Universidad de Valladolid

Facultad de **Derecho**

Grado en **Derecho**

Protección de datos, menores de edad y redes sociales

Presentado por:

Carla González Gómez

Tutelado por:

Cristina Guilarte Martín-Calero

Valladolid, 30 de noviembre de 2023

ABREVIATURAS

- AEPD: Agencia Española de Protección de Datos.
- AN: Audiencia Nacional.
- Art: Artículo.
- C 108: Convenio número 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.
- CdE: Consejo de Europa.
- CE: Constitución Española.
- DNI: Documento Nacional de Identidad.
- DPD: Delegado de la Protección de Datos.
- DRAE: Diccionario de la Real Academia Española.
- EEE: Espacio Económico Europeo.
- EEUU: Estados Unidos de América.
- ET: Encargado del Tratamiento.
- LO: Ley Orgánica.
- LOPD: Ley Orgánica de Protección de Datos de Carácter Personal.
- LOPDGDD: Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.
- LORTAD: Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal.
- MF: Ministerio Fiscal.
- Pág.: Página.
- RGPD: Reglamento General de Protección de Datos.
- RLOPD: Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- RRSS: Redes Sociales.
- RT: Responsable del tratamiento.
- SS: Seguridad Social.
- STC: Sentencia.
- STJUE: Sentencia del Tribunal de Justicia de la Unión Europea.
- TC: Tribunal Constitucional.
- TEDH: Tribunal Europeo de Derechos Humanos.
- TFUE: Tratado de Funcionamiento de la Unión Europea.

- TIC: Tecnologías de la Información y Comunicación.
- TJUE: Tribunal de Justicia de la Unión Europea.
- UE: Unión Europea.
- Vid.: Vide (véase).
- Vol.: Volumen.

ÍNDICE

1-. RESUMEN.

A continuación, en nuestro trabajo de fin de grado, vamos a desglosar y a analizar el tema de la protección de datos en sí y en cómo afecta sobre los menores de edad, sobre todo en las redes sociales debido a la gran actividad que estos realizan en ellas desde hace unos años y como ha ido incrementándose hasta la actualidad. He desglosado las redes sociales más utilizadas por ellos para relacionarse, darse a conocer públicamente y como forma de entretenimiento; también en este trabajo he analizado las diferentes situaciones a las que se pueden ver expuestos incluyendo los riesgos que pueden sufrir y sus consecuencias; así como también la manera de ponerle solución utilizando las herramientas adecuadas tanto por parte del entorno educativo como en el ámbito familiar. Por otro lado, también he incluido las regulaciones legales tanto a nivel nacional como internacional y su aplicación en la materia para poder proteger de la mejor manera a los menores. Para concluir he añadido la forma de consentimiento en el tratamiento de datos de éstos.

2-. INTRODUCCION.

En el presente trabajo de fin de grado vamos a tratar sobre tres temas estrechamente relacionados y de plena actualidad debido a la importancia que ha cobrado la tecnología entre los más jóvenes. Nuestro tema versa sobre los menores, la protección de datos y las redes sociales. Vamos a explicar cómo se regula de manera especial todo aquello que tiene que ver con los menores, por ser un grupo considerado vulnerable y dónde el Reglamento General de Protección de Datos les otorga una protección específica, y cómo es la interacción de éstos con internet y las redes sociales.

Internet es una herramienta en pleno auge donde desde hace dos décadas no dejan de producirse avances debido a la nueva tecnología que va surgiendo, proporcionando así todo tipo de posibilidades y funcionalidades hasta el día de hoy, que es utilizado por los usuarios para absolutamente todo: compras, viajes, trabajo, negocios, relaciones sociales, entretenimiento, aprendizaje y una larga lista infinita. Es obvio e innegable que supone una manera de facilitarnos la vida cotidiana ahorrándonos mucho tiempo y llegando a posibilidades que sin ello no sería posible. Pero no todo son ventajas si no se da el uso adecuado y es por ello por lo que, si no hay un control de la red, se pueden producir graves

daños, tanto económicos en el ejemplo de las estafas, muy a la orden del día en internet; como psicológicos e incluso físicos en el caso del ciberacoso o ciberbullying, grooming o sexting, entre otros.

Pero este tipo de consecuencias negativas se agravan aún más cuando las víctimas que lo padecen son menores de edad, es por ello que en este trabajo vamos a tratar de explicar cuánto de importante es la vigilancia, tanto en el entorno familiar como en los centros educativos, del acceso a las tecnologías de la información y comunicación (TIC) y cómo se pueden disponer de ciertos límites para que los menores no puedan o tengan que pasar ciertos filtros para poder acceder a contenidos inadecuados. También vamos a mencionar cómo detectar en ellos comportamientos que, conociendo la información sobre los riesgos, pueden darnos indicios claros de que estén siendo víctimas de alguna de las situaciones mencionadas anteriormente.

En lo referente a los datos personales de los menores de edad se pueden tratar siempre y cuando se respete lo dispuesto en el RGPD y en la LOPDGDD (Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales) en cuanto a derechos obligaciones y consentimiento; además también se debe tener en consideración la Ley Orgánica 8/2021 referida a la protección integral de la infancia y la adolescencia frente a la violencia, conocida como ley de protección de menores, donde se hace referencia a contenidos ilícitos o violentos que afecten a los menores publicados en internet.

En cuanto a la protección de los menores en internet la LOPDGDD en su artículo 82 recoge que los padres o tutores legales de los menores deben asegurarse de que estos hagan un uso equilibrado y responsable de los dispositivos digitales y así esto garantizar un desarrollo adecuado de su personalidad y para preservar su dignidad y derechos fundamentales.

También va a garantizar la protección específica del menor y su derecho a la protección de datos en centros educativos o cualquier otro lugar donde desarrolle sus actividades, así como va a hacer referencia a la vigilancia sobre información personal o el uso y difusión de imágenes en redes sociales solicitando la intervención del Ministerio Fiscal en defensa del menor afectado cuando así convenga.

Por consiguiente, vamos a continuar con el análisis específico en la interacción de los menores de edad con las TIC y cómo actúa la protección de datos para ellos, ya que, debido a la rápida evolución de internet, se han convertido en una herramienta de uso diario

produciéndose su acceso con edades cada vez más tempranas fijándose la franja entre los 8 y 10 años o incluso antes en ciertas aplicaciones como WhatsApp o TikTok

3-. CONCEPTO Y TIPOS DE DATOS PERSONALES.

3.1-. Concepto y clasificación de los datos personales.

Para poder definir correctamente el concepto de datos personales nos vamos a remitir a la ley donde podemos encontrar su regulación, que es la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales[1] (en adelante, LOPDGDD), así como el 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[2] (en adelante, RGPD). La LOPDGDD recoge el concepto de datos definido como "cualquier información concerniente a personas físicas identificadas o identificables", es decir, "cualquier información que permita identificarse directa o indirectamente a una persona física".

Según el Diccionario de la Real Academia de la Lengua (DRAE)[3], el término Protección de Datos se define como "un conjunto de medidas para garantizar y proteger los datos de carácter personal; que es cualquier información concerniente a personas físicas identificadas o identificables, registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores público y privado, a los efectos de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

Este tipo de medidas se van a basar en los derechos de las personas a la impugnación de valoraciones, el derecho de información, en la recogida de datos, el consentimiento del afectado, los datos relativos a la salud, la seguridad de los datos, el deber de secreto, el acceso a los datos por parte de terceros, etc.…

En el artículo 4.1 del RGPD encontramos diferentes definiciones y entre ellas, se hace alusión al término "identificable". Con identificable se refiere a cuando una persona puede ser

[1] España. Ley Orgánica 3/2018, de 5 de diciembre, Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado, de 6 de diciembre de 2018, núm. 294 (última consulta el 21 de marzo de 2023). Disponible on-line en https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[2] Reglamento (UE) 2016/679, de 27 de abril, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, n.º L119/1, de 4 de mayo de 2016.

[3] https://dpej.rae.es/lema/protecci%C3%B3n-de-datos (última consulta 28 de marzo de 2023).

identificada, directa o indirectamente, especialmente mediante un identificador como, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de esa persona.

Establece, además, que los datos personales son información confidencial y privada y están protegidos por el derecho fundamental a la protección de datos personales, y que su tratamiento debe realizarse de manera transparente, lícita y con respeto a los derechos y libertades fundamentales de las personas. Además, la ley establece la obligación de garantizar la privacidad, integridad y disponibilidad de los datos personales durante su tratamiento.

En la actualidad, cada vez más personas y empresas recopilan datos personales, como nombres, direcciones, números de teléfono, correos electrónicos y detalles financieros. Esto puede tener consecuencias negativas para nuestra privacidad, seguridad y reputación si no son utilizados y tratados con la suficiente cautela que requiere, y por ello deben tomar las medidas oportunas para protegernos de situaciones como el espionaje, robo de identidad, acoso, entre otras y obtener siempre el consentimiento informado antes de utilizar o compartir dichos datos personales.

En cuanto a la clasificación de los datos personales es importante porque permite a las empresas y organizaciones identificar y gestionar adecuadamente los datos que manejan, aplicando las medidas de seguridad y privacidad adecuadas según su categoría. Por ejemplo, la clasificación de los datos personales, entre las que se encuentra la categoría de datos sensibles, ayuda a las empresas y organizaciones a identificar los datos que requieren una protección especial, como los datos de salud o la afiliación política, y así garantizar su protección y cumplir con las obligaciones legales y reglamentarias recogidas en la LOPDGDD y en el RGPD en su artículo 9, así como en diferentes considerandos como pueden ser el 51, 53, 54, 56 y 71.

A continuación, vamos a presentar una clasificación[4] común de las diferentes categorías en las que podemos encuadrar los datos personales debido a su sensibilidad, vulnerabilidad y al riesgo de discriminación o prejuicios que puede provocar en un individuo y que podemos encontrar encuadrada en el artículo 4 RGPD, en diferentes de sus apartados:

[4] Art. 4 de RGPD.

- Datos personales sensibles: son aquellos que revelan información sobre la salud, origen étnico o racial, creencias religiosas o filosóficas, orientación sexual, entre otros aspectos que puedan generar discriminación o prejuicios (Art. 9 RGPD)
- Datos personales identificativos: permiten identificar directamente a una persona, como el nombre, número de identificación, fecha de nacimiento, entre otros.
- Datos personales médicos: nos aportan información sobre informes, alergias, condiciones o registros médicos.
- Datos personales de contacto: permiten contactar a una persona, como la dirección correo electrónico o número de teléfono
- Datos personales financieros: se refieren a la situación económica de una persona, como ingresos, préstamos hipotecarios, deudas, cuentas bancarias, entre otros.
- Datos personales de ubicación: permiten conocer la ubicación de una persona, como la dirección de su domicilio o el registro de su localización a través de dispositivos móviles.
- Datos personales laborales: aquellos que se refieren a la situación laboral de una persona, como su historial laboral, experiencia profesional, cargo actual, entre otros.

3.2-. Datos sensibles.

Los datos sensibles o datos especialmente protegidos son una categoría de datos que, debido a su incidencia en los derechos fundamentales, libertades públicas e intimidad de las personas, necesitan una protección mucho más severa, ciertos requisitos especiales y un tratamiento más cuidadoso que el resto de los datos por la trascendencia que puede suponer a los usuarios su revelación. Estos datos sensibles quedan recogidos tanto en el RGPD como en la LOPDGDD.

El art. 4 y el art. 9 del RGPD señalan como datos sensibles a aquellos que revelen información sobre la ideología, religión, afiliación sindical, creencias, salud, origen racial o étnico, vida sexual, datos genéticos y biométricos, así como datos relativos a condenas e infracciones penales (los cuales se recogen en el art.10 del RGPD). También aparecen recogidos en varios considerandos del art. 9 del RGPD.

Por otro lado, en el art.9 LOPDGDD, se establece un especial tratamiento para esta categoría de datos que podemos resumir de la siguiente manera[5]:

Quedará prohibido el tratamiento de los datos personales anteriormente mencionados salvo que se produzca alguna de las siguientes circunstancias y siempre aplicando las medidas de seguridad oportunas:

- Que se haya otorgado consentimiento explícito por parte del interesado y con la finalidad especificada.
- Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del ámbito laboral y la seguridad y protección social.
- Que el tratamiento sea necesario para la protección de intereses vitales del interesado, en el supuesto de que éste no esté capacitado física o jurídicamente para dar su consentimiento.
- Que el tratamiento sea efectuado en el ámbito de fundaciones o asociaciones cuya finalidad sea política, filosófica, religiosa o sindical.
- Que el tratamiento se refiera a datos personales que el interesado ha hecho manifiestamente públicos.
- Que el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.
- Que el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública.
- Que el tratamiento sea necesario con fines de archivo e interés público, fines de investigación científica o histórica o fines estadísticos.

Podemos decir entonces que, en España, la LOPDGG es más exigente que el RGPD para el tratamiento de estos datos y que además del consentimiento explícito, se requieren otro tipo de requisitos que vamos a mencionar a continuación:

- Creación de un registro de actividades de tratamiento, de manera que obligue a un responsable o encargado a tenerlo actualizado y queden así registrados todos estos datos.
- Designación de un delegado de protección de datos.

[5] Art.9 de LOPDGDD. Disponible on-line en https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673 (última consulta el 17 de mayo de 2023).

- Se efectuará una evaluación de impacto, que es un análisis del riesgo que puede suponer el tratamiento de dichos datos para los derechos y libertades fundamentales.
- Y, por último, se aplicarán las medidas de seguridad adecuadas para la protección de éstos como puede ser el cifrado de datos, el registro de accesos con fecha y personal que accedió la elaboración de una lista de personas autorizadas o establecer un procedimiento seguro para su tratamiento[6].

3.3-. Titulares de los datos personales y principios básicos de la Protección de Datos.

El término que vamos a utilizar para referirnos a los individuos cuyos datos son objeto de tratamiento va a ser el de "interesados". A lo largo de la historia, desde que se ha empezado a tratar la protección de datos, han ido siendo definidos de diferentes formas; en las primeras regulaciones se referían a los titulares de datos como "personas concernidas" o "sujetos de datos", pero es con la directiva 95/46/CE donde se empiezan a denominar como interesados, afectados o usuarios[7]. Vamos a hacer una distinción entre personas físicas y personas jurídicas.

En el derecho de la Unión Europea, tanto el art. 1 del RGDP, como el Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento de Datos Personales; conocido como Convenio 108 modernizado, consideran como interesados a las personas físicas, siendo así las únicas beneficiarias de las normas de protección de datos. Las personas jurídicas también gozan de cierta protección y podemos encontrar jurisprudencia sobre ello, donde la protección se puede extender a personas jurídicas como empresas y asociaciones en su Derecho Nacional. Sin embargo, a diferencia del Convenio 108 modernizado, la legislación de la UE sobre protección de datos "no cubre el tratamiento de datos que conciernan a personas jurídicas, y en particular no afecta a las empresas establecidas como personas jurídicas. No obstante, la directiva sobre la privacidad

[6] Datos especialmente protegidos. Disponible on-line en https://protecciondatos-lopd.com/empresas/datos-especialmente-protegidos-sensibles/#Que_son_los_datos_sensibles_o_especialmente_protegidos (última consulta el 17 de mayo de 2023).

[7] GARCIA ESPOSITO, A.L., Tesis doctoral sobre "El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (En busca del equilibrio entre la libertad y la seguridad)" con fecha del 24 de julio de 2014. Disponible on-line en https://www.tdx.cat/handle/10803/284352#page=257 pp. 253-265.

y las comunicaciones electrónicas sí protege la confidencialidad de las comunicaciones y los intereses legítimos de las personas jurídicas en relación con el incremento de la capacidad de almacenamiento y tratamiento automatizado de datos relativos a abonados y usuarios"[8].

