TRABAJO FIN DE GRADO

GRADO EN DERECHO

CURSO ACADÉMICO 2020-2021

29-07-2021

LA RESPONSABILIDAD CIVIL POR VULNERACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES

CIVIL LIABILITY FOR INFRINGEMENT OF DATA PROTECTION

Autor: PABLO MORENO FERNÁNDEZ

Tutor: JOSE LUIS SÁNCHEZ GALL

ÍNDICE

Responsabilidad civil por vulneración de la protección de datos

INTRODUCCIÓN

El rápido avance de las tecnologías, especialmente en el siglo XXI, ha propiciado un incremento en el número de redes sociales y por tanto, en usuarios adscritas a las mismas. Esta nueva modalidad de comunicación, mucho más masiva y ágil que las anteriores, puede dar lugar a violaciones continuas de derecho reconocidos constitucionalmente, como por ejemplo, el derecho al honor, a la intimidad personal y el derecho a la protección de los datos personales. Este trabajo se centra en la protección de los datos personales, cuya vulneración se produce a través del incumplimiento de las disposiciones de dos normas principalmente, la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales y del Reglamento (UE) 2016/679. También se estudiará cómo situaciones, como por ejemplo, la obtención de datos sin consentimiento, los datos de los menores sin consentimiento de sus tutores y la omisión a las solicitudes del interesado para ejercitar sus derechos, generarán responsabilidad civil, y pueden ser objeto de sanción conforme al régimen previsto en los artículos 70 y siguientes de la ley Orgánica 3/2018, e incluso los prestadores del servicio pueden incurrir en responsabilidad penal por sus actos, conforme a lo establecido en el Código Penal.

Abstract

The rapid advance of technologies, especially in the 21st century, has led to an increase in the number of social networks and, therefore, in the number of users attached to them. This new form of communication, much more massive and agile than the previous ones, can give rise to continuous violations of constitutionally recognized rights, such as the right to honour, personal privacy and the right to protection of personal data. This paper focuses on the protection of personal data, whose violation occurs through non-compliance with the provisions of two rules mainly, the Organic Law 3/2018 on Personal Data Protection and guarantee of digital rights and Regulation (EU) 2016/679. It will also be studied how situations, such as, for example, obtaining data without consent, data of minors without consent of their guardians and the omission to the requests of the data subject to exercise their rights, will generate civil liability, and may be subject to sanction under the regime provided in Articles 70 and following of the Organic Law 3/2018, and even the service providers may incur criminal liability for their actions, as provided in the Criminal Code.

DERECHO AL HONOR

La protección de los datos personales entra en colisión de forma directa contra dos derechos fundamentales recogidos en el artículo 18 de la Constitución Española como son el derecho al honor y el derecho a la intimidad personal.

Los derechos que recaen sobre la esfera privada de las personas no fueron recogidos en las constituciones españolas del siglo XIX y por tanto podemos considerar que su protección constitucional es bastante reciente[1]. Fue la Declaración Universal de Derechos Humanos de 1948 quién recogió por primera vez en su artículo 12 las injerencias en la privacidad de la vida de las personas, aunque no concretó expresamente el derecho al honor y a la intimidad sino que simplemente establecía que *"nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.* [2]

La posterior inclusión de estos derechos en la sección I, capítulo II, título I de la Constitución, garantiza una mayor protección de los mismos ya que junto a los recursos ordinarios, los individuos que vean vulnerados sus derechos al honor y a la intimidad personal gozan de legitimación para interponer el recurso de amparo. Este recurso de amparo solo es viable si la resolución judicial ordinaria no ha otorgado la protección a este derecho y es requisito previo e inexcusable agotar todos los recursos posibles en vía judiciales. En la práctica son pocos los recursos de amparo que superan el filtro exigido por el Tribunal Constitucional. [3]

La ley orgánica encargada de desarrollar de forma conjunta estos derechos es la "Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen."[4] Esta ley no establece unos criterios claros de distinción entre los derechos mencionados, sino que será la jurisprudencia del Tribunal Constitucional la que delimite el contenido esencial de cada uno de ellos.

[1] Francisco Balaguer Callejón, Manual de Derecho Constitucional Volumen II, 2018, Pág. 155.
[2] Resolución Asamblea General ONU 217 A (III), de 10 de diciembre de 1948.
[3] Ángel Acedo Penco, Los derechos de la Personalidad, Pág. 123
[4] LO 1/1982 BOE núm. 115, de 14/05/1982.

Respecto al derecho al honor, la STC 49/2001 de 26 de febrero (FJ 5) lo define como *"un derecho que ampara la buena reputación de una persona, protegiéndola frente a expresiones o mensajes que puedan hacerla desmerecer en la consideración ajena al ir en su descrédito o menosprecio o al ser tenidas en el concepto público por afrentosas."*[5]

El Tribunal Constitucional también aclara en su STC 216/2006, de 3 de julio (FJ 7) que este derecho es *"un concepto jurídico indeterminado cuya delimitación depende de las normas, valores e ideas sociales vigentes en cada momento, y de ahí que los órganos judiciales dispongan de un cierto margen de apreciación a la hora de concretar en cada caso qué deba tenerse por lesivo del derecho fundamental que lo protege (SSTC 180/1999, de 11 de octubre; 297/2000, de 11 de diciembre, FJ 7)"* [6]

DERECHO A LA INTIMIDAD PERSONAL

Por su parte, el derecho a la intimidad personal se puede definir en palabras del Diccionario del Español Jurídico,[7] como "el derecho a disfrutar de un ámbito propio y reservado para desarrollar una vida personal y familiar plena y libre, excluido tanto del conocimiento como de las intromisiones de terceros."

El Tribunal Constitucional amplia el concepto en su STC 231/1988 (FJ 4) ya que expone que *"el derecho a la intimidad personal, se extiende, no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen"* [8]

Al igual que el derecho al honor, cuya realidad es intangible y cuya delimitación va a depender de las normas sociales, valores e ideas sociales vigentes en cada momento, con el derecho a la intimidad personal ocurre algo similar. La STC 171/1990 de 12 de noviembre (FJ 4) matiza el perfil del derecho a la intimidad personal, la cual es concebida como una *"realidad intangible cuya extensión viene determinada en cada sociedad y en*

[5] BOE núm. 77, de 30 de marzo de 2001
[6] BOE núm. 185, de 04 de agosto de 2006
[7] https://www.conceptosjuridicos.com/derecho-a-la-intimidad/
[8] BOE núm. 307, de 23 de diciembre de 1988

cada momento histórico, cuyo núcleo esencial en sociedades pluralistas ideológicamente heterogéneas deben determinar los órganos del Poder Judicial." [9]

Ambos derechos fundamentales aparecen como derechos estrictamente ligados a la personalidad y por tanto vinculados íntimamente al respeto a la dignidad de la persona (STC 231/1988 FJ 3), recogido en el artículo 10.1 de la Constitución, que junto a "los derechos inviolables que le son inherentes, el libre respeto de la personalidad y el respeto a la ley y los derechos de los demás, son fundamento del orden político y de la paz social". [10]

El derecho a la intimidad es normalmente el más afectado al verse arrollado por el imparable avance de la tecnología y especialmente de Internet.[11] Todas las redes sociales y páginas web hoy en día requieren para su utilización el registro a través de un usuario y una contraseña privadas. Además de este paso previo, posteriormente, y dependiendo del tipo de web, se van a verter gran cantidad de datos personales en la web, ya sean fotos, datos bancarios etc., y se corre el riesgo de perder el control de esa información, lo cual hace que sea especialmente necesaria una protección por parte del legislador a los usuarios.

En referencia al derecho a la intimidad personal surge la denominada "teoría del mosaico", en contraposición a la teoría clásica de las esferas de privacidad, la cual diferenciaba entre "lo íntimo" en un círculo concéntrico más pequeño, y "lo privado" en un círculo más amplio. [12]

La "teoría del mosaico" afirma que existen gran cantidad de datos que por sí mismos son completamente irrelevantes. Ahora bien, si estos datos se relacionan con otros que aunque por sí mismos también puedan ser irrelevantes, esa combinación puede sacar a la luz la personalidad de un individuo. El símil con un mosaico es que las piedras individuales que forman parte del mismo no tienen ningún significado por si mismas pero cuando se unen entre sí, pueden formar un conjunto con un significado claro.

