Universitat
Abat Oliba CEU

El Derecho a la Protección de Datos

TRABAJO FIN DE GRADO

Autor: Philippe V. Mombaers Martín

Tutor: Elena Palomares Balaguer

Grado en: Derecho y CCPP

Año: 2023

DECLARACIÓN

El que suscribe declara que el material de este documento, que ahora presento, es fruto de mi propio trabajo. Cualquier ayuda recibida de otros ha sido citada y reconocida dentro de este documento. Hago esta declaración en el conocimiento de que un incumplimiento de las normas relativas a la presentación de trabajos puede llevar a graves consecuencias. Soy consciente de que el documento no será aceptado a menos que esta declaración haya sido entregada junto al mismo.

Firma: ……

Nombre y APELLIDOS (del alumno/a)

VAS SER EL FAR EN LA TEMPESTA
L'ESTEL POLAR ENMIG DEL NO-RES
LA MEVA VÀLUA ÉS TESTIMONI
DEL QUE HEM COMPARTIT I EL QUE HEM APRÈS.

PER A GERARD

Resumen

La globalización del internet y la facilidad de su acceso a propiciado el intercambio de datos de toda índole entre sus usuarios de forma masiva. En un principio su alcance era limitado, ahora, su regulación, representa uno de los mayores retos legislativos en el ámbito internacional. En este trabajo desarrollamos el origen legislativo y la historia que hay detrás del Derecho a la Protección de Datos, especialmente en Europa y España, a la luz de las implementaciones normativas más recientes, por un lado, el Reglamento (UE) 2016/679 General de Protección de Datos y, por otro, la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

Resum

La globalització de la internet i la facilitat del seu accés a propiciat l'intercanvi de dades de tota índole entre els seus usuaris de manera massiva. Al principi el seu abast era limitat, ara, la seva regulació, representa un dels majors reptes legislatius en l'àmbit internacional. En aquest treball desenvolupem l'origen legislatiu i la història que hi ha darrere del Dret a la Protecció de Dades, especialment a Europa i Espanya, a raó de les implementacions normatives més recents, d'una banda, el Reglament (UE) 2016/679 General de Protecció de Dades i, per un altre, la Llei orgànica 3/2018 de Protecció de Dades Personals i garantia dels drets digitals.

Abstract

The globalization of the internet and the ease of access to it has led to the massive exchange of data of all kinds between its users. Initially limited in scope, its regulation now represents one of the greatest legislative challenges at the international level. In this paper we develop the legislative origin and history behind Data Protection Law, especially in Europe and Spain, taking in consideration the most recent normative implementations, on the one hand the General Data Protection Regulation (EU) 2016/679 and, on the other hand, the Organic Law 3/2018 on Personal Data Protection and guarantee of digital rights.

Palabras claves / *Keywords*

Protección de Datos de Carácter Personal – Autodeterminación Informativa — Intimidad – Datos – Información – Reglamento – Tratamiento – Responsable – Interesado – Ley Orgánica – LOPD – RGPD

Sumario

1. Introducción

1.1. Presentación del tema

Desde la labor pionera desarrollada por el Consejo de Europa a partir de la década de los sesenta, hasta la consagración en el artículo octavo de la Carta Europea de Derechos Fundamentales, pasando por el 18.4 de nuestra Carta Magna, el derecho a la protección de datos ha evolucionado de forma constante dejando muy atrás las pretensiones legislativas de la Directiva 95/46/CE y de la LOPD de 1999.

En vista de la creciente datificación, o *verdatung* (Heredero, M. 1983) como es conocida originalmente, la Unión Europea puso en marcha un proceso de armonización normativa que pretendía abarcar nuevos retos y horizontes. Bajo esa óptica se desarrolló el Reglamento 2016/679 General de Protección de Datos y, en consecuencia, la Ley Orgánica 3/2018, las cuales han revolucionado algunos paradigmas de gran importancia en torno a este derecho fundamental, pero, por otro lado, pueden haber dejado algunos frentes abiertos.

1.2. Motivación personal

El gusto por la informática lleva curtiéndose en mí desde hace ya muchos años. Con poco más de diez años ya creaba carpetas con comandos ejecutables como el *shutdown* para gastar bromas a mis amigos, con 14 desarrollé una modesta base de datos relacional que aglutinaba información del mundo de los videojuegos. La curiosidad por el funcionamiento de las redes y, sobre todo, la monetización que se generaba en ellas me condujo a querer aprender, realmente, como funcionaba y cuáles eran las normas que lo delimitaban. Con poca idea y mucho corazón emprendí este trabajo con dos objetivos, el primero y más evidente, culminar mis estudios de derecho, en segundo lugar, el puro deseo de saber. A esto le precedió también algunas dudas de si, en un futuro próximo, quería embarcarme en las oposiciones para la Agencia Española de Protección de Datos, y, ya que tenía que realizar un trabajo de esta envergadura de forma imperativa, quise sacarle partido a la situación e informarme de este tema que tanto me atraía.

1.3. Objetivos, Hipótesis y metodología

La hipótesis principal del trabajo era comprobar si la funcionalidad, implementación y desarrollo del Reglamento Europeo de Protección de Datos, así como la Ley Orgánica 3/2018, han sido los adecuados para afrontar los problemas de la “era de la información”. Para ello se han seguido dos diferentes tipologías de objetivos, en

primer lugar, el bibliográfico, sintetizando y exponiendo el origen del derecho a la protección de datos y resumiendo su historia en Europa y, en segundo lugar, redescubrir un tema ciertamente investigado, pero con el enfoque de reunir en una sola obra el RGPD y la LOPD y extraer de su estudio el impacto que tienen en la actualidad.

Por lo que respecta a la metodología, hemos realizado, principalmente, un análisis diacrónico de tal manera que hemos estudiado el derecho a la protección de datos de carácter personal a lo largo del tiempo y observado como esta ha ido manteniendo, modificando y suprimiendo diferentes características que ha determinado su impacto en la sociedad. No obstante, otras metodologías empleadas han sido la de observación del desarrollo de este derecho y las características de su evolución legislativa, así como su posterior razonamiento en la búsqueda de recomendaciones y alternativas.

1.4. Relevancia del tema.

En 1983, a través del método matemático-estadístico, ya era posible determinar a un individuo concreto de entre 100.000 personas con siete de sus datos personales (Heredero, M. 1983 p. 149). Los ordenadores en los 80 tenían procesadores con 29.000 transistores, tecnología de 3000 nanómetros y una velocidad de hasta 10 MHz, en la actualidad tienen 7, 10 o 14 nanómetros, miles de millones de transistores y alcanzan frecuencias de más de 5000 MHz (Xataka, 2019, December 31). Un IBM PC[1] solo permitía trabajar con dos *diskketes* de cinco pulgadas y cuarto de 360KB cada uno (Dans, E. 2011), hoy en día, cualquier ordenador tiene varias decenas, sino cientos *gigabytes* de espacio.

Las TIC se han convertido en un bien primario y su acceso es, cada vez, más sencillo. En 2007 se superó un hitó cuando el 53% de la Unión Europea contaba con acceso a internet, en 2019 ascendió al 90% (Euroestat Statistics Explained, 2020).
Con ello, el tráfico de datos ha aumentado en consonancia a sus usuarios, los cuales, cada vez pasan más tiempo navegando por la red y consumiendo diferentes servicios. A este hecho se le suma que las herramientas de procesamiento de datos cada vez son más sofisticadas, permitiendo un tráfico mucho más acelerado con la capacidad de viajar entre servidores de forma internacional.

[1] Un modelo de ordenador personal introducido en el mercado desde 1981 por la empresa IBM.

Todas estas cuestiones son las que han determinado el rumbo normativo actual y cuál deberá ser el siguiente movimiento en aras a la protección de los individuos frente a una tecnología que parece, cada día, más ajena a nuestra comprensión.

2. El derecho a la intimidad

El derecho a la intimidad personal y familiar aparece primeramente en la Constitución Española (en adelante CE); concretamente en el Título primero, Capítulo segundo, Sección primera, artículo decimoctavo, donde se garantiza y consagra sincrónicamente con el derecho al honor en su primer punto.

Como derecho fundamental, y en consonancia con lo previsto en el artículo 81 CE, el derecho a la intimidad es objeto de protección civil en Ley Orgánica, concretamente en la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.[2]

Este implica la existencia, según las sentencias 231/1988[3] y 151/1997[4] de la Sala segunda del Tribunal Constitucional, de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de nuestra cultura– para mantener una calidad mínima de la vida humana, tal es así que, ni en los supuestos de convivencia conyugal, existe una completa transferencia recíproca encaminada al acceso de cada uno de los aspectos de intimidad del otro que antes permanecían en exclusiva, por lo que, en ningún caso, supondría para los implicados la desaparición total del espacio íntimo (STS 569/2013, Andrés Ibáñez).
En este sentido, el artículo 18, protege también la divulgación de los datos obtenidos sin consentimiento, así como la injerencia que supine la acción ajena y, con ello, a la sin duda contundente intromisión que significa la sanción de los comportamientos desarrollados en el área de la intimidad. El mismo tribunal afirmó, en la STC 117/1994[5], en su fundamento jurídico tercero, que el derecho a la intimidad limita la intervención de otras personas y de los poderes públicos en la vida privada, al igual

[2] Avanzando al lector al contenido que le precede, todos los bienes jurídicos derivados de la LO 1/1982 están cubiertos por el concepto *right of privacy*, que, en forma expansiva y maximalista, fue desarrollado por la jurisprudencia norteamericana (Heredero, M. 1983).
[3] Sala Segunda. Sentencia 231/1988, de 2 de diciembre. Recurso de amparo 1.247/1986. Contra Sentencia de la Sala Primera del Tribunal Supremo que anula la dictada en apelación por la Audiencia Territorial de Madrid, en autos sobre vulneración del derecho a la intimidad.
[4] Sala Segunda. Sentencia 151/1997, de 29 de septiembre. Recurso de amparo núm. 3983/1994 del Ponente Don Carles Viver y Pi-Sunyer.
[5] Sala Segunda. Sentencia 117/1994, de 25 de abril de 1994. Recurso de amparo 2.016/1990. Contra Sentencia de la Sala Primera del Tribunal Supremo por la que se declara no haber lugar el recurso de casación interpuesto contra la dictada por la Audiencia Territorial de Barcelona en apelación contra la Sentencia del Juzgado de Primera Instancia número 2 de Barcelona, en autos de protección civil del derecho al honor, a la intimidad y a la propia imagen. Supuesta intromisión en el ámbito protegido por el artículo 18 C.E.: efectos de la revocación del consentimiento prestado por la recurrente.

que las injerencias en la intimidad "arbitrarias o ilegales" (STC 110/1984[6], fundamento jurídico octavo).

Este derecho se extiende incluso a las personas más expuestas al público (STC 134/1999, de 15 de julio), sin embargo, su extensión viene condicionada, precisamente, por el carácter de la persona o el aspecto concreto de su vida que se ve afectado, de acuerdo también con las circunstancias particulares del caso, incluso el propio TC (STC 115/2000, de 5 de mayo, STC 83/2002 y STC 196/2004) ha interpretado que el alcance de la intimidad puede alterarse en función del propio afectado adoptando la concepción formal, en otras palabras (Real Academia de Jurisprudencia y Legislación, 2016, definición derecho a la intimidad e imagen (D.º Const.)), cada persona delimita por sí misma su ámbito de intimidad y deben tenerse en cuenta los antecedentes que haya establecido mediante sus propios actos. Por otro lado, tendríamos la visión material (también empleada por el TC pero sin tanto éxito como la anterior) por la que solo determinados actos son protegidos en función de su propia naturaleza.

En cualquier caso, es necesario ponderarse frente a otros derechos como, por ejemplo, la libertad de información, la investigación de la paternidad (STC 7/1994, de 17 de enero), de la maternidad (STC 95/1999, de 31 de mayo) o controles fiscales (STC 110/1984, de 26 de noviembre), supuestos en los que, la intimidad, cederá frente a bienes jurídicamente protegidos, siempre de una manera justificada y proporcionada teniendo en cuenta otros derechos o bienes jurídicamente protegidos de interés general, como son los derechos de los hijos (art. 39 CE) o la garantía de la proporcionalidad impositiva (art. 31CE) (Elvira, A. 2003).

Asimismo, la protección del derecho a la intimidad se propaga al ámbito laboral, debiendo deslindar aquel control idóneo, necesario y equilibrado de la actividad laboral (STC 186/2000, de 10 de julio), de aquéllos otros que supongan una injerencia en la intimidad de los trabajadores afectados de forma injustificada o desproporcionada (STC 98/2000, de 10 de abril).

Históricamente este derecho fue más bien tardío, siendo la inviolabilidad del domicilio y de las comunicaciones la primera manifestación concreta de la intimidad hasta llegar al canon interpretativo sostenido por la Constitución de 1978, que

[6] Sala Primera. Recurso de amparo número 575/1983. Sentencia número 110/1984, de 26 de noviembre.

abarcaba el efecto positivo de los convenios internacionales sobre el ordenamiento nacional (Ruiz, C. 1992, p. 76-84). En este sentido, dichos convenios contienen preceptos relativos al derecho a la intimidad, como la Declaración Universal de Derechos Humanos donde, en su art. 12, establece 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."*

Igualmente, el art. 17.1 del Pacto Internacional de Derechos Civiles y Políticos del 19 de diciembre de 1966 de Nueva York suscribe una máxima muy similar, de igual modo que lo hace la Convención Internacional sobre los derechos del Niño, adoptada por la Asamblea General de las naciones Unidas el 20 de noviembre de 1989 en su artículo 16, en protección a la intimidad de los infantes.

Es menester señalar que, en todos los textos, la vida familiar y privada, la inviolabilidad del domicilio y el derecho al honor, evidencian un nexo común; la intimidad. Hay quienes interpretarían el honor como un derecho independiente o análogo, es decir, por un lado encontraríamos el derecho a la intimidad y por otro al de la buena fama, que, en el mismo orden, el primero protegería el ámbito privado, de libertad y la no publicidad (que recoge la vida personal, familiar y otros ámbitos privados como la amistad, así como el lugar donde se desarrollan primariamente) y el segundo ampararía las acciones dirigidas a extender mediáticamente faltas o defectos no públicos o imputar falsamente injurias o delitos (Ruiz, C. 1992, p. 87-88). Encauzándolo en el ámbito que desea tratar esta investigación, la intimidad, ya en tiempos primarios de las telecomunicaciones, abarcaba los medios de expresión y comunicaciones privadas, tales como la correspondencia o el teléfono.

No obstante, y sin perjuicio del párrafo anterior, la Sentencia del Tribunal Constitucional 14/2003 es claudicante en cuanto a que señala que *el derecho al honor, el derecho a la intimidad (personal y familiar) y el derecho a la propia imagen son tres derechos autónomos y sustantivos, aunque estrechamente vinculados entre sí en tanto que son derechos de la personalidad derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas* (Elvira, A. 2003)

Conviene detenernos en el artículo 8.1 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma el 4 de

noviembre de 1950, puesto que significo uno de los paradigmas más importantes en el desarrollo del derecho a la intimidad en el marco europeo. El artículo en cuestión dice así:

> *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*

Por las características de este trabajo, nos detendremos brevemente a examinar dos de sus elementos primarios; el respeto por la vida privada y por la correspondencia y telecomunicaciones, dejando el derecho a la autodeterminación informativa para más adelante.

