esperar a la entrada en vigor del reglamento para observar de cerca qué mecanismos proponen las empresas responsables del tratamiento.

[25] Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Boletín Oficial de las Cortes Generales de 24 de noviembre de 2017. http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF

3.2.3.- Otras normas establecidas en el Reglamento General aplicables a menores.

De otro lado, el artículo 40 posibilita la realización de códigos de conducta dirigidos directamente a la protección de los menores que pueden recoger y ordenar *"la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño".* Habrá que esperar a la entrada en vigor del Reglamento para ver si efectivamente las organizaciones encargas los elaboran. También impone una función a las autoridades de control, como es en España la Agencia, dentro de la función general de promover la sensibilización del público, en su artículo 57.1.b), indica que las actividades dirigidas a los menores deberán ser objeto de especial atención.

3.3.- Normas españolas y otros recursos educativos para los menores.

3.3.1.- Normativa nacional aplicable a la protección de datos de menores: la edad mínima de consentimiento.

Al igual que en Europa, en España no existe una norma específica para la protección de datos de menores. Pero sí son de aplicación los principios generales de protección vistos con anterioridad.

La primera norma fundamental cuando se trata de la protección del menor, en cualquier ámbito, es la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, que sienta las bases de la protección del menor. Dedica su artículo 4 a la protección del derecho a la propia imagen frente a intromisiones ilegítimas en su intimidad, ya sea difundiendo información o utilizando imágenes, fijando en su apartado tercero los límites del concepto de "intromisión ilegítima", definiéndolo como "*cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales*"[26]. Esto implica que incluso en los casos en que exista consentimiento del menor o de sus representantes, si la publicación va en contra de su propia imagen, podría ser ilícita.

[26] Artículo 4.3 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

En cuanto al ámbito de la protección de datos, el aspecto de mayor relevancia, y la que mayor jurisprudencia atesora, es la cuestión de la edad mínima de consentimiento, que como analizamos en el apartado anterior, actualmente se fija en 14 años. El límite está fijado en el artículo 13 del Reglamento que desarrolla la LOPD –en adelante, el RLOPD-, y que según la AEPD, es así en interpretación del artículo 162.1º del Código Civil, cuando exceptúa la representación de los progenitores o tutores para *"los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo"*, como aplicable al acto de dar su consentimiento al tratamiento de sus datos personales en internet.

Este mismo artículo 13 del RLOPD excluye la posibilidad de recabar del menor, cualquiera que sea su edad, datos sobre sus progenitores, siempre que no se trate de comunicarse con ellos a efectos de la autorización de tratamiento de datos del hijo. Y en su último apartado, menciona ya la obligación del responsable del fichero o del tratamiento a garantizar la comprobación de la edad y del consentimiento paterno, aunque no establece los mecanismos para llevarlo a cabo ni métodos de control de cumplimiento sobre estos responsables.

Cuando se dictó el Reglamento, surgió una controversia alrededor de este artículo, por entenderse que constituía una obligación nueva al margen de la LOPD y de la Directiva 95/46/CE, infringiendo así estas normas, y que dicha obligación era "*de difícil o imposible cumplimiento y desproporcionada*" [27]. Sobre el tema se pronunció el Tribunal Supremo en su Sentencias de 15 de julio de 2010[28], en cuyo Fundamento Octavo establece que ni la LOPD ni la Directica 95/46/CE "*contienen una regulación específica del consentimiento de los menores, habilitando así el desarrollo reglamentario que en nada infringe, ni siquiera se sostiene, las previsiones de las indicadas normas*", dando así plena validez a los preceptos del artículo 13 y a las normas contenidas.

Así mismo existen Informes realizados por la AEPD a lo largo de los años, destacando a este respecto el Informe 466/2004[29], en el que la Agencia establece límites

[27] Andreu Martínez, Mª B., 2013, *La protección de datos personales de los menores de edad*, Thomson Reuters, Aranzadi.

[28] STS 4050/2010 de 15 de julio de 2010

[29] Informe 466/2004 del a AEPD sobre: *La comunicación a los padres de las calificaciones de sus hijos*

a la edad de consentimiento para casos en los que el tratamiento de los datos lleve aparejada algún tipo de disposición patrimonial por parte del menor, siendo entonces que pese a que el menor de edad posea la plena capacidad para consentir el tratamiento de sus datos, carece de la suficiente capacidad para contratar, puesto que el artículo 1263 de nuestro Código Civil no lo permite para menores no emancipados. Por lo tanto, para que un menor pueda consentir por sí mismo el tratamiento de sus datos en casos de contratación debe estar emancipado. De no ser así, se precisa el consentimiento de sus progenitores o representantes legales.

En la jurisprudencia, al igual que en las resoluciones de la AEPD toma relevancia esta materia, por cuanto podemos encontrar gran cantidad de sentencias sobre la falta de consentimiento o bien del menor, o bien de los progenitores o representantes legales, sobre todo en el ámbito de la educación, de la publicidad y de la contratación ejercida por un menor. En referencia a este último ámbito, encontramos por ejemplo la Resolución de 22 de noviembre de 2008 de la AEPD[30], que resuelve condenar a una empresa de telefonía por no cumplir con los requisitos de consentimiento establecidos en la LOPD en sus artículos 4.3 y 6, por no comprobar de forma fehaciente que estaba contratando un servicio con una menor de 14 años. La compañía no sólo no comprobó si los progenitores o tutores de la menor daban su consentimiento por ningún cauce, sino que ni si quiera verificaron si el usuario contratante era o no mayor de edad, pues sólo se le solicitó su DNI, según testimonio de la menor. Dado que pese a existir una grabación de la llamada, la empresa no la presentó en el procedimiento, no se pudo comprobar si efectivamente se había hecho la constatación, y por lo tanto se condenó a la empresa por falta de calidad del dato, por no asumir su debida diligencia para tratar los datos de un menor. Más aún cuando es una empresa cuya actividad principal pasa por tratar gran cantidad de datos de los usuarios, debiendo tener un especial cuidado con las normas de tratamiento[31].

---

menores de edad, en *Compendio LOPD par centros educativos*, Informes jurídicos, tutelas de derechos y preguntas más frecuentes, Gesdatos Software, S.L:
http://www.gesdatos.com/descargas/Compendio_LOPD_para_Centros_Educativos.pdf

[30] Resolución 1359/2008 AEPD de 22 de noviembre de 2008. Procedimiento Nº PS/00330/2008.

[31] Mencionando aquí las Sentencias de la Audiencia Nacional, Recursos 104/2006 y 143/2006, que tratan sobre la especial consideración de las empresas cuya actividad está relacionada con la protección de datos y la ponderación de la condena.

En el mismo sentido, encontramos la Resolución 1663/2010[32] que resuelve un procedimiento contra una Página Web orientada a jóvenes y adolescentes que no comprobaba de forma suficiente que los usuarios con un perfil en su web fueran mayores de 14 años, ya que sólo solicitaba la fecha de nacimiento; eso sumado a que era una plataforma de libre acceso a la que también podían suscribirse adultos, y la información con la que trabajaban se consideraba sensible, decidió condenar a la infractora.

3.3.2.- Otros recursos habilitados para la educación y prevención en protección de datos.

Además de la legislación y recursos normativos, podemos encontrar en la página web de la AEPD recursos para la educación de los niños, sus progenitores y personas de su entorno que tienen incidencia en sus datos personales como demás familiares, educadores, centros escolares, etc.

Bajo el nombre de "Tú decides en internet", podemos encontrar en este apartado contenidos audiovisuales así como guías para la utilización segura del internet por parte de los niños, e incluso, números de contacto para que pongan en conocimiento de la Agencia los problemas que puedan experimentar en internet.

En cuanto a los recursos para educadores, existe la Guía para centros educativos[33]. Los niños pasan en estos centros gran parte de su tiempo, y desde el momento en que se les matricula en ellos, ya comparten datos. Es tras sus muros donde harán los primeros amigos, aprenderán todas las materias, y se relacionarán con distintas personas. La protección comienza con los propios centros, ya que estos, como instituciones, deben tener muy presente la protección de datos, tanto de los datos que procesan de los alumnos, sus progenitores, profesores y demás trabajadores, como en su deber de que tanto el personal como los niños en su horario escolar, cumplan con las exigencias de esta protección. A modo de resumen, cabe decir que esta guía se encarga de explicar los principales conceptos en la materia, los métodos a seguir para la recogida, publicación y comunicación de los datos de los alumnos, así como el

[32] Resolución 1663/2010 AEPD, de 30 de julio de 2010. Procedimiento Nº 23/2010.