[9] BOE núm. 287, de 30 de noviembre de 1990
[10] BOE núm. 311, de 29/12/1978.
[11] Patricia Escribano Tortajada, "Los derechos a la intimidad y a la privacidad en el siglo XXI" Pág. 73
[12] Teoría del mosaico Fulgencio Madrid Conesa: Derecho a la intimidad, informática y Estado de Derecho, Valencia, Universidad de Valencia, 1984, pág. 45.

La jurisprudencia del Tribunal Constitucional se desvincula de la teoría del mosaico en su STC 110/1984, de 26 de noviembre (FJ 5) ya que en referencia a los datos bancarios afirma que *"estos datos en sí no tienen relevancia para la intimidad personal y familiar del contribuyente, como no la tiene la declaración sobre la renta o sobre el patrimonio"*. **13**

Por último, una breve referencia a las diferentes vías de protección de estos derechos de la personalidad su protección.

En primer lugar, la vía penal es el recurso más utilizado para la tutela de estos derechos. Los títulos X y XI del Código Penal recogen los delitos más graves contra la intimidad y el derecho al honor entre los que se encuentran la revelación de secretos, injurias y calumnias.**14**

En los casos en los que la lesión a estos derechos de la personalidad sea causada por la Administración Pública o en su caso por un ente público sometido al derecho administrativo será el orden contencioso-administrativo el encargado de llevar a cabo la protección necesaria.**15**

Junto a la vía constitucional y concretamente el recurso de amparo, ya comentada anteriormente, se encuentra la vía civil. En la normativa preconstitucional se acudía al "cajón de sastre" del artículo 1902 del Código civil *"El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado."***16** La vaga y abierta redacción de este artículo da lugar a que se puedan sujetar a él prácticamente todo tipo de reclamaciones. La Ley Orgánica 1/1982 de 5 de mayo afirma en la exposición de motivos que estos derechos gozarán de protección civil, y por tanto quedan sujetos a la protección que ofrece el orden jurisdiccional civil, sin perjuicio de su eventual protección penal.

En conclusión, los derechos al honor y a la intimidad personal, a pesar de ser derechos fundamentales van a tener sus límites a causa de su convivencia con los derechos de los demás, por tanto deben ser objeto de interpretación casuística para determinar en qué

[13] BOE núm. 305, de 21 de diciembre de 1984
[14] BOE núm. 281, de 24/11/1995.
[15] Francisco Balaguer Callejón, Manual de Derecho Constitucional Volumen II, Pág. 163
[16] Real decreto de 24 de julio de 1889 por el que se publica el Código Civil «Gaceta de Madrid» núm. 206, de 25/07/1889.

casos se vulneran de forma ilícita, o por el contrario, esa vulneración o intromisión está expresamente permitida por las leyes.

En ocasiones esa delimitación no se produce por la colisión con los derechos de los demás sino a raíz de proteger otros bienes constitucionalmente protegido como destaca el Tribunal Constitucional en la sentencia anteriormente citada (STC 110/1984, de 26 de noviembre, FJ 5) donde en esa ocasión, la revelación de datos bancarios no fue considerada como una intromisión ilegítima en el derecho a la intimidad personal ya que estaba *"justificada con la necesidad de proteger un bien constitucional, como es en este caso la distribución equitativa del sostenimiento del gasto público."* [17]

NORMATIVA REGULADORA

DERECHO DE LA UNIÓN EUROPEA

Europa cuenta con un complejo sistema normativo en materia de protección de datos personales. Parte de la base de las diversas declaraciones universales de derechos humanos y fundamentales y de las normas de derecho originario de la Unión, es decir los tratados, y se concreta con las diversas normas de derecho derivado emanadas de las instituciones de la Unión como son los reglamentos y las directivas comunitarias

En primer lugar, nos encontramos con la Carta de los Derechos Fundamentales de la Unión Europea del año 2000 la cual es jurídicamente vinculante para los Estados miembros a partir del 1 de diciembre de 2009, al entrar en vigor junto con el Tratado de Lisboa. Esta Carta, como se recoge en su preámbulo, tiene como objetivo el refuerzo de la protección de los derechos fundamentales con el fin de garantizar también así uno de los principios claves de la Unión como es la libre circulación de personas, servicios, mercancías y capitales. El artículo 8 de la Carta recoge el derecho de toda persona a la protección de los datos de carácter personal que le conciernan. Se exige un tratamiento leal de los datos y siempre mediando consentimiento del afectado o fundamento legítimo previsto en la ley. Por último recoge que será una autoridad independiente la que vele por el respeto de las normas.[18]

[17] BOE núm. 305, de 21 de diciembre de 1984
[18] DOUE, núm.364, de 18 de diciembre de 2000 (2000/C 364/01).

En segundo lugar, también está el Tratado de la Unión Europea, elaborado en Maastricht el 7 de febrero de 1992 por el que se sustituye la Comunidad Económica Europea para crear la actual Unión Europea. La nueva Unión se fundamentará tanto en este Tratado como con el Tratado de Funcionamiento de la Unión Europea, y ambos tendrán el mismo valor jurídico. El artículo 39 de este Tratado establece que será el Consejo el que establezca las normas acerca de la protección de las personas físicas en la relación con la protección de datos de carácter personal.

Por último en relación al derecho originario de la Unión tenemos el ya mencionado Tratado de Funcionamiento de la Unión Europea. ART 16. El artículo 1 establece que "*a través del presente Tratado se organiza el funcionamiento de la Unión y se determinan los ámbitos, la delimitación y las condiciones de ejercicio de sus competencias.*" Por tanto junto con el TUE, este será el texto del que posteriormente se concretarán las normas de derecho derivado. El artículo 16 del mismo hace una referencia casi calcada a lo anteriormente mencionado con la aclaración de que también el Parlamento Europeo participará junto al Consejo, y a través del procedimiento legislativo ordinario, en el *"establecimiento de las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos."* **[19]**

Considero que estos tres textos mencionados son suficientes para comprender la dimensión y la importancia que brinda la Unión a la protección de los datos personales. Estos textos son completados con las diversas directivas y reglamentos comunitarios a los que me referiré a continuación.

Las directivas comunitarias son normas que emanan de las instituciones de la Unión Europea pero no son directamente aplicables en los Estados miembros. Estos necesitan la denominada norma de transposición para incorporar una directiva a su ordenamiento jurídico.

[19] DOUE, núm. 149 de 7 de junio de 2016 (07/06/2016). Tratado de la unión Europea y Tratado de Funcionamiento de la Unión Europea (Versión consolidada)

Haciendo un recorrido por las directivas europeas en materia de protección de datos personales nos encontramos con 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 lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" cuyo plazo para ser transpuesta finalizó en 1998 y fue la primera regulación de esta materia a nivel europeo.

Se concretaron como objetivos iniciales la armonización de las normativas nacionales en esta materia, la eliminación de obstáculos para la libre circulación de los datos pero siempre con la garantía de los derechos que corresponden al interesado. [20]

Posteriormente se encuentra la directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Esta introduce ya los primeros caracteres de la protección de datos en materias más concretas como son las telecomunicaciones, en pleno auge en esos años. La Unión pretende con esta regulación acelerar la implantación de la tecnología e Internet a través de incrementar los servicios de telecomunicaciones entre los Estados miembros y siempre garantizando el respeto de los derechos de los afectados. Se configura como una directiva sectorial ya que hace referencia a una materia concreta, y por tanto debe colmarse con la normativa mencionada anteriormente, como es la directiva 95/56/CE que contiene el régimen general en materia de protección de datos personales. [21]

La directiva 2002/58/CE es modificada por una nueva en el año 2009, que es la directiva 2009/136/CE por la que se modifican tanto la ya mencionada, como la 2002/22/CE, y el Reglamento 2006/2004. En el tema que nos concierne, esta nueva norma refuerza las garantías del afectado estableciendo como el punto clave el consentimiento del mismo. Esto se recoge en el artículo 5 que establece "*Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE".* [22]

[20] Víctor Cazurro Barahona, Antecedentes y fundamentos del Derecho a la protección de datos, 2020, Pág. 125
[21] María de los Reyes Corripio Gil-Delgado, Revista de Contratación Electrónica
[22] «DOUE» núm. 337, de 18 de diciembre de 2009

Con las normas mencionadas anteriormente, podemos concluir con la evolución normativa que ha sufrido esta materia en lo que a directivas respecta, que se ha ido completando y modificando con el paso de los años, fruto del rapidísimo avance de las tecnologías en Europa lo cual ha exigido una constante adaptación de la normativa europea. Todo esto sin perjuicio de las normas nacionales de transposición, ya que la directiva al no aplicarse de forma directa y automática en cada país, cada Estado debe transponerla a su ordenamiento jurídico manteniendo obviamente los aspectos esenciales de las mismas pero ajustándolo a las exigencias y a la situación de cada Estado.