Acotaremos primeramente el análisis de este desgranado como lo lleva a cabo el Dr. Carlos Ruiz Miguel en su obra *La configuración constitucional del derecho a la intimidad*, por la cual examina el Convenio a la luz de la interpretación hecha por el TEDH, que, en este sentido, afirma que el 8.1 protege las manifestaciones esencialmente privadas de la personalidad humana como es, por ejemplo, la vida sexual. A tenor de esta máxima se extrae pues que, dentro de la vida privada existen diversos grados de intimidad, doctrina reiterada en diversas ocasiones (STEDH 10581/83, 26 de octubre de 1988). Este mismo tribunal entiende que la integridad psíquica y moral forma parte de la vida privada y, sin casar cuidadosamente con la interpretación de la Constitución Española, resultan finalmente derechos protegidos por ambas partes.

Por lo que se refiere al respeto por la correspondencia ajena, si bien puede ser limitada en virtud del artículo 8.2 del Convenio[7] y con expresa previsión de la ley, sus efectos alcanzan incluso a sujetos con sujeción especial como los reos de prisión (STEDH 4451/70, Caso Golder[8]). Conviene subrayar, por el peso que subyace en esta afirmación, que, como se observa en la sentencia de 6 de septiembre de 1978 del TEDH (Caso Klass[9]), "*el Tribunal opina con la Comisión que se encuentran comprendidas en las nociones de «vida privada» y de «correspondencia»"*,

[7] No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[8] Derecho a la obtención de justicia por un tribunal y al secreto de la correspondencia en la cárcel (artículos 6.1 y 8 del Convenio).

[9] Fundamentos de derechos II (sobre la alegada violación del artículo 8), párrafo 41.

refiriéndose a las conversaciones telefónicas, y que, incluso, podrían significar un rebasamiento al respeto de su domicilio.

Igualmente, en materia de jurisprudencia comparada, cabe resaltar el caso López Ostra v. España desarrollado en la Corte Europea de Derechos Humanos donde se condenó al Estado Español por la violación del artículo octavo del Convenio Europeo de Derechos Humanos, en este caso por haberse probado la vulneración de la privacidad personal y familiar al verter sustancias contaminantes y emitir ruidos estridentes procedentes de una planta de residuos sólidos y líquidos a escasos metros de su domicilio privado. Esto es sino una prueba inequívoca de que el alcance del derecho a la intimidad invade también la del domicilio, donde su perturbación con ruidos y olores puede provocar una vulneración de los derechos ya citados.

2.1. Secreto de las comunicaciones

Nuevamente nos encontramos con un derecho fundamental, establecido en el punto tercero del artículo 18, por el cual se protege la libertad de las comunicaciones y por ello se garantiza su secreto frente a cualquier intromisión, proveniente tanto de los poderes públicos como de particulares, salvo autorización por resolución judicial (Real Academia de Jurisprudencia y Legislación, 2016, definición Secreto de las Comunicaciones). Su ámbito material protegido debe entenderse en sentido amplio puesto que garantiza la impenetrabilidad de las comunicaciones para terceros (públicos o privados), tanto en el contenido del mensaje como en la identidad de los interlocutores o corresponsales (STEDH, de 2 de agosto de 1984, Malone) y otros aspectos del proceso de comunicación, como el momento o la duración de esta.

Para que la autorización judicial (que permite la intromisión de las comunicaciones por parte de los poderes públicos) sea viable ha de satisfacer una serie de requisitos como son: una resolución motivada (que se extiende en caso de prorrogar la intervención (STC 138/2001, FJ 6) un juicio de proporcionalidad (STC 49/1999 FFJJ 7 y 8) y el principio de especialidad, esto es, que la autorización se conceda para la investigación de unos determinados delitos, estos reproducidos en una disposición penal especial que reproduce todos los elementos de una ley general añadiendo ulteriores características individualizadoras por las que, por dicho motivo, resulta de aplicación preferente respecto a la general (Real Academia de Jurisprudencia y Legislación, 2016, def. Concurso de leyes (D.º Pen.)).

Por añadidura, en la reciente STC 14/2001, de 29 de enero, en su fundamento jurídico segundo expone que:

> "*la intervención de las comunicaciones telefónicas sólo puede entenderse constitucionalmente legítima si está legalmente prevista con suficiente precisión, si está autorizada por la autoridad judicial en el curso de un proceso mediante una decisión suficientemente motivada y si se ejecuta con observancia del principio de proporcionalidad, es decir, si su autorización se dirige a alcanzar un fin constitucionalmente legítimo, como acontece cuando se adopta para la prevención y represión de delitos calificables de infracciones punibles graves y es idónea e imprescindible para la investigación de los mismos* (SSTC 166/1999, de 27 de septiembre, FFJJ 1 y 2; 171/1999, de 27 de septiembre, FJ 5; 126/2000, de 16 de mayo, FJ 2 y 299/2000, de 11 de diciembre, FJ 2, entre las últimas)".

Asimismo, es necesario exteriorizar en la resolución, entre otras cuestiones, datos o hechos objetivos que puedan considerarse indicios de la existencia del delito, que no simples sospechas, y la conexión de los investigados con ellos, siempre fundadas en alguna clase de dato objetivo (SSTC 171/1999, de 27 de septiembre, FJ 8, y 299/2000, de 11 de diciembre, FJ 4), en el doble sentido de ser accesibles a terceros para permitir su control y proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito.

Tales precisiones derivan de la necesidad de realizar un juicio de constitucionalidad sobre si la decisión judicial aprecio razonadamente la conexión entre los sujetos que iban verse afectados y el delito investigado (existencia del presupuesto habilitante) para comprobar si se tuvo en cuenta la gravedad de la intromisión como su idoneidad e imprescindibilidad para asegurar la defensa del interés público (STC 138/2001 FJ 3), pues su conexión es un prius lógico del juicio de proporcionalidad (STC 49/1999, de 5 de abril, FJ 8, doctrina que reiteran las SSTC 166/1999, de 27 de septiembre, FJ 8; 171/1999, de 27 de septiembre, FJ 8).

En palabras del Tribunal Europeo de Derechos Humanos en los casos Klass, y Lüdi[10], las sospechas han de fundarse en "*datos fácticos o indicios que permitan suponer que alguien intenta cometer, está cometiendo o ha cometido una infracción grave",* o *"en buenas razones o fuertes presunciones de que las infracciones están a punto de cometerse*". En la misma línea se expresa el artículo 579 de la Ley de Enjuiciamiento Criminal que dice; *si hubiera indicios de obtener por estos medios*

[10] TEDH 12433/86. Caso Lüdi. Sentencia de 15 de junio de 1992

(refiriéndose a correspondencia privada, postal y telegráfica) *el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa*[11].

Es de imperativa mención que, en virtud del artículo 25.2 de la CE, “el condenado a pena de prisión que estuviere cumpliendo la misma gozará de los derechos fundamentales de este Capítulo, a excepción de los que se vean expresamente limitados por el contenido del fallo condenatorio, el sentido de la pena y la ley penitenciaria”, por lo que, constitucionalmente, el reo goza del derecho al secreto de las comunicaciones, aun pudiendo verse afectadas por las limitaciones allí establecidas y es que, como nos recuerda la STC 175/1997, este derecho tiene especial incidencia en el desarrollo de la personalidad de los internos, donde adquiere suma relevancia, en orden al cumplimiento de la finalidad, no exclusiva, de desinserción social en las penas privativas de libertad, ya que, cierta parte de los reclusos mantienen su comunicación oral y escrita con otros sujetos, no quedando así reducidos exclusivamente al mundo carcelario y, permitiendo, relacionarse con el exterior preparándose para su futura vida en sociedad.

Asimismo el art. 51 de la Ley Orgánica General Penitenciaria (LOGP) reconoce el derecho del recluso a las comunicaciones, no obstante, su ejercicio varía en función de la modalidad a la que esté sujeta, como prevén el art. 51.1 y 51.2, que, respectivamente se refieren a las comunicaciones genéricas, en cuanto a que autoriza a los internos a "*comunicar periódicamente, de forma oral y escrita, en su propia lengua, con sus familiares, amigos y representantes acreditados de Organismos internacionales e instituciones de cooperación penitenciaria, salvo en los casos de incomunicación judicial*" y a las comunicaciones específicas con su abogado y procurador. Cabe añadir que en el primer punto de este mismo artículo especifica que las comunicaciones deben celebrarse respetando al máximo su intimidad para llevarse a cabo, sin embargo permite que sean restringidas "*por razones de seguridad, de interés de tratamiento y del buen orden del establecimiento*" y pueden ser también "suspendidas o intervenidas motivadamente por el Director del establecimiento, dando cuenta a la autoridad judicial competente" excepto aquellas realizadas entre el interno y su Letrado o procurador. Por otro lado,

[11] Siempre que la investigación tenga por objeto 1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión. 2.º Delitos cometidos en el seno de un grupo u organización criminal. 3.º Delitos de terrorismo.

en el art. 51.3 LOGP se regulan las comunicaciones mantenidas con profesionales acreditados, asistentes Sociales y Sacerdotes[12].
En suma, podemos afirmar que el derecho al secreto no está configurado constitucionalmente con carácter absoluto, ni en el art. 18,3, ni en lo que respecta al 25.2 CE (STC 37/1989), cubierta, a su vez, por el art. 51.1 *in fine* de la LOGP

La vulneración del derecho al Secreto de las comunicaciones perpetrado en un proceso judicial sin las garantías necesarias puede tener implicaciones más amplias de las que deja entrever en un principio, como la concatenación del quebrantamiento de derechos como son el de un proceso con todas las garantías (24.2 CE), la tutela judicial efectiva (art. 24.1 CE), la presunción de inocencia (art. 24.2 CE) o el principio de legalidad (art. 25.1 CE) por la evidente interconexión entre sí (STC 138/2001 FJ 1).

Deteniéndonos brevemente en materia de derecho comparado y poniendo el foco en el ordenamiento alemán, podemos observar cómo parten jurídicamente del art. 10 de su Ley fundamental que se compone de dos puntos, el primero declarando la inviolabilidad del secreto de la correspondencia, correo y telecomunicaciones y el segundo estableciendo que *solo en virtud de ley podrán establecerse limitaciones a dicho derecho* siempre y cuando *obedezca al propósito de proteger el orden básico liberal y democrático o la existencia y salvaguardia de la Federación o de un estado regional*, permitiendo *disponer que no se comunique la restricción al afectado y que el control sea asumido por órganos y auxiliares designados por representación del pueblo, en vez de correr a cargo de la autoridad judicial*.

[12] O Ministros de una religión.

3. Derecho a la autodeterminación informativa

El Derecho a la autodeterminación informativa fue consagrado por el Tribunal Constitucional Federal alemán en su sentencia sobre la Ley del Censo de Población, Profesiones, Viviendas y Centros de Trabajo de 15 de diciembre de 1983, por la que se anuló la ley del Censo de Población de 1982[13] y, además, se revisó sustancialmente la ley federal de 1977, así como sus leyes del Ejercito y del Servicio Secreto (*Cuervo, J. 2015)*. El tribunal en cuestión lo describe como "*la facultad del individuo de decidir básicamente cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida, haciendo necesaria la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión limitada de los datos concernientes a la persona* (Ruiz, C. 1992, p. 97). La sentencia sigue explicando como la elaboración automática de datos ha ensanchado en una medida hasta ahora desconocida las posibilidades de indagación e influencia susceptibles de incidir sobre la conducta del individuo, (…).

> *"La autodeterminación del individuo supone que se conceda a este la libertad de decisión sobre las acciones que vayan a realizar o, en su caso, a omitir (…) El que no pueda percibir con seguridad suficiente que informaciones relativas a este son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse substancialmente cohibido en su libertad de planificar o decidir por autodeterminación* (…)."

Como ejemplo, el tribunal razona un hipotético caso donde un sujeto que *sepa de antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales (…) Y acaba concluyendo que; De este modo un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo la elaboración automática de datos, ninguno" sin interés*".

Paralelamente el derecho a la autodeterminación informativa se había emitido desde el vocablo anglosajón como *right of privacy (Cuervo, J. 2015)*.

[13] Para muchos conocida como "Ley de Censos de 1983", aun siendo del 25 de marzo de 1982 (Gaceta Legislativa I, p. 369)

Antes de seguir ahondando en la autodeterminación informativa es conveniente repasar cuales son los motivos del segundo proyecto de la Ley de Censo de 1982, que, de entre otros hechos, la propuesta legislativa precisaba armonizar los datos del registro o padrón de habitantes con los del censo implicando una excepción al secreto estadístico para contrastarlos, y, para ello, era necesario conocer la identidad del individuo. Como contramedida se impulsó, a través del artículo 9, una proposición por la cual la información obtenida con ayuda de dichas comparaciones no pueda ser utilizada por los municipios o agrupaciones como base de medidas que perjudicaran a los censados (Heredero, M. 1983, p. 140).

El entonces comisario federal de Protección de Datos[14],el profesor H. P Bull, reveló que los legisladores no se esperaban que una ley de estas características pudiera comportar semejante reacción pública con la que se dieron movilizaciones masivas de desobediencia civil, recursos de amparo constitucional, etc. En contra de lo dicho, el proyecto de ley no fue el único motor de movilización ciudadana, recientemente, el Estado, había mantenido una actitud poco activa en cuanto a la localización de misiles, lo que, en conjunción con la colosal operación censal, desencadenaron en protestas multitudinarias. Tras cierta evolución y transfiguración de los motivos por los que se exigía protección con relación al tráfico de datos, finalmente el debate político alemán fue centrándose en dos cuestiones: la "cosificación" del ciudadano como fuente de información marginada al conteo y la excesiva transparencia que la exhaustividad de la información del censo podía llevar aparejada[15] (Heredero, M. 1983, p. 141).