[33] Guía para Centros Educativos de la Agencia Española de Protección de Datos (AEPD).- http://www.tudecideseninternet.es/agpd1/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf

tratamiento de las imágenes de los alumnos, que constituyen una parte fundamental de la protección en la actualidad, por cuanto el uso de estas para promoción y difusión de las actividades realizadas por el centro en perfiles y páginas creadas en redes sociales es un reclamo en los últimos años para sobresalir con respecto de ofertas educativas de otros centros, pues parece que ya no sólo se busca la excelencia en la enseñanza, sino demostrar ser un centro dinámico y familiarizado con los medios técnicos y sociales del momento. Este último punto se desarrollará algo más en el siguiente punto del presente trabajo, por la problemática que presenta.

Además, encontramos dos guías específicas para educadores y familiares[34], que pone de relevancia todos los problemas a los que un menor se puede enfrentar en internet, y cómo prevenirlas. Explica una a una las conductas delictivas que pueden darse y métodos para combatirlas. De este punto también hablaremos más extensamente más adelante.

Por último, las guías para los protagonistas de este ámbito, los jóvenes[35]. Intentan que el menor analice el uso que le da a las redes sociales y los datos que comparte, y qué podría estar haciendo mal. Posteriormente explican las conductas delictivas de internet, cuándo se incurre en ellas, y cuándo podrían estar usándolas contra él/ella.

En general podemos ver que enseñamos a los niños a proteger sus datos personales, a no compartir contenido que pueda dar demasiada información al público general de internet, y con qué se puede encontrar. Sin embargo, es imposible no hacerse una pregunta básica, ¿nuestro ordenamiento protege suficientemente a los niños en internet frente a las conductas delictivas?, y de otro lado, ¿enseñamos a los niños a hacer un uso correcto de estas tecnologías?. Está claro que el primer paso para una protección completa es la educación, y en ello, poco puede hacer el derecho, pues está

[34] Guía para formadores y familiares de la AEPD.- http://www.tudecideseninternet.es/agpd1/images/guias/Guia_formadores2016.pdf y Guía para profesores y padres de la AEPD.- http://www.tudecideseninternet.es/agpd1/images/guias/guia-formadores.compressed.pdf

[35] Guía para jóvenes de la Agencia Española de Protección de Datos: "Sé legal en internet".- http://www.tudecideseninternet.es/agpd1/jovenes/guias/se-legal-en-internet.html#ficha-4-ciberbullying y Guía para jóvenes de la Agencia Española de Protección de Datos: "No te enredes en internet".- http://www.tudecideseninternet.es/agpd1/jovenes/guias/no-te-enredes-en-internet.html

en manos de las instituciones, centros educativos y, más importante, de los progenitores. Pero, ¿qué pasa cuando la sociedad falla en ese punto?, cuando una persona usa los datos de un menor sin consentimiento, ¿hay consecuencias?; y si un menor hace uso de internet y de sus redes sociales para entrometerse en el derecho de protección de otro menor, ¿qué consecuencias se prevén? Estas son las preguntas que intentaremos responder en el siguiente apartado.

4.- Menores y el uso de las redes sociales, consecuencias de la intromisión en los datos personales ajenos.

El uso de aparatos electrónicos tales como ordenadores personales, ordenadores portátiles, "*tablets*" y "*smartphones*", sobre todo estos últimos que pueden llevarse consigo a cualquier parte, ha crecido, y con ello, la proliferación de medios para conectar con otras personas, en su mayoría, redes sociales.

El término red social, se puede entender según el profesor Félix Requena[36] como "*un conjunto de puntos (actores sociales) vinculados por una serie de relaciones que cumplen determinadas propiedades. Las redes sociales gozan de una estructura y una morfología propias, cuyas cualidades, como la posibilidad de cuantificar las relaciones y su consiguiente tratamiento matemático, evidencian importantes aplicaciones para el análisis e interpretación de las conductas sociales*". Pese a ser un concepto establecido años atrás, encaja perfectamente con lo que seguimos entendiendo por red social, y es que no son más que medios por los cuáles distintas personas crean vínculos. Una definición más actualizada es la que da el Grupo de Trabajo del Artículo 29 en su Dictamen 5/2009[37], en su apartado 2, cuando la define como plataforma online de comunicación que posibilita a individuos a unirse a una red predeterminada o crear nuevas redes de usuarios con mismos o parecidos intereses a los propios. Añadiendo una serie de notas características que toda red social deben compartir entre sí: la invitación a los usuarios a compartir datos personales para la creación de un perfil;

[36]Requena, Félix. (1989). «El concepto de red social» Reis, vol 48, pp. 137-152 http://www.reis.cis.es/REIS/PDF/REIS_048_08.pdf

[37]*Opinion 5/2009 on online social networking*, de 12 de junio de 2009, del Grupo de Trabajo del Artículo 29: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

proveer herramientas que permitan a los usuarios compartir contenido como textos, música, fotografías o vídeos; y herramientas para obtener una lista de contactos para cada usuario con los que puede interactuar.

En estas redes sociales confluye un gran número de personas, mejor denominadas, usuarios. Para tomar conciencia de la dimensión que tenemos entre manos, el número de usuarios de las redes más destacadas es el siguientes: Facebook cuenta con 1,71 mil millones de usuarios[38], Whatsapp con 1,2 mil millones[39], Instagram con 400 millones[40] y Twitter con 320 millores[41]; cantidades bastante abrumadoras, sobre todo si tenemos en cuenta que cualquiera de estos usuarios puede tener acceso a una mínima parte de nuestros datos, dependiendo de las opciones de seguridad que tengamos establecidas en nuestros perfiles.

En cuanto a los menores, la tendencia de los últimos años es que tengan acceso a estos dispositivos electrónicos a cortas edades, muchas veces antes de los 14 años, y dada la facilidad para crearse un perfil en una red social, también tienen acceso a las mismas. Así los reflejan las estadísticas. Según el Instituto Nacional de Estadística (INE)[42], la edad media en la que los menores comienzan a tener contacto con internet con menos de los 10 años. Además, en la "Encuesta sobre hábitos de uso y seguridad de internet de menores y jóvenes en España" realizada por el Ministerio del Interior se establece que "el 19% de los menores de 11 años tiene creado un perfil en una red social, cuando la edad mínima permitida de acceso son los 14 años"[43]

---

[38]Tynan, D. (2016). *"Facebook's journey 'only 1% done' after surge in revenue, Zuckerberg says".* The Guardian: https://www.theguardian.com/technology/2016/jul/27/facebook-ad-sales-growth-quarterly-results

[39]Niu, E., 2017, "*Facebook's WhatsApp Now Has 1.2 Billion Users. Time to Start Monetizing?", Nasdaq:* http://www.nasdaq.com/article/facebooks-whatsapp-now-has-12-billion-users-time-to-start-monetizing-cm746480

[40]Blog de Instagram (2015) "Celebrating a Community of 400 Million": http://blog.instagram.com/post/129662501137/150922-400million

[41]Smith, K., 2016, *96 estadísticas y datos increíbles de las redes sociales para 201*6, Brandwatch: https://www.brandwatch.com/es/2016/08/96-estadisticas-redes-sociales-2016/

[42] La encuesta sobre equipamiento y uso de las tecnologías de la información en los hogares (TIC-H) http://www.ine.es/prensa/tich_prensa.htm

[43] R. Sanmartín, O., 2015, *El "ciberacoso" comienza a los 10 años,* El Mundo, versión digital. http://www.elmundo.es/espana/2015/10/14/561d590be2704e3a7e8b45fb.html

En palabras de la profesora Ana Aba Catoira[44], *"las generaciones más jóvenes utilizan, casi de forma exclusiva, estos nuevos cauces para informarse, comunicarse, divertirse, e incluso para actividades más nocivas o perjudiciales para su correcto desarrollo"*. Esto conlleva que los niños están compartiendo datos personales bien dando su nombre u otras circunstancias, bien compartiendo contenido como fotografías o imágenes en vídeo suyas, de sus familiares y amigos[45], con un número indeterminado de personas, que no siempre son conocidos de forma personal por lo niños, como dicen las profesoras Eva Espinar y María José González: *Para muchos usuarios, tener una agenda repleta de agregados implica que se multiplican las posibilidades de entablar contactos*[46], y más para los jóvenes, para los que el número de seguidores y de "me gusta" son algo primordial.