El reglamento europeo es una norma que al igual que las directivas emana de las instituciones europeas, pero la principal diferencia con esta es que es directamente aplicable y vinculante para los Estados miembros sin necesidad de implantarla en su ordenamiento jurídica a través de una a norma de transposición.

Me voy a centrar en el Reglamento 2016/679 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. Fue aplicable a partir del 25 de mayo de 2018 y en ese periodo transitorio se aplicaban las disposiciones de la Directiva con sus normas de transposición nacionales correspondientes, pero los Estados en ese período deben ir preparando sus mediadas para cumplir con las previsiones recogidas en el Reglamento. [23]

Se optó por la figura del Reglamento con el fin de unificar todas las normativas de los Estados miembros, por lo que al no dar lugar a normas de desarrollo diferentes en cada Estado, se conseguía la armonización perseguida por la Unión en esta materia.

En cuanto a los ámbitos de aplicación, el ámbito objetivo se incluye el "tratamiento total o parcialmente automatizado o tratamiento no automatizado de datos contenidos o destinados a un fichero". Este principio tiene alguna excepción como son por ejemplo las actividades no sometidas al derecho de la Unión. El ámbito de aplicación territorial se circunscribe principalmente a los datos de residentes en la UE como por ejemplo, en compra y venta de bienes o servicios y en controles de comportamiento. [24]

[23] «DOUE» núm. L 119, de 4 de mayo de 2016

[24] Publicaciones de la Agencia Española de Protección de Datos (AEPD)

Este reglamento recoge una serie de principios que son los principios de transparencia, minimización, confidencialidad y responsabilidad proactiva o "accountability".

Para la consecución de su objetivo introduce un conjunto de herramientas entre las que se encuentran un registro de actividades de tratamiento, evaluaciones de impacto sobre la privacidad, la posible creación de la figura de un delegado de protección de datos y las notificaciones de las violaciones de datos. [25]

Por último también se unifica el sistema de supervisión y el régimen sancionador en los territorios de aplicación del Reglamento. Se obliga a cada Estado Miembro a contar con una autoridad encargada de velar por la correcta aplicación del reglamento, que en el caso de España es la Agencia Española de Protección de Datos, cuyas competencias y funciones comentaré posteriormente.

Las sanciones pueden ser multas económicas, que deben ser disuasorias, proporcionales y efectivas, o pueden ser un elenco de "acciones correctivas" las cuales pueden aplicarse de forma individual o complementando a una multa económica. Dentro de este abstracto apartado de acciones correctivas se encuentran entre otros los apercibimientos, advertencias, limitaciones temporales e incluso la prohibición definitiva de tratamiento de datos.

DERECHO INTERNO

La Constitución, como ya he hecho alusión anteriormente, recoge en su artículo 18.4 el derecho de los ciudadanos a la protección de sus datos personales, mediante la limitación por ley del uso de la informática. Se reconoce este derecho, pero no de forma autónoma, sino vinculado al honor y a la intimidad personal. No será hasta el año 2000 cuando el Tribunal Constitucional reconozca al mismo como un derecho autónomo en su STC 290/2000 donde recalca que *"el apartado 4 del art. 18 CE garantiza un nuevo derecho fundamental, autónomo de otros, y muy en particular de los previstos en el apartado 1 de ese mismo precepto, esto es, los derechos al honor, a la intimidad personal y familiar y a la propia imagen"*. [26]

[25] M. Àngels Barbarà, Revista de Derecho VLEX
[26] BOE núm. 4, de 04 de enero de 2001

La primera norma que va a regir en nuestro país sobre esta materia, ya que antes se carecía de una regulación legal más allá del precepto constitucional, fue la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, más conocida como "LORTAD", que entró en vigor el 31 de octubre del año 1992. Fija por primera vez los principios relativos al tratamiento de los datos personales como el consentimiento y el deber de secreto entre otros. También crea la Agencia de protección de datos que pasará a denominarse Agencia Española de protección de datos en la LOPD de 2018.[27]

Posteriormente entra en vigor la Ley Orgánica 15/1999 de 13 de diciembre relativa a la protección de los datos de carácter personal. Esta norma transpuso la directiva europea 95/46/CE al ordenamiento español fuera de plazo, ya que el año límite de trasposición era 1998. A diferencia de la LORTAD, la nueva ley no ve la informática como un instrumento lesivo, sino como un medio necesario para el progreso de la sociedad, que debe complementarse con la protección de los derechos fundamentales.[28] Establece alguna novedad más a destacar frente a la LORTAD, como su artículo 2.1 [29] que afirma que la ley se aplica a los datos que se encuentren registrados en cualquier soporte, mientras que la LORTAD circunscribe su ámbito de aplicación únicamente a los figurados en ficheros automatizados.

En 2007 se dicta el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre. Entre las novedades destaca la exclusión del ámbito de aplicación los datos de las personas jurídicas. [30]

Por último y tras la aprobación del Reglamento Europeo 2016/679 de 27 de abril de 2016, desembocamos en la promulgación de la ley vigente actualmente en materia de protección de datos, la "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales

[27] XX Aniversario de la LORTAD: 20 años de protección de datos., Actualidad jurídica VLEX, 6 de noviembre de 2012
[28] Lucrecio Rebollo Delgado , Carlos Eduardo Saltor, El derecho a la protección de datos en España y Argentina. Orígenes y regulación vigente (2013), pág. 77 y pág. 104
[29] BOE núm. 298, de 14/12/1999.
[30] «BOE» núm. 17, de 19/01/2008.

y garantía de los derechos digitales". Fue aprobada con un 93% de apoyo parlamentario y se publicó en el Boletín Oficial del Estado el 6 de diciembre de 2018. [31]

Es una ley que consta de 97 artículos divididos en 10 títulos. Cabe resaltar una única disposición derogatoria, donde se indica expresamente la derogación de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de datos de carácter personal.

El objeto de esta ley, como afirma el artículo 1 de la misma es la adaptación del ordenamiento jurídico español al Reglamento Europeo 2016/679 y garantizar los derechos digitales de los ciudadanos conforme al artículo 18.4 del texto constitucional.

PRINCIPIOS DE PROTECCIÓN DE LOS DATOS

CONSENTIMIENTO DEL AFECTADO

El consentimiento del afectado es uno de los pilares básicas sobre los que pivota la regulación en materia de protección de datos. Según la Real Academia Española, se define como *"la manifestación de voluntad, expresa o tácita, por la cual un sujeto de vincula jurídicamente*." [32]

Por su parte, el Reglamento Europeo 2016/679, concreta aún más esta definición de consentimiento, exigiendo una "manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen." [33]

Como se puede observar, el concepto de consentimiento va acompañado de unas características inherentes al mismo, sin las cuales, no será válido. La Ley Orgánica 3/2018 se remite a la normativa europea a la hora de definir el consentimiento, concretamente en su artículo 6.1.