Gestado el caldo de cultivo en Hamburgo, rápidamente emergió un efecto de mimesis a lo ancho del territorio germánico que, de entre muchos de sus efectos, el más relevante surge a colación de la iniciativa de las abogadas de Hamburgo, la Dra. Wild y la Srta. Stadler-Euler, de formular ante el TC Federal recurso de amparo constitucional, por estimar que la Ley del Censo del 83 lesionaba sus derechos fundamentales derivados de los arts 1º, primer párrafo; 2º, primer párrafo; 5º, primer párrafo, proposición primera, y 19, párrafo cuarto; de la ley fundamental, que son; el

[14] Günter Grass contra H. P. Bull (Heredero, M. 1983)

[15] Los propietarios, al conocer la dotación de servicios e instalaciones de la vecindad, podrían justificar aumentos de los alquileres si sus viviendas estaban mejor equipadas; las empresas podrían instalarse en zonas en las cuales los salarios fueran más bajos; el estudiante de Kiel que declaraba Berlín como domicilio principal con el fin de eludir su servicio militar, quedaría al descubierto: etc. Otro aspecto consistía en que, así como no es posible negarse a ser registrado e introducido en memoria en los ordenadores de las cajas del seguir de enfermedad, compañías de seguros, bancos, empresas o autoridades del padrón de habitantes, todo el mundo podría en cambio negarse a dar los datos censales como acción defensiva común.

derecho al libre desenvolvimiento de la personalidad, en relación con el derecho a la dignidad humana (sujeta al principio de adecuación); el derecho a la libre expresión de la opinión y el derecho a la garantía procesal. En la sentencia se estimaron que existían razones a tenor de la Ley del Tribunal (art. 32) para suspender provisionalmente su aplicación. (Heredero, M. 1983, p. 143, 146, 147). Las recurrentes, invocaron con especial énfasis, la sentencia del "microcenso" del Tribunal Constitucional Federal, de 16 de julio de 1969[16] donde se pronuncia acerca de la constitucionalidad de una estadística de muestro donde sostiene que:

> "*El estado no puede lesionar la dignidad del hombre con medida alguna, ni aun por medio de la ley, o violar la libertad de la persona en su contenido esencial, excediendo los límites trazados por el artículo 2º, primer párrafo, de la Ley Fundamental. Con ello, la Ley Fundamental otorga al ciudadano un ámbito inviolable de configuración de su vida privada, que está sustraído a la intervención del poder público…*"

Siguiendo esta afirmación, el tribunal continúa diciendo que no es conciliable con la dignidad del hombre que el Estado se atribuya la capacidad de catalogar coactivamente a sus ciudadanos con relación a su entera personalidad, ni aun en el anonimato de un censo estadístico, y, de este modo, tratarlo como una cosa susceptible de recuento. Tal irrupción en la esfera de la personalidad imposibilita su desenvolvimiento libre y responsable por lo que es preciso que dicho espacio quede reservado para uno mismo al cual pueda retirarse y, a su vez, no haya ningún medio circundante que pueda entrometerse, asegurando un espacio de paz y derecho a la completa soledad.

Las recurrentes conocían que no toda estadística referente a la vida lesiona la dignidad, pues todo ciudadano vive en comunidad y, por una cuestión de orden público, es susceptible de formar parte de un recuento, ahora bien, la Ley del Censo de 1983 rebasaba ampliamente ese hecho debiendo aportar los administrados datos como su nombre completo, dirección, teléfono, sexo, fecha de nacimiento, estado civil, confesión, nacionalidad, convivencia, sucesivos domicilios, actividad profesional, estudios medios y universitarios, etc[17]. Individualmente, dicha información parece inofensiva, sin embargo la inconstitucionalidad del hecho es la combinación de tales datos y su adscripción a la persona. Con solo la respuesta de

[16] Colección de sentencias del Tribunal Federal Constitucional (abreviatura original "BVerfGE"). 27. 1.

[17] Medios de comunicación utilizados, tiempo empleado diariamente en desplazamientos, jornada laboral, clase, extensión, dotación y usos de la vivienda, número y uso de las habitaciones, cuantía de los alquileres mensuales… (Heredero, M. 1983)

una de las hojas censales o cuestionarios podía ya recabarse basta información de la esfera privada e íntima, pudiendo elaborarse un cuadro de la personalidad del individuo, que, sumado al tratamiento automático de datos en gran escala, podemos hablar de la existencia de un "enmallamiento", término acuñado por Manuel Heredero, o de "datificación", en alemán *verdatung*.

En síntesis, podemos afirmar que el problema (de la Ley del Censo de 1983) gravitaba en torno a tres cuestiones principales, en primer lugar, la posibilidad que brindaba el artículo 9 de contrastar los datos facilitados por el interesado con los contenidos en el padrón de habitantes, en segundo lugar, la instrumentalización del secreto estadístico, que eliminaba la posibilidad real del anonimato de los datos, pues estos, en el entorno cibernético, construyen una base de datos que facilita enormemente la capacidad de identificación de, prácticamente, cualquier persona[18]. En tercer lugar, la perdida absoluta del dominio de la información personal por parte del interesado a tenor de la interconexión de los sistemas informáticos o intercambio de los datos entre distintos órganos públicos[19], perdiéndose así el rastro de estos.
La formula que siguió el tribunal de la Primera Sala en su sentencia, de 15 de diciembre del 83[20] fue, en primer lugar declarar el §2, párrafos 1 a 7, así como los §§ 3 a 5 de la "Ley sobre un censo de población, profesión, vivienda y lugares de trabajo" del 25 demarzo de 1982 compatible con la Ley Fundamental, aun debiendo ocuparse el legislador de complementar la reglamentación de la organización y el procedimiento del censo. El § 9, párrafos 1 a 3 de la Ley de Censos de 1983 como incompatible con el Art. 2, párrafo 1, en relación con el Art. 1, párrafo 1 de la Ley Fundamental, y por tanto nulos. Y, por último, violación del art. 1, párrafo 1 de la ley Fundamental, en el alcance especificado en los párrafos 1 y 2.

La legislación alemana situaba la tilde de su ordenamiento constitucional en el valor y dignidad de la persona, autodeterminada libremente como miembro de una sociedad libre. Su protección es necesaria, junto a las garantías de libertades especiales, para asegurar el derecho general de la personalidad, consagrado en el art.2, primer párrafo, en relación con el art. 1 de la Ley fundamental, que, sin duda,

[18] Recordemos que, ya en 1983, a través del método matemático-estadísitico, es posible determinar a un individuo concreto de entre 100.000 personas a partir de unos seis o siete datos del susodicho. (Heredero, M. 1983 p. 149)
[19] En concreto las estrechas relaciones entre los Servicios Territoriales de Estadística y los Centros de Datos. En Hamburgo se procesaban en el mismo Centro de Cálculo el padrón de Habitantes, no autoimatizado, el Registro de la Información Policial, las Liquidaciones Tributarias, Los Datos de la Defens Constitucional, los de la Función Pública, etc. (Heredero, M. 1983 p. 148 *in fine*)
[20] BvR 209, 269, 362, 420, 440, 484/83

han ganado fuerza debido a los desarrollos contemporáneos y a los peligros para la personalidad humana vinculados a ellos[21].
Hasta entonces la concreción jurisprudencial que describía el contenido del derecho de la personalidad no era concluyente. Ahora bien, diversas sentencias del BVerfGE (Schwabe, 2009) coinciden en que la capacidad de los individuos, que se deriva del concepto de autodeterminación, fija el derecho de decidir por sí mismos, cuando y dentro de qué limites los asuntos de su vida personal habrán de ser públicos.
Para garantizar esta facultad se necesitan medidas de protección a tenor, primordialmente, del futur, ya muy previsible, de la evolución de los procesamientos automatizados de los datos.

Por aquel entonces, ya se podía, con la ayuda del procesamiento automático, consultar información individual sobre las relaciones personales y materiales de una persona determinada o determinable, archivada esta de forma ilimitada, y que puedes ser revisada en escasos segundos, que, combinado con los sistemas de información integrados con otras bases de datos, pudieran generar una imagien más o menos completa de la peprosnalidad sin que el implicado pueda controlar suficientemente su exactitud y la utilización que se le diera. Esto, ya permitía una flagrante injerencia ilegitima en la vida de las personas que podía llegar a influir de manera determinante en el comportamiento de los individuos.
En el drcho. a la autodeterminación se presupone que el ciudadano tiene libertad para decidir sobre qué actividades emprender y cuáles omitir, incluyendo la posibilidad de comportarse efectivamente en conformidad con esa decisión. Siguiendo esta línea quien no pudiera;

> *"estimar con suficiente seguridad, qué informaciones sobre sí mismo son conocidas en determinadas esferas de su medio social, y quien no pueda de algún modo valorar el conocimiento previo que los posibles interlocutores tienen de uno mismo, puede verse restringido esencialmente en su libertad para planear o decidir con base en su propia autodeterminación. (…)"*
>
> Como ejemplo el tribunal expone que "*Quien piense que los comportamientos atípicos pueden en todo momento pueden ser registrados y archivados como información, utilizados o retransmitidos, intentará no llamar la atención incurriendo en ese tipo de comportamientos. Quien crea que, por ejemplo, la participación en una asamblea o una iniciativa ciudadana será registrada por las autoridades y que ello pueda generarle algún riesgo, posiblemente renunciará al ejercicio de su derecho fundamental (Arts. 8, 9 de la*

[21] BVerfGE 54, 148

Ley Fundamental). Esto no sólo iría en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar.

De esto se deduce lo siguiente: el libre desarrollo de la personalidad presupone en las modernas condiciones para el procesamiento de datos, la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales."[22] (Schwabe, 2009)

Todo ello no implica que sea un derecho ilimitado, en palabras del Tribunal, el individuo es, ante todo, una personalidad que se desarrolla en el interior de una comunidad social y que está obligada a la comunicación. La información individual conforma una imagen de la realidad social, la cual en algunas ocasiones no puede atribuirse exclusivamente sólo a los implicados y, en este sentido, el individuo debe admitir ciertas restricciones a su derecho a la autodeterminación informativa, especialmente cuando se trate del interés general preponderante.

Por otro lado, el que tan sensibles sea la información recolectada no dependerá únicamente del hecho de que aparezcan asuntos íntimos, se requiere, para valorarlo conocer el contexto en que va a ser utilizado y, solo cuando haya una tajante claridad sobre su finalidad y las posibilidades que hay de utilizarla y relacionarla podrá responder si la restricción es admisible. Se diferencian los datos recolectados y procesados de forma individual, no anónima y aquellos que se han determinado con fines estadísticos.

Como explica Lucas Murillo de la Cueva[23], hablar del derecho a la autodeterminación informativa es hablar de la Protección de Datos de Carácter Personal (PD. / PDCP o DchoPD. en adelante), pues hay plena coincidencia en su contenido y la diferencia de denominaciones obedece a que el término acuñado por el tribunal alemán difiere al que se estableció en el artículo octavo de la Carta de los Derechos Fundamentales de la Unión Europea, que dice; *toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*; por lo que se le denominará, en este trabajo, con absoluta indiferencia.

[22] Protección del derecho fundamental prevista en el Art. 2, párrafo 1, en relación con el Art. 1, párrafo 1 de la Ley Fundamental. El derecho fundamental garantiza de esta manera la capacidad del individuo principalmente para determinar la transmisión y empleo de sus datos personales

[23] En "El derecho a la autodeterminación informativa y la protección de datos personales", página 44.

Igualmente, el artículo 16.1 del Tratado de Funcionamiento de la Unión Europa (en adelante TFUE) hace referencia a esta facultad bajo la denominación de derecho a la protección de los datos de carácter personal, delegando, además, la tarea al Parlamento Europeo y el Consejo a regularlo en su punto segundo, dando como resultado lo que hoy conocemos como Reglamento (UE) 2016/679 del parlamento europeo y del consejo, de 27 de abril de 2016[24]. Cabe mencionar que en este mismo artículo in fine menciona, haciéndose eco de las normas referentes a la protección del tratamiento y de la circulación de los datos personales, el sometiendo de estas al control de autoridades independientes, como son, por ejemplo, la Agencia Española de protección de datos o la Autoridad Catalana de Protección de Datos. Más aun, en el Capítulo III del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se recogen los "Derechos del interesado", entre los que se encuentran el de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos y oposición, que, a su vez, se materializan en la LO 3/2018.

Por lo que respecta al ordenamiento español, la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental extraído de los artículos 18.4 de la Constitución española a la luz de los instrumentos que el artículo 10.2 proporciona para interpretar derechos fundamentales y libertades.

Ahora bien, dicho rango se lo dio, en un principio, el Tribunal Constitucional en su sentencia 292/2000, de 30 de noviembre, promovida por el Defensor del Pueblo respecto a los artículos 21.1 y 24.1 y 2 de la LO 15/1999 de Protección de Datos de Carácter Personal. Por la trascendencia de la misma nos detendremos brevemente en su contenido.

En primer lugar, el recurso de inconstitucional es en contra de incisos que contienen ambos artículos señalados, el 21.1 en relación con la comunicación de datos entre las Administraciones Públicas, el 24.1 por la excepción cuando se "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las AP y todo el primer párrafo del segundo punto del artículo 24 que dice:

[24] por el que se derogó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (Reglamento general de protección de datos)

> *Lo dispuesto en el artículo 15 [derecho de acceso a sus datos por los afectados] y en el apartado 1 del artículo 16 [derecho de rectificación y cancelación] no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección*.

La impugnación parcial del 21.1 se debía, en palabras del Defensor del Pueblo en su recurso, por dos motivos, el primero de ellos por la posibilidad de que la AP llevara a cabo cesiones de datos para fines distintos a los que motivaron su recogida, el segundo por la falta de información del titular d ellos mismos cuando se recabaran en dicha cesión y, por ende, sin su consentimiento expreso. Todo ello facilitado con una autorización que se regulaba en una norma de rango inferior a la ley (vulnerando así lo dispuesto en el 53.1 CE). Este artículo debía ponerse en relación con el 20, que regulaba la creación, modificación y supresión de ficheros de titularidad pública y que esta solo podrá hacerse por medio de una "disposición general publicada" en el BOE, indicando las características y el contenido del fichero creado o modificado. El problema es que esa disposición general podía ser una norma de rango infra legal, que, en último término, significaba que una norma de rango reglamentario autorizara una cesión estableciendo así una excepción a la prohibición genérica de cesión impuesta en ese mismo apartado del art. 21 y, también, a la regla del art. 11LOPD[25], según el cual la cesión solo es posible con el previo consentimiento del titular (garantía establecida en los arts. 4, 5 y 11 LOPD), que solo podría ser excepcionado con previa disposición en Ley (11.2.a)) . En definitiva, la LOPD permitía que, reglamentariamente, se impusiera un límite al derecho fundamental como es la autodeterminación informativa.

Eso no quiere decir, dice el Defensor del Pueblo, *que el derecho a la intimidad sea absoluto, la Ley puede imponerle límites con el fin de proteger otros derechos o bienes constitucionalmente protegidos, siempre que ese límite sea necesario, proporcionado y respetuoso con el contenido esencial del derecho fundamental* (STC 110/1984, donde se pondera la intimidad frente a otros bienes jurídicamente protegidos como el control de la fiscalidad y STC 143/1994 *donde se cuestiona la legitimidad constitucional de una norma que, a través de un instrumento de recopilación de información, puede propiciar un uso indebido de esta y, en*

[25] Las siglas LOPD se empleaban, originalmente, para hacer referencia a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Sin embargo, en la actualidad también hace referencia a la nueva Ley orgánica que la sustituye, la 3/2018, pero, que estrictamente sus siglas son LOPDGDD debido a que le siguen las palabras " y garantías de los derechos digitales"

consecuencia, la efectiva invasión de la esfera privada de los ciudadanos afectados (SIUV, 2022[26])).