Esto crea una serie de desafíos para nuestra sociedad. De un lado, la protección del propio menor y sus datos frente a otros usuarios; y de otro, el control y educación de los menores para que no incurran en conductas que vayan en contra de los datos personales de otros usuarios.

4.1.- El menor como sujeto pasivo de la protección de datos

Como es de esperar, la protección de datos va orientada a proteger los intereses y derechos de los menores en el ámbito de internet. Y el principio general por el que las políticas de protección se deben guiar, al igual que todo ámbito que involucre a menores, es el interés superior del menor, un derecho que "*supone y exige que todas las decisiones y acciones que sean adoptadas de cara a los menores han de ser interpretadas y ejecutadas poniendo en primer lugar el interés del menor*" [47],

[44] Aba Catoira, A., 2011, *La protección de los derechos de los menores ante las nuevas tecnologías. Internet y las redes sociales*, en Cotino Hueso, L, "Libertades de expresión einformación en Internet y las redes socuales: ejercicio, amenazas y garantías, PUV (publciaciones de la Universidad de Valencia), Valencia, pp 486-511.

[45] Pues se entiende que entran dentro de la definición de dato personal fijada en el artículo 3.A de la LOPD.

[46]Espinar Ruiz, E. y González Río, M.J., 2009, *Jóvenes en las redes sociales virtuales. Un análisis exploratorio de las diferencias de género*, Revista Feminismo/s, nº º4, pp. 87-106.

[47] Dávara Fernández de Marcos, L., 2017, *Menores en internet y redes sociales: Derecho aplicable y deberes de los padres y centros educativos,* Agencia Española de Protección de Datos, Agencia Estatal

prevaleciendo este derecho sobre cualquiera otro.

Teniendo este derecho como base, a la hora de estudiar las conductas que atentan contra los derechos de un menor en cuanto a la protección de sus datos, lo primero que debemos hacer es diferenciar entre las conductas más agresivas que pueden conllevar responsabilidad penal, de las que, sin llegar a ese extremo, vulneran los derechos de un menor a ver cumplido su derecho y muchas veces pasan inadvertidas en la sociedad.

Para prever tanto unas como otras, es importante educar a los menores en el uso del internet y las redes sociales, el Prof. Carlos Oliva Marañón recomienda llevar a cabo las siguientes precauciones a la hora de hacer uso de las mismas: "*Plantearse qué datos personales publicar y cuáles es conveniente que no se conozcan; los menores de edad deberían evitar revelar sus domicilios o números de teléfono; utilizar seudónimo en vez del nombre real; y por último, prestar especial cuidado al publicar información de otros sin su consentimiento.*"[48].

4.1.1.- Conductas lesivas derivadas de un uso doloso de las redes sociales y las consecuencias que acarrean.

Las conductas lesivas que se llevan a cabo a través de las redes sociales se pueden clasificar en dos grandes grupos, en primer lugar las que llevan aparejada una tipificación penal, y en segundo lugar, las que son sancionables administrativamente por infracción de la LOPD.

En ese primer grupo, la cantidad y naturaleza de los delitos puede llegar a ser muy variada: delitos relativos a la intromisión en la intimidad, contra la propiedad intelectual, industrial, apología del terrorismo, incitación al odio y a la violencia, delitos de odio, apología a la anorexia y bulimia, inducción al suicidio[49]. Sin embargo, a

---

Boletín Oficial del Estado, Madrid.

[48] Oliva Marañón, C., 2012, *Redes sociales y jóvenes: una intimidad cuestionada en internet", Aposta, Revista de Ciencias Sociales, nº54, julio, agosto y septiembre.*

[49] Ejemplo de este caso es el conocido caso de *la ballena azul*, un juego creado en internet por el que se proponían una serie de retos a los menores, que siempre conllevaban autolesionarse, hasta llegar al último reto, que era suicidarse. Al respecto ver noticias en medios españoles: Ruiz Fájula, D., 2017, "*Una menor de Marbella, primera víctima del juego 'Ballena Azul' en Andalucía*", El Mundo, versión digital:

efectos del presente estudio nos interesan las que conllevan una injerencia en los datos personales, como los delitos contra la indemnidad sexual, integridad moral, llegando a coacciones y amenazas, descubrimiento y revelación de secretos, injurias y calumnias, entre otros.

Para ello debemos hacer un pequeño análisis de las conductas llevadas a cabo en internet que derivan en la comisión de dichos delitos. Algunas de estas conductas son el ciberbullying[1], ciberbaiting[2], grooming[3] y sexting[4].

[1]El ciberbullying o ciberacoso, hace referencia a las situaciones de acoso que un menor puede sufrir a través de internet ya sea de un menor a otro, o de un grupo de menores hacia un menor determinado. Implica llevar el acoso escolar al ámbito digital. Esta es quizás la conducta más frecuente, dado que es un medio usado generalmente para continuar un acoso iniciado de forma personal. A este respecto existe el tipo delictivo del artículo 172 ter, que castiga el acoso a una persona llevándolo a cabo *"de forma insistente y reiterada"*, determinando una pena de privación de libertad de 3 meses a 2 años. El caso tipo sería llevar a cabo pautas como burlas, insultos, persecución, incluso suplantación en actos personales, con el objetivo de alterar el desarrollo de su vida[50], y que los sujetos, tanto el acosador como la víctima sean menores de edad, dentro del mismo rango de edad, todo ello de forma reiterada, no como un momento puntual[51].

[2]El ciberbaiting, concepto que no se ha traducido al castellano, es una modalidad dentro de la conducta anterior con la variación de los sujetos, siendo este un acto de acoso de un menor o grupo hacia un profesor. Esta conducta será analizada con más énfasis en el siguiente apartado puesto que el sujeto activo en este caso es el menor, siendo el sujeto pasivo un adulto.

---

http://www.elmundo.es/andalucia/2017/05/18/591d91d322601df6728b45af.html; Prado, B. del, 2017, "Un adolescente de Gandía, víctima mortal de la 'ballena azul"**,** Cadena Ser, versión digital: http://cadenaser.com/emisora/2017/09/22/radio_valencia/1506077201_604009.html; y Durán, L.F., 2017, "*Investigan dos casos incipientes de Ballena Azul en Madrid",* El mundo, versión digital: http://www.elmundo.es/madrid/2017/06/12/593dc087e2704e152d8b4576.html

[50] Artículo 172.1 ter Código Penal.

[51] En este sentido se expresa la Audiencia Provincial de Barcelona en su Sentencia 9805/2017, cuando establece que "para la apreciación del acoso escolar no es suficiente un incidente aislado, sino varios actuaciones mantenidas en el tiempo".

[3]El grooming o engaño pederasta[52] es definido por la AEPD como "*el embaucamiento y acoso al que se ve sometido un menor por un adulto mediante acciones a través de medios digitales que buscan ganarse la confianza del menor haciéndose pasar por otro menor con fines de abuso sexual o pornografía infantil, sin descartar otros tipos de chantaje o extorsión"* [53]. Sus dos notas características son pues: los sujetos, el acosador, un adulto, y el acosado un menor de edad*;* y el objeto, necesariamente de contenido sexual –que puede ir desde la obtención de imágenes para sí o para compartir con otros, incluso hacer negocio con ellas, hasta la obtención de favores sexuales. Dándose estas circunstancias, estamos ante un delito autónomo tipificado en el artículo 183 bis del Código Penal.

[4]El sexting o "sextorsión"[54] implica el envío de imágenes propias, fotografías y propios menores o por terceros con su consentimiento y posteriormente difundidas de manera no consentida. El origen se encuentra por tanto en una acción voluntaria y confiada por parte de quien toma sus imágenes y las envía, pues sus destinatarios suelen ser personas de su confianza, como la pareja o los amigos íntimos. Esta conducta está tipificada en el artículo 197 del Código Penal.