El consentimiento debe ser libre, es decir, no puede ser arrancado con intimidación o amenazas físicas. Según el artículo 1265 de nuestro Código Civil, "será nulo el consentimiento prestado por error, dolo, violencia e intimidación. El error invalidante deberá recaer sobre el objeto principal, de lo contrario el consentimiento será válido

[31] Gabilex. Revista del gabinete jurídico de Castilla la Mancha
[32] https://dle.rae.es/diccionario
[33] «DOUE» núm. 119, de 4 de mayo de 2016

(art. 1266 CC.). Por tanto, el consentimiento carecerá de validez si el sujeto no ha gozado de libertad para prestarlo. El considerando 43 del Reglamento 2016/679 recoge la presunción de que el consentimiento no ha sido libre cuando no se permita la autorización por separado de diferentes tratamientos. La presunción es "iuris tantum" por lo que se admite prueba en contrario, cuya carga corresponderá al encargado del tratamiento de datos. Dentro de este derecho al consentimiento libre también se encuentra la retirada del mismo a la que me referiré a continuación. [34]

En cuanto al requisito de "específico", se intenta otorgar un nivel mínimo de transparencia al interesado, ya que el consentimiento debe recaer en el uso concreto y específico al que se van a destinar esos datos, con el fin de no desviar la actividad, a la que se afectan esos datos, ya que en ese caso no contará con el consentimiento del afectado. La Agencia Española de protección de datos ha considerado que si al tercero no se le permite conocer la finalidad a la que se van a destinar sus datos, el consentimiento será nulo. [35]

El consentimiento también debe ser informado, esto es, el interesado debe conocer como mínimo ciertos aspectos esenciales, que según el considerando 42 del reglamento europeo, son tanto la identidad del responsable del tratamiento como la finalidad y el destino de los datos personales. En caso de desconocimiento por parte del afectado de algo no tipificado como "contenido mínimo" según lo establecido en el Reglamento, se podría acudir subsidiariamente al régimen contemplado en el Código Civil sobre el error invalidante, como por ejemplo el que recae sobre condiciones que principalmente hubiesen dado motivo a celebrarlo (art 1266), en nuestro caso, a consentir el tratamiento de datos.

Por último, un consentimiento inequívoco es aquel que se presta sin que dé lugar a dudas, equivocaciones o interpretaciones. El Reglamento europeo contempla varias posibilidades entre las que se encuentran el marcado de una casilla en una página web, o las conductas tendentes claramente a la aceptación de la propuesta de tratamiento de datos. Por otro lado, se prohíbe expresamente que el silencio, o la inacción den lugar a un consentimiento válido, y se exige una clara acción afirmativa, como recoge el considerando 32 del Reglamento.

[34] Andoni Polo Roca, El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado, Revista de Derecho Político

[35] Recomendación de la AEPD sobre Comercio Electrónico del 2000.

Sendas sentencias del Tribunal Constitucional han recogido la posibilidad de revocar el consentimiento, ya que la revocación, según el TC, entra dentro de la esfera del derecho del individuo. La STC 196/2006, de 3 de Julio (FJ 6) afirma que *"debemos inmediatamente considerar que pertenece a su ámbito de libertad revocar en cualquier momento ese consentimiento*"[36]. Por su parte la STC 159/2009, de 29 de junio (FJ 3) sostiene que *" la afectación no será ilegítima cuando medie el previo consentimiento (eficaz) del afectado, que permite la inmisión en el derecho a la intimidad y que, lógicamente, puede ser revocado en cualquier momento"* [37]. Es importante resaltar que la revocación del consentimiento goza de efectos *"ex nunc"* es decir, desde ahora, a diferencia de los efectos *"ex tunc"* que son "desde siempre" por tanto el tratamiento previo a la retirada del mismo no se verá afectado.

En conclusión, si el interesado decide retirar su consentimiento por cualquier motivo, este debe poder hacerlo libremente sin sujeción a condiciones, de lo contrario verá vulnerado su derecho.

CONSENTIMIENTO DE LOS MENORES DE EDAD

Con la expansión al alza de la tecnología y la informática, cada vez son más personas las que tienen acceso a las redes, entre los que evidentemente, se encuentran los menores de edad. La mayoría de edad en España se alcanza a los 18 años cumplidos, como se expresa en el artículo 315 del Código civil. Se requiere una protección especial para este sector de la sociedad que comporta casi el 20% de la población total y que es especialmente más vulnerable.[38]

El artículo 1263 del Código Civil establece que no pueden prestar consentimiento *"Los menores no emancipados, salvo en aquellos contratos que las leyes les permitan realizar por sí mismos o con asistencia de sus representantes, y los relativos a bienes y servicios de la vida corriente propios de su edad de conformidad con los usos sociales"*. [39] Se

[36] BOE núm. 185, de 04 de agosto de 2006
[37] BOE núm. 181, de 28 de julio de 2009
[38] https://datosmacro.expansion.com/demografia/estructura-poblacion/españa
[39] Real decreto de 24 de julio de 1889 por el que se publica el Código Civil «Gaceta de Madrid» núm. 206, de 25/07/1889

entiende por tanto que en este caso serán sus padres quienes ostenten la representación legal del menor no emancipado.

Sin embargo, el artículo 162 del Código Civil establece una excepción a lo anterior, y es que para *los "actos relativos a los derechos de personalidad del hijo, que de acuerdo a su madurez, pueda ejercitar por sí mismo, no se requerirá de la representación legal de los padres".* Como se ha reiterado anteriormente, el derecho a la protección de los datos es un derecho de la personalidad, por ello es de aplicación este artículo.

El Reglamento Europeo consideró que la edad adecuada para que un menor de 18 pueda prestar consentimiento por sí mismo es de 16 años. Sin embargo se dejó libertad a los Estados miembros para establecer una edad mínima por debajo de 16, siempre que no fuera inferior a 13 años, que es por tanto, un límite absoluto.[40]

El legislador español fijó esta edad en los 14 años. El tratamiento de datos será lícito si se ha obtenido con el consentimiento del mayor de 14 años salvo excepciones que contemplen las leyes específicas o determinados contratos. Actualmente no hay una disposición reglamentaria que desarrolle la Ley Orgánica 3/2018 por lo que mencionaré brevemente lo que recogía el derogado Real Decreto 1720/2007, por el que se desarrollaba la Ley Orgánica 15/1999.

El artículo 13 de la norma reglamentaria recogía, para los mayores de 14 años, una presunción general de madurez gracias a la cual se les permitía prestar el consentimiento de forma válida. Esta corriente ha sido tomada también por la Ley 3/2018. Para los mayores de 14 años se establece también alguna limitación respecto a la materia sobre la cual pueden prestar el consentimiento ya que por ejemplo, se veta la información relativa a los miembros del núcleo familiar. [41]

Volviendo al Reglamento Europeo 2016/679, una curiosidad a destacar es que hace referencia a los menores utilizando el término "niños". Establece que estos necesitan una especial protección en la materia al no ser apenas conscientes de los riesgos y las consecuencias que supone el tratamiento de datos. [42]

[40] «DOUE» núm. L 119, de 4 de mayo de 2016
[41] Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua (2016)
[42] Víctor Cazurro Barahona, Derecho digital (2017), pág. 249

En relación al principio de transparencia, cuya exigencia principal es que la información facilitada sea accesible y sencilla de comprender, el considerando 58 del Reglamento recoge que la información concerniente a los niños les sea transmitida en un lenguaje adecuado a su edad, madurez y comprensión, es decir, utilizando un vocabulario sencillo y sin abusar de tecnicismos.

Por último, mencionar que la situación de los incapaces es prácticamente igual que la de los menores. Si por su cuenta no pueden prestar el consentimiento debido al grado de incapacidad que tienen, serán sus representantes legales los encargados de otorgarlo. En este supuesto no rige una edad mínima como en el caso de los menores, sino lo dispuesto en una resolución judicial firme que acredite el grado de incapacitación que tiene el afectado. En régimen jurídico de los incapaces se recoge en los artículos 199 y siguientes del Código Civil.

TRATAMIENTO DE DATOS POR OBLIGACIÓN/IMPERATIVO LEGAL

A pesar de que el consentimiento es un requisito indispensable para el tratamiento de datos personales, existen excepciones, en las cuales no será necesario. Están recogidas taxativamente en el Reglamento Europeo y en la Ley Orgánica 3/2018.

La primera excepción tiene un carácter más general y es que según el artículo 8.1 de la Ley Orgánica 3/2018, *''no será necesario el consentimiento cuando el tratamiento pueda fundarse en el cumplimiento de una obligación legal exigible al responsable, siempre que esté dispuesto en una norma de derecho europeo o en una norma de derecho interno de rango legal*." El artículo 8 de la Ley 3/2018 se remite prácticamente en su totalidad a lo establecido en el reglamento europeo.