No obstante, recordemos que en el art. 11 de la LOPD se asienta el principio de que solo cabe la cesión de datos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, siempre mediando con el previo consentimiento del interesado (11.1), consentimiento el cual es revocable (11.4) por nulidad en los términos previstos del 11.3[27], pero teniendo en cuenta las excepciones del punto segundo que establece que no será preciso el consentimiento cuando, *(a) este autorizado en una norma con rango de Ley, (b) cuando se trate de datos accesibles al público, (c) cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique la conexión de dicho tratamiento con ficheros de terceros* (solo legitima en cuanto a que se limite a la finalidad que la justifique su comunicación), (d) *cuando la comunicación tenga por destinatario al Defensor del Pueblo, Ministerio Fiscal, Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.*

Tampoco será preciso el consentimiento cuando *la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas, (e) cuando se produzca entre AAPP y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos* y (f) cuando la cesión sea relativo a cuestiones de salud y necesarias para solucionar una urgencia que requiera acceder a un fichero o, paralelamente, que sea necesaria para realizar estudios epidemiológicos (en los términos de la legislación sobre sanidad). Todas las excepciones mencionadas, a ojos del Defensor del Pueblo serían conforme al art. 53.1 de la norma magna, pero se quiebra con la adición de una nueva excepción del art. 21.1 LOPD que supone una deslegalización de una materia reservada a Ley y una remisión en blanco al reglamento con la pretensión de regular un derecho fundamental, premisa ya rechazada en la STC 83/1984.

[26] Servicio de Informática de la Universitat de València, extracto sentencia STC 143/1994.

[27] "*Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar*".

En cuanto a los incisos del artículo 24.1 y 2, el Defensor del Pueblo impugna en recurso por infracción de los artículos 18.1 y 53.1 CE arguyendo que, por lo que respecta al inciso del primer punto, se exime a la AP de cumplir sus obligaciones de información y advertencia contenidos en el artículo quinto (primero y segundo punto) de la LOPD[28] cuando "*la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas*".

En el caso del segundo punto, el titular perderá las facultades brindadas por el art. 15 (Derecho de acceso) y el art. 16 (derecho de rectificación y cancelación) cuando, *ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o de un tercero más digno de protección. A juicio del Defensor del Pueblo estas excepciones a los derechos de los titulares de los datos lesionan el contenido esencial del derecho fundamental a la intimidad frente al uso de la informática* (arts. 18.1 y 4, y 53.1 C.E.).

[28] 1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.
2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

4. Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.[29]

No es sorpresa que, el primer cometido de la Ley Orgánica tiene por objeto, en su primer artículo, primer apartado, la adaptación del ordenamiento nacional al RGPD, así como tampoco es que se cite la conformidad con esta ley en 251 ocasiones, pues, en muchos artículos se hace una remisión directa, sin, tan siquiera, puntualizar o ampliar aquello que, por derecho, pueden hacer. No obstante, veremos algunas de las particularidades de la adaptación normativa nacional y otras se comentarán juntamente con el análisis del RGPD, donde pondremos más atención al detalle de los artículos en sí.

La Ley Orgánica 3/2018 pone fin a un largo proceso, iniciado el 25 de enero de 2012 con la Comisión Europea, cuando esta presentó sendas iniciativas[30] dirigidas a posibilitar una revisión global del sistema europeo de protección de datos. A su vez, y como ya hemos visto exhaustivamente, el *article 29 working party*, realizó sus aportaciones que resultaron decisivas en la elaboración del nuevo reglamento europeo. Fue, pero, en 2009, cuando la Comsión Europea empezó el examen del marco jurídico de la Directiva 95/46/CE, partiendo de una conferencia de alto nivel seguida de una consulta pública, lo que determinó que los principios de la directiva eran válidos pero que habían ciertos problemas como el impacto de las nuevas tecnologías, el mercado interior, las consecuencias de la globalización, las mejoras de las transferencias internacionales, la aplicación efectiva de la normativa y la coherencia legislativa de la Unión, lo que suponía reelaborar la ley.

En 2010 la Comisión presentó un comunicado, trabajado previamente en el contexto histórico de esta ley, que presentaría las propuestas legislativas destinadas a revisar el marco jurídico de la protección de datos. Esta iniciativa fue toda una sorpresa

[29] Para conocer más a cerca del contexto histórico hasta la entrada en vigor de la LOPD, ver el Anexo III.

[30] Por un lado, el «Proyecto de Reglamento del Parlamento Europeo y del Consejo para la protección de los ciudadanos en relación con el tratamiento de los datos personales y la libre circulación de dichos datos» y, por el otro el «Proyecto de Directiva del Par- amento Europeo y del Consejo sobre protección de los ciudadanos en relación al tratamiento de los datos personales por las autoridades competentes con la finalidad de prevenir, investigar, detectar y perseguir delitos o ejecutar penas, y sobre el libre movimiento de dichos datos»

pues, la Comisión ya había presentado un comunicado en 2003[31] por el cual había apostado por mantener la Directiva 95/46/CE y reforzar su aplicabilidad. En 2007, en el «Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos» afirmaba no tener prevista ninguna propuesta legislativa para modificar la directiva.

Todo parecía tender hacía el inmovilismo, no obstante, resurgió una voluntad reformadora a la que se le sumaron el Parlamento Europeo en 2009 y el Consejo en 2010 desde el Programa Estocolmo, a lo que le siguió el grupo de trabajo del artículo 29 en su dictamen de 1 de diciembre de 2009 «The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data[32]» (Rallo Lombarte, A., 2019).

Los elementos tradicionales sobre los que se asienta el Dcho. PD han sido objeto de adecuación a los retos del nuevo entorno tecnológico, lo que ha conllevado una intensificación de la transparencia e información, completando los tradicionales derechos ARCO con nuevos perfiles adaptados al ámbito digital y el sistema de garantías apostando por un modelo más represivo y gravoso con una estrategia preventiva sustentada en el *accountability principle*. También se amplía el *data minimization principle* por el cual solo son objeto de tratamiento los datos necesarios para cada din específico y que solo se consever por el tiempo y cantidad minimos necesarios para sus fines (Rallo L., A., 2019). Se consolida también la figura delegado de protección de datos en aras a cumplir con la nueva estrategia basada en la rendición de cuentas (accountabiliy) sustituyendo el modelo anterior basado en obligaciones de los responsables y encargados sometidas a potestades reactivas de las autoridades de protección de datos por un nuevo paradigma basado en el enfoque de riesgo cuya evaluación corresponde a responsables y encargados y que consolidan un nuevo modelo de responsabilidad activa (Raphaël Gellert, 2017).

Debemos añadir que, la ya no tan nueva base jurídica europea de la que emana el reglamento convive cómodamente con las constituciones de los estados miembros que, progresivamente, han ido forjando este derecho fundamental y sus elementos definitorios, consagrado en el art. 8 de la Carta de Derechos Funfdamentales de la

[31] Primer Informe sobre la aplicación de la Directiva 95/46/CE.

[32] Puede acceder al informe desde el siguiente enlace: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

Unión Europea, y digerido por parte de la doctrina estableciendo aportaciones dogmáticas como, por ejemplo, la de la obra de Lucas Murillo de la Cueva.

Recordemos algunas cuestiones ciertas, como los considerando primero al séptimo de la Directiva 95/46/CE, donde ya afirmaba lo siguiente: (a) el establecimiento y funcionamiento del mercado interior obligaba a la libre circulación de merancias, personas, servicios y capitales y hacia necesaria la libre circulación de datos personales entre Estados miembros, (b) máxime cuando la integración económica u social resultante del establecimiento y funcionamiento del mercado interior implicaría necesariamente un aumento notable de los flujo transfronterizos de datos personales y un intercambio de datos personales entre empresas establecida en los diferentes estados miembros (c). Las diferencias entre los niveles de protección de la intimidad, en el tratamiento de datos personales, podría impedir la transmisión de dichos datos entre Estados miembros y, en consecuencia, estas diferencias podrían constituir un obstáculo para las actividades económicas a escala comunitaria, falseando la competencia e impidiendo que las administraciones cumplieran.

La elección del reglamento como instrumento jurídico comporta una voluntad excluyente de cualquier intervención estatal dirigida a regular este derecho fundamental y en consecuencia, la previsión constitucional del art. 8.4 se limita a mandatar al legislador que garantice los dchos. fundamentales frente al uso de la informática y, a diferencia de la Constitución portuguesa, ni explicita el reconocimiento del derecho del protección de datos ni asegura un contenido constitucional mínimo (Rallo Lombarte, A. 2019).

No obstante, el TC, en sus sentencia número 254/93, se encargó de anclar a este precepto el reconocimiento de dcho. fundamental autónomo, explicando, primeramente en su punto 5 de los antecedentes, que “La inexistencia de desarrollo legislativo unitario (…) constitucionales plantea el problema de la aplicabilidad y fuerza vinculante del Convenio de Estrasburgo, aclarado en parte por el art. 96.1 CE no se puede entender que dicho Convenio suponga un desarrollo del derecho fundamental a la intimidad, atendiendo a que el art. 81.1 C.E. exige una Ley Orgánica” y, sigue diciendo en su punto 7, “a falta de desarrollo de la legislación que prevé el art. 18.4 C.E. no puede implicar que el derecho de todas las personas a la intimidad y al honor quede en un mero reconocimiento teórico sin efectividad práctica. El incumplimiento o el retraso del legislador no ha impedido que la Norma fundamental sea directamente aplicable, así el derecho a la objeción de conciencia,

art. 30.2 C.E., STC 15/1982). Aun partiendo del hipotético supuesto de que no fuera directamente aplicable el Convenio de 28 enero 1981, para la recta interpretación del contenido fundamental reclamado, que existe por aplicación directa de la Constitución, habría de acudirse a dicho Convenio por remisión del art. 10.2 C.E. Finalmente, en el fundamento jurídico número 6 añadió: "*estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama informática*.

La doctrina del Tribunal Constitucional lo tenía claro, el derecho fundamental que se estaba protegiendo garantiza a la persona un poder de control y disposición sobre sus datos, pues confiere al interesado la capacidad de consentir la recogida y el uso de sus datos, así como conocerlos, oponerse a su posesión y tratamiento, ser informados de quien los posee, con que utilidad (STC 292/2000).

Con todo, tocaba la adaptación nacional al RGPD, cuestión que evidenciaba algunas limitaciones de la Ley Orgánica, pues esta tiene como función el desarrollo normativo inmediato de la Constitución en aspectos básicos o fundamentales del orden constitucional, necesarias e indispensables para la obra del constituyente. El RGPD es la norma llamada a desarrollar el derecho fundamental consagrado en el art. 8CDFUE y a regular sus elementos esenciales[33] (STC 127/1994), si bien en otras sentencias se ha calificado a la LO como legislación extraordinaria dotada de considerable dosis de abstracción (STC 127/1994 f.j.3). Si bien la Directiva implicaba alguna trasposición, la implementación del Reglamento no la necesitaba de per se, pues ya entraba en vigor, como dice su artículo 99.2, bajo el principio de aplicabilidad en todos los estados miembros.

[33] Y así lo ha hecho de forma bien exhaustiva al normar la práctica totalidad de los elementos conformadores de este derecho: el objeto y ámbito de aplicación material y territorial (arts. 1 a 3) —incluyendo veintiséis definiciones de conceptos básicos (art. 4)—; los principios básicos (arts. 5 y 6); las condiciones del consentimiento (arts. 7 y 8); las reglas relativas a categorías especiales de datos (arts. 9 y 10); los derechos de transparencia, información, acceso, rectificación, supresión (olvido), limitación, notificación, portabilidad y oposición (arts. 12 a 22); las obligaciones de responsables y encargados de los tratamientos (arts. 24 a 33); las técnicas de garantía preventiva como las evaluaciones de impacto46, el nombramiento de delegados de protección de datos y los códigos de conducta y certificaciones (arts. 35 a 42); las transferencias internaciones (arts. 44 a 50)47; el estatuto básico de las auto- ridades de control (arts. 51 a 60); los procedimientos europeos de cooperación y coordinación (arts. 61 a 67); el estatuto del Comité Europeo de Protección de Datos (arts. 68 a 76); el régimen de recursos y responsabilidad (arts. 77 a 82); el régimen sancionador (arts. 83 y 84); regulaciones específicas (arts. 85 a 88) y excepciones (art. 89) (Rallo Lombarte, A. 2019)

De todas maneras, los reglamentos europeos pueden habilitar a los estados a completar su regulación, como recuerda la sentencia del TJUE en su caso Azienda Agricola Monte Arcosu SRL (STJUE C-403/98), aunque la razón propia de un reglamento y de su función de sistema de fuentes, sus efectos tienen, por lo general un efecto inmediato en las naciones, sin que sea necesario que estas adopten medidas de aplicación, pero, en el caso que nos ocupa el RGPD contiene varias remisiones al derecho de los estados miembros posibilitándoles su adaptación nacional hasta el extremo de debiliar extraordinariamente su potencia armonizadora y convertire en un *tertium genus* en el sistema de fuentes del derecho europeo (Rallo Lombarte, A., 2019), como son los ejemplos del art. 89 RGPD, que se verá más adelante, y el 51, que establece las autoridades de control, sin embargo, en contra de la opinión de Rallo, este artículo, precisamente, armoniza los sistemas de control bajo autoridades independientes pero estrechamente unidas a la Comisión pues, además de notificar a esta todas las disposiciones legales que adopten (en conformidad con el reglamento), mecanismo útil también para establecer un régimen de cooperación entre todas las autoridades (la de control principal y demás autoridades interesadas (art.60 RGPD)) o, también asistencia mutua (art. 61) y lo más importante, forman parte del Comité Europeo de protección de datos todas las autoridades de control mediante el director de dicha institución que representará a su estado miembro en esta materia.

Otros artículos donde se cede cierto terreno al legislador nacional es en el art. 8.1 *in fine*[34] pero estableciendo techos normativos (no puede ser inferior a 14 años) o el 9.2 que habla sobre el tratamiento de categorías especiales de datos personales o 10, que se ejemplifica en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Como novedad también destaca la regulación de los datos referidos a los fallecidos, que, tras su exclusión, la ley permite que las personas vinculadas al fallecido, por razones familiares o de hecho, o sus herederos, puedan solicitar el acceso a los mismos, así como una rectificación o supresión siempre y cuando el fallecido no lo hubiera prohibido expresamente.

[34] Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.

El principio de seguridad jurídica obligaba a una depuración, a la cual contribuyó en gran medida el Informe con número de expediente 757/2017 que examinaba el expediente relativo al Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Dicha derogación explícita de todas las normas nacionales que resulten incompatibles con el Reglamento de acuerdo con lo señalado desde el TJUE en la comisión/España en el caso C-205/04:

> La incompatibilidad de una legislación nacional con las disposiciones del derecho comunitario, aunque sean directamente aplicables, sólo puede quedar definitivamente eliminada mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse.

Cumpliéndose en la disposición derogatoria de la LOPD, la cual derogaba a la ley orgánica 15/1999 y aprovechando sus habilitaciones expresas, la LOPD, en su primer artículo ya cita el doble objeto que tiene la ley, adaptar el ordenamiento jurídico al reglamento y complementar sus disposiciones, en muchas ocasiones por razones de oportunidad política y coherencia temática, tanto es así que, el título X, que incorpora las garantías de los derechos digitales de la LOPD (Martínez Rodríguez, N. 2018), fue introducido durante el *iter* legislativo a raíz de una enmienda presentada por el PSOE de forma que el inicial Proyecto de ley se vio modificada en el trámite de enmiendas ampliándose el objeto, modificándose su denominación e incorporándose un amplio y sistemático elenco de derechos digitales en el título décimo (Rallo Lombarte, 2019).