Hay que tener en cuenta que esto puede dejar en los menores, secuelas psíquicas e incluso físicas. Ejemplos de estos efectos nos las da el autor Juan de Dios Meseguer[55], cuando expresa que los ataques producen alteraciones en la salud como estrés postraumático, delirio de persecución, insomnio, ambios de personalidad que puede a llegar a destruir o anular a la persona del menor, sensación de inferioridad respecto al resto del entorno, nerviosismo e hipersensibilidad a toda injusticia, incapacidad para disfrutar y estar seguro de lo que se es y se hace y/ o miedo general. Desde luego estas

[52] Término aconsejado en castellano por la Fundéu BBVA: http://www.fundeu.es/recomendacion/engano-seduccion-pederasta-grooming/

[53]Guía para formadores y familiares de la AEPD.- http://www.tudecideseninternet.es/agpd1/images/guias/Guia_formadores2016.pdf

[54]Término extraído de: Dávara Fernández de Marcos, L., 2017, *Menores en internet y redes sociales: Derecho aplicable y deberes de los padres y centros educativos*, Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, Madrid.

[55] Meseguer González, J.D, 2012, *Tratamiento y protección penal contra el ciberacoso escolar o cyberbullying,* El Derecho, versión digital: http://tecnologia.elderecho.com/tecnologia/ciberseguridad/Tratamiento-proteccion-ciberacoso-menores-cyberbullying_11_485680003.html

representan consecuencias de por sí gravosas para una persona adulta, cuanto más lo serán para un menor en pleno desarrollo.

Para finalizar, aunque no es misión de este estudio ahondar más en las conductas penales[56], sí es importante insistir en la importancia que cobra la educación de los menores para que sean capaces de evitar ser víctimas de estas conductas y también para que comprendan las gravosas consecuencias que conllevan, y lo fácil que es incurrir en ellas, a veces sin tener intención de ello, y sin saber el daño que puede llegar a hacerse.

Como decíamos al principio, existe un segundo grupo de acciones o conductas dolosas que no conllevan responsabilidad penal: aquellas que infringen las normas de la LOPD, las cuáles acarrean sanciones administrativas, impuestas por la propia AEPD a través del sistema sancionador.

El artículo 44 LOPD establece los tipos de las infracciones, clasificando estas en leves, graves y muy graves. Tipifica como grave, el tratamiento de "*datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo*", siendo en el caso de los menores, obligatorio obtener su consentimiento en todo caso, y siendo menores de 14 años, el de sus progenitores o representantes legales, como ya hemos visto. Así mismo, para las infracciones graves la sanción impuesta por la ley en el artículo 45.2, oscila entre los 40.001 y 300.000 euros, cantidad que para un ciudadano medio son cantidades exorbitantes. Entendemos pues, que la publicación de datos personales de cualquier tipo, como fotografías o imágenes, con el fin de dañar o hacer burla de un menor, en un entorno como el perfil público de una red social, y por supuesto, sin el consentimiento ni del menor ni de sus progenitores, es incurrir en una infracción de la LOPD y por lo tanto, conllevará una sanción de las características descritas. Además, cabe decir que el apartado 4 del artículo 45, propone una serie de circunstancias que al concurrir en los hechos podrían agravar dichas sanciones. Como ejemplo de la aplicación de dichas circunstancias encontramos la Resolución de la AEPD de 15 de noviembre[57], en la que una entidad bancaria es condenada a pagar una sanción de 40.001€ por infracción del artículo 9 del LOPD en cuanto a la seguridad de

[56] Para un estudio más a fondo de las conductas penales acudir a las guías referenciadas con anterioridad, y el trabajo de Laura Dávara Fernández Marcos de la referencia anterior.

[57] Resolución 2699/2017 AEPD de 15 de noviembre de 2017. Procedimiento Nº PS/00235/2017.

datos, aplicándose 4 de estas circunstancias agravantes. En el mismo sentido la Resolución 1486/2011[58], en la que en aplicación del artículo 45.4, resuelve elevar la cuantía mínima de la multa por la vinculación de la actividad de la entidad infractora con la realización de tratamientos de datos de carácter personal y el volumen de negocio de la misma, dos de las circunstancias del apartado 4; y la Resolución 1988/2017[59], sobre el tratamiento de datos de una menor sin consentimiento por parte de una entidad, en la que se aplica una agravación de la sanción por cumplirse el artículo 45.4.a) en cuanto al carácter continuado de la infracción, que opera como agravante debido a que la denunciada ha tratado la imagen del menor en los citados portafotos desde el año 2011, fecha en que se captó, hasta el año 2016, fecha en que aparece en el portafotos aportado por la madre del menor.

4.1.2.- Conductas lesivas de derechos derivadas de un uso imprudente de las redes sociales y sus consecuencias.

Cuando hablamos de un uso imprudente, nos referimos a aquellas acciones que *a priori* pueden parecer un uso normal e incluso positivo de las redes sociales, acciones que cualquier persona realiza constantemente en el uso de sus perfiles, como por ejemplo compartir una foto de hijo menor de edad con sus compañeros de clase en su perfil –de forma que todo el público de la red social en cuestión puede ver la fotografía-, ello claro sin preguntar al resto de padres; o la publicación por parte del colegio de imágenes de sus actividades para publicitar su oferta educativa en los meses próximos a las matrículas, para hacerlo más atractivo con respecto a otros centros, sin solicitar consentimiento de los progenitores o alumnos. Pues bien, estas conductas también son sancionables por la LOPD. Se puede ir un paso más allá, analizando el perjuicio que puede ocasionar la constante publicación de imágenes de los menores por parte de sus familiares sin tener en cuenta el impacto que pueda tener, y quienes sin ningún tipo de intencionalidad de dañar la protección de sus hijos, pueden incurrir en ello.

El desconocimiento general que existe en cuanto a lo que se considera infringir las normas de protección de datos se debe en su mayoría a que gran parte de las personas carecen de lo que el profesor Juan María Martínez Otero llama, educación

[58] Resolución 1486/2011 AEPD de 18 de julio de 2011. Procedimiento Nº PS/00045/2011.

[59] Resolución 1988/2017 AEPD de 17 de julio de 2017. Procedimiento Nº 312/2017.

digital[60]. Y es que el uso de las redes sociales se ha vuelto tan cotidiano, que hacemos un uso irresponsable de las mismas. Lo cierto es que incluso la doctrina y la jurisprudencia tienen dificultades para establecer los límites entre un uso correcto y un uso negligente de estos medios. Un ejemplo es la publicación de una fotografía que se ha recabado del perfil de su titular sin permiso de este para su publicación en perfil distinto al suyo. Esto se ha dado sobre todo en publicaciones periodísticas, en las que se utilizan fotografías, ya sea de víctimas, como de presuntos delincuentes o cualquier implicado en un hecho, obtenidas a través de los perfiles de estas personas en redes sociales. Al respecto existe ya jurisprudencia, como la sentencia del Tribunal Supremo analizada por el Profesor Gerardo Pérez en su artículo de opinión[61], resolución en la que este Tribunal considera que lejos de autorizarse este tipo de conductas, va en contra del derecho a la propia imagen pues "el hecho de subir una fotografía a una red social haciéndola accesible al público en general, no autoriza a un tercero a reproducirla en un medio de comunicación sin el consentimiento de su titular". De esta forma, estaríamos ante una violación del derecho a la propia imagen del artículo 18.1 CE, cuya protección se atribuye a la Ley Orgánica 1/1982[62], lo cual es discutido en todo momento por el profesor Sánchez, para quien lo afirmado por Tribunal va en contra del Derecho de información, también de configuración constitucional, no ponderando sus implicaciones constitucionales.

4.1.2.1.- Conductas exentas de sanción por la LOPD.

Sin embargo a lo anterior, no todas los hábitos incorrectos en las redes sociales son sancionables por la LOPD. Teniendo como referencia lo regulado en el artículo 2.2.a) de la LOPD, quedan excluidos de la norma "*los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas*", quedando incluidos en esta definición los perfiles en redes sociales privados o que sea accesible a un número limitado de usuarios. Así lo podemos presumir a *sensu contrario*

[60] Martínez Otero, J. M., 2016, *Derechos Fundamentales y Publicación de imágenes ajenas en las redes sociales sin consentimiento*, Revista Española de Derecho Constitucional, 106, enero abril, pp. 119-148.

[61] Pérez Sánchez, G., 2017, *Redes sociales y derecho a la propia imagen*, http://www.gerardoperez.es/redes-sociales-y-derecho-a-la-propia-imagen/

[62] Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

de la Resolución 2261/2011 AEPD, en la que condena a la titular de un perfil de la red social *Facebook* por publicar un vídeo con imágenes de menores sin su consentimiento ni el de sus progenitores, argumentando la AEPD que aunque era una persona física, su perfil era abierto al público general de la red social, por lo que no podía aplicarse la exención del artículo 2.2.a).