En los casos de ejecución de un contrato donde el interesado es parte no será tampoco exigido el consentimiento, ya que se sobreentiende que para el perfeccionamiento del contrato ya otorgó ese consentimiento, sin el cual no existiría, como indica el artículo 1261 del Código Civil. [43]

Tampoco se requiere el consentimiento cuando sea necesario la protección del interés vital del afectado o de otra persona física. Se entiende por interés vital algunas situaciones

[43] Miguel Marcos Ayjón, La protección de datos de carácter personal en la justicia penal (2020)

extraordinarias, como catástrofes naturales o de emergencia humanitaria. La actual situación de pandemia derivada del Covid-19 se puede considerar como un interés vital para la licitud del tratamiento de datos.[44]

Un supuesto en el que voy a profundizar más es en el tratamiento de datos sin necesidad de consentimiento derivado de las funciones propias de la Administración Pública, y particularmente en referencia a la pandemia del coronavirus y el tratamiento de datos relativos a la salud por las administraciones sanitarias.

Interpretando el Reglamento Europeo se puede dilucidar que éste considera a las autoridades sanitarias como "responsables del tratamiento" ya que su función es reducir la expansión del virus y esto es claramente un interés vital que permite el tratamiento de datos sin el consentimiento del interesado. [45]

Añadir también que el considerando 54 del Reglamento Europeo incorporado el interés público en el ámbito de la salud pública, que también habilita el tratamiento de datos sin consentimiento, aunque recoge diversas exigencias para su licitud. Establece textualmente que *"Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) nº 1338/2008 del Parlamento Europeo y del Consejo (1), es decir, todos los elementos relacionados con la salud, concretamente el estado de salud".*

En lo que en el entorno de esta pandemia respecta, entre los principales tratamientos de datos relacionados con la salud que gozan de interés público han destacado, aparte del estado de las hospitalizaciones como es evidente tanto en planta como en UCIs, las pruebas PCR y los contactos estrechos de los afectados. Sobre todo, los positivos arrojados por dichas pruebas, ya que estos tienen una influencia directa tanto en la imposición como en la relajación de medidas y restricciones adoptadas por las diferentes administraciones territoriales para la lucha contra el virus. [46]

Por tanto, se puede concluir que el tratamiento de datos de salud ha sido un elemento rigurosa actualidad en este período actual, y la licitud del mismo no ha sido basada

[44] https://www.iberley.es
[45] Estado de alarma y protección de la privacidad en tiempos de pandemia UNED. Revista de Derecho Político N.º 110, enero-abril 2021
[46] Martín Guardado, S. (2020). La protección de los sanitarios ante el coronavirus como interés público: reflexiones más allá del derecho a la seguridad y salud en el trabajo

mayoritariamente en el consentimiento, como es habitual en esta materia, sino que ha sido respaldado por las excepciones que recoge las normas europeas e internas frente al régimen general, como son el interés vital y el interés público.

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RÉGIMEN JURÍDICO

La normativa europea impuso a los Estados miembros la creación de una autoridad independiente con el fin de controlar el cumplimiento de las disposiciones en materia de protección de datos. La autoridad en nuestro país fue creada por la LORTAD en el año 1992 y cambió su denominación con la entrada en vigor de la Ley Orgánica 3/18 pasándose a denominar Agencia Española de Protección de datos (AEPD).

Este órgano es uno de los previstos en los artículos 109 y 110 de la Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público. Las define como autoridades que gozan de personalidad jurídica propia y vinculadas a la Administración del Estado, en este caso, la AEPD está relacionada con el Ministerio de Justicia. Van a tener unas funciones atribuidas por ley y que desempeñarán de forma independiente en una sección determinada como es la materia de protección de datos. Otros ejemplos de Agencias estatales pueden ser la de medicamentos y productos farmacéuticos o la de antidopaje. Como se puede observar, se les asignan una serie de materias más específicas que las generales de Justicia y Sanidad. [47]

COMPOSICIÓN

Será el Gobierno, a propuesta del Ministro de Justicia el que nombre a la Presidencia y a su adjunto de la AEPD *"entre personas de reconocida competencia especialmente en materia de protección de datos"*, como dispone el artículo 48.3 de la LO 3/2018.

La directora de la AEPD hoy en día es Mar España Martí, y fue nombrada en julio de 2015. Como directora, ostenta la representación de la Agencia y es de su competencia el dictado de resoluciones y ejecuciones que se requieran en el ejercicio de sus

[47] BOE núm. 294, de 06 de diciembre de 2018

competencias. Así mismo la compete la resolución de los expedientes sancionadores y en materia de inspección, es la encargada de autorizar la entrada a locales y demás establecimientos donde se encuentren los ficheros objeto de la inspección. [48]

Por último, corresponde a la Directora la aprobación de gastos y la ordenación de pagos siempre dentro del límite presupuestario, llevar a cabo la supervisión y el control económico- financiero, y convocar las reuniones del Consejo Consultivo.

El artículo 48.5 de la Ley 3/2018 establece que *el "mandato tendrá la duración de 5 años desde el nombramiento, y puede ser renovado por otro período igual al anterior"*

El mandato de la Presidencia puede expirar antes de los 5 años, ya sea a instancia propia o disolución acordada por el Consejo de Ministros, si concurren alguna de las causas recogidas en el artículo 48.5 de la LO 3/2018 que *son "incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad, o condena firme por delito doloso"*. En todos estos supuestos a excepción de la condena firme por delito doloso, será necesaria para llevar a cabo la separación, una ratificación por parte del Congreso con una mayoría de tres quintos en primera votación, y de no alcanzarse ésta, una mayoría absoluta en la 2 votación.

Existe una problemática actual en la dirección de la AEPD, ya que el mandato de Mar España Martí expiró en julio de 2020 puntualizando que no se presentaría a la reelección y por tanto no renovaría su cargo por otros 5 años. El Ministerio de Justicia a través del BOE, sí publicó la lista de posibles candidatos con 2 meses de antelación a la expiración del mandato como exige el artículo 48. El Gobierno hizo oídos sordos y no se ha nombrado ningún sucesor en la presidencia de la AEPD y actualmente continúa Mar como directora de la Agencia a pesar de que ella misma bromea con que "está en un mandato caducado". [49]

El artículo 49 de la Ley Orgánica 3/2018 decreta que la Presidencia de la AEPD estará asesorada por un Consejo Consultivo formada un número amplio de miembros entre los que se encuentran un diputado, un senador, un representante designado por el Consejo General del Poder Judicial y una miembro de la Administración General del Estado. Todos ellos deben contar con aptitudes y veteranía en la materia.

[48] https://www.aepd.es/
[49] vozpopuli.com

El Consejo consultivo debe reunirse como mínimo una vez al semestre, y cuando así lo disponga la Presidencia. A pesar de todo El consejo Consultivo no va a ser de gran importancia real, pues como dispone el artículo 49.5, "*las decisiones tomadas por el Consejo Consultivo no van a tener en ningún caso carácter vinculante."*

Por último, no existe únicamente un órgano competente en esta materia en nuestro país, sino que existe una descentralización de Agencias de Protección de datos que corresponden con las 17 comunidades autónomas y se denominan autoridades autonómicas de protección de datos. Van a gozar de competencias dentro del ámbito territorial de su comunidad autónoma, incluyendo los entes locales, y deben actuar siempre conforme al Reglamento 2016/679 y la Ley Orgánica 3/2018. Será la AEPD estatal la encargada de subsanar posibles incumplimientos de las agencias autonómicas, imponiendo un mes para que encaucen sus medidas, o de lo contrario tienen legitimación activa para acudir ante la jurisdicción contencioso-administrativa.

FUNCIONES Y POTESTADES

Las competencias de la AEPD denominada por el Reglamento 2016/679 como autoridad de control principal, ya que en cada Estado miembro tiene una denominación, vienen recogidos en los artículos 52 y siguientes de la Ley Orgánica, y en los artículos 57 y 58 del Reglamento Europeo.