Otro de los aspectos que vamos a tratar en este epígrafe va a ser los principios fundamentales[9] relativos al tratamiento de los datos personales, y a como su cumplimiento es esencial para garantizar la privacidad y seguridad de la información personal; en caso de imponerles una limitación, deberá establecerse por ley, servir a un fin legítimo y ser una medida necesaria y proporcionada. De esta manera tanto el RGPD en su art. 5, como los artículos 5, 7, 8 y 10 del Convenio 108 modernizado del Consejo de Europa (CdE en adelante) recogen los siguientes principios:

3.3.1-. Principio de licitud, lealtad y transparencia[10]*:* en el art.5.1.a) del RGPD se recoge que los datos personales serán tratados de manera lícita, leal y transparente con relación al interesado. Estrechamente relacionado, el art. 6 del RGPD, especifica que el tratamiento solo se considerará lícito si se cumple al menos una de las siguientes condiciones: que el interesado haya dado su consentimiento, que deberá ser tácito, inequívoco, y en ciertas ocasiones expreso o incluso por escrito; que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte; que el tratamiento sea necesario para el cumplimiento de una obligación legal; para proteger intereses vitales del interesado o de otra persona física; para el cumplimiento de una misión para un interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.
Este principio excluye el tratamiento de datos que hayan podido ser obtenidos de forma desleal o sin proporcionar toda la información necesaria sobre los fines, consecuencias o posibles riesgos, obligando así a los responsables a tratarlos con la mayor transparencia y deben ser capaces de demostrar que las operaciones de tratamiento no se han realizado en secreto. Como ejemplo podemos decir que una empresa de luz, gas o cualquier otro servicio, no podrá utilizar los datos personales de un individuo para realizar una contratación

[8] Manual de legislación europea en materia de protección de datos. Edición de 2018. Disponible on-line en https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf (última consulta el 19 de abril de 2023). Pp. 96-98.

[9] Manual de legislación europea en materia de protección de datos. Op. Cit., pp. 133-153.

[10] Manual de legislación europea en materia de protección de datos. Op. Cit., pp. 134-138.

fraudulenta de un servicio que éste no ha solicitado[11]. Este principio está vinculado a la ética en el tratamiento de los datos personales.

En cuanto al último precepto de este principio referido a la transparencia, se determina en el capítulo III de los Derechos del Interesado que "los responsables del tratamiento utilizarán un lenguaje claro y sencillo para que pueda ser entendido en todos sus sentidos, con los riesgos que pueda suponer, las normas, las salvaguardias y los derechos que les pertenecen, así como deben informar sobre la finalidad del tratamiento, dirección, identidad, etc."[12].

3.3.2-. Principio de limitación de la finalidad[13]: es uno de principios fundamentales de la protección de datos, el RGPD en su art. 5.1.b) nos dice que "los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines" y por supuesto, permitidos por el ordenamiento jurídico. El RGPD prohíbe el tratamiento de datos para fines que no sean compatibles, es decir, no puede realizarse un tratamiento posterior que sea incompatible con la finalidad original, aunque existen excepciones siempre y cuando se cumplan ciertos requisitos, que en este momento no vamos a tratar.

Como ejemplo de este principio podemos poner un centro de belleza que recoge y almacena los datos de sus clientes, pero una vez que una persona deja de ser cliente de ese centro, la finalidad para la que se recogieron esos datos no existe y por lo tanto deben ser eliminados.

3.3.3-. Principio de minimización de los datos[14]: se refiere a que "únicamente se van a tratar los datos que sean adecuados, pertinentes y no en relación con el fin para el que se obtienen o tratan"[15]. No se recogerán datos que no sean necesarios para el objetivo que se persigue; como ejemplo podríamos decir que, en un taller de coches, sería innecesario solicitar a un cliente, los datos de la nómina laboral para un servicio como puede ser la reparación de una rueda. La solicitud de datos personales tiene que ser acorde al fin legítimo perseguido y aquellos que no sean proporcionados, serán considerados excesivos.

---

[11] Guía de protección de datos para el ciudadano de la Agencia Española de Protección de Datos. Disponible on-line en https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf (última consulta el 20 de abril de 2023), pp. 7-9.

[12] Considerando 39 del RGDP.

[13]Manual de legislación europea en materia de protección de datos. Edición de 2018. Op. cit., pp. 139-142.

[14] Manual de legislación europea en materia de protección de datos. Edición de 2018. Op. cit., pp. 142-145.

[15] Art. 5.1.c) del RGPD. Art. 5.4.c) del Convenio 108 modernizado.

3.3.4-. Principio de exactitud de los datos[16]: "El responsable del tratamiento que disponga de información personal no utilizará dicha información sin adoptar medidas que garanticen, con una certeza razonable, que los datos son exactos y están actualizados"[17].

Los datos que sean inexactos o que por cualquier motivo hayan quedado desactualizados, deberán ser suprimidos o modificados a la mayor brevedad posible para evitar así cualquier tipo de confusión; en una empresa de servicios, el tener desactualizada la dirección de facturación de uno de sus clientes puede ocasionar pérdidas económicas entre otros perjuicios.

3.3.5-. Principio de limitación del plazo de conservación[18]: "Los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos, podrán conservarse durante períodos más largos siempre que tengan fines de archivo en interés público, de investigación científica o histórica o estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el Reglamento para proteger los derechos y libertades del interesado"[19]. Por lo tanto, el responsable del tratamiento suprimirá los datos cuando se hayan cumplido dichos fines, para que no se conserven más del tiempo estrictamente necesario; y además a la hora de recabar tus datos personales será éste el que deberá informar sobre su período de conservación. La única forma lícita de conservar datos que hayan dejado de ser necesarios es la anonimización de éstos; y también el Convenio 108 permite ciertas excepciones a este principio, siempre y cuando estén establecidas por ley y respetes los derechos y libertades fundamentales y sea para perseguir una serie de fines legítimos como la protección de la seguridad nacional, la investigación y enjuiciamiento de delitos penales, la ejecución de sanciones penales, la protección del interesado y la protección de los derechos y libertades fundamentales de otras personas[20].

---

16 Manual de legislación europea en materia de protección de datos. Edición de 2018. Op. cit., pp. 145-146.

17 Art. 5.1.d) del RGPD. Art 5.4.d) del Convenio 108 modernizado.

18 FERNANDEZ GONZALEZ, C.M., en "Estudio sobre el sistema de protección de datos personales con finalidad de prevención, detección e investigación policial de infracciones penales". Madrid, 2022. Disponible on-line en https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/seguridad-ciudadana/Estudio_sobre_el_sistema_de_proteccion_de_datos..._126220091.pdf (última consulta el 29 de mayo de 2023).

19 Art. 5.1.e) del RGPD. Art 5.4.e) del Convenio 108 modernizado.

20 Art 9.1 del Convenio 108 modernizado.

3.3.6-. Principio de integridad y confidencialidad[21]*:* este principio requiere la aplicación de ciertas medidas para proteger los datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito[22]. La seudonimización y el cifrado de los datos son medidas que pueden garantizar la seguridad de éstos; esta técnica consiste en sustituir los atributos que contienen los datos personales por un seudónimo, y mantener dichos atributos separados aplicando medidas organizativas[23]; es un proceso diferente al de la anonimización donde se elimina cualquier vínculo que identifique a una persona; mejora la privacidad y se recomienda para reducir los riesgos de los interesados y para ayudar a los encargados y responsables de los datos a cumplir con sus obligaciones, así queda especificado en el Considerando 28. Como ejemplo de seudonimización podemos poner el siguiente: Carlos González, ha sido el conductor que ha atropellado a dos personas ---- C.G., ha sido el conductor que ha atropellado a dos personas.

3.3.7-. Principio de responsabilidad proactiva[24]*:* tanto en el art.5.2 del RGPD como en el Convenio 108 modernizado se estable que el responsable del tratamiento de los datos personales será el encargado de asegurar el cumplimiento de este principio, aplicando medidas técnicas y organizativas; y también le atribuye esta función de responsabilidad al encargado del tratamiento. Entre estas medidas se encuentran el análisis de riesgo con la finalidad de adoptar las correspondientes medidas de seguridad, el registro de actividades de tratamiento, la notificación de brechas de seguridad o la realización de evaluaciones de impacto de protección de datos. Este principio exige determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

---

[21] Principio de confidencialidad en la LO 3/2018 (LOPDGDD) y en el Reglamento general de protección de datos (RGPD). Disponible on-line en https://www.iberley.es/temas/principio-confidencialidad-lopdgdd-rgpd-62808 (última consulta el 28 de mayo de 2023)

[22] Art 5.1.f) del RGPD y Considerando 39. Art. 7 del Convenio 108 modernizado.

[23] Art 32.1 del RGPD.

[24] Manual de legislación europea en materia de protección de datos. Edición de 2018. Op. cit., pág. 153.

4-. OBJETO Y REGULACION DE LA PROTECCION DE DATOS.

En este apartado vamos a analizar la evolución y regulación a la que se han ido sometiendo los datos personales debido a la importancia que han cobrado en la era digital, donde la información personal se almacena y se comparte en línea con frecuencia. Las leyes y regulaciones de protección de datos se han desarrollado en muchos países para garantizar que los datos personales estén protegidos y que las empresas y organizaciones que recopilan y utilizan esta información cumplan con los estándares adecuados de privacidad y seguridad.

Esta protección ha cobrado gran importancia debido a que los almacenamientos de datos crecen desmesuradamente con las nuevas tecnologías y es por eso por lo que está regulada en las siguientes leyes para poder preservar al usuario, su confidencialidad e integridad.

La primera vez que se hizo referencia al derecho fundamental a la protección de datos personales fue en la Constitución Española de 1978 en su art. 18.4, configurándose ésta como norma suprema y venía anticipándose a los riesgos que podía suponer la informática y su evolución; en este artículo reconoce este derecho fundamental diciendo que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[25].

A continuación, vamos a realizar un breve resumen cronológico sobre la evolución a la que se ha ido sometiendo la regulación de la protección de datos:

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD). Es el primer antecedente en nuestro país referido a la protección de los datos personales refiriendo en su art. 1 que su objeto era "limitar el uso de la informática junto con otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para así poder garantizar el derecho al honor a la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos".

[25] https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia (última consulta el 3 de abril de 2023)

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y su Reglamento de Desarrollo. Conocida como LOPD, aprobada por las Cortes Generales y con fundamento también en el art. 18.4 de la Constitución Española al igual que la LORTAD, ratificada posteriormente por la Sentencia 292/2000 del Tribunal Constitucional. Esta ley fue considerada pionera en cuanto a la protección de las personas físicas en relación con el tratamiento de datos personales, anteriormente denominado "habeas data"; supuso una gran evolución de la regulación del derecho fundamental a la protección de datos en España y se fue complementando después con jurisprudencia de los órganos de la jurisdicción contencioso-administrativa[26].

Su objetivo principal era el tratamiento de los datos de carácter personal y los ficheros donde éstos estaban recogidos independientemente de su soporte, también trataba de regular los derechos de las personas físicas y obligaciones de aquellos que se ocupaban de los ficheros y trataban los datos, ya fueran responsables o encargados de su tratamiento.

Su marco normativo fue completado por la aprobación del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, al que se conoce como RLOPD. Esta ley adaptó nuestro ordenamiento a lo dispuesto por la directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en cuanto al tratamiento de datos personales y de la libre circulación de estos derogando la anterior Ley Orgánica 5/1992, de 29 de octubre.

En su art. 1 prevé "garantizar y proteger, en lo que concierne al tratamiento de los datos personales las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal". La importancia que el legislador otorga a su objeto hace que subsistan ciertas normas reglamentarias y en concreto, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos y el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, entre otros.

[26] DE LA FUENTE MIGUELEZ, A., "El estatuto de los titulares de datos personales y la función estadística pública", en Estadística Española, Volumen 60, número 196/2018, pp. 89-90. Disponible on-line en https://www.ine.es/ss/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=ContentDisposition&blobheadervalue1=attachment%3B+filename%3Dart_196_1.pdf&blobkey=urldata&blobtable=MungoBlobs&blobwhere=616%2F339%2Fart_196_1%2C0.pdf&ssbinary=true (última consulta el 24 de abril de 2023)

4.1-. El Reglamento General de la Protección de Datos (RGPD).

Actualmente en España la disposición general vigente sobre la protección de datos personales es el RGPD, su aplicación data del 25 de mayo de 2018, pese a ser aprobado el 27 de abril de 2016; y con él se deroga la anterior Directiva 95/46/CE (Reglamento general de protección de datos). Se comienza a aplicar por encima y con preferencia de cualquier otra norma que haya sido previamente aceptada sin necesidad de legislación anterior alguna, ya que tiene un carácter internacionalmente imperativo y supone una unificación llamada a sustituir a las legislaciones nacionales, salvo en determinados aspectos[27].

Recoge en su art. 2.1 como derecho fundamental de la protección de datos a las personas físicas en lo que respecta al tratamiento de sus datos, independientemente de su nacionalidad o lugar de residencia y respetando siempre sus derechos y libertades; excluye el tratamiento de los datos personales de toda persona jurídica y en concreto a empresas constituidas como tal; mientras que en el art. 18.4 de la Constitución Española, el derecho fundamental que se recoge es el de los ciudadanos.

Se ha marcado como uno de sus objetivos contribuir al logro de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas, y así se establece en el apartado 2 de dicho Reglamento[28].

También en él se recoge la protección de los datos relativos a empresarios individuales, pero únicamente cuando no actúen en calidad de comerciantes industriales o navieros ya que cuando esto sea así quedarán excluidos de este régimen de protección.

Este reglamento no incluye la protección de los datos referidos a personas fallecidas así que de este modo las personas vinculadas al fallecido podrán dirigirse a los ficheros o tratamientos que contengan datos de éste para notificar la defunción siempre y cuando aporten la documentación necesaria para acreditar la vinculación con la persona fallecida, pero sobre este tema también haremos un desarrollo más profundo más adelante.

---

[27] MIGUEL ASENSIO, P.A., en "Competencia y derecho aplicable en el Reglamento General sobre protección de Datos de la Unión Europea". Revista Española de Derecho Internacional, Vol. 69, Tomo I, 2017. Pp. 75-77.

[28] DE LA FUENTE MIGUELEZ, A., Op. cit., pp. 89-90.

4.1.1-. Principales aspectos y modificaciones incluidos en el RGPD:

Como ya hemos mencionado anteriormente el Reglamento desarrolla el derecho originario de protección de datos como derecho de fondo e intenta mantener la seguridad jurídica y práctica de las personas[29]. La sustitución de la Directiva 95/46/CE por el actual Reglamento supone la homogenización de este derecho en todo el territorio de la Unión, solventando así las diferencias tanto formales como prácticas creadas entre los Estados europeos debido al amplio margen de autonomía del que disponían y facilitando la libertad de circulación de los datos. De esta manera, el Reglamento establece en sus art. 60 a 64 los mecanismos de control y cooperación entre las autoridades de control.

A través del RGPD se pretende dar protección también a otro tipo de derechos como son el derecho a la intimidad, el respeto de la vida privada y familiar, del domicilio y las comunicaciones, el derecho al honor y a la personalidad; pero por otro lado colisiona con otro tipo de derechos como puede ser la libertad de expresión, de acceso y difusión de la información o la libertad de circulación de esos datos[30].

El uso de la Directiva suponía la aplicación de los derechos nacionales de cada Estado creando así una desigualdad e inseguridad jurídica en el territorio de la Unión, en la cual tuvo que tomar partido el Tribunal de Justicia en diferentes sentencias, como por ejemplo la conocida "Google Spain"[31], para poder solucionar las controversias surgidas. Otra de las modificaciones introducidas por el Reglamento se encuentra en el art. 3 donde define su ámbito de aplicación territorial como norma aplicable en forma directa, lo que significa que es una norma íntegra que solo requiere de normas complementarias para su desarrollo y que la completen en los aspectos de regulación estatal[32].

---

[29] Considerando 7 del RGPD.

[30] REYES KAHANSKY, C.M., en Tesis Doctoral sobre "Vigencia del Derecho Europeo de Protección de Datos personales", pp. 121-126.

[31] Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, en asunto C131/12; que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Audiencia Nacional, mediante auto de 27 de febrero de 2012, en el procedimiento entre Google Spain, S.L., Google Inc. y la Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

[32] Directrices 3/2018 relativas al ámbito territorial del RGPD. Art.3. Versión 2.1 del 12 de noviembre de 2019. Disponible on-line en https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_es.pdf (última consulta el 24 de mayo de 2023).