Quedando las conductas llevadas a cabo en un perfil de uso doméstico a lo establecido en la LO 1/1982, por ser una violación del derecho a la propia imagen y no una intromisión en la protección de datos[63], materia que no analizaremos en el presente trabajo.

4.1.2.2.- Conductas sancionables por la LOPD de forma atenuada.

En cuanto a las consecuencias de las acciones que son sancionables por la LOPD, en España hay que acudir al artículo 45 de esta ley, modificado en el año 2011, en el que se añadió un sistema de atenuantes y rebaja de las sanciones, llegando a permitir en su apartado 6 la sustitución de la sanción por un apercibimiento si se cumplen con los presupuestos de la ley[64]. En este sentido se pronuncia la Resolución de 25 de octubre de 2017[65], que conoce de un procedimiento abierto contra un colegio por infracción del artículo 6 LOPD y el 12 RLOPD, al haber publicado imágenes en medios digitales de acceso público constando de forma explícita la negativa de los progenitores a dicho tratamiento. En dicha resolución se decide archivar el procedimiento por entender que efectivamente se cumplían los requisitos de aplicación del art. 45.6, puesto que el colegio había suprimido de todo medio o red social dicha fotografía, y no existía intencionalidad de lesionar la imagen del menor, cabiendo la sustitución de la sanción por un apercibimiento, y yendo un paso más allá, entendió que las medidas correctoras que se habrían incluido en dicho apercibimiento ya habían sido cumplidas por la infractora y por lo tanto cabía directamente el archivo sin dictar dicho apercibimiento.

No cabiendo la sustitución, a la hora de imponer la sanción de un hecho como los descritos en este apartado, la AEPD tiene en cuenta por un lado, las circunstancias

[63] Para un estudio más en profundidad de la diferenciación, acudir a Martínez Otero, J. M., 2016, *Derechos Fundamentales y Publicación de imágenes ajenas en las redes sociales sin consentimiento*, Revista Española de Derecho Constitucional, 106, enero abril, pp. 119-148.

[64] Básicamente, los presupuestos son, de un lado que los hechos fuesen constitutivos de infracción leve o grave y que el infractor no hubiese sido sancionado o apercibido con anterioridad.

[65] Resolución 2285/2017 AEPD, de 25 de octubre de 2017. Procedimiento Nº A/00286/2017.

por las que puede graduar las sanciones descritas en el apartado 4 del artículo 45, interesando en este apartado aquellas que atenúan la culpabilidad y antijuricidad de la acción, que son los apartados d), e) f), h), i) y, el j) que puede tener una doble función de atenuar o agravar las sanciones. Quizás la que más cabida tenga en las conductas que nos interesan, es la del apartado e), en cuanto a **"***los beneficios obtenidos como consecuencia de la comisión de la infracción*", entendiendo que la ausencia de beneficios, puede conllevar la minoración de la sanción; así como el apartado f), en cuanto al "*grado de intencionalidad*" mostrado por el infractor. Esta circunstancia en casos como los descritos puede ser primordial a la hora de establecer la sanción, dado que en muchos casos de los hechos puede presumirse que el autor no buscaba violar el derecho de protección de datos de los menores, como es el ejemplo de la constante publicación por parte de los progenitores de imágenes fotográficas o vídeo de sus hijos que puede llegar a ser considerada una intromisión en su derecho de protección pero nunca existirá una intencionalidad por parte de los progenitores.

Entre las Resoluciones de la AEPD encontramos ejemplos de estas circunstancias, como la Resolución 555/2009[66], en la que se comprende un procedimiento en contra del titular de una cuenta en la red social Youtube por infringir el artículo 6.1 LOPD, al incluir en su perfil imágenes en vídeo señalando a una serie de menores como criminales, mostrando sus fotografías sin su autorización o la de sus progenitores. La AEPD dictamina imponer una multa de 1.500€ al autor aplicando las circunstancias atenuantes del artículo 45.5 por entender en primer lugar que los hechos se realizaron en el ámbito privado y no en el de una actividad profesional, además que las circunstancias hacían necesario que parte de la conducta debía tratarse por los cauces establecidos en la LO 1/1982 y no desde la perspectiva de la protección de datos, y que además se cumplía con la circunstancia del apartado e) del artículo 45.4 en cuanto a la ausencia de beneficios obtenidos, de ahí que la sanción pese a ser considerada grave sea tan inferior con respecto al mínimo de 40.001€ que impone el artículo 45.2 para las infracciones graves. Otro ejemplo es la Resolución 580/2016[67], en la que se resuelve un procedimiento contra una entidad por infringir el deber de información del artículo 5 LOPD, y de recabación del consentimiento paterno en un casting ofertado para menores de 14 años. Resuelve aplicar una sanción de 5.000€ en base a que operan como

[66] Resolución 555/2009 AEPD de 30 de marzo de 2009. Procedimiento Nº PS/00508/2008.

[67] Resolución 580/2016 AEPD de 1 de marzo de 2016. Procedimiento Nº PS/00476/2016.

atenuantes los apartados d) y e) del artículo 45.4, ante la falta de pruebas de que el volumen de negocio o actividad de la denunciada se haya visto afectado por la infracción indicada, no habiendo pruebas, tampoco, de que como consecuencia de su comisión la denunciada haya obtenido beneficios.

En cuanto a la falta de intencionalidad tenemos la Resolución 2116/2016[68], en la que se considera que concurren circunstancias necesarias para que pueda aplicarse, en el presente supuesto, lo dispuesto en el artículo 45.5 de la LOPD, ya que no se ha obtenido ningún beneficio, el blog ha sido eliminado de manera inmediata al tener conocimiento que la imagen de una de las menores seguía apareciendo vinculada al Colegio Británico de Sevilla, no ha existido intencionalidad ya que cancelaron las imágenes de al menos 8 webs y links, imputando una sanción de 900 euros, muy por debajo del límite mínimo de una sanción grave del artículo 45.2 LOPD.

Por último, para la cuantificación de la sanción, debe analizarse si los hechos encajan en alguno de los supuestos del apartado 5. Si es así, la AEPD puede aplicar una sanción menor, dando lugar a cuantías mucho más reducidas. Sobre la naturaleza de este apartado se pronunció la Audiencia Nacional en su Sentencia estableciendo que dicho precepto "*no es sino manifestación del llamado principio de proporcionalidad (Art. 131.1 de la Ley 30/1992), incluido en el mas general de prohibición de exceso, y reconocido por la jurisprudencia como Principio General del Derecho*"[69], dando plena validez a su aplicación dentro de los límites que los supuestos establecen. Para ilustrar esta norma cabe analizar la Resolución 2636/2011 AEPD[70], en la que se procede a aplicar el artículo 45.5 LOPD, minorando así la sanción a imponer. La argumentación realizada es la concurrencia de más de uno de los criterios del artículo 45.4 (como requiere el artículo 45.5.a), como son: la falta de intencionalidad (artículo 45.4.f); la ausencia de beneficios obtenidos (artículo 45.4.e); que la recogida de datos por Internet de sus clientes, en el resto de procedimientos utilizados por la entidad denunciada, eran conformes con la LOPD (artículo 45.4.i). A esto se añade la existencia de un reconocimiento espontáneo de los hechos por el infractor (artículo 45.5.d). Por todo ello, se impone una multa de 20.000€ minorada en la mitad del mínimo de 40.001€ que corresponde para infracciones graves según el artículo 45.2.

[68] Resolución 2116/2016 AEPD de 30 de septiembre de 2016. Procedimiento Nº PS700155/2016

[69] SAN 273/2004 de 21 de enero de 2004.

[70] Resolución 2636/2011 AEPD, de 22 de diciembre de 2011, Procedimiento Nº PS/00339/2011.

Además de todo lo anterior, cabe hacer mención a las consecuencias para los menores derivadas de un uso excesivo que le dan a las redes sociales. Y es que los menores dedican tanto de su tiempo a las redes sociales que trae resultados negativos sobre ellos mismos. Véase adicción a las redes sociales[71] por no establecer medidas de control sobre dicho uso. Sobre la cuestión existen publicaciones al uso que explican la definición y síntomas que revelan que los menores presentan adicción[72]. Algunos de los síntomas son la revisión repetida de los perfiles a lo largo del día, una mentalidad de compartir todo por redes sociales, sus datos y su día a día o no poder pasar más de un par de horas sin conectarse a estas.