Se establece como regla general un deber de colaboración con la AEPD, previsto en el artículo 52, para las Administraciones públicas, donde se recalca la Seguridad Social y la tributaria, pero también para los particulares, de aportar los documentos con el fin de facilitar las pertinentes investigaciones.

En materia de investigación, en caso de que sea necesario el ingreso a un domicilio protegido por el artículo 18.2 de la Constitución, se requiere el beneplácito del interesado, o en ausencia de esta, una autorización judicial. Sin embargo, esto no es de aplicación a inspecciones llevadas a cabo por ejemplo, en locales comerciales, ya que no se consideran domicilio constitucionalmente protegido, y por tanto es suficiente una autorización de la dirección de la AEPD.

En el ámbito internacional, la AEPD es competente para la firma de Convenios y acuerdos en el marco de la Unión y también representará al Reino de España en las Asambleas y congresos internacionales ajenos a la Unión.

Por último, y en relación a la situación actual, la AEPD ha emitido un comunicado en el que habilita al Ministerio del Interior a monitorizar las redes sociales con el fin de acabar con la difusión de "fake news" acerca del Covid-19.

Con ello, se pretende acabar con la expansión de bulos y noticias falsas acerca de la pandemia, y que puedan aumentar la tensión y crispación social a cambio de una rentabilidad económica. La vigilancia se circunscribe únicamente al ámbito de las redes sociales, principalmente Twitter y Facebook, quedando fuera del control, entre otros, la prensa escrita.[50]

DERECHOS DEL INTERESADO

La Ley Orgánica 3/2018 y el Reglamento Europeo 2016/679 recogen un elenco de derechos del interesado frente al tratamiento de sus datos personales. El afectado podrá ejercitar estos derechos de forma directa o a través de un apoderado ya sea voluntario o legal. En el caso de los menores de edad, serán los que ostenten la patria potestad los representantes encargados de ejercitar estos derechos.

En primer lugar se encuentra el derecho de acceso, recogido en el artículo 13 de la LOPD, que dispone que el afectado tiene el derecho a solicitar al responsable el acceso a los datos que está tratando. En caso de ser una cantidad amplia de datos, el responsable puede exigir previamente la especificación de los datos a los cuales quiere acceder. Entre la información la cual el afectado tiene derecho a supervisar se encuentran entre otros, los destinatarios de los datos y la finalidad del tratamiento.

Posteriormente nos encontramos ante el derecho de rectificación, regulado en el artículo 14 de la LOPD, que remite al artículo 16 del Reglamento 2016/679. Como su propio nombre indica, el afectado tiene derecho a rectificar datos personales erróneos o

[50] https://www.europapress.es/

equivocados que le atañen, e incluso a través de una declaración adicional posterior, puede completar los mismos en caso de que sean insuficientes.

El derecho de supresión, también denominado "derecho al olvido" se recoge en el artículo 15 de la LOPD y el en artículo 17 del Reglamento 2016/679. Se habla del derecho al olvido como un derecho de cancelación cuya esencia es la supresión por parte del responsable y a petición del afectado de los datos que le incumban. [51]

El reglamento europeo exige la manifestación de alguna de las condiciones siguientes para el ejercicio de este derecho de supresión. De entre los requisitos más importantes para llevar a cabo la supresión se encuentran la retirada del consentimiento, la irregularidad del tratamiento, o la exigencia de supresión en aras del cumplimiento de una obligación legal.

El artículo 16 de la LOPD recoge el derecho a la limitación del tratamiento, donde el afectado puede exigir la limitación del tratamiento si concurren alguna circunstancia como la impugnación de la exactitud de los datos, o en caso de tratamiento ilícito, el interesado puede renunciar al ejercicio del derecho de supresión apostando por la limitación de los mismos.

Por último se encuentran los derechos de portabilidad y el derecho de oposición, recogidos en los artículos 17 y 18 respectivamente de la LOPD.

El derecho de portabilidad se basa sencillamente en el "transporte o transmisión" de los datos un responsable a otro, llevado a cabo por el interesado, y sin que lo impida el responsable originario. El artículo 20 del Reglamento exige que *"el tratamiento se realice por medios automatizados"*. También decreta en el punto 4 que este derecho no puede colisionar con los derechos y libertados de los terceros si supone un perjuicio para ellos.

Finalmente el derecho de oposición ofrece la posibilidad al interesado de impedir que sus datos personales sean objeto de tratamiento. El interesado puede alegar motivos vinculados con sus circunstancias personales.

Todos estos derechos surgen por el mero tratamiento de datos, por lo que su ejercicio no supone que haya habido un incumplimiento por parte del responsable ni dan lugar a

[51] Anuario de la Facultad de Derecho de la Universidad de Alcalá Núm. X-2017, Enero 2017 Nuevos perfiles del derecho al olvido en Europa y España

responsabilidad civil o penal. Será el título VII de la LOPD el que recoja el procedimiento en caso de vulneración de la protección de datos así como el régimen sancionador.

PROCEDIMIENTO DE RESPONSABILIDAD

Este procedimiento se regula en los artículos 63 y ss. de la LOPD y los supuestos en los que se inicia son en caso de vulneración de los derechos comentados anteriormente, regulados en los artículos 15-22 del Reglamento Europeo, y en las investigaciones de la AEPD sobre presuntas infracciones de lo establecido en la LOPD o el Reglamento europeo.

Las normas reguladoras de este procedimiento serán tanto lo dispuesto en el Reglamento 2016/679 como la Ley Orgánica 3/2018 y de forma subsidiaria se aplicarán las disposiciones de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

El Reglamento 2016/679 en su artículo 79 recoge el derecho de los interesados a la tutela judicial efectiva contra los responsables del tratamiento de datos por la una violación de sus datos en el transcurso del mismo. Señala que la competencia para conocer de estos asuntos recaerá sobre los tribunales donde el responsable del tratamiento esté establecido. Recoge también un foro de competencia alternativo, dando la posibilidad al interesado de acudir a los Tribunales del Estado miembro donde tenga su residencia habitual. En este último caso, se excepciona lo dispuesto anteriormente en el caso de que el encargado sea una autoridad pública de un Estado miembro actuando en el ejercicio de sus funciones públicas. Por tanto, los foros de competencia serán alternativamente los tribunales del Estado miembro donde se encuentre el establecimiento del encargado o la residencia habitual del interesado.

El afectado, como recoge el artículo 80 del Reglamento Europeo, goza del derecho de apoderar a una entidad o asociación sin ánimo de lucro, experta en materia de protección de datos, para que ostente su representación en el procedimiento, lo que incluye la presentación de la reclamación, y el ejercicio de los derechos que corresponden al interesado, donde se inserta el derecho a la indemnización del artículo 82 del Reglamento.

Como he mencionado anteriormente, podemos encontrarnos ante varios tipos de reclamaciones.

En caso del procedimiento por caso omiso del responsable a los requerimientos de los interesados para ejercitar sus derechos de los artículos 15-22 del Reglamento (derecho de acceso, rectificación etc.), se iniciará el procedimiento por acuerdo de admisión a trámite. El procedimiento durará 6 meses, y el "dies a quo" [52] corresponde con la fecha de notificación del acuerdo de admisión a trámite. En caso de silencio administrativo, operará la vertiente positiva del mismo tras el transcurso de ese plazo, es decir, el interesado podrá considerar estimada su reclamación, como dispone el artículo 64.1 LOPD.

El otro tipo de procedimiento al que me referiré es el de la violación de las disposiciones del Reglamento Europeo o la LOPD, regulado en el artículo 64.2 de la LOPD. En este caso el procedimiento puede iniciarse a través de 2 vías, bien derivado de una reclamación, o a instancia de la Agencia Española de Protección de Datos.

En este caso, a diferencia del anterior, la duración del procedimiento de prolonga hasta los 9 meses desde el acuerdo de inicio. La finalización del procedimiento sin una resolución expresa determinará la caducidad del mismo. La LOPD no recoge en este caso la posibilidad de un silencio administrativo favorable o desfavorable para el interesado.

El artículo 65 de la LOPD regula la admisión a trámite de las reclamaciones ante la AEPD. Es un paso esencial, ya que para incoar el procedimiento, primero debe ser admitido, es decir debe cumplir unos requisitos mínimos.