Este título obedece a la necesidad de abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el 18.4 CE. Son objeto de regulación derechos y libertades como: la neutralidad en internet, acceso universal, derechos a la seguridad y educación informática y la protección de menores, también reconoce el derecho de rectificación y el de actualización de informaciones en medios de comunicación digitales, el derecho al olvido, portabilidad en redes sociales, derecho testamentario digital y, en el ámbito laboral, derecho a la intimidad frente a los dispositivos de videovigilancia, grabación de sonidos y geolocalización, así como los derechos digitales de negociación colectiva (Martínez Rodríguez, N. 2018)

Las habilitaciones expresas del Reglamento europeo no agotan ni impiden las posibilidades normativas del legislador español y, además, la garantía de aplicación

del RGPD ha llevado a la LOPD ha incorporar diversas referencias en aras de la seguridad jurídica como se testifica en el art. 2.2 LOPD, art.3, art 4.2, art. 11 (transparencia) art. 13 (Dcho. acceso), art. 32 (bloqueo de datos) y art.34, que trata la designación de un delegado de protección de datos, otra importante novedad que incorpora el reglamento, y que la LOPD regula los aspectos más relevantes de la figura como su designación, cualificación, posición dentro de las organizaciones e intervención con motivo de reclamación ante la AEPD.

En el Título IV, se contemplan disposiciones aplicables a situaciones específicas de tratamiento de datos, que incluye casos donde el interés legítimo del responsable prevalece de manera presuntiva (presunción *iuris tantum*), tales como el tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales, sistemas de información crediticia y ciertas operaciones mercantiles. También contemplan situaciones como videovigilancia, ficheros de exclusión publicitaria y sistemas de denuncias internas, donde la licitud del tratamiento se deriva de un interés público. Asimismo, se mencionan tratamientos lícitos como los destinados a funciones estadísticas, archivos en interés público y datos relativos a infracciones y sanciones administrativas. Sin embargo, estos tratamientos lícitos no eximen al responsable de cumplir con las medidas de responsabilidad activa establecidas en el RGPD y en la misma Ley Orgánica.

La ley subraya la transición del RGPD de un modelo de control de cumplimiento a uno basado en el principio de responsabilidad activa (obligaciones del Título IV y medidas de responsabilidad activa, Título V, capítulo I). Este principio impone una evaluación previa del riesgo potencial del tratamiento de los datos personales por parte del responsable o encargado, y en base a dicha evaluación, la adopción de las medidas pertinentes, incluyendo las obligaciones generales del responsable y encargado del tratamiento, supuestos de corresponsabilidad, el registro de las actividades de tratamiento y la obligación de bloqueo de los datos.

Otra innovación del RGPD, recogida en esta Ley Orgánica, es la creación del Delegado de Protección de Datos, una figura independiente cuya función es identificar los riesgos en el tratamiento de los datos y buscar soluciones a posibles brechas. La ley permite que esta figura sea obligatoria o voluntaria, integrada o no en la organización del responsable o encargado, y puede ser tanto una persona física como jurídica. La ley regula aspectos relevantes como su designación, cualificación, posición en las organizaciones y su intervención en caso de reclamaciones ante las autoridades de protección de datos.

Una particularidad de nuestro Título VI, la cual regula las transferencias internacionales de datos es que las autoridades de protección de datos pueden aprobar tantos modelos contractuales o normas corporativas vinculantes, como supuestos de autorización o supuestos de información previa. (Martínez Rodríguez, N. 2018).

Pero, sin lugar a duda, uno de los mayores ejercicio de desarrollo normativo es bajo el título IX al regular el régimen sancionador y tipificar un catálogo de vulneraciones legislativas no desarrolladas en el Reglamento (Rallo Lombarte, 2019). El RGPD establece un sistema de sanciones que permite un amplio margen de apreciación y, en esta línea, tras enumerarse los sujetos responsables, se tipifican las conductas y distingue entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento establece al fijar la cuantía de estas, categorizando de las infracciones que hace a los efectos de determinar los plazos de prescripción. También se regulan en la ley orgánica los supuestos de interrupción de la prescripción, como las sanciones y medidas correctivas.
(Martínez Rodríguez, N. 2018).

Como novedad también destaca la regulación de los datos referidos a los fallecidos, que, tras su exclusión, la ley permite que las personas vinculadas al fallecido, por razones familiares o de hecho, o sus herederos, puedan solicitar el acceso a los mismos, así como una rectificación o supresión siempre y cuando el fallecido no lo hubiera prohibido expresamente.

Sin embargo, recordemos que el RGPD tiene por objetivo la armonización normativa a través de la coherencia y comprensión, es decir, principios de certeza y seguridad jurídica, por lo que, dentro de su maleabilidad, las normas nacionales deben perseguir una reproducción literal de los preceptos reglamentarios, lo que explica la regulación explicita y las remisiones al RGPD contenidas, por ejemplo, en los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición (art. 13 a 18) aunque, incorpora dos nuevos derechos como son el derecho de limitación y el de portabilidad.

Debemos resaltar la disposición adicional decimocuarta por la cual las:

> Normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE (…), que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.

Otras modificaciones relevantes a raíz de la entrada en vigor de la LOPD son las que tienen que ver con la Ley de Enjuiciamiento Civil, concretamente su artículo 15 bis, así como los artículos 10, 11, 12 y 122 de la Ley 29/1998, los artículos 58, 66, 74 y 90 de la ley 6/1982, y los arts. 6 y 15 de la Ley 19/2013, así como casi una decena más de leyes[35] (Martínez Rodríguez, N. 2018).

4.1. Ley orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

En este apartado pondremos de manifiesto las modificaciones de la LOPD en consecuencia de la entrada en vigor de la LO 7/2021. Una de las grandes novedades fue la modificación del artículo 2, añadiendo un apartado más, el quinto:

> El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.

Otra modificación, a tenor del contenido de la LO 7/2021, en la LOPD fue en su artículo 44.3. por la disposición final 4.2 de la LO/2021:

[35] la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (artículos 6 y 15); la Ley 14/1986, de 25 de abril, General de Sanidad (artículo 105 bis); la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (artículo 16); la Ley 39/2015, de 1 de octubre, del Procedimien- to Administrativo Común de las Administraciones Públicas (artículo 28); la Ley Orgáni- ca 2/2006, de 3 de mayo, de Educación (artículo 2); la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (artículo 46); el Texto Refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre (artículo 20); y el Texto Refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre (artículo 14).

> 3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

De igual forma sucedió con la disposición adicional número 15 de la LOPD que habla sobre los requerimientos de información por parte de la Comisión Nacional del Mercado de Valores.

5. Reglamento (UE) 2016/679 del parlamento europeo y del consejo, de 27 de abril de 2016.[36]

5.1. Consideraciones previas

En las consideraciones previas de la ley hace mención del artículo octavo primer apartado de la Carta de los Derechos Fundamentales de la UE introduciendo que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental y que, por lo tanto, es aplicable, sus principios y normas, a cualquiera, independientemente de su nacionalidad o residencia.

Para este Reglamento el derecho a la protección de datos personales debe "servir a la humanidad" y, dejando de lado su grandilocuencia, esta máxima hace alusión a que, simplemente, no es un derecho absoluto puesto que debe considerarse en relación con su función en la sociedad, mantener el equilibro con otros derechos fundamentales con arreglo al principio de proporcionalidad.

En su elaboración se ha tenido en cuenta una retahíla de derechos, de los cuales destacamos los ya presentes en el artículo 18 de nuestra constitución, así como en el 14, 16 o el 20.

La aplastante realidad en cuanto al incremento de la magnitud de flujos transfronterizos de datos personales en la unión entre operadores públicos y privados, incluidas las personas físicas, las asociaciones y empresas, han planteado, como ya sabemos, nuevos retos en este campo por lo que era necesario un marco más sólido y coherente, respaldado por una ejecución estricta, en parte, en aras a desarrollar confianza en la economía digital a la hora de su desarrollo en el mercado interior. Las personas físicas deben tener el control de sus propios datos y por ello, es necesario reforzar la seguridad jurídica.

La Directiva 95/46/CE era válida en principios, pero tenía abierta una brecha por donde calaba la inseguridad jurídica y una percepción, que se había generalizado en la opinión pública, de que existen riesgos importantes para la protección. La discordancia de la protección de los datos de carácter personal entre los estados

[36] (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, RGPD)

miembros impedía una libre circulación garantista, lo que constituía un obstáculo en el ejercicio de las actividades económicas de la zona del EEE.

Como ya se mencionó el Reglamento como acto legislativo permite la uniformización de la protección de este derecho de una forma coherente, exigiendo a los estados facultarse a fin de estar preparados para adoptar las disposiciones del Reglamento.
Aun así, en el presente Reglamento se permite un margen de maniobra para que cada estado especifique sus normas inclusive para categorías especiales como "datos sensibles".

Sea como fuere, la protección efectiva de un derecho interconectado en diversos estados solo puede darse si se refuerzan y delimitan claramente los derechos de los interesados y las obligaciones de los que tratan datos y que en cada estado miembro existan poderes con la facultad de supervisar y garantizar el cumplimiento de las normas. El universalismo que pretende esta ley necesita de garantías para los operadores económicos, incluidas las PYMES y que estas puedan ofrecer a las personas físicas de todos los EEMM el mismo nivel de derechos y obligaciones exigibles, cono las responsabilidades para los encargados del tratamiento, con el objetivo de asegurar la supervisión coherente de dicho tratamiento y, en caso de ser sancionable, que la sanción sea equivalente en todos los estados.
Ahora bien, sería pretencioso que la exigencia sea equivalente para microempresas que, para una sociedad con más de 250 empleados, así pues, por debajo de este número existen excepciones en materia de llevanzas de registros, alentando además a que las disposiciones complementarias que se lleve a nivel nacional tengan en cuenta la condición de estas PYMES[37] .

En esta ley se protege especialmente a las personas físicas, sin tener en cuenta su nacionalidad ni residencia, en relación con sus datos, ya que no regula el tratamiento de datos personales relativos a personas jurídicas, incluido el nombre, la forma y sus datos de contacto.

[37] El concepto de microempresas, pequeñas y medianas empresas debe extraerse del segundo artículo del anexo de la Recomendación de la Comisión de 6 de mayo de 2003 que establece que las PYMES (incluye microempresas) son empresas con una plantilla menor de 250 personas y cuyo volumen de negocios anual no excede de los 50 millones de euros o cuyo balance general anual no excede de 43 millones.
En lo concreto, una pequeña empresa ocupa menos de 50 personas y su volumen de negocios o balance general anual no supera los 10 millones de euros. Una microempresa ocupa menos de 10 personas y su volumen anual y balance no supera los dos millones de euros.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:es:PDF

Capítulo I – Disposiciones Generales

El Reglamento General de Protección de Datos, como es recurrente en cualquier acto legislativo, comienza encapsulando su objeto (art.1) y ámbito material de aplicación que, en definitiva, son las personas físicas en lo relativo al tratamiento, automatizado o no (art. 2.1) de los datos personales. Esto incluye aquellos que pueden ir destinados manualmente o de forma automática a ficheros[38].

Quedan excluidos de su aplicación:

> *los Estados miembros en el desarrollo de sus actividades comprendidas en el capítulo segundo del título quinto del TUE, las relativas a las disposiciones específicas sobre la política exterior y de seguridad común* (art.2.b); *el tratamiento de datos de personas físicas en el ejercicio de actividades exclusivamente personales, es decir, aquellas que no rebasan el ámbito autogestionado y privado* (2.c); *actividades no comprendidas en el ámbito de aplicación de derecho de la Unión* (2.a); *aquellas que tienen que ver con la prevención, investigación, detección y enjuiciamiento de procesos penales* (2.d).

Además, es necesario tener en cuenta que, en contra de la actualización del artículo 2.3, el tratamiento de datos personales de personas físicas llevada a cabo por instituciones, órganos y organismos de la Unión se efectuará en consonancia con el Reglamento 2018/1721 (analizado brevemente más adelante) que derogó el anterior Reglamento 45/2001.

Por lo que respecta al comercio electrónico, particularmente las normas a cerca de la responsabilidad de los prestadores de servicios de intermediarios, establecidos

[38] Aunque en el artículo cuarto, apartado sexto, de este mismo reglamento encontramos una definición para "fichero" y que sirve como definición para todo su desarrollo («fichero»: *todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica*), desde la escuela de ingenierías industriales de la Universidad de Valladolid ofrecen una definición para un fichero informático bastante acurada que es la siguiente: *colección ordenada de datos que tienen entre sí una relación y que se almacenan de forma permanente en un dispositivo de memoria no volátil*. Con permanente se refiere a que, salvo fallos catastróficos o por eliminación intencionada, los datos permanecen en el medio (magnético o de otro tipo) continúan existiendo después de que el programa que los creó deja de ejecutarse, lo que lo diferencia sustancialmente de los datos almacenados en la memoria RAM, una memoria volátil y que no sobrevive al programa que los crea. El concepto de fichero informático realmente *es una abstracción del Sistema Operativo, que, de forma transparente al programador, utiliza los recursos del hardware creando sobre ellos una estructura lógica para representarlos, facilitando a los lenguajes de programación el uso de interfaces de usuario simples y versátiles*. (*Concepto De Fichero — Fundamentos De Programación En C++*, 2020) Para ampliar a cerca de la jerarquía de los distintos tipos de datos véase el Anexo I.

del art. 12 al 15 del presente Reglamento, se aplicarán sin perjuicio de la Directiva 2000/31[39].

En el ámbito territorial, respecto a su predecesora, presenta algunas novedades que pueden observarse simplemente con la extensión del artículo tercero. El Reglamento se aplica al tratamiento de DP en el contexto de las actividades de un establecimiento del responsable o del encargado de la UE, independientemente de que el tratamiento tenga lugar allí o no (3.1). Ahora bien, también será de aplicación cuando los DP sean de una persona de la Unión, aunque su responsable no se ubique en ningún país miembro, siempre que la actividad esté relacionada con (2.a) la oferta de bienes o servicios a dichos interesados o (2.b) en la medida en la que el control de su comportamiento se esté dando dentro del espacio de la Unión.