De todo lo visto, vemos cómo el menor puede ser víctima por existir una persona o personas que vulneren su derechos, provocando un daño –ya sea más o menos evidente-, y de forma consciente como sin intencionalidad de ocasionar el mismo; o serlo por sus propios actos. Y todo ello, sin que se den soluciones efectivas en la educación, prevención y corrección de estas conductas.

4.2.- El menor como sujeto culpable en el uso de redes sociales.

Debemos en este momento cambiar la perspectiva con la que analizamos el derecho de protección de datos de menores. No hacerlo sólo desde el punto de vista de la defensa de los derechos de los niños frente a sujetos mayores de edad que pueden ejercer sobre ellos influencia por ostentar una superioridad por ser para ellos una autoridad; sino también desde el plano de menor contra menor, incluso menor contra adulto, siendo este último el sujeto pasivo.

No hablamos de aprovechar una circunstancia dada por la edad o la posición de superioridad sobre el menor para hacer uso de sus derechos o realizar una intromisión en los mismos, sino del uso culpable por parte de los menores de las redes sociales, incurriendo así en una de las conductas descritas anteriormente.

Es preciso diferenciar dos grupos de entre los menores. Siguiendo el modelo de

[71] Dávara Fernández de Marcos, L., 2017, *Menores en internet y redes sociales: Derecho aplicable y deberes de los padres y centros educativos*, Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, Madrid

[72]En este sentido el monográfico que podemos encontrar en: http://www.monografias.com/trabajos89/adiccion-redes-sociales/adiccion-redes-sociales.shtml#sintomasa

la legislación, distinguimos los menores de 0 a 14 años, rango de edad al que no se le reconoce ni la capacidad de dar su consentimiento para el tratamiento de sus datos ni tampoco responsabilidad directa, ni civil ni penal, sobre sus actos[73]. A esto existen dos única excepciones: en cuanto a la toma de decisiones, como ya se ha mencionado anteriormente, cuando las capacidades y la madurez del menor lo aconsejen podrán tomarse en consideración su opinión respecto del tratamiento de sus datos; y en cuanto a su responsabilidad, la LO 5/2000 en su artículo 3, en su último inciso determina que en los casos en que menores de 14 años se ven involucrados en un delito, "*el Ministerio Fiscal deberá remitir a la entidad pública de protección de menores testimonio de los particulares que considere precisos respecto al menor, a fin de valorar su situación, y dicha entidad habrá de promover las medidas de protección adecuadas a las circunstancias de aquél conforme a lo dispuesto en la Ley Orgánica 1/1996, de 15 de enero*"

En cuanto a este grupo de edad, la edad media para comenzar a hacer uso de las redes sociales es a partir de los 10 años, como ya hemos visto. Edad a la que los niños comienzan a obtener de sus progenitores sus primeros teléfonos móviles, tablets y ordenadores personales, y por consecuencia a redes de todo índole. Esto sumado a que el ordenamiento jurídico no establece un sistema de responsabilidad –más allá de la responsabilidad civil en que incurran sus progenitores o representantes legales por las acciones de los menores, implica que los menores se ven expuestos a todas estas conductas sin tener ni formación ni límites en su uso. Todo ello pese a que las conductas descritas en el apartado anterior no sólo son cometidas por los mayores de 14 años. Debemos entender que no por ser llevadas a cabo por menores, son menos graves, ya que las consecuencias son las mismas.

El segundo grupo, comprende el rango de edad que va desde 14 hasta los 18 años, quienes sí asumen tanto la capacidad para dar su consentimiento para tratar sus datos, como la responsabilidad directa por sus actos en los términos establecidos en la

[73] Así lo establece el artículo 3, de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores –en adelante LO 5/2000-, sobre el régimen de los menores de catorce años cuya redacción es la siguiente: *"Cuando el autor de los hechos mencionados en los artículos anteriores sea menor de catorce años, no se le exigirá responsabilidad con arreglo a la presente Ley, sino que se le aplicará lo dispuesto en las normas sobre protección de menores previstas en el Código Civil y demás disposiciones vigentes".*

LO 5/2000 sobre responsabilidad penal de los menores, que establece las medidas que pueden imponérseles, como amonestaciones, prestaciones en beneficio de la comunidad, realización de tareas socioeducativas, permanencia en el domicilio durante el fin de semana, el internamiento, etc, además de la responsabilidad civil que pueda exigírsele por daños y perjuicios causados y de la que responden solidariamente sus progenitores y tutores[74].

En cuanto a las conductas penales interesa en este apartado el análisis de aquellas que se realizan por los menores, es decir, el ciberbullying, el ciberbaiting e incluso el sexting.

Como ya hemos visto, el ciberbullying o ciberacoso es una conducta en la que los menores pueden ser tanto autores como víctimas. Es sin duda la más extendida dado que los casos de ciberacoso escolar han incrementado y es cada vez más común encontrarse noticias sobre menores acosados por sus compañeros. Es el caso de cuatro menores detenidos por acosar a una compañera[75], maltratándola verbalmente, provocando en la menor acosada miedo a acudir a las clases y una crisis de ansiedad, hasta el punto de cambiarse de centro escolar, circunstancia que no cambió su situación, manteniendo el acoso por redes sociales. Y es que es una situación difícil de controlar primero por que los jóvenes no lo denuncian a sus progenitores o a los centros, y segundo porque al tener acceso a las redes, tanto los acosadores como las víctimas, ese sufrimiento es continuo.

En cuanto al ciberbaiting es una transgresión no sólo a la integridad moral de una persona, sino a una autoridad como es un educador en la vida del menor, o al menos como debería ser. Es una actitud que está proliferando entre los alumnos, que se dedican a subir fotos de un profesor continuamente, y sin si consentimiento para hacer burla. Por lo pronto no se encuentra entre la jurisprudencia ningún caso de estas características por lo que hemos de entender que los conflictos quedan en el sistema del propio para castigar a estas conductas.

[74]Guía para formadores y familiares de la AEPD.- http://www.tudecideseninternet.es/agpd1/images/guias/Guia_formadores2016.pdf

[75]*Detenidos cuatro menores de 14 años en Alicante por acosar a una compañera de clase*, Rtve, versión digital: http://www.rtve.es/noticias/20161117/detenidos-cuatro-menores-14-anos-alicante-acosar-companera-clase/1444811.shtml

Hay otros muchos comportamientos adoptadas por los menores y de manera creciente, como la suplantación de la identidad de la víctima, creando perfiles falsos en las redes sociales, colgando en ellos datos personales así como fotografías e imágenes en vídeo. El problema de todos estos actos es que son muy difíciles de detectar, quedando muchas veces en el silencio de las víctimas. Pese a ello, los jóvenes enter 14 y 18 que cometan este tipo de conductas hallan sus consecuencias en la LO 5/2000, en la que regula las medidas a tomar en los casos en que sean menores de edad los que cometen un delito.

Por último, y siguiendo el modelo de análisis de las consecuencias realizado en el apartado anterior, cabe mencionar aquellas conductas realizadas por los menores que no implican una responsabilidad penal, como el tratamiento de datos de otros menores sin autorización suya o de sus progenitores. Está claro que es muy difícil encajar un asunto con estos parámetros en los preceptos de la LOPD ya vistos, y es que *a priori* el perfil de un menor debería entenderse como doméstico en todo caso. Pero ¿y si aun siendo menores alcanzan un número de personas o "seguidores" suficiente para entender que se vulnera la protección de datos de otro menor? ¿O si este perfil es abierto al público? ¿Se debería optar por la protección ofrecida por la LOPD o acudir a la protección del derecho a la propia imagen que ofrece la ley 1/1982? Es una pregunta que parece no tener respuesta, dado que en la búsqueda de resoluciones al uso, no se han encontrado casos de estas características.

Además de la responsabilidad directa derivada de sus conductas, cabría mencionar también la responsabilidad de centros educativos y progenitores, quienes al formar parte activa y primordial de la vida y educación de los menores, es su función prevenir y actuar en estos casos, fundamentalmente a través de la educación y formación. Lo primero que deben hacer es informarse ellos mismos sobre el uso de las redes sociales y los peligros que conlleva para sus hijos, para después pasar toda esa información a los menores de forma clara para que estos tomen las mejores decisiones al navegar. No se trata de prohibir su uso o controlar de forma taxativa la forma en que interactúan, sino tener claro y dejarles claro que deben tener límites a la hora de usar internet y de no ser así, sus actos tendrán consecuencias. Dado que para los menores de 14 no existe un sistema reglado, todo el peso queda sobre estas personas e instituciones.