El artículo 65.2 no recoge los requisitos expresamente, sino que regula a "sensu contrario" lo que no debe contener la reclamación. Afirma que cuando las solicitudes no se refieren a temas de protección de datos, no tengan fundamento manifiesto o sean desmesuradas no pasarán este filtro y serán inadmitidas.

La resolución de la admisión a trámite se debe notificar al interesado en el plazo de 3 meses a contar desde la fecha de presentación de la reclamación. En caso de silencio, se entenderá admitida a trámite la petición y se continuará con el procedimiento.

El artículo 67 de la POPD prevé la posibilidad de que la AEPD lleve a cabo unas investigaciones previas cuya duración no puede ser superior a 12 meses, cuya finalidad

[52] https://guiasjuridicas.wolterskluwer.es/

es la especificación de los hechos y las vicisitudes con el fin de justificar si es conveniente la preparación del procedimiento.

Por su parte, el artículo 69 establece unas medidas provisionales, también denominadas cautelares en el curso del procedimiento con el fin de proteger el derecho a la protección de datos y que no se desvirtúen el proceso, concretando como una de las principales medidas el bloqueo cautelar de datos.

El Reglamento también da solución a un posible caso de litispendencia, es decir, la problemática existente derivada de juzgarse 2 asuntos en distintos tribunales en los que coinciden objeto causa e identidad.

Contempla la posibilidad de que el segundo tribunal, en cuanto conozca que el tribunal ante que se presentó la acción es competente, puede suspender el procedimiento en tanto no se resuelva el anterior. En caso en que el primer tribunal se declare de oficio incompetente, el tribunal que suspendió temporalmente el procedimiento podrá reanudar al mismo y dictar la resolución que considere.

Por último, el artículo 82 del Reglamento contempla la indemnización al afectado por la vulneración de la normativa de datos personales, indemnización que correrá a cargo del responsable o encargado del tratamiento. Eso sí se establece expresamente que el encargado sólo será responsable en caso de incumplimiento de las obligaciones dispuestas en el Reglamento, o de la actuación al margen de las mismas, pero no en otros casos. Por tanto, se circunscribe la responsabilidad del responsable del tratamiento al ámbito únicamente de las obligaciones recogidas en el Reglamento.

Como es lógico, el responsable goza de la presunción de inocencia y no puede ser declarado responsable salvo que se pruebe fehacientemente y con los medios de prueba admitidos en derecho que es el culpable del incumplimiento de las obligaciones recogidas anteriormente.

Si se da una pluralidad de sujetos responsables, es decir concurren encargados y responsables en la vulneración de la normativa, o no es posible determinar exactamente a quién corresponde la responsabilidad, el Reglamento opta por la responsabilidad solidaria, y cada persona será responsable por todos los daños causados, ya que el bien jurídico a proteger es siempre el interesado, que debe recibir su pertinente indemnización.

Sin perjuicio de lo anterior, una vez el afectado haya recibido su indemnización, abonado en su totalidad por uno de los responsables como consecuencia de la responsabilidad solidaria, éste gozará de una acción de regreso para repercutir contra el resto de responsables y reclamar la parte correspondiente a su cuota de participación, que normalmente será la misma para todos. Por tanto al igual que ocurre en el ámbito civil en caso de deudores solidarios, uno de los responsables paga la totalidad de la indemnización al afectado pero luego está legitimado para solicitar al resto que le abonen la parte que les correspondería .

RÉGIMEN SANCIONADOR

Tanto la Ley Orgánica 3/2018 como el Reglamento Europeo contemplan una serie de sanciones de carácter administrativo para los responsables de tratamiento de datos que hayan incurrido en la violación de las normas de carácter comunitario.

Se tipifican en tres categorías (muy graves, graves y leves) las infracciones, distinción imprescindible a la hora de fijar la horquilla de la cuantía de la multa y el plazo de prescripción de cada acción que da lugar al nacimiento de la responsabilidad.

En primer lugar, el artículo 72 de la Ley 3/2018 establece un elenco de las infracciones más graves en el que se aprecian las constantes remisiones a la normativa europea.

Entre ellas destacan el impedimento y la oposición de la correcta realización inspectora de la autoridad competente, el desvío en la utilización de los datos sobre los que recayó el consentimiento del afectado y la transferencia internacional de datos a un tercero ubicado en un país sin apenas controles y garantías en la materia, lo que supone una manifiesta violación de la protección del interesado.

Las infracciones muy graves, prescribirán a los 3 años, como así lo refleja el artículo 72 LO 3/2018.

Las infracciones graves, tipificadas en el artículo 73 de la Ley Orgánica 3/2018, tienen un plazo de prescripción de 2 años, siempre a contar desde el día que se cometió el acto ilícito, y en caso de ser continuado desde que se realizó el último acto.

Entre las infracciones consideradas graves, se encuentran el tratamiento de datos sin la previa obtención del consentimiento por parte del afectado y las trabas a la hora de

garantizar los derechos de los artículos 13 al 18 de la Ley, como son el derecho de acceso, rectificación y sucesivos.

Por último, las infracciones leves, recogidas en el artículo 74 de la Ley Orgánica 3/2018, y cuyo plazo de prescripción es de 1 año, se basan en incumplimientos de menor grado respecto a las anteriores. Tienen el carácter de leves la falta de llevanza de códigos de conducta y de un registro de tratamiento, las notificaciones defectuosas a la autoridad supervisora, y la desatención a las solicitudes de los interesados.

La prescripción de las infracciones, puede ser interrumpida, como recoge el artículo 75 de la Ley Orgánica 3/2018, por el acuerdo de incoación del procedimiento sancionador puesto en marcha por la autoridad competente.

Es necesario la válida notificación al afectado, ya que en caso de que la notificación no llegue al interesado por adolecer de vicios, seguirá corriendo el plazo. Además si el procedimiento sancionador se detiene sin culpa del afectado, éste caducará a los 6 meses y el plazo de prescripción se reiniciará.

Al igual que prescriben las infracciones, las sanciones hacen lo propio, y su régimen se recoge en el artículo 78 de la Ley Orgánica 3/2018. Se establece la diferencia a razón de la cuantía. Prescribirán a los 3 años las sanciones cuyo importe sea superior a 300000 euros, al año las que su cuantía se fije en 40000 euros o menos, y las sanciones situadas en la horquilla de los 40001 a los 300000, prescribirán en el plazo de 2 años. El "dies a quo" comenzará con la ejecutividad de la sanción, es decir, al día siguiente del dictamen de la resolución sancionadora, o cuando finaliza el periodo que goza el afectado para interponer el recurso pertinente. La prescripción, al igual que el caso anterior se interrumpirá en caso de notificarle al afectado la iniciación del procedimiento para ejecutar la sanción, procedimiento que caduca a los 6 meses.

Por último, se establece un régimen especial en el artículo 77 de la Ley Orgánica 3/2018 para las sanciones impuestas a determinados organismos, entre los que destacan los órganos jurisdiccionales, las administraciones territoriales, los grupos parlamentarios y el Banco de España.

En caso de que estas instituciones comentan una posible vulneración de lo dispuesto en la ley orgánica y en el reglamento europeo, la autoridad competente emitirá un apercibimiento, es decir, un aviso o una amonestación previa, con el fin de que la entidad

cese en su conducta. Por tanto, no se aplica directamente el régimen sancionador, como ocurre con el resto de responsables.

Este régimen se ve alterado cuando se aprecien vestigios o indicios por parte de la autoridad competente de que ha existido una conducta antijurídica. En este caso, se seguirá el régimen general sancionador dispuesto en los artículos 70 a 78 de la Ley Orgánica 3/2018.

RESPONSABILIDAD PENAL

La responsabilidad penal se recoge en sendos artículos de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

El artículo 27 del Código Penal dispone que tanto autores como cómplices serán responsables criminalmente de los delitos cometidos. Dentro de la definición de autor, que obviamente incluye al que lleva a cabo la comisión del delito, se considera también autor, al inductor al delito, es decir quién hace nacer a otra la actitud delictiva. A su vez, también se considera autor al cooperador directo, es decir, aquel que realiza un acto que no comete directamente el delito, pero sin el cual su comisión no se habría producido.