También se prevé, en virtud del artículo 3 ter.1 y 3 del Tratado de Lisboa[40], que el RGPD se aplique al tratamiento de datos por parte de un responsable no ubicado en la unión pero que, sin embargo, le sea de aplicación su derecho en virtud del derecho internacional público.
Es preciso señalar en este apartado que, la Comisión, puede reconocer un país no miembro, territorio, sector específico o una organización, como falto de garantías en cuestión del Dcho. PD. por el cual no permita la transferencia siempre que no se cumplan las garantías previstas como son:

> El recurso a normas corporativas vinculantes, cláusulas de protección adoptadas por la Comisión o autoridad de control, clausulas tipo de PD adoptadas por la Comisión o por una autoridad de control o cláusulas contractuales autorizadas por una autoridad de control, que aseguren la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, esto incluye la disponibilidad de derechos exigibles y acciones legales efectivas como el derecho a la reparación

[39] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
[40] Por el que se modifican el Tratado de la Unión Europea y el Tratado Constutivo de la Comunidad Europea, inscribió el principio de subsidiariedad en el artículo 5.3: "*En virtud del principio de subsidiariedad, en los ámbitos que no sean de su competencia exclusiva, la Unión intervendrá sólo en caso de que, y en la medida en que, los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, ni a nivel central ni a nivel regional y local, sino que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión*.", y derogó la disposición correspondiente del Tratado de Amsterdam, si bien retomó la formulación de dicho artículo y, además, el TL sustitutyó el Protocolo de 1997 por uno nuevo (el nº2) cuya principal novedad radica en el papel de los Parlamentos nacionales en relación con la garantía del respeto del principio de subsidiariedad (1.3.5) (Eeva Pavy, 2023)

administrativa o judicial efectiva y, evidentemente, reclamación de indemnizaciones, en espacio de la UE o en un tercer país u organización[41].

Aprovechando el transcurso lineal de la propia ley, pondremos en manifiesto alguna de las definiciones del artículo cuarto, que no se haya tratado con anterioridad a lo largo de este trabajo, bajo dos criterios, en primer lugar, el número de ocasiones en las que aparece un término o concepto a lo largo del Reglamento y por utilidad o matiz (obviando, por el momento, lo más irrelevantes o evidentes).

Empezando por el primer criterio, el término "tratamiento" se lleva la corona pues aparece casi novecientas veces a lo largo de la normativa supranacional, este se refiere a cualquier operación o conjunto de estas realizada sobre DP, mediante procedimientos automáticos o manuales, de cualquier índole.
Por otro lado, el "responsable del tratamiento" puede ser una persona jurídica o física, autoridad pública, servicio u otro organismo, que de alguna manera, determine los fines y medios del tratamiento y, por cuenta suya, puede ejecutarlo subsidiariamente un encargado o no. Las "autoridades de control" son autoridades públicas independientes establecidas por un estado miembro con arreglo al primer artículo del Capítulo VI dedicado a esta figura y que veremos más adelante.

Capítulo II – Principios

Los principios de la norma aplicables al tratamiento de datos en el RGPD se regulan en el artículo 5, que pueden resumirse en el principio de licitud y transparencia, el principio de limitación de la finalidad, principio de minimización de datos, principio de exactitud, principio de limitación del plazo de conservación, los principios de integridad y confidencialidad y, finalmente, el principio de responsabilidad proactiva, objeto de desarrollo del artículo 24[42] (M. Gómez, R., 2016).
Trasladándolo a otras palabras podemos afirmar que el tratamiento debe ser (1) lícito, leal y transparente, lo que implica también que sus fines se determinen explícitamente y sean legítimos, de manera que no se trataran ulteriormente salvo aquellos datos que entren en consonancia con las disposiciones del artículo 89.

[41] Reglamento 2016/679, Considerandos previos 108.
[42] El art.24 RGPD establece la responsabilidad del responsable en el tratamiento, pues este deberá tener en cuenta el contexto, naturaleza y fines, así como los riesgos de diversa probabilidad y gravedad para los derechos de las personas físicas, aplicando las medidas técnicas y organizactivas apropiadas para grantizas y demostrar que el tratamiento es conforme a ley. Algunas de las maneras de demostrar la proactividad es la adhesión a códigos de conducta aprobados en el art. 40 de este mismo reglamento o a un mecanismo de certificación aproado a tenor del art. 42

También serán adecuados, pertinentes, limitados y exactos, pues, de no cumplir la última condición, se deben adoptar todas las medidas razonables para que se supriman o rectifiquen. Todo ello debe, en conformidad del art. 89, no extenderse por un tiempo más largo del estrictamente necesario para el fin al que sirve y siempre tratados de manera que se garantice su seguridad en contra del tratamiento no autorizado o ilícito. Por último, el responsable siempre debe poder demostrar el cumplimiento del reglamento y ser proactivo en esa postura.

Adelantamos el contenido del artículo 89, pues sus garantías y excepciones es una de las disposiciones relativas a situaciones específicas de tratamiento más relevantes por sus características e influencia en el articulado general y en algunos específicos con tanta relevancia como son los artículos 14 a 21 del presente reglamento. En esencia, el art. 89 dice que, los datos personales podrán conservarse en archivos en la medida en la que cumplen un fin de interés público, de investigación científica, histórica o estadística, ahora bien, sujeta a las garantías adecuadas como es el principio de minimización de datos personales y a las que también se puede sumar medidas de seudonimización siempre que, en este tratamiento ulterior, se permita identificar.

La licitud del tratamiento, como ya se adelantó en el apartado en el que se hablaban sobre los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales adoptados por la Asamblea General de la ONU, la información de las personas debe ajustarse a los requerimientos, propósitos y principios de la Carta de las Naciones Unidas, no obstante, el artículo sexto del reglamento general específica que el tratamiento solo será lícito cumpliéndose, al menos, uno de los siguientes requisitos: que sea necesario para la ejecución de un contrato, para el cumplimiento legal aplicable al responsable, para la protección de los intereses vitales del interesado u otra persona física, para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable o sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o tercero siempre que sobre dichos interese no prevalezcan sobre los del interesado que requiera protección, particularmente si se trata de un niño.

Uno de los artículos más importantes de los casi cien que hay en vigor es el artículo 7 RGPD, donde se determinan las condiciones para el consentimiento. Este artículo empieza diciendo: “Cuando el tratamiento se basa en el consentimiento del

interesado" hecho el cual constituye la mayoría de las relaciones de tratamiento de datos, el responsable será quien deba demostrar que se dio dicho consentimiento y, si este fue en una declaración escrita que también se refeira a otras cuestiones, la solicitud de consentimiento se presentará de forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo, que, además, el interesado, podrá retirar el consentimiento previamente dado en cualquier momento, sin afectar, eso sí, a la lícitud del tratamiento basado en el consentimiento previo a su retirada.

Uno de los aspectos más controversiales por su nula aplicabilidad en la realidad material es la última premisa del 7.3 in fine, aquella que dice: *"será tan fácil retirar el consentimiento como darlo"*. Esta cuestión, que en las conclusiones se tratará, es una de las políticas garantistas más esenciales en la protección de la intimidad de nuestros datos personales, así como la capacidad de "autodeterminar" la información que nos atañe.

De momento solo dejaré plasmada la siguiente reflexión: Para adquirir, contratar o utilizar cualquier producto o servicio es necesario firmar (virtualmente) una casilla, en la que, de forma explícita, cedes tu consentimiento. Este hecho obvia que (el consentimiento) esta "informado" de las cientos de cláusulas a las que te dejan acceder desde un enlace colindante a la casilla o, a veces, a través de una *preview* que te ejemplifica, rápidamente, lo tortuoso que es el propio texto, el cual, claramente, no van a leer una gran mayoría de consumidores por puro desinterés o incapacidad de estar asimilando miles de líneas, encima escritas con un lenguaje jurídico (lo que ya contraviene el 5.1 y el 7.2), diariamente en la vorágine tecnológica que supone navegar por internet. Esto, que por supuesto equivale a coartar el consentimiento[43], pues este desconoce aquello que consiente, requeriría medios parecidos para ser revocado, es decir, un sistema automatizado tan imperativo para el funcionamiento del servicio, como cuando el consentimiento se dio.

Siguiendo con las condiciones del consentimiento, el artículo octavo debemos considerar que, de ser, el interesado, un niño menor de 16 años, será ilícito el tratamiento de sus datos personales, de tal manera que solo el titular de su patria potestad o tutela puede autorizar el procesamiento de su información personal. Se

[43] Ya que, como bien dice el art.4.11 RGPD el consentimiento del interesado es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción informativa, el tratamiento de datos que le conciernen.

permite que, en las legislaciones nacionales en materia de Protección de datos, se establezca una edad inferior, pero nunca menor a 13 años. En el art. 12.6 la LOPD establece la representación del consentimiento a los menores de 14 años en todo lo relativo al acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles, si bien debe tenerse en cuenta el art. 162.1 del CC por el cual exceptúa de la representación legal del titular de la patria potestad a "*los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con su condición de madurez, pueda realizar por sí mismo*", abriendo la necesidad de considerar si el menor tienes condiciones suficientes de madurez para prestar consentimiento. En añadidura, el informe de la AEPD a cerca del consentimiento otorgado por menores de edad[44] nos recuerda *los supuestos de adquisición de la nacionalidad por el ejercicio del derecho de opción o por residencia*, que se efectuará en, también, un mayor de 14, asistido de su representante, o la capacidad para testar (con excepción del testamento ológrafo del 662.1 del CC). Por otro lado, según la ha señalado la resolución de 3 de marzo 1989 de la DGRN[45]:

> No existe una norma que, de modo expreso, declare su incapacidad para actuar válidamente en el orden civil, norma respecto de la cual habrían de considerarse como excepcionales todas las hipótesis en que se autorizase a aquél para obrar por sí; y no cabe derivar esa incapacidad ni del artículo 322 del Código Civil, en el que se establece el límite de edad a partir del cual se es capaz para todos los actos de la vida civil, ni tampoco de la representación legal que corresponde a los padres o tutores respecto de los hijos menores no emancipados.

De lo que la agencia extrae que la minoría de edad no supone una causa de incapacitación (de las reguladas en el art. 200CC), *por lo que aquélla habrá de ser analizada en cada caso concreto a los efectos de calificar la suficiencia en la prestación del consentimiento en atención a la transcendencia del acto de disposición y a la madurez del disponente*. A lo que concluye que se debe recabar su información considerando la totalidad de los extremos contenidos en el 5.1 de la LOPD (deber de confidencialidad), pero que, cabe considerar que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismo, el tratamiento automatizado de sus datos de carácter persona.

A lo que debemos calificar como un graso error, ya que, teniendo la vertiente moderada (art. 8.1RGPD), que, en definitiva, ofrece la mayor protección al menor, se

[44] https://www.aepd.es/es/documento/2000-9905.pdf

[45] Dirección General de Registros y del Notariado

opta por dejar a manos de un responsable no determinado, bien podría ser el poseedor de la *patria potestad* o tutor (parece la más razonable por las condiciones materiales de actuación y valoración), bien podría ser el responsable del tratamiento, que determine si el menor, de entre 14 y 16 años, es lo suficientemente maduro como para prestar consentimiento. Estamos obviando, a parte, la justificación que daba en su informe, pues se trata, claramente de una falacia *ad populum*, pues, para responder a la pregunta que motiva ese texto, se remiten al Código Civil, en materia de adquisición de nacionalidad o, también testamentaria y, en adición, a la resolución de la DGRN, vista pocas líneas más arriba, las cuales tratan cuestiones absolutamente distintas al basto mundo de posibilidades contractuales que permite acceder internet, para justificar que un mayor de 14 años es razonablemente maduro como para dar su consentimiento.

Para más inri, el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal señala, en su primer punto, *que solo podrá procederse al tratamiento de los datos de los mayores de catorce años cuando la ley no exija para su prestación la asistencia de los titulares de la patria potestad o tutela*, por lo que, solo teniendo en cuenta esta disposición y la jerarquía normativa del Reglamento General de Protección de Datos podemos concluir que la afirmación de nuestra Agencia es erróneo.
Siguiendo con este mismo artículo resaltaría, asimismo, su punto tercero y cuarto, donde, en el primero, se establece que el lenguaje para obtener datos de un menor de edad debe ser fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo. El cuarto punto dice que será el responsable del fichero o tratamiento el responsable de articular procedimientos que garanticen que se ha cotejado de manera efectiva la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

En caso del art.8.1 RGPD, decreta que, el responsable de tratamiento, deberá hacer *"esfuerzos razonables" para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela*. En caso de España, concretamente el 73.b), *no acreditar la realización de estos esfuerzos razonables está considerado una infracción grave, así como recabar información de un menor sin el consentimiento de su tutor legal*.

Ahora bien, un apunto importante, de parte de nuestra Agencia de protección de datos (AEPD), en su guía del RGPD para responsables de tratamiento, es que, los "esfuerzos razonables", no son una obligación de resultados, sino una obligación de medios, por los cuales, se espera que el encargado o responsable del tratamiento lleve a cabo los procedimientos razonables para establecer la intervención real de padres o tutores, teniendo en cuenta, como es lógico, los medios tecnológicos disponibles (AEPD, s.f.). Importante resaltar la condición de "esfuerzos razonables" como concepto jurídico indeterminado, el cual puede tener resultados viciados en la práctica y más teniendo en consideración el número de estados miembros que conforman la Unión Europea, todas ellas con su desarrollo normativo, previsto por el propio Reglamento, lo que rompe en parte en principio armonizador del RGPD.

Otro punto interesante de este artículo (art.8 RGPD) lo contiene su primer punto en el momento que dice: *Cuando se aplique el art. 6, apartado 1, a)*[46]*, en relación con la oferta directa a niños de "servicio de la sociedad de la información",* ya que es oportuno señalar que su definición se encuentra en el artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, remitidos por el art. 4.11 RGPD, que dice: *todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios*, que, a su vez, lo amplia el apartado e) "reglas relativas a los servicios" estableciendo que, a efectos de la siguiente definición:

> (i) se considerará que una norma que se refiere a los servicios de la sociedad de la información cuando, por lo que respecta a su motivación y al texto de su articulado, tenga como finalidad y objeto específicos, en su totalidad o en determinadas disposiciones concretas, regular de manera explícita y bien determinada dichos servicios. De igual forma, (ii) se considerará que una norma no se refiere específicamente a los servicios de la sociedad de la información cuando sólo haga referencia a esos servicios implícita o incidentalmente (Directiva 2015/1535).

Como novedad, el artículo noveno, introduce, respecto a su predecesora normativa, los datos genéticos y biométricos (art. 4.13 y 14 RGPD), a los datos de categoría especial[47], cuyo tratamiento, en consecuencia, pasa a estar prohibido, con carácter

[46] el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

[47] Se incluyen también en esta categoría los datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos relativos a la salud o relativos a la vida sexual y los que indiquen la orientación sexuales de una persona física.

general, siempre que se lleve a cabo con el fin de identificar de forma unívoca a una persona física (Mayor Gómez, R., 2016), siempre teniendo en cuenta las correspondientes excepciones que, en el presente caso se tratan de las señaladas en el punto segundo[48] de este mismo artículo. Además, respecto a estas dos categorías nuevas, los estados miembros podrán introducir condiciones adicionales y limitaciones.

Cabe señalar, en vistas del análisis de los artículos 15 a 20, que aquellos datos personales tratados con un fin que no requiere la identificación, además de que su responsable no estará obligado "reindentificar" a su interesado, podrá, demostrando que no está en condiciones de identificarlo, informarlo si puede y no le será de aplicación los artículos señalados, siempre y cuando a efectos de su ejercicio, el interesado aporte información adicional que permita su identificación (art. 11.2)

Capítulo III – Derechos del interesado (y deberes del responsable)

En el siguiente capítulo se contienen los derechos de los interesados que, suponen, al menos en lo que se refiere a la normativa nacional en materia de protección de datos[49], la incorporación de novedosos derechos como el de supresión o derecho al olvido, portabilidad de datos lo que, de alguna manera, supera los denominados Dchos. ARCO: Acceso, Rectificación, Cancelación y oposición, que también están presentes (Mayor Gómez, R., 2016).