A continuación, vamos a enumerar algunos de los rasgos fundamentales del RGPD[33]:

1. Consentimiento: las organizaciones deben obtener el consentimiento explícito de los individuos para procesar sus datos personales, y debe ser siempre libre, inequívoco, informado y no se acepta como válido el consentimiento tácito.
2. Derechos de los individuos: los individuos tienen el derecho de acceder, rectificar, suprimir, que es el llamado derecho al olvido, limitar y transferir sus datos personales.
3. Notificación de violaciones de datos: las organizaciones deben notificar a las autoridades competentes y a los individuos afectados en caso de violaciones de seguridad que impliquen datos personales en un plazo máximo de 72 horas.
4. Protección de datos por defecto: las organizaciones deben diseñar sus sistemas personales y procesos para proteger los datos por defecto y por diseño registrando todas las actividades que contengan ciertos datos.
5. Responsabilidad: las organizaciones deben tomar medidas adecuadas para proteger los datos personales y son responsables en caso de incumplimiento.
6. Transferencias internacionales: las organizaciones deben garantizar que los datos personales transferidos fuera de la Unión Europea estén protegidos de acuerdo con las normas del RGPD.

4.1.2-. Los derechos de los interesados.

En este epígrafe vamos a tratar sobre los derechos de los interesados que se encuentran regulados en el RGPD, en concreto, lo referente a los derechos ARCO y el derecho al olvido. Estas siglas hacen referencia a los derechos de acceso, rectificación, cancelación (supresión) y oposición. Y además vamos a referirnos a nuevos derechos que han sido añadidos con la incorporación del RGPD, como son el derecho a la limitación de datos o el de portabilidad.

El derecho de acceso se establece en el art. 15 de dicho reglamento otorgando pleno derecho al interesado para poder obtener del responsable del tratamiento la confirmación de si se están tratando sus datos personales. Tiene una doble vertiente, primero saber si alguna entidad o responsable tiene datos de los interesados o no y segundo, en caso de que la respuesta sea afirmativa poder tener cierta información sobre ello, como pueden ser los fines del tratamiento, las categorías, los destinatarios a los que se les puede comunicar los datos,

[33] GÓMEZ VIEITES, A., "Principales aspectos del Reglamento General de Protección de Datos (GDPR) de la Unión Europea" dispone on-line en: https://contactcenterhub.es/principales-aspectos-del-nuevo-reglamento-general-de-proteccion-de-datos-2016-01-5217/#Alvaro_Gomez_Vieites_consultor_de_Seguridad_Informatica_en_INPROSEC (última consulta el 24 de mayo de 2023)

especialmente si se trata de terceros países u organizaciones internacionales[34]. También implica conocer el plazo previsto de conservación, las opciones para el ejercicio del derecho de rectificación o cancelación y las autoridades de control a las que dirigirse para presentar una posible reclamación. Cuando estos datos sean transferidos a terceros países u organizaciones internacionales, el interesado tendrá derecho a ser informado de las garantías correspondientes. El responsable del tratamiento está obligado a facilitar una copia de los datos que sean objeto de tratamiento.

El derecho de rectificación se recoge en el art. 16 y realizará sin demora injustificada. Se relaciona con el principio de exactitud, y esto quiere decir que los datos que estén incluidos en un fichero deben de ser exactos y actualizados; de esta manera si en un fichero hay datos inexactos o incompletos, los usuarios tienen el derecho de solicitar su rectificación para que sean correctos, justificando su solicitud con la documentación pertinente.

El derecho de supresión se recoge en el art. 17, llamado derecho de cancelación anteriormente con la ley orgánica de 1999 y conocido en la actualidad como derecho al olvido, sobre el que vamos a profundizar más adelante por la importancia que adquiere en internet. Otorga el derecho al usuario de poder solicitar al responsable, la eliminación de sus datos del fichero; no se va a poder ejercer siempre ni en todos los supuestos, pero existe una lista en los que sí vamos a poder utilizarlo. La primera de ellas incluida de forma expresa en este artículo y que se refiere a aquellos datos que ya no sean necesarios en relación con los fines para los que se recogieron. Las siguientes circunstancias serían que el interesado retirara su consentimiento; que éste se oponga al tratamiento, relacionado con el art.21 de dicho Reglamento[35]; que los datos hayan sido tratados de manera ilícita, que los datos deban suprimirse para el cumplimiento de una obligación legal o que se hayan obtenido en relación con la oferta de servicios de la sociedad de la información. Este derecho está estrechamente relacionado con el derecho al olvido, recogido en el artículo

[34] https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf (última consulta el 20 de mayo de 2023).

[35] En dicho art.21 del RGPD se hace referencia al derecho de oposición y establece que el interesado dispondrá de un verdadero derecho a oponerse en cualquier momento justificándolo con su situación particular. Asimismo, el responsable del tratamiento dejará de tratar los datos personales del interesado, salvo motivos legítimos que prevalezcan sobre los intereses, derechos y las libertades del interesado. Además, el interesado podrá ejercer este derecho por medios automatizados.
Cuando los datos personales se traten con fines de investigación, el interesado tendrá derecho a oponerse salvo que sea necesario para el cumplimiento de una obligación pública.

El derecho a la limitación del tratamiento queda recogido en el art.18, es un derecho relativamente nuevo ya que no estaba regulado en la anterior ley orgánica; se refiere a la paralización del tratamiento durante un tiempo determinado en ciertas ocasiones, de las cuales vamos a poner algún ejemplo a continuación: cuando queramos impugnar la exactitud de nuestros datos a una empresa u organización, a la misma vez ejerceremos este derecho para poder hacer la comprobación requerida y el tratamiento de nuestros datos quedará paralizado; una vez que se dilucide si son o no exactos se podrán volver a tratar. Otro ejemplo es que el tratamiento haya sido ilícito pero el interesado se oponga a la supresión de éstos solicitando en su lugar la limitación del tratamiento.

El derecho de la portabilidad de datos se regula en el art.20 y es un derecho novedoso con nueva regulación. En él encontramos la posibilidad de poder solicitar al responsable del tratamiento de nuestros datos su traspaso directo a otro responsable cuando sea técnicamente posible a través de formatos interoperables que permitan su portabilidad, pero el RGPD no exige un formato concreto; esto quiere decir que no se aplicará en situaciones en que el tratamiento de los datos personales tenga un fundamento jurídico que no sea el consentimiento o un contrato[36]. El derecho a la portabilidad de datos respalda la elección, el control y la capacitación de los usuarios para que los interesados tengan control sobre sus propios datos personales[37].

El derecho de oposición, el art. 21 refiere a este derecho en sentido estricto y el art. 22 referido a las decisiones individuales automatizadas, ambos estrechamente relacionados. El derecho de oposición nos proporciona el derecho de poder oponernos a que se traten nuestros datos, no se puede ejercer siempre ni en todo caso y vienen recogidos una serie de supuestos, como ejemplo para poder entender mejor este derecho, diremos que tenemos el derecho de oponernos a que un responsable utilice nuestros datos para fines de mercadotecnia directa, como puede ser la publicidad por teléfono. En cuanto a los derechos relacionados con las decisiones individuales automatizadas[38], son algoritmos que analizan, de forma totalmente automatizada, información de las personas con el objetivo de determinar patrones de conducta, de personalidad, preferencias, gustos, temas de localización para

[36] Considerando 68 del RGPD.

[37] Grupo de Trabajo del Artículo 29 "Directrices sobre el derecho a la portabilidad de los datos", WP 242, diciembre de 2016, pág.13. (Última consulta el 27 de mayo de 2023)

[38] Manual de legislación europea en materia de protección de datos. Edición de 2018. Op. cit., pp. 264-266.

intentar revelar aspectos relevantes de las personas físicas y así puedan tomar decisiones que nos afecten. Muy relacionado con la elaboración de perfiles donde en su propio art.4.4 define como "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física". Como ejemplo podemos poner la actuación que hace la banca, que es el *scoring*, que son algoritmos que trabajan en función de la información financiera de sus clientes, y que les otorga una nota o puntuación y dependiendo de ella hacen la toma de decisiones como conceder o no una hipoteca, dar un tipo u otro de interés, etc. Este derecho nos da la posibilidad a oponernos a que se tomen estas decisiones basadas únicamente en esos perfiles[39].

4.1.3-. El derecho al olvido.

En un primer momento este derecho surge en una época anterior a la era de internet y es definido como el derecho que tiene un individuo a que no se publiquen informaciones relacionadas con asuntos que lo incumban y que anteriormente hubieran sido publicadas legítimamente cuando haya pasado un periodo importante de tiempo, y se refiere a acontecimientos de interés o hechos públicos.

Con la aparición de internet este concepto se ha hecho popular en los últimos años y además ha ido sufriendo modificaciones. Con esta expresión se hace referencia al derecho de eliminar de la red información de una persona, que ella misma u otras personas hayan subido a internet. Es como un derecho a ser olvidado de las redes; y en el caso de que no se pudieran eliminar, que al menos no se indexen en los resultados de búsqueda o se utilicen sin autorización[40]. Estrechamente relacionado con el derecho de supresión y oposición, es una manifestación de ellos en el entorno on-line, y el RGPD ha querido incluirlo en el apartado 2 de su art.17 para facilitar la cancelación de los datos que hayan ido multiplicando en las redes.

De esta manera, se entiende este derecho como la posibilidad de limitar el uso de los buscadores de internet para obtener información de una persona. Este mismo apartado 2

[39] VILASAU SOLANA. M. y PEGUERA, M., en "Introducción a la protección de datos de carácter personal", pp. 32-33.

[40] MONTALBANO, L., en Tesis Doctoral sobre "El reglamento europeo de protección de datos personales y el derecho al olvido". Madrid, 2019. Pp. 203-206.

añade que cuando el responsable del tratamiento haya hecho públicos los datos, y esté obligado a suprimirlos, adoptará las medidas necesarias para avisar de la solicitud de supresión a los subsiguientes responsables para eliminar cualquier replica, copia o enlace a esos datos. Para ello las medidas deben ser razonables[41].

El procedimiento a seguir será el siguiente: el interesado se dirigirá al responsable que haya publicado la información, acreditando su identidad e indicando cual es el contenido que desea eliminar. Las redes sociales más populares disponen de servicios de ayuda que informan al usuario cuando se sospecha de la vulneración de la privacidad[42]. La LOPDGDD ha incluido una regulación especial también referente a este derecho en su art. 93 y en su art. 94 titulado "Derecho al olvido en servicios de redes sociales y servicios equivalentes" en el que se establece el derecho al usuario a retirar los datos que él mismo haya facilitado para su publicación en RRSS.

Vamos a hacer referencia y a analizar una de las sentencias basadas en este derecho: es el caso **Google Spain**, en el que el TJUE (Gran Sala) el 13 de mayo de 2014, dictó sentencia en el asunto C-131/12, Google Spain S.L. y Google Inc contra la Agencia Española de Protección de Datos (AEPD) y Mario Costeja[43]. Dicho caso versa sobre el ejercicio por parte del señor Costeja del derecho de oposición al tratamiento de sus datos personales contra Google y el periódico La Vanguardia, con la intención de que se eliminaran dos anuncios oficiales publicados con anterioridad en dicho periódico relativo a la subasta de inmuebles del afectado para poder solventar sus deudas con la Seguridad Social (SS)[44].

El afectado reclamó ante la AEPD la falta de atención a su derecho de oposición por parte de Google y de dicho periódico, pero ésta en su sentencia del 30 de julio de 2010, solo estimó la reclamación contra el buscador instándole a tomar las medidas necesarias para eliminar la información e imposibilitar el acceso a ella ya que consideró que lesionaba el derecho

41 PEGUERA, M., en "Introducción a la protección de datos de carácter personal", pp. 37-38.

42 FERNANDEZ GONZALEZ, C.M., en "Estudio sobre el sistema de protección de datos personales con finalidad de protección, detección e investigación policial de infracciones penales". Madrid, 2022. Pp. 180-182.

43 STJUE (Gran Sala), de 13 de mayo de 2014, Google Spain, S. L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12).

44 VILASAU SOLANA, M., en "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido" (análisis de la STJUE de 13 de mayo de 2014). Revista d'internet, dret i política. Junio, 2014.

fundamental a la protección de datos y a la dignidad de la persona[45]. Sin embargo, desestimo esta acción contra el periódico ya que la publicación obedecía a una orden gubernamental.

Como respuesta a la AEPD, Google Spain y Google Inc recurrieron a la Audiencia Nacional (AN), la cual decidió suspender el procedimiento y plantear ciertas cuestiones frente al Tribunal de Justicia (TJ); que fueron analizadas por la Sala del TJUE y eran tales como el ámbito de aplicación territorial; la interpretación de los términos y responsable del tratamiento; y la procedencia de la pretensión del afectado de que se eliminen sus datos.

No es necesario acreditar que al afectado ha sufrido un daño por la aparición de la información en el buscador ni tampoco hace falta que la ésta sea falsa o ilícita, pero sí que concurran los requisitos necesarios para el ejercicio del derecho de cancelación o supresión.

Por su parte difiere bastante del abogado general en muchos de los aspectos[46]. La cuestión ya no es analiza si existe una cuestión legítima o no, si no si la solo voluntad del afectado permite la retirada de la información. Finalmente el TJUE en el párrafo 88 de la sentencia determinó que "el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita".

También determinó que los sujetos, cuyos datos personales se puedan encontrar en motores de búsqueda, puedan solicitar que ya no se encuentren a disposición de cualquiera en la lista de los resultados, ya que su derecho a la privacidad y la protección de sus datos personales prevalecen sobre el interés económico del gestor del motor de búsqueda y sobre el interés del público que haga la búsqueda de su nombre[47]. No obstante, el Tribunal enfatizó que el derecho a tal solicitud puede dejar de existir cuando el acceso a información personal se justifique por el interés preponderante de dicho público en tener acceso a la información de que se trate[48].

---

[45] STJUE (Gran Sala), de 13 de mayo de 2014, Google Spain, S. L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12). Par. 17.

[47] STJUE (Gran Sala), de 13 de mayo de 2014, Google Spain, S. L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12). Par. 81, 97.

[48] https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/?lang=es (última consulta el 29 de mayo de 2023)

4.1.4-. Régimen sancionador.

Como novedad de este Reglamento, se incluyen las elevadísimas sanciones económicas, en materia de responsabilidad administrativa, en el caso de incumplimiento con la normativa de protección de datos personales, igualándose en este aspecto todos los países de la UE. En el art.10 del CdE, se estipula que cada parte contratante deberá establecer sanciones y recursos adecuados para las violaciones de las disposiciones de derecho nacional recogidos en el Convenio 108 ya que éste no impone sanciones concretas. Lo que sí establece este Convenio es que las medidas deben ser efectivas, proporcionadas y disuasorias[49].

El régimen sancionador del RGPD divide las sanciones en dos grupos, las graves y las muy graves. Ha desestimado el grupo de las sanciones leves anteriormente regulado por la AEPD debido a que en el marco europeo y según establece su art.83.2, se considera que todas las infracciones son como mínimo graves e irán impuestas en función de cada circunstancia personal, pero esto no es incompatible con que cada Estado haga su propia regulación con sanciones judiciales o no judiciales, penales, administrativas o civiles; de hecho, en España se han establecido sanciones leves, graves y muy graves.

A la hora de establecer la cuantía de las sanciones van a influir diferentes factores que harán variar su cantidad, algunos de estos factores son la naturaleza, gravedad y duración de la infracción; la intencionalidad o negligencia en la infracción; cualquier medida adoptada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados; el grado de responsabilidad del encargado del tratamiento; las infracciones cometidas con anterioridad; el grado de cooperación con la autoridad de control; las categorías de los datos afectados; etc.

Para las sanciones LEVES, la penalización puede ir desde una sencilla amonestación hasta la aplicación de medidas correctivas, pudiendo llegar a una multa de hasta 40 mil euros. Esta infracción leve prescribe al año.

Para las GRAVES sería desde 40.001 hasta 10 millones de euros o el 2% de la facturación anual de la empresa en el último año, optando por la cuantía de mayor de valor. Su prescripción se produce a los 2 años según el art. 83.4 del RGPD. Las causas por las que se considerará esta sanción será la vulneración de las obligaciones de control, certificación, y las del encargado y responsable.

[49] Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 100.