5.- Labor del abogado en la protección de datos de menores

En un ámbito tan novedoso en el que están surgiendo tantos conflictos, el abogado debe estar formado en la materia, para el asesoramiento y resolución de intromisiones ajenas en el derecho de protección de datos de los clientes.

De esta forma, y aunque es un derecho reconocido al individuo, el abogado puede actuar en representación, en la petición inicial al responsable del tratamiento de datos que se desee cancelar, que debe efectuarse enviando una solicitud a este en la que se exprese el deseo de hacer efectivos los derechos de acceso, rectificación, cancelación u oposición –derechos ARCO-, y en caso de no ser atendida, plantear el asunto ante la AEPD.

En casos en que exista una violación de los derechos del cliente o de sus hijos, habrá que acudir directamente a la AEPD, presentando un escrito de denuncia en el que consten: "*nombre y apellidos del interesado y, en su caso, de la persona que le represente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones; hechos, razones y petición en la que se concrete, con toda claridad, la solicitud; lugar y fecha; firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio; identificación de los presuntos responsables; y todos aquellos documentos o cualquier otro tipo de prueba o indicio que permita corroborar los hechos denunciados*."[76]. Se comienza así el procedimiento sancionador que acabará con una resolución de la AEPD, cuyos pronunciamientos pueden ser: imponer una sanción, conceder un apercibimiento, establecer la sustitución de la sanción, o el archivo de la cuestión por inexistencia de responsabilidad, o bien por haber cumplido con las medidas correctoras con anterioridad a la finalización del procedimiento.

"*Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la*

[76]Canal del ciudadano AEPD: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/index-ides-idphp.php

Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13/07, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal."[77]. Momento en el que alcanza mayor importancia la actuación del abogado, por cuanto se accede a la jurisdicción.

Por otro lado, cuando esa violación de los derechos implica una conducta delictiva, habrá que acudir directamente a un proceso penal, bien el establecido en la Ley de Enjuiciamiento Criminal[78], bien el de la Ley de Responsabilidad Penal de los menores.

Por último cabe también mencionar el derecho al olvido y el procedimiento a seguir para eliminar fotos y vídeos de internet, para el que nos remitimos a la guía para el ciudadano preparada por la AEPD[79].

6.- Conclusiones.

La primera conclusión a la que podemos llegar es que los jóvenes no son conscientes de la manera en que se exponen en sus redes sociales, y se encuentran muchas veces con situaciones que no saben identificar como dañinas, normalizando situaciones que no deberían serlo. Y cuyo impacto no comprenderán hasta llegar a la edad adulta, momento en el que será tarde para reparar el daño.

Este desconocimiento es un problema que deriva de la falta de información. Las nuevas generaciones no están formadas suficientemente en educación digital, ello se puede deducir del incremento de casos de conflictos entre menores en las redes sociales, que no dejan de aumentar cada día. Y la solución es clara: deberían existir campañas

---

[77] Pie de recurso de la Resolución 1870/2017, de 21 de agosto de 2017, Procedimiento Nº PS/00082/2017. La cual resuelve un procedimiento abierto de oficio por la AEPD contra la Red Social Facebook, cuya lectura es recomendable.

[78] Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal

[79] Protección de Datos: Guía para el ciudadano: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO.pdf

dirigidas específicamente a los padres y a los niños de concienciación sobre los peligros de internet y el daño que se puede llegar a hacer con un mal uso del mismo. Otro punto importante de la formación es aprender el conductas perjudiciales existentes, para que tanto unos como otros sepan distinguirlas y no permitir que se sigan produciendo, mediante la denuncia tanto a los padres, como a los centros, como a la AEPD en casos de intromisión en la protección de datos, como a los juzgados y tribunales de ser necesario. Esta formación debe ser impulsada desde el propio Estado, que no quede en documentación escrita, que se hagan conferencias y debates en los colegios para llegar mejor a los jóvenes. Formación también al profesorado, para que puedan descubrir los síntomas y puedan tomar medidas. Y del mismo modo, que los centros envíen información a los padres, mediante los niños, para que comprendan la importancia de formarse en protección de datos.

Otro punto es el de la formación para que no cometan transgresiones a los derechos de otros menores. La prevención es fundamental, debemos formar a los menores no sólo para protegerse, sino para evitar que se conviertan en agresores. Que se vean reflejados en las víctimas, y no sientan la necesidad de hacer daño al de al lado. Este problema no ocurre sólo en el ámbito de las redes, debe darse un cambio social general, para que los jóvenes no se críen en la insensibilidad, que lo único que provoca es la falta de empatía con sus iguales. Deben crecer en valores a la vez que se forman en todo lo demás. Hacer que comprendan lo insufrible que puede ser para un compañero el convertirse en objeto de acoso, burlas, amenazas y de agresiones continuas, y que ese sufrimiento se vuelve peor cuando los agresores son personas de su entorno, del colegio, instituto, academia, y de su misma edad, a los que tiene que ver cada día.

Y para los casos en los que la educación llega tarde, el Estado debe ser capaz de demostrar que dispone de los medios necesarios para castigar estas conductas, siempre desde el punto de vista de la reeducación y reinserción –principio básico de nuestro sistema penal-, sobre todo cuando se trata de menores de edad, que todavía no alcanzan a comprender el impacto de sus actos y que como sus víctimas, están en desarrollo.

Queda patente que en los casos en los que un adulto es el agresor, la ley responde, existiendo un catálogo de delitos dirigidos a combatir las conductas en internet. En el caso de los mayores de 14 años, también existe a través de la Ley Orgánica 5/2000, que con medidas ajustadas a esas edades, tratan de solventar y reconducir los motivos que han llevado a esos jóvenes a delinquir. Pero para el caso de

los menores de 14 años, edades entre los 10 y los 14, en las que aun comprenden menos el alcance de sus actos, no existe ninguna consecuencia.

Es ingenuo pensar que en una sociedad en la que todavía vamos atrasados en educación digital, los más pequeños cumplen con las normas y entienden los peligros existentes. Más cuando sus referentes no les han transmitido ninguna advertencia sobre ello. Y dado que la formación ha fallado, debería existir un sistema por el que se muestre a los menores que sus actos tienen consecuencias. Es obvio que a un menor de menos de 14 años no se le pueden imponer penas como a los mayores, primero por ser abusivo, y segundo porque tampoco ayudaría a solventar el problema; pero sí que podrían ser efectivas medidas de reeducación. Una buena opción sería, por ejemplo, un programa educativo al que los niños deban acudir a modo de actividad extracurricular, en el que puedan descubrir qué han hecho mal, el daño que han podido hacer, y aprender a no reiterar esas conductas.

Como conclusión final, a España le queda un largo recorrido en cuanto a protección de menores en las redes, y es un problema que no va a desaparecer, ya que los avances tecnológicos no van a frenar. Hace 30 años era impensable que nuestra sociedad se enfrentara a estos problemas, y el ordenamiento no ha sido capaz de prevenirlo. Es el momento de dar soluciones certeras, y adelantarse a los nuevos retos que puedan aparecer en el futuro, para lograr desarrollar una legislación impenetrable en protección de los menores.

7.- Bibliografía

Aba Catoira, A., 2011, "La protección de los derechos de los menores ante las nuevas tecnologías. Internet y las redes sociales", en Cotino Hueso, L, "Libertades de expresión einformación en Internet y las redes socuales: ejercicio, amenazas y garantías, PUV (publciaciones de la Universidad de Valencia), Valencia, pp 486-511.

Agencia de los Derechos Fundamentales de la Unión Europea, 2014, "*Manual de legislación europea en materia de protección de datos*" (a través de la página del Consejo de Europa: https://www.coe.int/en/web/human-rights-rule-of-law/information-society).

Andreu Martínez, Mª B., 2013, *La protección de datos personales de los menores de edad*, Thomson Reuters, Aranzadi.

Blog Oficial de Instagram, 2015, "Celebrating a Community of 400 Million": http://blog.instagram.com/post/129662501137/150922-400million

Conde, Ortiz, C., 2006, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Dykinson, ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/bull-ebooks/detail.action?docID=3170265

Dávara Fernández de Marcos, L., 2017, *Menores en internet y redes sociales: Derecho aplicable y deberes de los padres y centros educativos,* Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, Madrid: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2016/Menores_en_Internet.pdf

Durán, L.F., 2017, "*Investigan dos casos incipientes de Ballena Azul en Madrid",* El mundo, versión digital: http://www.elmundo.es/madrid/2017/06/12/593dc087e2704e152d8b4576.html

Espinar Ruiz, E. y González Río, M.J., 2009, *Jóvenes en las redes sociales virtuales. Un análisis exploratorio de las diferencias de género*, Revista Feminismo/s, nº º4, pp. 87-106.