5.2. Derecho a la portabilidad (art. 20)

Respecto a la portabilidad (art. 20) podemos definirlo como la capacidad del interesado para recibir los datos que le incumban, previamente facilitados al responsable, de forma estructurada, de uso común y lectura mecánica para transmitirlo a otro responsable de tratamiento sin que lo impida el responsable a quien se le facilitaron, concurriendo los siguientes presupuestos: a) el tratamiento

[48] Son excepciones arquetípicas en este campo del derecho, como son: cuando el interesado cede explícitamente dichos datos personales; o bien para el imperativo cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable; o necesario para proteger interesas vitales; tratar datos manifiestamente públicos a voluntad de su autor; por razones de interés público esencial (puede ser en el ámbito de la salud, art.9.h o con fines de archivo por razones de interés público art. 9.j) en base al derecho de la Unión; fines de medicina preventiva (con las garantías del punto tercero que obliga a que el tratante profesional este sujeto a la obligación de secreto profesional); o con fines estadísticos, de investigación científica.

[49] Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y Real Decreto 1720/2007 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.

esté basado en el consentimiento con arreglo al art. 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a)[50], o en un contrato con arreglo al art. 6, apartado 1, letra b); y b) el tratamiento se efectué por medios automatizados."

Su ejercicio no puede afectar peyorativamente a los derechos y libertades de otros, sin perjuicio del art. 17, el derecho al olvido, y no se aplica al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. También implica que, los datos que se transmitan, no tiene por qué ser transferidos intermediariamente al interesado, sino que pueden hacerlo de un responsable a otro.

5.3. Supresión ("derecho al olvido")

Una de las cuestiones más revolucionarias de esta ley se encuentra en su artículo 17, donde se regula el derecho de supresión o, también conocido por "el derecho al olvido". Es un derecho emergente que, previamente, fue recogido desde el derecho de cancelación y portabilidad de los datos en Internet reconocidos por la Directiva 95/46/CE y, posteriormente en la Comunicación de la Comisión Europea presentado en Bruselas el 4 de noviembre de 2010, tratando a este como una cancelación de los datos personales, bajo la premisa de reforzar los derechos de los ciudadanos europeos, conclusión a la que ya llegó el TJUE, pues teniendo en cuenta el mantenimiento ad infinitum de la información publicada en internet y que, esta cuestión, puede provocar serios efectos lesivos en la vida personal, (y entendiendo además como un derecho fundamental) debe ofrecerse al sujeto la posibilidad de su libre desarrollo personal, es es, garantizar un mínimo dignidad humana (Arenas Ramiro M., 2015)

En la actualidad, el derecho al olvido es aquel que, bajo ciertas condiciones, te posibilita solicitar que los enlaces a tus datos personales no figuren en los resultados de una búsqueda en internet realizadas por tu nombre (AEPD, 2022, 14 julio), o, dicho con un lenguaje más jurídico: el interesado tiene derecho, sin dilación indebida del responsable, a solicitar la supresión de los datos que le conciernen, concurriendo alguna de las siguientes circunstancias: que estos no sean necesarios en relación con los fines de recogida, el interesado retire el consentimiento en que se basa el

[50] Art. 9.2. *El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado*.

tratamiento o se o se oponga y no prevalezcan otros derechos preponderantes, así como cuando hayan sido tratados de manera ilícita o, directamente, deban ser suprimidos en cumplimiento de una obligación legal. También se aúnan en estas circunstancias cuando los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de información, así como cuando se han hecho públicos pero exista unar razón legitima para ser suprimidos.

En el ya célebre caso Google Inc. contra la AEPD y Don M. Costeja, en el asunto C-131/12 del TJUE (2014), trataron esta cuestión desde la prematura óptica que les proporcionaba la Directiva 95/46. El Sr. Costeja González, así como los Gobiernos español e italiano (en representación de sus agencias) son de la opinión de que:

> *El interesado puede oponerse a la indexación de sus datos personales por un motor de búsqueda cuando la difusión de estos datos por la intermediación de éste le perjudica y de que sus derechos fundamentales a la protección de dichos datos y de respeto a la vida privada, que engloban el «derecho al olvido», prevalecen sobre los intereses legítimos del gestor de dicho motor y el interés general en la libertad de información.* (STJUE, C-131/12, Litigio principal y cuestiones perjudiciales, 90.)

Esto significa que el derecho al olvido ya había sido un derecho reconocido por la jurisprudencia europea y nacional. En esta sentencia se tenía por objeto una petición de decisión prejudicial planteada con arreglo al art. 267 TFUE, por la Audiencia Nacional, mediante auto de 27 de febrero de 2012, que dio paso al Tribunal de Justicia.

La jurisprudencia española, por otro lado, desde nuestro Alto Tribunal, se dictó en STS 545/2015 un pronunciamiento sobre el derecho al olvido, donde consideró que la difusión de una noticia a través de una página en de una hemeroteca digital (Ediciones El País) supone una vulneración del derecho al honor, que, por otro lado, el derecho de supresión no podía suponer una censura retrospectiva de las informaciones correctamente publicadas en su día ya que la integridad de los archivos digitales es un bien jurídico protegido por la libertad de expresión que excluye las medidas que alteren su contenido eliminando o borrando datos contenidos en ellos (Mayor Gómez, R., 2016). La sentencia que precedía esta afirmaba que la finalidad de la información ya se había logrado en los ochenta cuando se publico la noticia por la que le volcado en la hemeroteca digital solo tenía una finalidad mercantilista de incremento de los ingresos publicitarios generados en este soporte, por lo que, el interés de la sociedad no podía prevalecer sobre los

derechos al honor, intimidad y a la protección de datos de personas demandantes, que no son personajes públicos, de hecho, el enjuiciamiento parte de la licitud de la publicación de la información en la que aparecía las personas demandandtes, y, desde allí, se ciñe al tratamiento de sus datos personales derivados de la digitalización de la hemeroteca[51].

La forma a la que llega el Tribunal a este derecho es a través de una concreción del campo de los *derechos derivados de los requisitos de calidad del tratamiento de datos personales, lo que no ampara que cada uno construya un pasado a su medida o que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, pero obliga a los editores web y gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian hechos que no se consideran positivos*, siempre que este no fuera un personaje público o que exista un interés histórico. En ningún caso puede suponer una censura retrospectiva de la información correctamente publicada en su día.(STS 545/2015, fundamentos de derecho, primero, 7).

5.4. Derecho de acceso (art. 15)

El derecho de acceso es aquel donde el interesado puede obtener del responsable la confirmación de si se están tratando datos que le conciernen y, en tal caso, acceder a los mimos, así como a sus fines, categorías de clasificación y destinatarios a los que fueron comunicados, en particular en terceros países. En consecuencia, se habilitan también los derechos de rectificación, limitación y oposición. Antes del reglamento actual, se debían facilitar todos los datos de base del afectado, pero no copias o documentos (excepto en el caso de la historia clínica) (AEPD, s.f.).

[51] Las hemerotecas digitales gozan de la protección de la libertad de información, al satisfacer un interés público en el acceso a la información. Por ello, las noticias pasadas no pueden ser objeto de cancelación o alteración. El TEDH ha considerado que la protección de las hemerotecas digitales por el artículo 10 del Convenio implica que las noticias pasadas contenidas en ellas, a pesar de que su contenido pueda afectar a los derechos de las personas, no pueden ser eliminadas. La libertad de expresión protege el interés legítimo del público en acceder a los archivos digitales de la prensa, de modo que «no corresponde a las autoridades judiciales participar en reescribir la historia» (STEDH de 16 de julio de 2013, caso Wergrzynowski y Smolczewski c. Polonia, párrafo 65, con cita de la anterior sentencia de 10 de marzo de 2009, caso Times Newpapers Ltd -núms. 1 y 2- contra Reino Unido). Por tanto, la integridad de los archivos digitales es un bien jurídico protegido por la libertad de expresión (en el sentido amplio del art. 10 del Convenio de Roma, que engloba la libertad de información), que excluye las medidas que alteren su contenido eliminando o borrando datos contenidos en ellos, como puede ser la eliminación de los nombres de las personas que aparecen en tales informaciones o su sustitución por las iniciales (STS545/2015.

A nivel nacional está regulado en el art. 13 y contiene algunas particularidades como es el hecho de que si el responsable trata una gran cantidad de datos del solicitante este concrete a cuáles quiere acceder. También, en su apartado segundo, menciona que se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los DP, lo cual bastará para tener poe atendida su solicitud de ejercicio de derecho.

También incluye el concepto de ejercicio repetitivo cuando se ejerce en más de una ocasión en el plazo mínimo de seis meses, a menos que exista una causa justa. Igualmente, si el afectado, escoge una opción para el ejercicio de este derecho desde un medio distinto al que se le ofrece y que suponga un coste desproporcionado, se considerará una solicitud excesiva.

Por otro lado, cuando se trata de acceso a información pública, también estaría regulado por el artículo 105.b) CE y desarrollado por la Ley 19/2013 de Transparencia, acceso a la información pública y buen gobierno.

5.5. Rectificación (art. 16)

El derecho de rectificación confiere al interesado la capacidad de obtener del responsable una rectificación de sus datos que sean inexactos teniendo en cuenta el fin por el que se concedieron.
Está regulada en la LOPD en el artículo 15 y añade, respecto al reglamento, que deberá acompañar cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los daros objetos de tratamiento.

5.6. Limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas. (art. 18)

El interesado tiene derecho a la limitación del tratamiento, y que estos no puedan ser tratados sin su consentimiento explicito (18.2), cuando se cumpla al menos uno de los siguientes requisitos: impugnación por inexactitud de los DP; por tratamiento ilícito y el interesado se oponga a su supresión, cuando los datos ya no se necesiten para el fin que estuvieron recopilados pero el interesado los necesite para el ejercicio i

defensa de reclamaciones. Es importante tener en cuenta que la limitación es un derecho de los interesados que no debe confundirse con el bloqueo de datos que existe en la legislación nacional.

En la LOPD se encuentra en el art. 16, remitiéndose al RGPD y añadiendo que, cuando el tratamiento este limitado deberá constar claramente en los sistemas de información del responsable.

5.7. Oposición (art. 21)

Este derecho supone que puedes oponerte a que el responsable realice un tratamiento de tus datos por motivos de la situación particular, salvo que se acrediten motivos legítimos imperiosos para que el tratamiento prevalezca sobre los derechos del interesado.
Ahora bien, cuando se tratan los datos con objeto de la mercadotecnia directa, estos podrán ser opuestos en cualquier momento que deberán dejarse de tratar inmediatamente, comunicándole al interesado, primeramente, la confirmación de su oposición de manera clara, explicita y al margen de cualquier otra información. Como es habitual, su limitación son las presentes en el artículo 89, a los cuales el interesado podrá oponerse salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Capítulo IV – Responsable y encargado del tratamiento

En este capítulo centraremos nuestra atención, primeramente, en el registro de las actividades de tratamiento, pues se trata de una de las obligaciones más recurrentes e importantes de los responsables y encargados del tratamiento de tal manera que, así como adelanta el art. 30.4, tienen la obligación de poner el registro a disposición de la autoridad de control que lo solicite, en el caso de España, la AEPD.

En esencia, cada responsable o, en tal caso, su representante, llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad anotando (4.1):

> el nombre, los fines de tratamiento las categorías de destinatarios, transferencias de datos personales a un tercer país u organización internacional (4.2) que, siempre, deberán constar por escrito (4.3), siempre y cuando la empresa emplee a más de 250 personas, de no ser así no les será de aplicación los dos primeros apartados del artículo.

Es necesario resaltar el art. 25 en tanto que otorga protección en el tratamiento de datos desde el diseño y, por lo tanto, su alcance se extiende no tan solo a la materia de este Reglamento sino también complementa a otro de gran interés: las cookies.
Así pues, este artículo impera al responsable de tratamiento aplicar, tanto en el momento de determinar los medios como el propio tratamiento, las medidas técnicas y organizativas apropiadas, como, por ejemplo, la seudonimización, la minimización de datos e integrar las garantías necesarias a fin de cumplir los requisitos del RGPD (25.1). Todo ello en miras de garantizar que de, forma predeterminada, solo sean objeto de tratamiento los datos personas necesarios para el fin específico, obligación aplicable a la cantidad, extensión, plazo y accesibilidad de la recogida de información personal.

En los artículos 33 (notificación de una violación de seguridad de los datos personales a la autoridad de control) y 34 (Comunicación de una violación de seguridad de los datos personales) *se implanta la obligación de notificar a la autoridad de control y comunicar a los interesados las violaciones de seguridad de los datos personales*. Esta disposición representa una innovación significativa en la normativa de protección de datos, dado que anteriormente no existía tal obligación.

> El responsable del tratamiento de los datos está obligado a notificar a la autoridad de control competente cualquier violación de la seguridad de los datos personales sin dilación indebida, y en todo caso, dentro de las 72 horas siguientes a haber tenido conocimiento de la misma, salvo que pueda demostrarse que dicha violación no supone un riesgo para los derechos y libertades de las personas físicas. Si la notificación a la autoridad de control no se realiza dentro de este plazo, deberá acompañarse de una justificación de la demora.

Además, el RGPD establece la obligación de comunicar al interesado la violación de la seguridad de los datos personales sin dilación indebida y en un lenguaje claro y sencillo, siempre que dicha violación pueda suponer un alto riesgo para sus derechos y libertades, permitiéndole así adoptar las medidas de precaución necesarias.

Esta comunicación debe realizarse *lo más pronto posible y en estrecha colaboración con la autoridad de control, siguiendo sus directrices o las de otras autoridades competentes, como las autoridades policiales*. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y proporcionar

recomendaciones para que la persona física afectada pueda mitigar los posibles efectos adversos derivados de la violación.

La evaluación del impacto relativa a la PD (EIPD), que emana del art. 35, será uno de los artículos clave para evitar la aplicabiliad desmesurada de algunos modelos de inteligencia artificial en el tratamiento automatizado de datos y la elaboración de perfiles, pues, desarrolla que cuando sea probable que un tipo de tratamiento, particularmente cuando se trata de nuevas tecnologías, entrañe, por su naturaleza y alcance, un alto riesgo para los derechos y libertades de las personas físicas, el responsable de tratamiento deberá hacer una evaluación del inmpacto de las operaciones, una única vez.

La autoridad de control tiene la responsabilidad de establecer y publicar una lista en el comité del artículo 68[52] de los tipos de operaciones de tratamiento que requieren una EIPD, así como una donde figuren aquellas que no requieren de dicha evaluación. Siempre, antes de adoptar estas listas, la autoridad de control debe aplicar el mecanismo de coherencia si las listas incluyen actividades de tratamiento que pueden afectar sustancialmente a la libre circulación de datos personales en la Unión.