En el caso de las sanciones MUY GRAVES, la cuantía oscilará desde 300.001 hasta 20 millones de euros o el 4% de la facturación anual global de la empresa, optándose por la de mayor cuantía. Según el art. 83 en sus aparatados 5 y 6, su prescripción se produce a los 3 años. Hay una serie de cuestiones que hacen que estas penalizaciones oscilen y varíen dependiendo de su naturaleza, gravedad, duración de la infracción, de si existe o no una política de protección de datos; de los beneficios que hayan producido; de si existía intencionalidad o negligencia; de si ha habido una advertencia anterior, en cuyo caso la cuantía aumentará según el número de veces que se hayan dado esas advertencias, etc.; siempre eligiendo la mayor cuantía a la hora de elegir entre una cuota fija o lo que se corresponda con el porcentaje de la facturación. Las causas de estas sanciones serán: la vulneración de los principios básicos de tratamiento, de los derechos de los interesados, la transferencia a terceros países y el incumplimiento de una resolución[50].

Además de estas sanciones administrativas, las autoridades de control van a poder imponer lo que conocemos como correctivos, se recoge en el art. 58 del RGPD y van desde advertencias, órdenes, apercibimientos a responsables y encargados hasta prohibiciones que podrán ser temporales o definitivas de las actividades de tratamiento.

Cuando se produce una sanción, se genera una serie de daños debido al incumplimiento de la normativa y se abrirá un expediente disciplinario, surgiendo así la necesidad de resarcir e indemnizar a los afectados, esto es lo que conocemos con el nombre de responsabilidad civil; que no solo va a requerir una compensación de los daños económicos sino también morales[51]. Este resarcimiento se contempla en el art. 82.1 según el cual "toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o del encargado del tratamiento una indemnización por los daños y perjuicios causados".

4.1.5-. Autoridades de control para la protección de datos.

En este apartado vamos a hacer referencia a dos figuras encargadas del tratamiento de datos, que van a ser el responsable del tratamiento (RT) y el encargado del tratamiento (ET).

[50] Pridatec en "Sanciones por incumplimiento e inadaptación al RGPD". Disponible on-line en https://www.pridatect.es/wp-content/uploads//2020/03/Sanciones_por_incumplimiento_RGPD-1.pdf (ultima consulta el 22 de mayo de 2023).

[51] VILASAU SOLANA. M. y PEGUERA, M., Op. cit., pp. 34-36.

En cuanto al **responsable del tratamiento** podemos definirlo según el art. 4.7 del RGPD, como la persona física o jurídica (suele ser en el sector privado), autoridad pública (suele ser en el sector público), servicio u otro organismo, que solo o junto con otros, determine los fines y medios del tratamiento. En el caso de que haya más de uno, éstos serán considerados corresponsables, según el art. 26 RGPD, y tratarán los datos conjuntamente para un fin común. De él depende el control del tratamiento y es la persona que asume esa responsabilidad, pero con las nuevas reformas en la protección de datos, los ET también han pasado a cumplir muchas de las obligaciones de las que antes solo eran responsables los RT.

En cuanto a sus funciones podemos separarlas en base a tres momentos: cuando se inicia, cuando se efectúa y cuando finaliza el tratamiento; y dentro de estas tres fases tienen funciones muy variadas como verificar el cumplimiento de la norma, adoptar garantías, dotarse de medios técnicos y personales adecuados, etc.

Pero lo que realmente vamos a enumerar son sus obligaciones recogidas en los art. 28 a 36 RGPD[52].

- Llevar un registro por escrito que deberá contener cierta información como el nombre y datos del RT, del corresponsable, y del delegado de protección de datos; los fines del tratamiento; las categorías de interesados y de los datos y destinatarios; las transferencias de datos a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional; la documentación de garantías adecuadas; los plazos previstos y a ser posible una descripción general de las medidas técnicas y organizativas de seguridad.
- Cooperar con la autoridad de control si es ésta lo solicita.
- Identificar los riesgos del tratamiento para poder aplicar así los mecanismos necesarios y además notificárselo a los afectados en caso de que se produzcan violaciones de seguridad. Los mecanismos más utilizados son la seudonimización, el cifrado de datos, los procesos de verificación, evaluación y valoración; la garantía de la confidencialidad, integridad y disponibilidad. etc.
- Realizar una evaluación de impacto relativa a la protección de datos, conocida con las siglas PIA (Privacy Imact Assessment).
- Consulta previa.

[52] VILASAU SOLANA. M. y PEGUERA, M., Op. cit., pp. 20-25.

- Designación del encargado del tratamiento: elegirá un solo encargado que sea capaz de aplicar los mecanismos organizativos.

En el caso de incumplimiento de sus funciones[53] podrá ser sancionado con una multa de 10 millones de euros o el 2% de la facturación anual (la cuantía que sea mayor; o con una multa de 20 millones de euros o el 4% de la facturación anual (la cuantía que sea mayor) dependiendo de las circunstancias.

A la hora de hablar del **empleado del tratamiento**[54] (ET), nos referimos a la persona física o jurídica (suele ser en el sector privado), autoridad pública (suele ser en el sector público), servicio u otro organismo, que trate datos personales por cuenta del responsable del tratamiento (art. 4.8). Deberá garantizar la aplicación de las medidas técnicas y organizativas, cumpliendo en todo caso con el RGPD. Estará vinculado al RT bajo un contrato o acto jurídico q lo acredite donde se establecerá la duración, objeto, naturaleza, finalidad, categorías de los interesados y tipos de datos personales, y las obligaciones y derechos del responsable.

EL art. 28.3 estipula que, si el encargado es consciente de una infracción del RGPD, informará automáticamente al RT. En cuanto a sus funciones diremos que:

- Llevará un registro por escrito de todas las categorías de tratamiento realizadas por el RT.
- No será necesario este registro para determinadas empresas u organizaciones.
- No podrá subcontratar a otro ET, salvo que exista autorización previa por escrito, especifica o general del RT.

Por último, vamos a hacer referencia al **delegado de protección de datos** (DPD)[55]. Esta figura se va a encargar de facilitar el cumplimiento de las disposiciones estipuladas en el reglamento, y será obligatoriamente designado por responsables y encargados en requeridas situaciones como puede ser el caso en el que el tratamiento lo lleve a cabo una autoridades u organismo público o cuando su actividad fundamental sea la observación sistemática de personas o el tratamiento de categorías especiales de datos a gran escala. Aunque a veces no sea de obligatoriedad su contratación, las organizaciones pueden considerarlo de gran utilidad, y lo nombran voluntariamente. Otra de sus funciones es la de actuar como

[53] Art. 83 del RGPD.

[54] Grupo del artículo 29 sobre protección de datos. "Dictamen 1/2010 sobre los conceptos de responsable del tratamiento y encargado del tratamiento", WP 169, diciembre de 2016. (Última consulta el 31 de mayo de 2023)

[55] Grupo del artículo 29 sobre protección de datos. "Directrices sobre los delegados de protección de datos (DPD), WP 243 rev.01, diciembre de 2016. (Última consulta el 31 de mayo de 2023).

intermediarios entre las partes interesadas correspondientes y ejercerá sus funciones desde la etapa más temprana en todas las cuestiones relativas a la protección de datos.

No serán responsables en caso de incumplimiento del RGPD, ni tampoco podrán ser destituidos ni sancionados por el desempeño de sus funciones por el responsable o encargado del tratamiento, lo cual le proporciona la autonomía y recursos suficientes para desarrollar su labor de forma efectiva[56]. El DPD debe ser una figura accesible y es por ello que se recomienda que su ubicación sea dentro de la Unión Europea, independientemente de si lo está el responsable o encargado.

Respecto a sus principales funciones serán:

- Supervisión de la observancia del RGPD: recabar información, asesorar, aportar recomendaciones…
- Colaborar en la evaluación de impacto realizada por el responsable del tratamiento.
- Cooperación con la autoridad de control y actuación como punto de contacto.
- Enfoque basado en el riesgo: teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.
- Colaborar en el mantenimiento de registros.

4.2-. Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Actualmente modificada y derogada prácticamente en su integridad la ley anterior, se produce la entrada en vigor de una nueva Ley Orgánica, el 6 de diciembre de 2018, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), con el objetivo de adaptar el marco jurídico español a la nueva normativa europea, que es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

En cuanto al objeto de esta ley, en su art. 1 podemos encontrar una doble finalidad, en primer lugar, la adaptación de nuestro ordenamiento jurídico al contenido del RGPD, que es directamente aplicable a sus estados miembros desde su aprobación, pese a que en España

[56] Art. 38.3 del RGPD.

tuviéramos vigente la LOPD, que debido a las nuevas tecnologías e innovaciones que han ido surgiendo aceleradamente y de una manera cada vez más vertiginosa, ésta se ha ido quedando obsoleta y es por este motivo por el que ha sido necesario la adaptación. En segundo lugar, garantizar los derechos digitales de la ciudadanía conforme al art. 18.4 de la Constitución.

De esta manera el Tribunal Constitucional (de ahora en adelante TC), entre la aprobación de unos y otros marcos normativos, siempre ha establecido su carácter de derecho constitucional y estableció jurisprudencia basándose en algunas de las siguientes sentencias que han sido determinativas en cuanto al derecho fundamental a la protección de datos:

- La Sentencia 254/1993, de 20 de julio de 1993, del Tribunal Constitucional. Recurso de amparo n.º 1827/1990. Es la primera sentencia que hace referencia a este derecho fundamental conocida por la doctrina y jurisprudencia como autodeterminación informativa. Toma relativa importancia en su fundamento jurídico sexto donde recoge el derecho a la intimidad y el derecho a la autodeterminación informativa como un derecho nuevo diciendo que se ha incorporado esta nueva garantía constitucional para así poder responder a una nueva amenaza a la dignidad y a los derechos de la persona, diferente a como se venían conociendo hasta ahora. Crea una garantía de otros derechos como el honor y la intimidad, pero también es un derecho o libertad fundamental en sí mismo frente a las posibles agresiones de un uso ilegítimo de la informática[57].
- La Sentencia del Tribunal Constitucional 94/1998, de 4 de mayo. Esta sentencia ratifica que estamos ante un derecho fundamental por el cual podemos decidir sobre el control, uso y destino de nuestros datos personales y así evitar el tráfico ilícito de estos; es una potestad que el ciudadano tiene y la cual puede exigir[58].
- La Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional sobre el recurso de inconstitucionalidad 1463-2000 y promovido por el Defensor del Pueblo. Esta sentencia cobra importancia debido a que se crea sobre la protección de datos personales un derecho fundamental y autónomo y que finalmente se acaba recogiendo en la Ley Orgánica 15/1999, de 13 de diciembre, teniendo así el ciudadano el derecho a decidir sobre sus datos personales. Este nuevo derecho fundamental a la protección de datos, según establece el fundamento n. º5, atribuye

[57] Sentencia del Tribunal Constitucional (Sala 1.ª), núm. 254/1993, de 20 de julio. (Aranzadi: RTC 1993/254)

[58] Sentencia del Tribunal Constitucional (Sala 2.ª), núm. 94/1998, de 4 de mayo. (Aranzadi: RTC 1998/94)

> a su titular la capacidad de imponer a terceros la realización u omisión en ciertos comportamientos cuya ley concreta, así como su tráfico ilícito y lesivo para la dignidad; y que de acuerdo con el artículo 18.4 de la Constitución debe limitar el uso de la informática, bien como derecho fundamental o regulando su ejercicio. Tiene una función diferente, y por lo tanto también su objeto y contenido son distintos que es principalmente en lo que difiere de las anteriores leyes. A la hora de hablar del objeto de protección del derecho, ya no se refiere únicamente a los datos íntimos de la persona sino también de cualquier otro tipo, sean o no íntimos, que por el uso o conocimiento de un tercero puedan verse afectados sus derechos; porque aquí ya no solo se recoge la intimidad individual del artículo 18.4 CE, sino también los de carácter personal y por lo tanto también a datos públicos que siempre van a ser accesibles al conocimiento de cualquiera. En cuanto a los otros de carácter personal quedan amparados todos aquellos que identifiquen a una persona y puedan aportar datos de perfil ideológico, racial, sexual, económico entre otros que puedan suponer una amenaza para el individuo, todo esto se recoge en el fundamento n.º 6. En el fundamento jurídico n.º 7 corroboramos que uno de los objetivos más importantes de este derecho es asegurar al individuo el control sobre sus datos personales, sobre su utilización y la finalidad a la que se van a destinar. De esta manera el individuo en todo momento será conocedor de quién posee sus datos personales ya par qué van a ser utilizados[59].

En su art. 2.1 se establece su aplicación a cualquier tratamiento total o parcialmente automatizado o no automatizado de datos personales contenidos o aquellos destinados a ser incluidos en un fichero, haciendo especial referencia a que se aplica "a cualquier tratamiento" mientras que el Reglamento 2016/279/UE no utiliza la expresión "a cualquier". Para poder entender este artículo vamos a definir brevemente dos conceptos que más adelante ampliaremos:

TRATAMIENTO DE DATOS: El art. 4 del RGPD lo define como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso,

[59] Sentencia del Tribunal Constitucional (Pleno), núm. 292/2000, de 30 de noviembre. (Aranzadi: RTC 2000/292). Disponible on-line en https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276 (última consulta: 28 de marzo de 2023).

cotejo o interconexión, limitación, supresión o destrucción". Señala que cuando este tratamiento sea con fines fuera de lo personal o doméstico, quien manejará estos datos será el responsable del tratamiento de datos personales; sin embargo, cuando éste los ceda a un tercero para poder llevar a cabo un servicio contratado, la persona que los manejará será el encargado del tratamiento de datos[60].

FICHERO DE DATOS PERSONALES: Es todo conjunto organizado de datos de carácter personal independientemente de su forma, modalidad de creación, almacenamiento, organización o acceso. Los ficheros no automatizados son conjuntos de datos personales organizados de forma no automática y estructurados en base a ciertos criterios para poder acceder a ellos fácilmente ya sea de una manera centralizada o descentralizada. Sin embargo, los automatizados están organizados de manera automática regulados por programas, soportes y equipos informáticos. Los datos se agrupan en diferentes categorías según como sean estos datos personales y por el nivel de seguridad que requieran[61].

4.3-. La Agencia Española de Protección de Datos (AEPD).

Fue creada en 1992 por la primera ley española sobre materia de protección de datos, que tal y como ya se ha apuntado, era la LORTAD, pero empezó a funcionar en 1994; su estatuto fue aprobado por el Decreto 428/1993, el 26 de marzo. Es un organismo público con sede en Madrid y con un ámbito de aplicación nacional y se encarga de velar por el cumplimiento de la LOPDGDD, entre otras que posteriormente mencionaremos. Es una autoridad administrativa independiente con personalidad jurídica y plena capacidad pública y privada y que tiene total independencia de los poderes públicos para el ejercicio de sus funciones. Es estatutaria y se relaciona con el gobierno mediante el Ministerio de Justicia. Su principal función es proteger los derechos y libertades fundamentales de las personas físicas respecto al tratamiento y libre circulación de los datos personales, bien a instancia de parte o de oficio. El presidente y su adjunto será nombrado por el gobierno a propuesta del Ministerio de Justicia entre personas de reconocida competencia profesional. En España, existen también

[60] https://protecciondatos-lopd.com/empresas/tratamiento-datos-personales/ (última consulta el 4 de mayo de 2023)

[61] DE LA TORRE RODRIGUEZ, P.J., En "Tipos de ficheros de datos personales". Disponible on-line en https://elderecho.com/tipos-de-ficheros-de-datos-personales#:~:text=Qu%C3%A9%20es%20un%20fichero%20de,%2C%20almacenamiento%2C%20organizaci%C3%B3n%20y%20acceso. (última consulta el 9 de mayo de 2023)

otras agencias de protección de datos a nivel autonómico que son las de Madrid, la de Cataluña, País Vasco y Andalucía, con límites en sus funciones[62]. Cuenta con un presupuesto integrado dentro de los Presupuestos Generales del Estado, del que puede disponer con total independencia.

En cuanto a su marco normativo podemos decir que está formado por el RGPD; la LOPDGDD; el Real Decreto 389/2021, de 1 de junio, por el que se aprueba su propio estatuto y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. El Título VII de la LOPDGDD se divide en dos capítulos, el primero enfocado a la autoridad nacional y el segundo, a las autoridades autonómicas[63].