Gabinete de Prensa de la AGPD, <<El Reglamento Europeo de protección de datos en 12 preguntas>>, nota de prensa, 2016 (http://www.agpd.es/portalwebAGPD/gabinete_prensa/notas_prensa/notas_prensa_indi

ce_2016/index-ides-idphp.php)

Guía para Centros Educativos de la Agencia Española de Protección de Datos (AEPD).- http://www.tudecideseninternet.es/agpd1/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf

Guía para formadores y familiares de la AEPD.- http://www.tudecideseninternet.es/agpd1/images/guias/Guia_formadores2016.pdf

Guía para profesores y padres de la AEPD.- http://www.tudecideseninternet.es/agpd1/images/guias/guia-formadores.compressed.pdf

Guía para jóvenes de la Agencia Española de Protección de Datos: "Sé legal en internet".- http://www.tudecideseninternet.es/agpd1/jovenes/guias/se-legal-en-internet.html#ficha-4-ciberbullying

Guía para jóvenes de la Agencia Española de Protección de Datos: "No te enredes en internet".- http://www.tudecideseninternet.es/agpd1/jovenes/guias/no-te-enredes-en-internet.html

Hernández López, J. M, 2013, *El derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*, Aranzadi.

Martínez Otero, J. M., 2016, *Derechos Fundamentales y Publicación de imágenes ajenas en las redes sociales sin consentimiento*, Revista Española de Derecho Constitucional, 106, enero abril, pp. 119-148.

Meseguer González, J.D, 2012, *Tratamiento y protección penal contra el ciberacoso escolar o cyberbullying*, El Derecho, versión digital: http://tecnologia.elderecho.com/tecnologia/ciberseguridad/Tratamiento-proteccion-ciberacoso-menores-cyberbullying_11_485680003.html

Niu, E., 2017, "*Facebook's WhatsApp Now Has 1.2 Billion Users. Time to Start Monetizing?", Nasdaq:* http://www.nasdaq.com/article/facebooks-whatsapp-now-has-12-billion-users-time-to-start-monetizing-cm746480

Pérez Sánchez, G., 2017, *Redes sociales y derecho a la propia imagen*, http://www.gerardoperez.es/redes-sociales-y-derecho-a-la-propia-imagen/

Prado, B. del, 2017, "Un adolescente de Gandía, víctima mortal de la 'ballena

azul”**,** Cadena Ser, versión digital: http://cadenaser.com/emisora/2017/09/22/radio_valencia/1506077201_604009.html

Requena, Félix, 1989, *“El concepto de red social”,* Reis, vol. 48, pp. 137-152, p. (http://www.reis.cis.es/REIS/PDF/REIS_048_08.pdf)

Ruiz Fájula, D., 2017, “*Una menor de Marbella, primera víctima del juego 'Ballena Azul' en Andalucía*”, El Mundo, versión digital: http://www.elmundo.es/andalucia/2017/05/18/591d91d322601df6728b45af.html

Sanmartín, O.R., 2015, *El “ciberacoso” comienza a los 10 años,* El Mundo, versión digital:

http://www.elmundo.es/espana/2015/10/14/561d590be2704e3a7e8b45fb.html

Smith, K., 2016, “96 estadísticas y datos increíbles de las redes sociales para 2016”, Brandwatch: https://www.brandwatch.com/es/2016/08/96-estadisticas-redes-sociales-2016/

Tynan, D., 2016, *“Facebook's journey ‘only 1% done’ after surge in revenue, Zuckerberg says”.* The Guardian: https://www.theguardian.com/technology/2016/jul/27/facebook-ad-sales-growth-quarterly-results

Enlaces

Página de la Agencia Española de Protección de Datos.-

(http://www.agpd.es/portalwebAGPD/index-ides-idphp.php)

Página de la Autoridad Catalana de Protección de Datos.-

http://apdcat.gencat.cat/es/inici/index.html

Página de la Agencia Vasca de Protección de Datos.-

http://www.avpd.euskadi.eus/s04-5232/es/

Página del Consejo de Europa.-

(https://www.coe.int/en/web/portal/home)

Página de la Comisión Europea.-

http://ec.europa.eu/justice/data-protection/index_en.htm

Página de la Federal Trade Comission.-

https://www.ftc.gov/

Página de la Comisión Europea, Documentación del Grupo del Artículo 29:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec15

Textos Normativos

Normas extraeuropeas

Children's Online Privacy Protection Rule ("COPPA"), EEUU, https://www.ftc.gov/sites/default/files/documents/federal_register_notices/childrens-online-privacy-protection-rule-16-cfr-part-312/990427childrensonlineprivacy.pdf

Children's Online Privacy Protection Rule: Final Rule Amendments To Clarify the Scope of the Rule and Strengthen Its Protections For Children's Personal Information
https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf

Normas Europeas y otros documentos de interés

La Declaración Universal de Derechos Humanos, proclamada por la Resolución 217 A (III), de 10 de diciembre de 1948, de la Asamblea General de las Naciones Unidas.

Versión Consolidada del Tratado de Funcionamiento de la Unión Europea, firmado en Roma el 25 de marzo de 1957, en Diario Oficial de la Unión Europea, C 83/47, de 30 de marzo de 2010.

Resolución 73 (22) de 26 de septiembre de 1973 del Consejo de Europa, respecto a “la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado”.

Resolución 73 (29) de 20 de septiembre de 1974 del Consejo de Europa, respecto a "la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público".

Convenio nº108 del Convenio de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. «DOCE» núm. 95, de 21 de abril de 1993, páginas 29 a 34.

Directiva 95/46/CE, del Parlamento Europeo y del Consejo de la Unión Europea, de 24 de octubre de 1995.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf

Opinion 5/2009 on online social networking, de 12 de junio de 2009, del Grupo de Trabajo del Artículo 29: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

Normas nacionales

Constitución Española de 1978.

Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal.

Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen

Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD).

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor

Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

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.

Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Boletín Oficial de las Cortes Generales de 24 de noviembre de 2017. http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF

Informes y Resoluciones de la AEPD

Informe 466/2004 del a AEPD sobre: *La comunicación a los padres de las calificaciones de sus hijos menores de edad*, en *Compendio LOPD par centros educativos,* Informes jurídicos, tutelas de derechos y preguntas más frecuentes, Gesdatos Software, S.L:

http://www.gesdatos.com/descargas/Compendio_LOPD_para_Centros_Educativos.pdf

Resolución 1359/2008 AEPD de 22 de noviembre de 2008. Procedimiento Nº PS/00330/2008.

Resolución 555/2009 AEPD de 30 de marzo de 2009. Procedimiento Nº PS/00508/2008.

Resolución 1663/2010 AEPD, de 30 de julio de 2010. Procedimiento Nº 23/2010.

Resolución 1486/2011 AEPD de 18 de julio de 2011. Procedimiento Nº PS/00045/2011.

Resolución 2636/2011 AEPD, de 22 de diciembre de 2011. Procedimiento Nº PS/00339/2011.

Resolución 580/2016 AEPD de 1 de marzo de 2016. Procedimiento Nº PS/00476/2016.

Resolución 2116/2016 AEPD de 30 de septiembre de 2016. Procedimiento Nº PS/00155/2016

Resolución 1988/2017 AEPD de 17 de julio de 2017. Procedimiento Nº 312/2017.

Resolución 1870/2017 AEPD, de 21 de agosto de 2017, Procedimiento Nº PS/00082/2017.

Resolución 2285/2017 AEPD, de 25 de octubre de 2017. Procedimiento Nº A/00286/2017.

Resolución 2699/2017 AEPD de 15 de noviembre de 2017. Procedimiento Nº PS/00235/2017

Jurisprudencia

Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre de 2000.

Sentencia de la Audiencia Nacional, 273/2004 de 21 de enero de 2004.

Sentencia del Tribunal Supremo, 4050/2010, Sala 3ª de lo contencioso administrativo de 15 de julio de 2010, consultada en:

Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014.

Sentencia de la Audiencia Provincial, 9805/2017 de 26 de octubre de 2017.