También se genera responsabilidad penal en concepto de cómplice definido negativamente por el artículo 29 del Código Penal como aquellos no comprendidos en los artículos precedentes pero que realizan actos que ayudan a la comisión del delito.

La comisión de delitos en redes se puede producir tanto por parte de los usuarios, como por parte de los prestadores del servicio y encargados de la gestión del mismo.

Los usuarios de las redes sociales son aquellos miembros que, previo registro en las mismas, participan de forma activa, ya sea colgando fotos o comentando situaciones. Debido al alto margen de libertad de expresión del que gozan, se suceden ciertos delitos denominados “típicos de las redes sociales” entre los que se encuentran el “cyberbullying”, la suplantación de identidad o “phishing”, difamación de informaciones falsas, y por último calumnias e injurias, todas ellas generadoras de responsabilidad penal como se recoge en los preceptos del Código Penal.

Por su parte, también los prestadores del servicio pueden generar responsabilidad penal como se deduce del artículo 13 de la ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

La ley exime de responsabilidad a prestadores en función de su papel, como por ejemplo, aquellos cuyo servicio consiste en el almacenamiento de datos, siempre que se cumplan dos condiciones; que carezcan del efectivo conocimiento de que se almacenan datos falsos e ilegales, y que actúen de forma diligente para eliminar el acceso a esos datos. Esto se recoge en el artículo 16 de la Ley de servicios de la sociedad de la información. [53]

Por tanto, los prestadores de servicios no siempre van a generar responsabilidad penal por sus actos, ya que la ley les exime en muchos casos siempre que actúen con diligencia, pero sí surgirá la responsabilidad penal en aquellos casos en los que contribuyan a cometer el ilícito penal tanto de forma activa, es decir a través de actos, como de forma pasiva, adoptando una posición de omisión respecto a sus deberes como prestadores del servicio.

CONCLUSIÓN

Tal y como se ha visto a lo largo del trabajo, la materia de protección de los datos personales forma parte de nuestro día a día, y está presente en casi todos los aspectos de nuestra vida, ya sea el ámbito laboral, en todo a lo relacionado con cuentas bancarias, y en las redes sociales, entre otros.

Por ello no puede ser considerado un tema baladí y los ciudadanos merecen una protección estricta de un derecho reconocido en el artículo 18.4 de la Constitución de 1978, que aparece también de la mano de los derechos al honor y a la intimidad personal.

Como he mencionado, la expansión de las redes sociales y su particular funcionamiento, donde hay prácticamente una libertad total de actuación y expresión da lugar a una sucesión de vulneraciones de los derechos inherentes a la personalidad, por ello considero que la legislación debe ser más "agresiva" en su lucha contra estas violaciones de

[53] «BOE» núm. 166, de 12/07/2002.

derechos y una medida a valorar sería la creación de una norma de rango reglamentario que desarrolle la Ley Orgánica 3/2018 con el fin de regular de forma pormenorizada todos los aspectos de esta materia.

El registro de los usuarios en una red social conlleva la transmisión de todos sus datos de carácter personal al prestador del servicio, que por otro lado se compromete a ofrecer un sistema eficaz de privacidad de sus datos frente a posibles filtraciones o intromisiones que puedan vulnerar su derecho. En caso de incumplir esta cláusula, el prestador del servicio se enfrentará a la responsabilidad civil que se ha visto en el trabajo, sin perjuicio de la posible responsabilidad penal.

Para finalizar, considero esta materia de gran interés, no sólo porque nos afecta a todos, sino que también está en una constante evolución debido a la continua digitalización de documentos, y por ello es necesario un compromiso inexcusable por parte de los legisladores, tanto nacionales, como de la Unión Europea, para brindar una protección eficaz y efectiva al conjunto de la ciudadana.

BIBLIOGRAFÍA

1- Francisco Balaguer Callejón, Manual de Derecho Constitucional Volumen II, 2018, Pág. 155
2- Resolución Asamblea General ONU 217 A (III), de 10 de diciembre de 1948
3- Ángel Acedo Penco, Los derechos de la Personalidad, Pág. 123
4- LO 1/1982 BOE núm. 115, de 14/05/1982
5- BOE núm. 77, de 30 de marzo de 2001
6- BOE núm. 185, de 04 de agosto de 2006
7- https://www.conceptosjuridicos.com/derecho-a-la-intimidad/
8- BOE núm. 307, de 23 de diciembre de 1988
9- BOE núm. 287, de 30 de noviembre de 1990
10- BOE núm. 311, de 29/12/1978
11- Patricia Escribano Tortajada, "Los derechos a la intimidad y a la privacidad en el siglo XXI" Pag 73
12- Teoría del mosaico Fulgencio Madrid Conesa: Derecho a la intimidad, informática y Estado de Derecho, Valencia, Universidad de Valencia, 1984, pág. 45
13- BOE núm. 305, de 21 de diciembre de 1984
14- BOE núm. 281, de 24/11/1995

15- Francisco Balaguer Callejón, Manual de Derecho Constitucional Volumen II, Pág. 163
16- Real decreto de 24 de julio de 1889 por el que se publica el Código Civil «Gaceta de Madrid» núm. 206, de 25/07/1889
17- BOE núm. 305, de 21 de diciembre de 1984
18- DOUE, núm.364, de 18 de diciembre de 2000 (2000/C 364/01).
19- DOUE, núm. 149 de 7 de junio de 2016 (07/06/2016). Tratado de la unión Europea y Tratado de Funcionamiento de la Unión Europea (Versión consolidada)
20- Víctor Cazurro Barahona, Antecedentes y fundamentos del Derecho a la protección de datos, 2020, Pág. 125
21- María de los Reyes Corripio Gil-Delgado, Revista de Contratación Electrónica,
22- DOUE núm. 337, de 18 de diciembre de 2009
23- DOUE núm. L 119, de 4 de mayo de 2016
24- Publicaciones de la Agencia Española de Protección de Datos (AEPD)
25- M. Àngels Barbarà, Revista de Derecho VLEX
26- BOE núm. 4, de 04 de enero de 2001
27- XX Aniversario de la LORTAD: 20 años de protección de datos., Actualidad jurídica VLEX, 6 de noviembre de 201
28- Lucrecio Rebollo Delgado , Carlos Eduardo Saltor, El derecho a la protección de datos en España y Argentina. Orígenes y regulación vigente (2013), pág. 77 y pág. 104
29- BOE núm. 298, de 14/12/1999
30- BOE núm. 17, de 19/01/2008
31- Gabilex. Revista del gabinete jurídico de Castilla la Mancha
32- https://dle.rae.es/diccionario
33- DOUE núm. 119, de 4 de mayo de 2016
34- Andoni Polo Roca, El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado, Revista de Derecho Político
35- Recomendación de la AEPD sobre Comercio Electrónico del 2000
36- BOE núm. 185, de 04 de agosto de 2006
37- BOE núm. 181, de 28 de julio de 2009
38- https://datosmacro.expansion.com/demografia/estructura-poblacion/españa
39- Real decreto de 24 de julio de 1889 por el que se publica el Código Civil «Gaceta de Madrid» núm. 206, de 25/07/1889
40- DOUE núm. L 119, de 4 de mayo de 2016
41- Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua (2016)
42- Víctor Cazurro Barahona, Derecho digital (2017), pág. 249
43- Miguel Marcos Ayjón, La protección de datos de carácter personal en la justicia penal (2020)
44- https://www.iberley.es
45- Estado de alarma y protección de la privacidad en tiempos de pandemia UNED. Revista de Derecho PolíticoN.º 110, enero-abril 2021
46- Martín Guardado, S. (2020). La protección de los sanitarios ante el coronavirus como interés público: reflexiones más allá del derecho a la seguridad y salud en el trabajo
47- BOE núm. 294, de 06 de diciembre de 2018

48- https://www.aepd.es/
49- vozpopuli.com
50- https://www.europapress.es/
51- Anuario de la Facultad de Derecho de la Universidad de Alcalá Núm. X-2017, Enero 2017 Nuevos perfiles del derecho al olvido en Europa y España
52- https://guiasjuridicas.wolterskluwer.es/
53- «BOE» núm. 166, de 12/07/2002