Entre sus principales funciones podemos mencionar[64]:

- Controlar la correcta aplicación del RGPD.

- Concienciar de la importancia del conocimiento sobre las normas, riesgos, garantías y derechos en relación con el tratamiento de datos.

- Concienciar también a los encargados y responsables del tratamiento de datos de sus obligaciones para con el Reglamento.

- Asesoramiento al Derecho de los Estados Miembros, al Parlamento nacional, al Gobierno y demás instituciones sobre las medidas relativas a la protección de los derechos y libertades fundamentales.

- Tratar las reclamaciones presentadas, investigar los motivos, informar al reclamante sobre el curso que va a seguir y dar el resultado al reclamante en el plazo previsto para ello.

- Realizar un registro interno de las infracciones que se producen en el Reglamento.

- Fomentar la creación de mecanismos de certificación de la protección de datos.

---

[62] https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia (última consulta el 28 de junio de 2023).

[63] REYES KAHANSKY, C.M. Op. cit., pp. 214-216.

[64] https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/funcion-y-poderes (última consulta el 28 de junio de 2023).

- Cooperar con todas las autoridades de control para que se lleve a cabo su función de la mejor manera posible.

- Elaborar una memoria anual presentada por el propio director ante las Cortes.

- Llevar a cabo las investigaciones en forma de auditorías de protección de datos.

- Representar a España en los foros internacionales sobre la materia.

Podríamos mencionar otras muchas funciones de la AEPD, ya que realiza un sinfín de ellas; pero también vamos a referirnos a los tipos de poderes que posee que son el poder de investigación, el correctivo y el de autorización y consultivo.

4.4-. Normativa Internacional.

En la década de los 80 fue cuando por primera vez en Europa, la Organización para la Cooperación y el Desarrollo Económicos, adoptó un documento donde se incluía ciertas referencias con respecto a la protección de datos personales.

Posteriormente, el 28 de enero de 1981, el Consejo de Europa, adopta el **Convenio 108 del Consejo de Europa**[65], para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Y el 24 de octubre de 1995, la Unión Europea adoptó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de éstos, pero a la vez impone ciertas restricciones a los países que considera que no garantizan la debida protección a los datos personales; convirtiéndose Europa en el continente donde se ha alcanzado el nivel más alto en base a la protección de datos[66].

Este Convenio establece unos mecanismos para establecer la detención de la recogida de datos privados de los sujetos de forma automatizada y es el único instrumento internacional legalmente vinculante en la protección de datos personales. Su principal función es proteger

[65] El Consejo de Europa está formado por 47 estados miembros, 27 de los cuales también lo son de la Unión Europea.

[66] https://dpd.aec.es/la-proteccion-datos-panorama-internacional-una-primera-aproximacion/(última consulta el 31 de mayo de 2023).

al individuo frente a los abusos que se puedan producir cuando se recopila y trata la información de los datos y además trata de regular el flujo transfronterizo de estos[67].

En el preámbulo y art. 1 de este Convenio se recoge el derecho al respeto a la vida privada y la necesidad de protección de los individuos sin tener en cuenta su nacionalidad, residencia u otro tipo de factores que no deben influir en este derecho, y según su art. 22 se obliga a las partes contratantes a adecuar su legislación nacional a los principios fundamentales establecidos en este Convenio. Además de lo anterior, se basa en una serie de principios como la legalidad y legitimidad a la hora de la recogida y tratamiento de datos, la obligatoriedad de la conservación de éstos solo durante los plazos previstos, la finalidad prevista sin abusar de ellos, la exactitud, entre otros muchos principios, y para que todo esto sea posible establece una serie de medidas y jurídicas sin las cuales no se cumpliría (art. 4.1 del Convenio 108). En cuanto a su ámbito material, está referido tanto en el sector privado como público y se aplica a los ficheros y tratamientos automatizados de los datos personales[68].

El RGPD fue el encargado de abolir la Directiva No. 46 de 1995, a la cual podemos considerar la pionera y uno de los principales instrumentos jurídicos en materia de protección de datos. Estaba articulada en 72 considerandos y 34 artículos divididos en 6 capítulos. En 1997 y a partir de esta Directiva surge el **Grupo del Artículo 29**[69], órgano importante para la evolución europea de la protección de datos. Algunas de sus funciones son garantizar el cumplimiento de dicha directiva en el ámbito europeo; es un órgano de consulta de la Comisión Europea y puede emitir dictámenes, recomendaciones y documentos de trabajo, hasta la fecha ha adoptado 233 recomendaciones y dictámenes. Pero sin duda su función principal es adoptar una serie de pareceres y opiniones comunes en relación con la correcta interpretación que se debe hacer de las disposiciones de la directiva para su aplicación en todo el territorio de los Estados miembros. También es importante su adaptación a los nuevos problemas que van surgiendo.

A nivel europeo el Reglamento no es la única norma de aplicación general para el tratamiento de los datos, sino que opera conjuntamente con la **Directiva (UE) 2016/680 del**

[67] MONTALBANO, L., Op. cit., pp. 41-.

[68] REYES KAHANSKY, C.M., Op. cit., pp. 39-42.

[69] Grupo del Artículo 29: formado por un representante de cada una de las autoridades de control de todos los Estados miembros, normalmente el presidente, por la autoridad de supervisión de los tratamientos de datos de las instituciones de la Unión Europea y por un representante de la Comisión Europea. Desarrolla funciones consultivas y se les garantiza toda la independencia posible con respecto a las instituciones comunitarias.

Parlamento Europeo y de Consejo del 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y a la libre circulación de éstos. A parte de esta Directiva opera también con la **Directiva (UE) 2016/681 del Parlamento Europeo y de Consejo del 27 de abril de 2016**, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR), para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave[70].

Para terminar con respecto al Convenio 108, en mayo de 2018, el Consejo de Europa ha actualizado el Protocolo Adicional creado en noviembre de 2001 con el fin de modificar las autoridades de control y las transferencias de datos a estados que no fueran parte; y en este caso la actualización ha consistido en la actualización de nuevas técnicas para el tratamiento de datos debido a toda la evolución de la tecnología y de cómo ha ido cambiando el derecho que la tiene por objeto; y también se ha abierto a la protección de otros derechos y libertades fundamentales[71].

Como ejemplo de ciertas modificaciones introducidas en este Protocolo podríamos señalar la modificación del art. 2.c donde ya no se refiere solamente al tratamiento de los datos automatizados, sino también al de los no automatizados; o el art. 3.1 donde ya no diferencia entre el ámbito material o territorial, si no que establece que se aplicará a los tratamientos de datos sometidos a la jurisdicción de cada parte, tanto en el sector público como privado.

[70] REYES KAHANSKY, C.M. 119-120.

[71] REYES KAHANSKY, C.M., Op. cit., pp. 43-48.

5-. PROTECCION DE DATOS DE LOS MENORES.

La LOPDGDD incluyó como novedad un nuevo derecho digital que es el derecho de los menores en internet, también queda regulado en el RGPD. Los menores de edad solo por el mero hecho de serlo son considerados personas vulnerables y por ello requieren una regulación específica por parte de los responsables a la hora del tratamiento de sus datos personales. Con todos los avances tecnológicos y las nuevas RRSS, se ha detectado según los estudios realizados por el Instituto Nacional de Estadística (INE)[72] que más de un 90% de los menores son usuarios de internet, con accesos a RRSS, lo que supone un grave riesgo para ellos si sus datos no reciben la protección necesaria y adecuada, y es por eso por lo que, tanto en el RGPD como en la LOPDGDD se ha incluido una protección reforzada con medidas concretas. En el siguiente epígrafe vamos a tratar las regulaciones, tanto nacional como internacional, donde se recoge la protección de datos de los menores.

5.1-. Regulación de la protección del menor y de sus datos personales.

La antigua LOPD no dedicaba ningún precepto donde incluyera una especial protección a los datos personales del menor; donde sí aparece una regulación específica por primera vez es en el art.13 del RLOPD, referido a las condiciones necesarias para prestar consentimiento para el tratamiento de éstos. Con la publicación de la LOPDGDD, en su art. 7 establece "que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años; exceptuando los supuestos donde la ley exija la asistencia de los titulares de la patria potestad para que se produzca el acto o negocio jurídico; y además se añade que el consentimiento del tratamiento de los datos de menores de 14 años solo será lícito si consta el consentimiento del titular de la patria potestad o tutela.

El art. 84 de la LOPDGDD, referido a la protección de menores en internet, señala que los padres, tutores, curadores o representantes legales deberán velar por un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la información para poder preservar la dignidad y derechos fundamentales de éstos. En el supuesto de que se produzca una intromisión ilegítima en los derechos fundamentales en el tratamiento de los datos,

[72] https://www.ine.es/jaxi/Datos.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c06002.px (Ultima consulta el 30 de octubre de 2023).

habilita al Ministerio Fiscal para que pueda tomar parte y se aplicarán así las medidas cautelares referidas en el art. 4 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, sobre el derecho al honor, a la intimidad y a la propia imagen. Este artículo comprende también la inviolabilidad del domicilio y el secreto de las comunicaciones, así como pena la difusión y uso de la información de menores en medios de comunicación que supongan una intromisión ilegítima en los derechos anteriormente mencionados[73].
Por otro lado, el artículo 92 de la LOPDGDD hace hincapié en el interés superior de protección del menor y sus derechos fundamentales en el desarrollo y difusión de actividades en el que éstos participan, por encima del interés de los centros educativos o demás personas físicas o privadas; además añade que cuando este desarrollo o difusión sea a través de RRSS o similares deberán contar con el consentimiento.

5.2-. Tratamiento de los datos en el ámbito escolar.

El tratamiento de datos de los menores se refiere a la recopilación, uso, y protección de la información personal de éstos, es de gran importancia y relevancia en ellos porque se encuentran considerados especialmente vulnerables, ya que carecen de la consciencia y trascendencia, o de los riesgos a los que pueden estar sometidos y es por ello que requieren una protección especial sobre todo cuando el uso de sus datos se va a llevar a cabo con el fin de crear perfiles de personalidad o con un fin comercial[74].

EL RGPD contiene un marco legal transparente que requiere como imprescindible el consentimiento de los padres o tutores legales en la mayoría de los casos, y que posteriormente vamos a tratar; y es por ello que las organizaciones y empresas que tratan con ellos deberán adoptar las medidas adecuadas para proteger su privacidad y seguridad, e implementar prácticas sólidas de seguridad de la información[75].

---

[73] Art. 4 LOPJM

[74] CASTRILLO DE LA FUENTE, M., en "El tratamiento de datos de menores de edad, ¿qué dice el RGPD al respecto?". Disponible on-line en https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/el-tratamiento-de-datos-de-menores-de-edad-que-dice-el-rgpd-al-respecto-2018-06-28/ (última consulta el 9 de junio de 2023).

[75] LLANEZA, PALOMA, en "La Generación Z: incógnitos y privados". Disponible en https://www.injuve.es/sites/default/files/2017/28/publicaciones/documentos_10._la_generacion_z._incognitos_y_privados.pdf Pp. 149-154. (Última consulta el 7 de junio de 2023).

Los centros educativos tienen la función de educar, orientar, formar e inculcar ciertos valores a sus alumnos y para ello es necesario disponer de cierta información importante, tanto suya como de sus progenitores o tutores legales, para así poder hacer su labor educativa de la mejor manera posible. Esta información se aporta cuando se hace la matriculación en el centro y va a permanecer en los ficheros, no solo durante la estancia del alumno, sino que, aunque éste decida cambiar de centro, los datos seguirán almacenados durante el plazo estipulado. Incidir en que bajo ningún concepto podrán recabarse datos sobre los familiares del menor de 14 años relativos a la actividad profesional, información económica u otros, sin el consentimiento de los titulares de los datos.

Algunos de los datos que se van a requerir son el origen, ambiente familiar y social; las condiciones personales o circunstancias familiares importantes y los datos escolares anteriores, necesarios para poder orientar mejor al alumno. También se solicitan ciertos datos especiales como los referentes a la salud o religión[76].

Los datos referentes a la salud son de vital importancia, ya que, en el caso de discapacidades, intolerancias alimenticias, enfermedades crónicas u otras, va a permitir a los educadores tener un comportamiento adecuado de comprensión, precaución, entendimiento y cuidados a los menores.

5.3-. Consentimiento del menor en el tratamiento de datos personales.

Tanto en el art. 6.1 de la LOPDGDD como en el art. 4.11 del RGPD, el consentimiento se define como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que se acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

El RGPD establece una serie de requisitos para que el consentimiento se considere válido y legítimo y de esta manera dice que:

- El responsable del tratamiento debe aportar cierta información para que el consentimiento cumpla con el requisito de ser informado, y para ello deberá aportar ciertos datos como su identidad, los destinatarios de los datos, la finalidad del tratamiento, el ejercicio de los derechos, los plazos de conservación y los derechos que posee el interesado (art 13.1 RGPD).

[76] Guía para centros educativos. Disponible en https://www.aepd.es/es/documento/guia-centros-educativos.pdf (última consulta el 7 de junio de 2023).

- La solicitud de consentimiento se prestará de forma inteligible y de fácil acceso, empleando un lenguaje claro, sin ambigüedades y sencillo (art. 7.2 RGPD).
- El interesado podrá retirar su consentimiento cuando considere oportuno en cualquier momento, sin ningún efecto retroactivo, con las mismas facilidades que tuvo al otorgarlo (art. 7.3 RGPD).

El consentimiento de los menores queda regulado por el art. 8 del RGPD, y establece que la edad mínima para que un menor pueda dar su consentimiento y éste sea considerado valido será de 16 años, pero permite a los Estados Miembros que puedan incluir ciertas excepciones reduciendo la edad siempre y cuando no sea inferior a 13 años.

En España, la LOPDGDD, establece, tal y como ya hemos tenido la ocasión de señalar, la edad mínima en 14 años. De este modo, los menores con edades comprendidas entre 14 y 18 años podrán dar su consentimiento para el tratamiento de sus datos personales siempre que las circunstancias no exijan la autorización o consentimiento de las personas que tengan su patria potestad o sean tutores legales, como ocurre por ejemplo en los actos o negocios jurídicos; y haciendo las comprobaciones necesarias para verificar que el consentimiento es real, ya que con todos los avances tecnológicos, cada vez es más sencilla la suplantación o falsificación de éste[77]. Además del RGPD y de la LOPDGDD, también debemos tener en cuenta la Ley Orgánica 8/2021, de protección integral de la infancia y la adolescencia frente a la violencia, conocida como ley de protección de menores, donde se regula la protección al menor frente a contenidos ilícitos o violentos que puedan quedar publicados en internet.

Para que el consentimiento de los padres sea válido, será necesario el permiso de ambos o, de uno solo con el consentimiento tácito o expreso del otro**.** Sólo será válido el consentimiento de uno sólo de los padres, en el caso de que alguno de los dos progenitores hubiese sido privado de la patria potestad[78]. En el posible caso de que se produjera un conflicto de intereses entre el menor y uno de sus progenitores o ambos, teniendo en cuenta lo mencionado en apartados anteriores, como prioridad siempre va a prevalecer el interés del menor, poniendo en marcha las vías necesarias para ello y solicitando el nombramiento de un defensor que vele por sus derechos e intereses y representándole en juicio y fuera de él si no se llegara a acuerdo alguno[79].

[77] Art. 8.2 del RGPD.

[78] CASTRILLO DE LA FUENTE, M., Op. cit.

[79] PIÑAR REAL, A., en "Los menores de edad en el Reglamento General de Protección de Datos".

En cuanto a las RRSS o el uso de las aplicaciones móviles, la información que proporcionan a la hora de otorgar el consentimiento son políticas de privacidad demasiado largas, incluso a veces incomprensibles por el uso de un lenguaje complejo y difícil para el entendimiento del usuario, que hacen que prácticamente nadie lea o preste atención, resultando así, ser un consentimiento simplemente ilusorio, donde se crea como un paso previo y necesario sin el que no se puede avanzar a la pantalla siguiente; esto hace que los usuarios accedan de manera automatizada pero sin saber a qué o dónde están prestando sus datos y consentimiento, y que en la mayoría de los casos los menores pueden acceder sin ningún tipo de impedimento ni necesidad de que sea un adulto el que otorgue ese consentimiento, lo cual supone un grave riesgo que en epígrafes posteriores trataremos[80].

Por otro lado, mencionar la "gratuidad" de las redes sociales, donde se establece un consentimiento contractual entre el usuario y la red social en cuestión; entrecomillamos la palabra gratuidad porque este término no es del todo como se entiende, sí en el sentido de que no supone un coste económico, pero sí conlleva que el usuario al registrase esté aceptando de manera implícita su consentimiento al tratamiento y cesión de datos, para que puedan ser utilizados para otros fines no claramente detallados pudiendo ser compartido con socios y otros proveedores de servicios, beneficiándose así ambas partes; el usuario al poder utilizar la red social de manera gratuita y la red social al estar autorizada al tratamiento de los datos de éste[81].

A continuación, vamos a hablar sobre un término que relaciona estrechamente el consentimiento de los menores con la exposición a la que pueden verse expuestos en las RRSS por partes de sus progenitores o aquellos que tengan su tutela. El término al que nos vamos a referir es el *sharenting*.

5.4-. Sharenting.

Con este término nos referimos a la práctica de la necesidad que surge en una generalidad de los padres, madres, tíos, abuelos y familiares en general de plasmar y compartir información, fotografías, videos y todo tipo de detalles sobre sus hijos y descendientes menores de edad y

[80] LLANEZA, P., en "La Generación Z: incógnitos y privados".

[81] AYLLON GARCIA, J.D., en "Consentimiento de los menores de edad en las redes sociales: especial referencia a Tiktok". Pp. 596-598. Disponible en: 24.-Jesús-Daniel-Aillón-580-609.pdf (revista-aji.com) (Ultima consulta el 30 de octubre de 2023)

de su ámbito privado en las plataformas de las RRSS; en muchos casos sobrepasando una delgada línea con la mera intención de conseguir los famosos "me gusta" o añadir seguidores, y bien es cierto que mientras esto afecte a mayores de edad, no parece haber controversia; el problema surge cuando se ve involucrada la vida de un menor, incluso desde antes de nacer, sobrepasando el entorno familiar y cercano y produciéndose una sobreexposición en el mundo digital de su vida privada, el cual no lo ha elegido y puede por ello verse afectado de por vida, ya que todo aquello que queda publicado va a pasar a formar parte de su huella digital[82].

Y es que, precisamente aquí, es donde se marca la diferencia entre la situación donde esos datos quedan solo para un ambiente familiar y doméstico o donde pueden sobrepasar a la pantalla de cualquiera. A la hora de exponer la imagen de un menor en cualquier red social la ley es clara y determina que ambos progenitores deben estar de acuerdo para que se pueda mostrar, independientemente de quien tenga la custodia, y en caso de no haber acuerdo se considerará ilícito.

Si con el consentimiento debido, decides compartir imágenes o videos de un menor hay ciertos pasos a seguir recomendables para no perjudicarle como, por ejemplo, no mostrar imágenes que en un futuro puedan avergonzarle, no mostrar su cara directamente sino pixelada, no compartir nunca la geolocalización, siempre que sea posible pídele permiso; estas son algunas de las pautas que se recomiendan[83].

Alguno de los riesgos a medio y largo plazo que pueden suponer son, por ejemplo, la violación de privacidad del menor y cómo éstos pueden afrontarlo cuando crezcan y sean conscientes de la información, videos o fotos publicados.

Para poner solución a este problema en concreto existe el derecho que tiene el menor al olvido, regulado en el art. 94 del RGPD que menciona lo siguiente "Toda persona tiene derecho a que sean suprimidos, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes". De esta manera el menor de edad entre los 13 y 16 años tiene el derecho a solicitar la eliminación y desaparición de los datos personales tanto desde donde se

[82] SAURAS, I., en "Sharenting o la doble cara de compartir contenido de tus hijos en redes sociales". Agoso,2022. Disponible on-line en https://bebloomers.com/nosotras/maternidad-y-crianza/sharenting/. (Última consulta el 9 de junio de 2023).

[83] VARIOS AUTORES en "Por el uso seguro de internet para niños, niñas y adolescentes". Disponible on-line en https://www.observatoriodelainfancia.es/ficherosoia/documentos/7051_d_FAPMI-TRIC.pdf (última consulta el 14 de junio de 2023).

publicaron como de todos los motores de búsqueda[84]. Otro de los riesgos a los que se exponen es la suplantación de identidad usando sus datos personales para cometer fraudes; otro puede ser un uso indebido de las fotografías y videos con un ánimos sexuales o pornográficos.

5.5-. Riesgos de un mal uso en las Tecnologías de la Información y Comunicación.

En este epígrafe vamos a hacer referencia a las mencionadas anteriormente en la introducción, tecnologías de la información y comunicación, más conocidas como TIC, basadas en el uso de internet e incluidas en nuestra vida cotidiana a través de nuestro móvil, ordenador o tableta para prácticamente todo: mensajería instantánea, estudio, trabajo, diversión, negocios, compras, información y noticias, bolsa y una larguísima lista interminable; donde han pasado de ser un medio a convertirse en una necesidad sin la que la vida se nos hace mucho más complicada y en ocasiones incide en la funcionalidad de nuestro día a día y, por supuesto, mucho más potenciado en los jóvenes, ya que han nacido en una era tecnológica y se encuentran totalmente familiarizados porque han crecido haciendo uso de ellas[85].

1. Lo que sí podemos afirmar es que, las nuevas tecnologías nos hacen la vida mucho más fácil y nos da accesibilidad a oportunidades a las que sin ellas nunca habríamos llegado; pero el alcance que llegan a tener nos hace olvidarnos de los múltiples riesgos que también conllevan si no se hace un uso adecuado de ellas, y éstas son algunas de las preocupaciones que envuelve a la mayoría de padres o responsables de menores: saber qué hacen sus hijos cuando acceden a internet, qué tipo de RRSS utilizan, cuánto tiempo emplean en ellas, si las utilizan de forma adecuada o a qué riesgos pueden estar expuestos; estas son algunas de las preguntas que vamos a intentar analizar.

Claramente, las RRSS se han convertido en la manera más común de los jóvenes a la hora de relacionarse, bien por la facilidad para conocer o integrarse en nuevos grupos o incluso

[84] VARIOS AUTORES en: "Cuadernos jurídicos de derecho de familia". Disponible en: https://dadun.unav.edu/bitstream/10171/63987/1/Sharenting%20Protecci%C3%B3n%20europea%20para%20la%20defensa%20de%20los%20derechos%20digitales%20de%20los%20menores.%20Espa%C3%B1a.pdf (Última consulta el 2 de noviembre de 2023).

[85] GARCIA JIMENEZ, L.N., en "Uso que los menores hacen de las redes sociales y control parental". Disponible en https://core.ac.uk/download/pdf/211103186.pdf (última consulta el 28 de junio de 2023) Pp. 14-15.

relacionarse con sus propios amigos, subir fotos o videos, mostrar sus sentimientos e ideas, descargarse música, ver series o películas, jugar on-line con otros adolescentes de diferentes países y un sinfín de actividades; pero todo esto supone una exposición de su perfil de la que fácilmente pueden perder el control sin ser conscientes de ello, ya que pueden llegar a normalizar ciertas cosas que no deberían; es por eso la importancia de que los padres controlen y sepan manejar las TIC para que puedan enseñar y educar a sus hijos a hacer un uso responsable y seguro de ellas, aunque también es cierto que a día de hoy se ven apoyados por los centros educativos donde se han incorporado desde hace ya unos años y cada vez en más ámbito, podemos encontrarlo reconocido en el art. 83 de la LOPDGDD que recoge el derecho a la educación digital, en su apartado 1 y 2 se menciona lo siguiente: " El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales. Las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior". Pero también es importante mencionar que este derecho a la educación digital no solamente va dirigido a niños y estudiantes, sino que es un derecho que debe garantizarse para todos, suponiendo un mayor esfuerzo para aquellos que no han nacido en la era digital.

A continuación, vamos a mencionar algunos de los riesgos[86] más frecuentes a los que se enfrentan diariamente los adolescentes y que les afectan en diferentes ámbitos:

1-. Abandono de otras actividades como leer, pasear, ir al cine, visitar familiares, incluso muchas veces algo tan básico como hacer algún tipo de **deporte**; esto pasa a producir

[86] SANCHEZ PARDO, L., CRESPO HERRADOR. G., en "Los adolescentes y las Tecnologías de la Información y Comunicación". Disponible on-line en https://digital.csic.es/bitstream/10261/132633/1/TICPadres.pdf (última consulta el 14 de junio de 2023)

consecuencias como el sedentarismo, sobrepeso, aislamiento de la vida social, adicción y dependencia a "estar conectado", etc.

2-. Acceso a contenidos inapropiados, en muchas ocasiones porque aparecen a modo publicitario y otras muchas por la curiosidad del adolescente, lo peligroso es que pueda llegar a tener acceso a ello. En cuanto a los contenidos pornográficos, para evitar este tipo de situaciones, existen unos programas que se instalan en el ordenador y permiten controlar a qué tipo de contenido acceden, pero no siempre son eficaces ya que la seguridad de estos se puede burlar. En el caso de los videojuegos, existe un programa llamado PEGI (Pan European Game Informativo) que los clasifica según el tipo de juego que sea y su contenido, e incluso añade símbolos como el de mayores de 18, miedo, violencia, drogas, juegos y apuestas[87], etc.

3-. Bullying y Ciberbullying: el bullying es el término que se refiere al acoso escolar, son un conjunto de comportamientos de carácter agresivo e intencional sobre la víctima empleando la fuerza o el poder. Puede ser físico, verbal, social o psicológico pero un factor importante que es que se prolongue en el tiempo[88]. Sobre este concepto se crea el término ciberbullying o ciberacoso referido al acoso a través de internet y entre ellos mismos (los menores); debe ser continuado y prolongado en el tiempo, con intencionalidad y con una clara desigualdad entre el agresor y la víctima, añadiendo la parte de que el agresor puede esconderse bajo el anonimato con un perfil falso. Suele realizarse mediante la publicación o difusión de videos, fotos e informaciones con contenido dañino o difamatorio para la víctima. Para la persona que sufre este tipo de violencia, se va a notar afectada su autoestima muy negativamente provocando así en ella trastornos en el sueño, físicos, psicológicos, ansiedad, aislamiento, malos resultados en las calificaciones e incluso depresiones afectando en todo tipo de ámbitos donde se relacione. Es fácilmente detectable ya que se va a producir un claro rechazo a la hora de ir al colegio, se pueden apreciar cambios repentinos en el carácter pasando de la tristeza al enfado o al llanto, visible tristeza persistente, entre otros muchos síntomas, ya que cada adolescente puede manifestarlo de una forma distinta e incluso puede presentar varios síntomas a la vez. En estos casos la mejor opción es ponerlo en manos de una persona cualificada en ello para que la situación le provoque la mínima lesión tanto psíquica como psicológica; y por supuesto, ponerlo en conocimiento de los facultativos del

[87] SANCHEZ PARDO, L., CRESPO HERRADOR. G., Op. cit., pág. 32.

[88] https://psicologiamonzo.com/todo-lo-que-debes-saber-sobre-el-bullying-y-el-ciberbullying/ (última consulta el 14 de junio de 2023)

centro educativo, así como a cualquier entorno donde el menor se desenvuelva, para poder apoyarle y comprender su comportamiento de la mejor forma posible[89].

4-. Grooming o acoso sexual: si hacemos una traducción literal nos referiríamos al término engatusamiento[90], es un acoso por parte de un adulto a un menor de edad, el agresor va creando una conexión basada en la confianza del menor para conseguir que éste acceda a sus peticiones y así obtener imágenes o videos de contenido sexual. El menor es ajeno a la situación que se está produciendo, ignorando ser una víctima, y se encuentra controlado emocionalmente tomando una actitud de silencio por miedo, vergüenza, culpabilidad, por estar sometido a chantaje, amenazas o incluso represalias[91]. El agresor puede ser de diferente categorías, aquél que hace cree a la víctima que realmente está estableciendo una relación sentimental con la víctima y busca su enamoramiento; aquél con el propósito de conseguir un encuentro sexual pero sin embargo se adapta a la víctima, normalmente tienen antecedentes por delitos sexuales; y después encontramos otro perfil denominado hipersexualizado, donde el agresor no pasa por ninguna etapa de preparación, sino que tiene una actitud directa para conseguir contenido o encuentros sexuales, normalmente con antecedentes por pornografía infantil y suele tener contacto con otros delincuentes sexuales o pederastas para compartir contenidos sexuales. Así que por lo general este término está estrechamente relacionado con la pederastia y la pornografía infantil. Este tipo de acoso ha llegado en ocasiones a límites tan extremos, que ha provocados en sus víctimas depresiones muy fuertes llegando incluso a intentos de suicidio o surtiendo efecto en muchos de los casos.

5-. Sexting: término que mezcla dos palabras sex (sexo) y texting (mensajes escritos por el móvil). Surgió en 2005 y ha ido evolucionando con el paso del tiempo y de las nuevas tecnologías, en 2008 se hizo eco un caso en EEUU, que desembocó en el suicidio de una joven que había practicado sexting con su pareja y éste decidió difundir el contenido, es aquí donde su madre empezó una lucha para hacer conocido el caso de su hija y se empezaran a conocer los riesgos a los que podían verse sometidos los menores con esta práctica. Consiste en la producción, envío, difusión o publicación de mensajes, imágenes o videos de contenido sexual, a través del móvil o mediante las RRSS, ya sean propios o de terceras personas,

[89] SANCHEZ PARDO, L., CRESPO HERRADOR. G., Op. cit., pp. 35-36.

[90] SANCHEZ PARDO, L., CRESPO HERRADOR. G., Op. cit., pág. 37.

[91] VARIOS AUTORES en "Por el uso seguro de internet para niños, niñas y adolescentes". Op. cit., pág. 19.

haciendo así un sexting activo o pasivo[92]. Esta práctica aparentemente no parece generar ningún riesgo, sin embargo, hay que prestar especial atención cuando en ellas están involucradas personas menores de edad, ya que pueden suponer una amenaza a su privacidad. Esto ocurre porque una vez que se produce este tipo de contenido, se puede perder el control sobre él, bien porque el receptor reenvíe el contenido para fardar entre su círculo o bien por robo o pérdida del teléfono, o mismamente porque el menor esté siendo víctima de un acoso. Esta difusión del contenido sexual puede derivar en el entorno del menor en bullying o ciberbullying provocándole daños psicológicos; también el menor puede ser víctima de sextorsión, término que significa que implica el chantaje o amenaza de la difusión de ese contenido por parte de otro menor o mayor de edad[93]. Es importante prestar atención a la difusión de imágenes, videos o cualquier tipo de contenido sexual de terceras personas ya que se atenta contra tres derechos fundamentales como son el derecho al honor, a la intimidad y a la propia imagen, cometiendo así un delito[94].

Algunas de las precauciones que se señalan para evitar las consecuencias que se pueden producir señalan como fundamental la educación por parte de los padres y el hablar sobre temas de este tipo, a veces tabú, para que puedan trasladar a los adolescentes los riesgos a los que se exponen y trasmitirles esa confianza para que el menor pueda comunicar sus dudas o miedos en un momento dado. Señala como importante también la ubicación del ordenador, ya que, si se encuentra en la habitación del menor, éste va a tener más libertad a la hora de realizar ciertas prácticas, por otro lado, como medida de protección existen también los programas de control parental. Si el menor ha recibido contenido sexual por parte de una persona mayor de edad, se deberán tomar las medidas adecuadas y ponerlo en conocimiento de la policía nacional, para que la brigada de investigación tecnológica pueda actuar acorde

[92] OJEDA PEREZ, M., en Tesis doctoral sobre "Sexting en la adolescencia: Prevalencia, factores asociados y líneas de actuación psicoeducativa". Sevilla, 2021. Disponible on-line en https://idus.us.es/bitstream/handle/11441/108917/Ojeda%20P%c3%a9rez%2c%20M%c3%b3nica%20Tesis.pdf?sequence=1&isAllowed=y. (Última consulta el 23 de junio de 2023).

[93] INTECO (Instituto Nacional de Tecnologías de la Comunicación). Guía sobre adolescencia y sexting: qué es y cómo prevenirlo. Disponible on-line en https://www.sexting.es/wp-content/uploads/guia-adolescentes-y-sexting-que-es-y-como-prevenirlo-INTECO-PANTALLASAMIGAS.pdf (última consulta el 24 de junio de 2023).

[94] Gutiérrez Morales, I. M. Cyberbullying y sexting: percepción y propuestas de estudiantes universitarios. Multidisciplina. Disponible on-line en https://www.revistas.unam.mx/index.php/multidisciplina/article/view/50686 (última consulta el 23 de junio de 2023).

con la situación y por otro lado se deberá poner en conocimiento de un profesional para poder ayudar al menor afectado.

6-. Falta de privacidad: normalmente se debe al desconocimiento del alcance que puede tener el proporcionar nuestro correo electrónico, número de móvil, dirección o muchas veces el compartir la ubicación en las historias de Instagram o estados de Whatsapp; este tipo de datos otorgan una información privilegiada para aquellos que nos espían en las redes sin siquiera darnos cuenta y es ahí donde nos volvemos vulnerables frente a aquellos que no tienen buenas intenciones. Para evitar esto es necesario revisar las opciones de privacidad de las RRSS que utilizamos con asiduidad, para que nuestra información solo sea compartida con nuestros amigos; no aceptar a personas que no conoces en persona, puesto que la elaboración de perfiles falsos está a la orden del día; no revelar direcciones, ni números de teléfono ni por supuesto, tarjetas de crédito o cuentas bancarias; por otro lado, tener instalado un antivirus en el ordenador evita la entrada de páginas fraudulentas, estafas, pornografía, falsos concursos, etc.[95].

7-. Contacto con personas desconocidas: en las RRSS la elaboración de un perfil falso puede realizarse en tan solo diez minutos, basta con crear un correo electrónico con el nombre que desees utilizar y copiar las fotos de un perfil verdadero; con esta facilidad puedes suplantar la identidad de otra persona detrás de la pantalla, y es este el motivo por el que se recomienda no intercambiar mensajes con perfiles desconocidos o aquellos de los que tengas certeza de su verdadera identidad; la curiosidad, inocencia y ansia de indagar en nuevos ámbitos dificulta en los adolescentes que esto no se produzca pero no solamente en ellos, sino que la soledad, la ajetreada vida laboral y un largo etc. de motivos personales hace que a veces nos impida relacionarnos de una manera personal y recurramos a aplicaciones de citas o simplemente con la intención de hacer nuevas amistades; es aquí donde puede producirse el engaño y la estafa porque la verdadera intención de la persona que está al otro lado de la pantalla no la conocemos.

8-. Phising: término inglés referido a la suplantación de identidad para obtener datos de los usuarios como números de tarjetas de crédito, cuentas bancarias, contraseñas u otros datos confidenciales para menoscabar su patrimonio; el estafador o *phiser* se pone en contacto con el usuario a través de una llamada telefónica, mensaje de texto, correo electrónico o ventana emergente haciéndose pasar por una entidad estatal como correos, telefónica cualquier

[95] SANCHEZ PARDO, L., CRESPO HERRADOR. G., Op. cit., pp. 38-39.

entidad bancaria para dar credibilidad a su mensaje y de esa manera que no dudes en confiar en la plataforma donde te solicitan ingresar los datos. El modus operandi es soltar un anzuelo creíble a la vista del usuario, cada día más sofisticado; en muchas ocasiones es suficiente con acceder al enlace recibido, de esa manera consiguen entrar en tu teléfono móvil pudiendo acceder a todos tus datos y aplicaciones descargadas, incluidas las bancarias, por ello es importante que inmediatamente seas consciente de ello acudas a ponerlo en conocimiento de la autoridad para que todos los movimientos bancarios que puedan realizar sin tu consentimiento sean bloqueados automáticamente. La retirada de dinero pasa a las cuentas bancarias de unos intermediarios, llamados muleros, y desde estas cuentas pasan a las cuentas bancarias de las organizaciones estafadoras, recibiendo los muleros el porcentaje de la comisión de cada operación[96].

5.6-. Edad de acceso a las RRSS.

Según los estudios realizados sobre la edad a la que los menores comienzan a acceder a las RRSS, se registra que la media de edad a la que comienzan a acceder con su smartphone oscila entre los 10 y 12 años, sin embargo, el art. 8 del RGPD determina que "el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó". Pero a pesar de que la edad mínima se establezca en 16 años, el reglamento también permite a los estados miembros, que esa edad pueda ser inferior "siempre que no sea inferior a 13 años"; siendo así la edad mínima fijada en España para poder acceder y registrarse a los 14 años y por debajo de esa edad con el consentimiento requerido[97].

Por el contrario, pese a la normativa vigente española y europea, la mayoría de redes sociales se rigen por normativas de otros países, fijando así cada red social una edad diferente y por ellos a continuación vamos a detallar la edad para algunas.

TWITTER: es una red social gratuita de comunicación bidireccional que sus usuarios utilizan para expresarse o recibir información sobre cualquier tipo de contenido, ya sean

[96] GUDIN RODRIGUEZ-MAGARIÑOS. F., en "Nuevos delitos informáticos: Phising, Pharming, Hacking y Cracking". Disponible on-line en https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf. Pp. 3-4. (Última consulta el 28 de junio de 2023).
[97] Art 7. LOPDGDD.

fotografías, noticias de actualidad, eventos, publicidad, descuentos, etc[98]. Fue creada en marzo de 2006 por Jack Dorsey, actualmente dirigida por Elon Musk desde 2022. Cuenta con más de 500 millones de usuarios y establece en sus términos y condiciones para sus usuarios la mínima de edad de 13 años[99].

INSTAGRAM: red social estadounidense creada en 2010 por Kevin Systrom y Myke Krieger, conocida como insta o IG y con más de 1.300 millones de usuarios; utilizada para comunicarse por privado o en grupo, compartir fotos y videos con una duración temporal o fija. Requiere como requisito indispensable la edad de al menos 13 años para su registro y dispone de un sistema de verificación de edad para sugerir temas apropiados y también solicitar un *videoselfie* si sospecha que se intenta burlar los filtros de edad[100].

FACEBOOK: red social gratuita estadounidense creada en 2004 por Mark Zuckerberg, cuenta con más de 2900 millones de usuarios y marca su edad mínima de acceso en los 13 años, aunque en ciertas legislaciones se requiere más edad. Algunas de sus funciones principales son encontrar y comunicarse con personas de cualquier parte del mundo, compartir fotos, videos y contenido variado, así como descubrir contenido, productos y servicios de tu interés.

TIKTOK: plataforma social de origen chino, creada en 2016 por Zhang Yiming, que cuenta en la actualidad con más de 1.000 millones de usuarios, utilizada para la creación y publicación de videos cortos con música acompañados de efectos. Exige la mayoría de 13 años y además bloquea cualquier cuenta detectada creada por un menor de ésta, pero sin embargo exige la edad de 16 años para otro tipo de actividades dentro de la aplicación como, por ejemplo, enviar o recibir mensajes privados, realizar un video en directo, para el que se requerirá la mayoría de edad; o permitir a otros usuarios la descarga de los videos del menor[101]. Como hemos mencionado en el apartado anterior sobre el consentimiento de los menores, no queda especificado el destino de los datos de los menores en la cesión de datos; es este uno de los

[98] https://www.webempresa.com/blog/que-es-twitter-como-funciona-2.html (Ultima consulta el 18 de septiembre de 2023).

[99] https://help.twitter.com/es/managing-your-account/account-restoration (Ultima consulta el 18 de septiembre de 2023).

[100] https://www.pantallasamigas.net/menores-redes-sociales-edad-minima-datos-personales/(Ultima consulta el 18 de septiembre de 2023).

[101] Guía de TikTok para padres y madres. Disponible on-line en: https://www.pantallasamigas.net/wp-content/uploads/2021/06/Guia-TikTok-Padres-Madres-PantallasAmigas.pdf (Ultima consulta el 18 de septiembre de 2023).

motivos por los que el consentimiento se puede considerar nulo, ya que según el considerando 32 del RGPD "El consentimiento debe darse mediante un acto afirmativo claro, que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta". Podemos decir entonces, que el usuario no conoce ni acepta específicamente el uso y destino de sus datos personales.

Sutilmente, y por debajo de la casilla donde se acepta el registro, aparece otra casilla sin opción a validar que menciona lo siguiente: "al dar a aceptar estás confirmando que has leído las condiciones de servicio y la política de privacidad"; pero la realidad es que no es una casilla opcional de elección si no que ya va preseleccionada directamente sin dar un consentimiento válido y específico[102].

Otro de los motivos por los que podríamos declarar nulo el consentimiento otorgado en esta red social es la contraposición con el art.7 de la LOPDGDD donde se establece una minoría de 14 años para sus usuarios mientras que la política de seguridad y bienestar de los menores de Tiktok dice "para tener una cuenta, debes tener al menos 13 años"[103]; se produce así una contrariedad donde el consentimiento podría declararse nulo si el menor tuviera 13 años y no figurase el consentimiento de sus padres o representantes legales, que es lo que se estipula legalmente en la LOPDGDD.

TWITCH: aplicación estadounidense creada en 2007 como plataforma *streaming* de video donde sus usuarios crean videos que pueden retransmitir en directo, utilizada principalmente

[102] AYLLON GARCIA, J.D., Op. cit. Pp. 601. (Última consulta el 30 de octubre de 2023)

[103] https://www.tiktok.com/community-guidelines/es-es/youth-safety/ (Ultima consulta el 31 de octubre de 2023).

para videojuegos, a través de un canal previamente creado. Esta plataforma no está disponible para menores de 13 años, si se comprende la edad entre 13 y 18 solo será posible su uso bajo la supervisión de los padres o tutores legales. Actualmente cuenta con más de 50.000 usuarios[104].

WHATSAPP: aplicación californiana de mensajería instantánea para teléfonos inteligentes creada en febrero de 2009 por Jan Koum y Brian Acton; actualmente cuenta con 2.900 millones de usuarios y para aquellos que residan fuera de Europa permite su uso con al menos 13 años, sin embargo, si resides en Europa la edad mínima legal será la de 16 años, o más si así lo estipula la legislación de tu país[105].

ONLYFANS: plataforma británica creada en 2015 por Fenix International Limited donde los usuarios pueden pagar por retransmisiones en vivo, fotografías, vídeos y contenido mayormente sexual y pornográfico, es por esto que la edad mínima para registrarse es de 18 años, y para comprobar que esto es así tiene un programa de verificación que requiere la fotografía del usuario sosteniendo su DNI[106]. Onlyfans asegura contar con más de 30 millones de suscriptores.

YOUTUBE: plataforma estadounidense creada con la finalidad de compartir videos a través de un canal creado previamente; fue creada en febrero de 2005 por tres antiguos empleados de Paypal. Cuenta actualmente con 2 billones de usuarios al mes, según fuentes registradas por la propia plataforma. Únicamente puede ser utilizada por mayores de 14 años y los menores podrán utilizar la versión Youtube Kids previamente autorizado por los padres o tutores legales[107].

SNAPCHAT: es una aplicación creada para realizar y compartir fotos y videos con filtros diferentes. Fue creada en Estados Unidos en 2012 por Evan Spiegel, Bobby Murphy, Reggie Brown y en la actualidad cuenta con más de 490 millones de usuarios. Esta aplicación de

---

[104] Guía de Twitch para padres y madres. Disponible on-line en: https://www.pantallasamigas.net/wp-content/uploads/2021/03/Guia-Twitch-madres-padres-PantallasAmigas-0523.pdf (Ultima consulta el 18 de septiembre de 2023).

[105] https://faq.whatsapp.com/695318248185629/(Ultima consulta el 18 de septiembre de 2023).

[106] https://onlyfans.com/terms#complaints-policy (Ultima consulta el 18 de septiembre de 2023).

[107] https://www.pantallasamigas.net/menores-redes-sociales-edad-minima-datos-personales/#:~:text=La%20edad%20media%20en%20la%20que%20un%20menor%20accede%20a%20su%20primer%20smartphone%20oscila%20entre%20los%2010%20y%20los%2012%20a%C3%B1os%2C%20aunque%20la%20edad%20m%C3%ADnima%20para%20acceder%20a%20una%20red%20social%20son%20los%2014%20a%C3%B1os. (Ultima consulta el 16 de septiembre de 2023).

mensajería requiere la edad mínima de 13 años y en caso de no ser así necesita del consentimiento de los padres o tutor legal[108].

Podríamos enumerar infinidad de redes sociales y plataformas tanto de mensajería instantánea como para compartir archivos, bien sean fotos, videos o directos; las anteriores mencionadas son solo algunos ejemplos de las más utilizadas actualmente.

[108] https://snap.com/es-ES/terms (Ultima consulta el 16 de septiembre de 2023).

6-. CONCLUSIONES

Para concluir este trabajo vamos a exponer ciertas conclusiones sobre la protección de datos, los menores de edad y su relación con las redes, ya que es un tema de suma importancia en la sociedad actual por la generalización producida respecto a su acceso. A medida que se ha ido generalizando, ha surgido la necesidad de establecer medidas efectivas para garantizar la seguridad y el bienestar de los niños y adolescentes. Algunas de las conclusiones clave son las siguientes:

Conclusión I: El uso de las tecnologías y de las redes sociales: a lo largo del estudio de nuestro trabajo hemos podido comprobar que los menores y adolescentes son, por excelencia, los usuarios más activos de éstas. Por regla general suelen acceder a aplicaciones como WhatsApp, Tiktok o Instagram a través de su smartphone. Las utilizan como forma habitual de relacionarse, desde las que pueden tener un alcance con sus iguales mucho mayor y cruzar fronteras geográficas que de otra manera sería prácticamente imposible. A través de ellas pueden compartir y recibir información, videos, fotos de influencers, famosos, cantantes de su interés o adolescentes como ellos de todas partes del mundo interactuando en línea. Según lo estudiado, podemos decir que aceptan tener en sus redes personas desconocidas con una falsa percepción de que lo importante es tener un mayor número de seguidores/as sin importar conocer su verdadera identidad; creen que esto les reafirma su valía aportándoles, en mi opinión, una sensación de importancia irreal en la sociedad, aunque he de decir que esto no solo ocurre en adolescentes. El problema y verdadero peligro de que ocurra en menores es su vulnerabilidad, no teniendo la perspicacia de apreciar si están siendo víctimas de una situación de abuso o engaño, pero más adelante hablaremos de esta conclusión.

Conclusión II: La educación, comunicación y concienciación por parte de los padres, son las herramientas más útiles para poder combatir ciertos riesgos, aunque a veces incluso tomando las precauciones apropiadas resulta inevitable. Por ello, no hay que perder el cuidado y se deben establecer reglas como la supervisión de las tareas que realizan en línea, fomentar la comunicación abierta, la orientación sobre el uso seguro, etc., ya que está presente en ellos prácticamente de una manera obligatoria como por ejemplo en sus tareas escolares, donde requieren del uso de internet para la búsqueda de información o programas didácticos convirtiéndose así en una herramienta escolar principal. Por el mismo motivo es importante que los menores sean conscientes de la importancia de proteger su privacidad en línea, y no hagan visibles sus datos personales, así como evitar compartir información

sensible que pueda comprometerles; pero todo esto resulta muy complicado de transmitir y de hacerles entender cómo y cuánto se ven expuestos si no siguen ciertas precauciones.

Por ello creemos que es necesario seguir una serie de pautas para poder concienciarles respecto a este tema.

- Fomentar la confianza en ellos dándoles la libertad de elegir a qué red social pertenecer, cómo crear su perfil, de qué grupo de amigos formar parte; todo esto les da una sensación de libertad y autogestión, pudiendo tomar sus propias decisiones acorde a su madurez; de esta manera se sienten respetados y apoyados por sus progenitores y esto hará que confíen más en ellos a la hora de tener que transmitirles cualquier tipo de situación.

- A pesar de darles esta libertad, siempre debe estar controlada y vigilada hasta cierto punto respetando su intimidad y privacidad, es recomendable saber en cada momento en qué están empleando su tiempo mientras se encuentran conectados a internet; para ello podemos por ejemplo situar el ordenador en lugares comunes de la casa, establecer límites horarios de uso, bloquear el acceso a ciertos contenidos, etc.

- El vínculo de confianza y naturalidad establecido con ellos es clave. Es importante que desde pequeños exista y se establezca una relación de complicidad y confianza donde ellos vean a sus padres como una ayuda y punto de apoyo con quienes poder desahogarse y a quienes acudir en busca de ayuda en el caso de una situación de dudas o complicada, el objetivo es evitar las barreras entre ambos.

- Conocer las redes que utilizan tus hijos a nivel usuario, no hace falta un conocimiento profesional, pero si tener un pequeño conocimiento de cómo funcionan, el alcance que pueden tener o las políticas y condiciones de privacidad.

Conclusión III: Por otro lado, y muy relacionado con la anterior conclusión, mencionar las herramientas de control parental y tecnología que aportan filtros de contenido para facilitar a los padres y tutores la supervisión y el acceso a contenido indeseado, pero sin olvidarnos de que éstos no son más que una ayuda, no un sustitutivo al diálogo, orientación y educación que deben ejercer sobre sus hijos. No se trata de actuar como policías, sino simplemente de velar por su seguridad porque la exposición en internet no tiene límites si no eres tú mismo el que los estableces. Estos filtros parentales se instalan en los ordenadores como un software o aplicaciones, y a través de ellos se adquiere el control sobre el acceso a las páginas, pueden

también bloquear los contenidos que consideren, el tiempo de conexión, señalar palabras clave que denieguen el acceso automático, marcar listas negras o blancas, etc. Algunas plataformas ya tienen integradas estas herramientas de control en sus propias configuraciones de privacidad lo que facilita a los padres esta supervisión. Es importante que este control parental no sea intrusivo y se vaya adaptando a medida que los adolescentes van creciendo para que se sientan cómodos y con la suficiente confianza a la hora de hablar de sus experiencias en línea, sin sentirse juzgados.

Conclusión IV: en este punto vamos a referirnos a la importancia de las políticas y ajustes de privacidad que deben establecer las empresas de las RRSS, para evitar también desde su posición el acceso a éstos. Estas medidas incluyen restricciones de edad que requieren generalmente a sus usuarios una mayoría de 13 años según la Ley Federal de Protección de la Privacidad en Línea de los Niños (COPPA) en los Estados Unidos para su registro, pese a que cada red social establece su propia política de privacidad, pero por lo general tienen una base común que coinciden en la restricción de edad, la obtención de consentimiento parental a la hora del registro en la plataforma, las configuraciones de privacidad predeterminadas, la educación sobre seguridad en línea; esto quiere decir que algunas de las plataformas ofrecen recursos educativos adaptados a los menores para que puedan comprender los riesgos en línea y sobre todo cómo poder evitarlos.

También se incluye como medida la prohibición de publicidad dirigida a menores por su contenido inapropiado, la seguridad de la cuenta con la autenticación mediante dos factores para evitar su sustracción (muy frecuente en Facebook e Instagram), la coincidencia de la ubicación; la propia red detecta que el usuario siempre accede desde un dispositivo localizado en tal situación geográfica y cuando esto no es así despliega su medida de seguridad solicitando ciertas verificaciones para cerciorarse de la autenticidad de su usuario.

Conclusión V: La conciencia sobre los riesgos por parte de los padres, tutores y educadores: deben ser conscientes de la sobreexposición a la que se pueden exponer y sufrir como es el caso del acoso cibernético, el contenido inapropiado, la suplantación de identidad, el contacto con desconocidos, la práctica de sexting, entre muchos otros ya comentados en el epígrafe 4.4.

Requiere dar importancia la dependencia a la validación social, la constante necesidad de aprobación por parte del resto, que puede conllevar a la falta de autoestima, ansiedad, trastornos alimenticios para llegar a alcanzar los cuerpos que supuesta y socialmente se aprueban como perfectos. Se estereotipan modelos de vida y físicos que en la mayoría de los

casos no coinciden con la realidad que se muestra en las pantallas, condicionando así a los adolescentes a imitar actitudes y comportamientos para alcanzarlo; siendo realistas debemos decir que no solo ocurre en adolescentes, sino también en adultos, pero es importante destacar que las vivencias y experiencias que se experimentan con edades inferiores infieren notoriamente en la personalidad que va a desarrollar el menor.

Cuanto más avanzada es la edad del menor, mayores son los riesgos a los que se ve expuesto; con 16 o 17 años, ellos mismos no se consideran menores como tal, sino que se determinan autosuficientes para poder tomar sus propias decisiones; en parte y legalmente es cierto, pero en muchos otros aspectos no tienen la madurez emocional ni experimental suficiente para poder identificar y afrontar determinadas situaciones; y éste es el motivo de la facilidad a la hora de manipularles y condicionarles.

Conclusión VI: En cuanto al derecho a la educación digital considero que es una actualización del derecho fundamental a la educación recogido en el art 27 de la CE suponiendo un nuevo desarrollo y adaptación a las necesidades de la tecnología que han ido surgiendo en la sociedad digital. Este derecho a la educación digital nos presenta infinidad de ventajas entre las que podemos señalar el amplio acceso a la información, permitiendo a sus usuarios la posibilidad de acceder a una infinidad de recursos educativos en línea, incluyendo cursos, bibliotecas virtuales, materiales de estudio, etc.

Por otro lado, la educación digital permite la adaptación a las necesidades individuales de cada alumno, personalizando así la enseñanza en ritmo y horarios, facilitando la combinación con responsabilidades familiares o laborales. Otra de las ventajas que podemos mencionar es la eliminación de barreras tanto geográficas como económicas, mejorando la comunicación y colaboración tanto entre particulares como en equipos; superando las desigualdades producidas por los diferentes niveles económicos entre las familias o entre países más y menos desarrollado, que es lo que socialmente conocemos como brecha digital.

Por último, mencionar lo que en mi opinión es una de las ventajas más importantes como es la reducción del uso de recursos físicos, como el papel, los espacios físicos para oficinas o almacenaje de documentación, que a día de hoy ya se encuentra informatizada contribuyendo a una mejor sostenibilidad ambiental; pero no solo es importante por este ahorro sino por la automatización, rapidez, eficacia, velocidad a la hora de elaborar cualquier tipo de tarea además de mencionar la grandísima actualización diaria que permite, gracias a que la información se renueva y actualiza no solo diariamente, sino en cada momento.

7-. BIBLIOGRAFIA.

ASENSIO, P.A., en "Competencia y derecho aplicable en el Reglamento General sobre protección de Datos de la Unión Europea". Revista Española de Derecho Internacional, Vol. 69, Tomo I, 2017.

AYLLON GARCIA, J.D., en "Consentimiento de los menores de edad en las redes sociales: especial referencia a Tiktok". Pp 580-601. Disponible en: 24.-Jesús-Daniel-Aillón-580-609.pdf (revista-aji.com)

CARABALLO FOLGADO, A., en "Como funcionan los filtros parentales para niños en internet". Disponible en https://www.guiainfantil.com/articulos/educacion/nuevas-tecnologias/como-funcionan-los-filtros-parentales-en-internet/

CASTRILLO DE LA FUENTE, M., en "El tratamiento de datos de menores de edad, ¿qué dice el RGPD al respecto?". Disponible on-line en https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/el-tratamiento-de-datos-de-menores-de-edad-que-dice-el-rgpd-al-respecto-2018-06-28/

Comité Europeo de Protección de Datos, "Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3). Versión 2.1 del 12 de noviembre de 2019". Disponible on-line en https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_es.pdf

Datos especialmente protegidos. Disponible on-line en https://protecciondatos-lopd.com/empresas/datos-especialmente-protegidos-sensibles/#Que_son_los_datos_sensibles_o_especialmente_protegidos.

DE LA FUENTE MIGUELEZ, A., "El estatuto de los titulares de datos personales y la función estadística pública", en Estadística Española, Volumen 60, número 196/2018, pp. 89-90.

DE LA TORRE RODRIGUEZ, P.J., En "Tipos de ficheros de datos personales". Disponible on-line en https://elderecho.com/tipos-de-ficheros-de-datos-

personales#:~:text=Qu%C3%A9%20es%20un%20fichero%20de,%2C%20almacenamiento%2C%20organizaci%C3%B3n%20y%20acceso.

FERNANDEZ GONZALEZ, C.M., en "Estudio sobre el sistema de protección de datos personales con finalidad de prevención, detección e investigación policial de infracciones penales". Madrid, 2022. Disponible on-line en https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/seguridad-ciudadana/Estudio_sobre_el_sistema_de_proteccion_de_datos..._126220091.pdf

GARCIA ESPOSITO, A.L., Tesis doctoral sobre "El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (En busca del equilibrio entre la libertad y la seguridad)" con fecha del 24 de julio de 2014. Disponible on-line en https://www.tdx.cat/handle/10803/284352#page=257

GARCIA JIMENEZ, L.N., en "Uso que los menores hacen de las redes sociales y control parental". Disponible en https://core.ac.uk/download/pdf/211103186.pdf

GÓMEZ VIEITES, A., "Principales aspectos del Reglamento General de Protección de Datos (GDPR) de la Unión Europea" dispone on-line en: https://contactcenterhub.es/principales-aspectos-del-nuevo-reglamento-general-de-proteccion-de-datos-2016-01-5217/#Alvaro_Gomez_Vieites_consultor_de_Seguridad_Informatica_en_INPROSEC
-https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf

Grupo de Trabajo del Artículo 29 "Directrices sobre el derecho a la portabilidad de los datos", WP 242, diciembre de 2016.

GUDIN RODRIGUEZ-MAGARIÑOS. F., en "Nuevos delitos informáticos: Phising, Pharming, Hacking y Cracking". Disponible on-line en https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf. Pp. 3-4.

Guía de TikTok para padres y madres. Disponible on-line en: https://www.pantallasamigas.net/wp-content/uploads/2021/06/Guia-TikTok-Padres-Madres-PantallasAmigas.pdf

Guía de Twitch para padres y madres. Disponible on-line en: https://www.pantallasamigas.net/wp-content/uploads/2021/03/Guia-Twitch-madres-padres-PantallasAmigas-0523.pdf

Guía para centros educativos. Disponible en https://www.aepd.es/es/documento/guia-centros-educativos.pdf

Guía de protección de datos para el ciudadano de la Agencia Española de Protección de Datos. Disponible on-line https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf

GUTIERREZ MORALES, I. M.; Cyberbullying y sexting: percepción y propuestas de estudiantes universitarios. Multidisciplina. Disponible on-line en https://www.revistas.unam.mx/index.php/multidisciplina/article/view/50686

Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 100.

INTECO (Instituto Nacional de Tecnologías de la Comunicación). Guía sobre adolescencia y sexting: qué es y cómo prevenirlo. Disponible on-line en https://www.sexting.es/wp-content/uploads/guia-adolescentes-y-sexting-que-es-y-como-prevenirlo-INTECO-PANTALLASAMIGAS.pdf

LLANEZA, PALOMA., en "La Generación Z: incógnitos y privados". Disponible en https://www.injuve.es/sites/default/files/2017/28/publicaciones/documentos_10._la_generacion_z._incognitos_y_privados.pdf

Manual de legislación europea en materia de protección de datos. Edición de 2018. Disponible on-line en https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf

MONTALBANO, L., en Tesis Doctoral sobre "El reglamento europeo de protección de datos personales y el derecho al olvido". Madrid, 2019. Pp. 203-206.

OJEDA PEREZ, M., en Tesis doctoral sobre "Sexting en la adolescencia: Prevalencia, factores asociados y líneas de actuación psicoeducativa". Sevilla, 2021. Disponible on-line en https://idus.us.es/bitstream/handle/11441/108917/Ojeda%20P%c3%a9rez%2c%20M%c3%b3nica%20Tesis.pdf?sequence=1&isAllowed=y.

PEGUERA, M., en "Introducción a la protección de datos de carácter personal".

PRIDATEC en "Sanciones por incumplimiento e inadaptación al RGPD". Disponible on-line en https://www.pridatect.es/wp-content/uploads//2020/03/Sanciones_por_incumplimiento_RGPD-1.pdf

"Principio de confidencialidad en la LO 3/2018 (LOPDGDD) y en el Reglamento general de protección de datos (RGPD)". Disponible on-line en https://www.iberley.es/temas/principio-confidencialidad-lopdgdd-rgpd-62808

REYES KAHANSKY, C.M., en Tesis Doctoral sobre "Vigencia del Derecho Europeo de Protección de Datos personales".

SANCHEZ PARDO, L., CRESPO HERRADOR. G., en "Los adolescent4es y las Tecnologías de la Información y Comunicación". Disponible on-line en https://digital.csic.es/bitstream/10261/132633/1/TICPadres.pdf

SAURAS, I., en "Sharenting o la doble cara de compartir contenido de tus hijos en redes sociales". Agoso,2022. Disponible on-line en https://bebloomers.com/nosotras/maternidad-y-crianza/sharenting/.

VARIOS AUTORES en "Por el uso seguro de internet para niños, niñas y adolescentes" Disponible on-line en https://www.observatoriodelainfancia.es/ficherosoia/documentos/7051_d_FAPMI-TRIC.pdf

VARIOS AUTORES en: "Cuadernos jurídicos de derecho de familia". Disponible en: https://dadun.unav.edu/bitstream/10171/63987/1/Sharenting%20Protecci%C3%B3n%20europea%20para%20la%20defensa%20de%20los%20derechos%20digitales%20de%20los%20menores.%20Espa%C3%B1a.pdf

VILASAU SOLANA. M. y PEGUERA, M., en "Introducción a la protección de datos de carácter personal".

VILASAU SOLANA, M., en "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido" (análisis de la STJUE de 13 de mayo de 2014). Revista d'internet, dret i política. Junio, 2014

PÁGINAS WEB CONSULTADAS.

-https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia

-https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/?lang=es

-https://protecciondatos-lopd.com/empresas/tratamiento-datos-personales/

-https://dpd.aec.es/la-proteccion-datos-panorama-internacional-una-primera-aproximacion/

https://www.ine.es/jaxi/Datos.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c06002.px

-https://psicologiamonzo.com/todo-lo-que-debes-saber-sobre-el-bullying-y-el-ciberbullying/

-https://www.webempresa.com/blog/que-es-twitter-como-funciona-2.html

-https://help.twitter.com/es/managing-your-account/account-restoration

-https://www.pantallasamigas.net/menores-redes-sociales-edad-minima-datos-personales

-https://faq.whatsapp.com/695318248185629/

-https://onlyfans.com/terms#complaints-policy

-https://www.pantallasamigas.net/menores-redes-sociales-edad-minima-datos-personales/#:~:text=La%20edad%20media%20en%20la%20que%20un%20menor%20accede%20a%20su%20primer%20smartphone%20oscila%20entre%20los%2010%20y%20los%2012%20a%C3%B1os%2C%20aunque%20la%20edad%20m%C3%ADnima%20para%20acceder%20a%20una%20red%20social%20son%20los%2014%20a%C3%B1os.

-https://snap.com/es-ES/terms

LEGISLACIÓN CONSULTADA

Reglamento (UE) 2016/679, de 27 de abril, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, n.º L119/1, de 4 de mayo de 2016.

Convenio 108 modernizado para la protección de las personas con respecto al tratamiento de datos personales, hecho en Estrasburgo el 28 de enero de 1981.

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

España. Ley Orgánica 3/2018, de 5 de diciembre, Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado, de 6 de diciembre de 2018, núm. 294. Disponible on-line en https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

JURISPRUDENCIA.

STJUE (Gran Sala), de 13 de mayo de 2014, Google Spain, S. L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12).

Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, en asunto C131/12; que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Audiencia Nacional, mediante auto de 27 de febrero de 2012, en el procedimiento entre Google Spain, S.L., Google Inc. y la Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

Sentencia del Tribunal Constitucional (Pleno), núm. 292/2000, de 30 de noviembre. (Aranzadi: RTC 2000/292). Disponible on-line en https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276

Sentencia del Tribunal Constitucional (Sala 1.ª), núm. 254/1993, de 20 de julio. (Aranzadi: RTC 1993/254)

Sentencia del Tribunal Constitucional (Sala 2.ª), núm. 94/1998, de 4 de mayo. (Aranzadi: RTC 1998/94)