La EIPD debe incluir una descripción sistemática de las operaciones de tratamiento previstas, una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento, una evaluación de los riesgos para los derechos y libertades de los interesados, y las medidas previstas para afrontar los riesgos.

El cumplimiento de los códigos de conducta aprobados se tendrá en cuenta al evaluar las repercusiones de las operaciones de tratamiento. Cuando sea apropiado, el responsable del tratamiento deberá recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto.

Si el tratamiento tiene su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, y ya se ha realizado una EIPD como parte de una evaluación de impacto general, no será necesario

[52] El comité de protección de datos, es un organismo de la Unión con personalidad jurídica compuesto por presidente, que, a su vez encabezará el comité conformado por el director de una autoridad de control de cada Estado miembro y por el supervisor europeo de PD o sus representantes. (art.68 RGPD)

aplicar las disposiciones relativas a la EIPD, a menos que los Estados miembros consideren necesario proceder a dicha evaluación.
Finalmente, el responsable del tratamiento debe revisar la conformidad del tratamiento con la EIPD, especialmente cuando exista un cambio en el riesgo que representen las operaciones de tratamiento.

El artículo que le sigue (art. 36) regula la consulta previa a la autoridad de control, por parte del responsable, que *deberá facilitar información detallada, antes de proceder al procesamiento en aquellos supuestos en los que una evaluación de impacto relativa al PD muestre que el tratamiento entrañaría un alto riesgo si el responsable no tomase las medidas necesarias para mitigarlo*.
Si la autoridad detecta que el tratamiento puede infringir la normativa, particularmente cuando el responsable no haya identificado mitigado suficientemente el riesgo, *esta deberá asesorar por escrito al responsable o responsable del tratamiento, en un plazo máximo de ocho semanas desde la solicitud, prorrogable a seis en función de la complejidad del tratamiento previsto y, suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de consulta*. Se contempla que los estados garanticen que se consulte a la autoridad de control durante la elaboración de cualquier propuesta legislativa que haya de adoptar del Parlamento nacional, o de una medida reglamentaria en dicha medida legislativa (Mayor Gómez, R., 2016).

Como hemos visto en la LOPD y como veremos, también, en el breve análisis del reglamento 2018/1725, existe una figura central en esta ley que es el Delegado de Protección de Datos, normativizado en los artículos 37 a 39, que responde a las siglas anglosajonas DPO (o DPD) y cuyo nombramiento es obligatorio en los organismos públicos (exceptuando los tribunales en su actividad profesional) y entidades cuyas actividades principales impliquen la observación habitual y sistemática de interesados o tratamiento de categorías especiales de DP o datos relativos a condenas e infracciones penales a gran escala.
En el artículo 24 de la Ley 3/2018 se detallan los responsables y encargados que, en todo caso, han de proceder a la designación obligatoria (art. 37.1) de DPD, y una vez hecho, comunicarlo a la autoridad de control en el plazo de diez días y publicitar su existencia a través de medios electrónicos.

Esta figura debe ser designado en función de sus cualidades profesionales (art. 37.5), conocimientos en normativa de protección de datos, experiencia en la materia

y capacidad para desempeñar las funciones establecidas en el RGPD (art.39). Puede ser un empleado del responsable o del encargado del tratamiento, o actuar mediante un contrato de servicios. El responsable y el encargado del tratamiento están obligados a apoyar al DPO en el desempeño de sus funciones, garantizando su independencia (sin recibir instrucción de algún responsable o encargado de tratamiento y con obligación de secreto y confidencialidad) y respondiendo únicamente ante el nivel jerárquico más alto de la organización. Se prohíbe expresamente la destitución o sanción del DPO por el desempeño de sus funciones[53]. (Mañas, J. L. P. et al.,2016)

El DPO debe prestar atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta su naturaleza, alcance, contexto y fines. Está obligado a mantener la confidencialidad en el desempeño de sus funciones, de acuerdo con el Derecho de la Unión o de los Estados miembros. Puede desempeñar otras funciones siempre que no generen un conflicto de intereses.
Entre las funciones del DPO se incluyen el asesoramiento en materia de protección de datos, la supervisión del cumplimiento de la legislación y políticas de privacidad, la elaboración de informes de evaluación de impacto para ciertos tratamientos de datos personales y la cooperación con las autoridades de control nacionales (Mayor Gómez, R., 2016).

Capítulo V – Transferencias de datos personales a terceros países u organizaciones internacionales.

A continuación, de los artículos 44 a 50, se establecen las disposiciones relativas a las transferencias internacionales de datos, consideradas así como aquellas que implican una transmisión de datos personales fuera del territorio del Espacio Económico Europeo, bien por una cesión o comunicación de os datos o bien para la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

[53] La AEPD ha elaborado un esquema de certificación de delegados de protección de datos de la agencia española de protección de datos, que tiene por objeto establecer las condiciones y requisitos que conforman y regulan el funcionamiento del esquema de certificación de personas para la categoría DPD, en consonancia con la sección IV y V del Reglamento. Se puede acceder aquí: https://www.aepd.es/es/documento/esquema-aepd-dpd.pdf

Las recientes sentencias del Tribunal de Justicia de la Unión Europea[54] han tenido una incidencia significativa en la regulación de las transferencias internacionales de datos. Estas sentencias han marcado un punto de inflexión en cómo se realizan las transferencias de datos de empresas de la Unión Europea a EE.UU., y han establecido las obligaciones que tienen las autoridades de control europeas de atender las denuncias que pueda presentar un ciudadano respecto a un tratamiento de sus datos que implique una transferencia de datos a EE.UU (Mayor Gómez, R., 2016).

En este sentido, Gómez, declaraba en 2016 que teniendo en cuenta que tras la disolución del acuerdo *Safe Harbor*, se abrió un periodo de negociación en el marco del cual, la Comisión Europea y el Departamento de Comercio de EEUU, y, a partir de allí, han alcanzado un acuerdo que permitirá llevar a cabo transferencias internacionales de datos con garantías suficientes, a través del denominado acuerdo Privacy Shield, el cual, en 2021 fue declarado, por el Tribunal de justicia de la Unión Europea, como inválido para la realización de transferencias internacionales en su sentencia[55] que anula la decisión 2016/1250 de la Comisión.

El RGPD establece que, si los datos personales se transfieren de la Unión Europea a responsables, encargados u otros destinatarios en terceros países u organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión Europea. Esta protección debe mantenerse incluso en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional.

Para garantizar este nivel de protección, la Comisión tiene la responsabilidad de evaluar el nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país. En ausencia de una decisión de adecuación por parte de la Comisión, la transferencia de datos personales puede realizarse en casos especiales o cuando existan garantías apropiadas, como cláusulas tipo de protección de datos, normas corporativas vinculantes o cláusulas contractuales. Así pues, podemos afirmar que,

[54] Véase la Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 (petición de decisión prejudicial planteada por la *High Court* – Irlanda - Maximillian Schrems / *Data Protección Commissioner*), Asunto C-362/14.

[55] Se puede acceder a ella a través de este enlace:
https://curia.europa.eu/juris/documents.jsf?num=C-311/18

en ausencia de una decisión que constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado.

Capítulo VII – Cooperación y coherencia

A continuación, resaltaremos algunas de las introducciones llevadas a cabo por el RGPD en los artículo 60 y 67. En primer lugar, nos detenemos en la figura de la Ventanilla única o "One Stop Shop" que permite que los responsables del tratamiento de datos que estén establecidos en varios Estados miembros, o que realicen tratamientos que afecten significativamente a ciudadanos en varios Estados de la UE, tengan a una única autoridad de protección de datos como interlocutora, distinguiendo a la autoridad de control principal de la interesada. La primera autoridad de control del establecimiento principal será competente para actuar como autoridad de control para el tratamiento transfronterizo realizado por parte del responsable o encargado (art.56) (Mañas, J. L. P. et al., 2016)

Este sistema implica que cada autoridad de protección de datos europea, en lugar de analizar una denuncia o autorizar un tratamiento a nivel estrictamente nacional, deberá valorar si el supuesto tiene carácter transfronterizo. En caso afirmativo, se iniciará un procedimiento de cooperación entre todas las autoridades afectadas buscando una solución aceptable para todas ellas. Si existieran discrepancias insalvables, el caso puede elevarse al Comité Europeo de Protección de Datos para que resuelva la controversia mediante decisiones vinculantes para las autoridades implicadas.

No obstante, los interesados pueden continuar planteando sus reclamaciones o denuncias ante su propia autoridad nacional (en España, la Agencia Española de Protección de Datos - AEPD), sin perjuicio de que la gestión será realizada por esa autoridad, que será también responsable de informar al interesado del resultado final de su reclamación o denuncia. La Ventanilla Única no afectará a empresas que sólo estén en un Estado miembro y que realicen tratamientos que afecten sólo a interesados en ese Estado (Mayor Gómez, R., 2016).

En la sección tercera del séptimo capítulo se regula todo lo relativo al Comité europeo de Protección de Datos, un órgano independiente el cual tiene las funciones descritas del art. 70[56].

Capítulo VIII – Recursos, responsabilidad y sanciones.

Por último, los artículos 82 a 84 establecen que ualquier interesado que considere que sus derechos han sido infringidos puede otorgar un mandato a una entidad, organización o asociación sin fines de lucro para que presente una reclamación en su nombre ante la autoridad de control, ejerza el derecho a la tutela judicial en su nombre e incluso el derecho a recibir una indemnización, siempre que así lo disponga la legislación del Estado miembro.

El RGPD estipula que el responsable o el encargado del tratamiento deberá indemnizar cualquier daño o perjuicio que una persona pueda sufrir como resultado de una infracción del Reglamento (artículo 82.1 RGPD). Sin embargo, se eximirá de responsabilidad a dichos actores si pueden demostrar que no son responsables de los daños y perjuicios ocasionados (artículo 82.3 RGPD).
El régimen de sanciones se endurece[57] y se vuelve más riguroso que el anterior. Una de las novedades que introduce el RGPD en materia sancionadora es la posibilidad de imponer sanciones o multas administrativas que pueden llegar hasta los 20.000.000 de euros o, en el caso de una empresa, una cantidad equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía (artículo 83.5 RGPD) (Mayor Gómez, R., 2016).

[56] De las que destacamos:
1. Garantizar la aplicación coherente del RGPD.
2. Supervisar y garantizar la correcta aplicación del RGPD en casos específicos.
3. Asesorar a la Comisión sobre cualquier cuestión relacionada con la protección de datos personales en la Unión.
4. Emitir directrices, recomendaciones y buenas prácticas para promover la aplicación coherente del RGPD.
5. Fomentar la cooperación y el intercambio de información y buenas prácticas entre las autoridades de control.
6. Promover programas de formación comunes y facilitar intercambios de personal entre las autoridades de control.
7. Emitir opiniones sobre los códigos de conducta elaborados a nivel de la Unión.
8. Mantener un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

[57] *El artículo 45.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), las infracciones muy graves son sancionadas con multas de hasta 600.000 euros (Mayor Gómez, R., 2016)*.

Breve conclusión del RGPD

El RGPD ha supuesto un cambio de paradigma sustancial respecto a las novedades que presentas, como el hecho de homogeneizar jurídicamente este sector en todos los estados miembros de la Unión, cuestión que beneficia a consumidores y empresas, pues incluso estas últimas disponen de más facilidades gracias a la seguridad jurídica y el avance en cuestión de trasparencia del RGPD. Otra cuestión interesante del Reglamento es su eficacia en la protección en materia de PD, así como en la circulación de la información, que, gracias a su regulación, extiende su ámbito de aplicación fuera de las fronteras de la UE, siempre que se trate de datos de ciudadanos europeos.

Es particularmente visible, pero, la vocación de centralización europea del RGPD en la creación de, por ejemplo, el nuevo Comité Europeo de PD, que adquiere importante posición institucional en la garantía de los nuevos mecanismos europeos de coordinación efectiva de las autoridades nacionales de control el deber de asistencia mutua, las investigaciones conjuntas y el mecanismo de coherencia que constituye la auténtica cláusula de salvaguarda de la armonización. El Reglamento no se da por satisfecho con su aplicación directa sino que ha querido impedir divergencias nacionales en su aplicación imponiendo a las autoridades nacionales un mecanismo de coherencia destinado a garantizar en el caso concreto la efectiva aplicación uniforme del RGPD (Rallo Lombarte, A., 2019).

Peca, en ocasiones de excesivo tecnicismo y, en otros de abusar de los conceptos jurídicos indeterminados, que, de entre otras cosas, dificulta su comprensión estricta y puede generar problemas interpretativos en el futuro y gran discordancia en la opinión de la jurisprudencia en dos niveles, el nacional y el del EEE. Aun siendo una normativa sustancialmente superior a su antecesora lo cierto es que ya nació desfasada en algunos aspectos, como por ejemplo, las tecnologías actualmente operativas y de uso masivo que tiene incidencia directa en los DP, como son el *cloud computing, el bid data*, la internet de las cosas, el *BiTech* y los diferentes modelos de inteligencia artificial.

Es una ley que intenta blindarse frente a las grandes corporaciones, y en ese sentido lo han conseguido en gran medida, pues son estas las que, normalmente, implementan mejor estas cuestiones, sin embargo, cuando se trata de empresas

pequeñas y medianas, no es tan rigurosa, aun siendo estas muchas veces las que recaban una gran parte de los datos en tratamiento (Gómez, R. M., 2016)

Antes de la salida en 2016 del RGPD, la Ley de protección de datos española encuadraba dentro del consentimiento tácito la forma de registro del consentimiento, con la formulación europea se ha obligado a las empresas a ser capaces de demostrar el consentimiento del interesado, a nuestra forma de ver, aun no suficientemente auditables, por su poco peso material. De la misma, antes de la entra en vigor del Reglamento en España se sancionaban las empresas pero no existía un régimen indemnizatorio, con la adecuación al artículo 82 RGPD, esto ha cambiado.

5.8. Breve análisis del Reglamento 2018/1725

Cuando se promulgó este acto legislativo se dispuso que el Reglamento N.º 45/2001 fuera adaptado, por lo que este quedo derogado por el Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos. Este hecho perseguía armonizar las normas de protección de datos y adaptar el reglamento 45/2001 a los principios del Reglamento 2016/679, que dio como resultado el Reglamento 2018/1725 con el que se podía hacer una interpretación homogénea de toda la normativa europea. Este reglamento enfatiza la protección de las personas cuyos datos personales son tratados especialmente por instituciones y organismos de la UE, excluyendo la de personas fallecidas y personas jurídicas. Se destacan las reglas específicas para la protección de datos personales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, alineándose con lo establecido en la Directiva 2016/680.
Tiene en consideración el tratamiento de datos personales operativos de la Unión, considerándolos como *lex specialis* (*lex specialis derogat legi generali*) y tampoco se aplica a la Europol ni a la Fiscalía Europea.

Los principios de esta ley se aplican a toda información relativa a una persona identificada o identificable. Los datos personales seudomizados, que se podrían atribuir a una persona con información adicional, deben considerarse información sobre una persona física identificable, ya que deben tenerse en cuenta todos los medios (factores objetivos), como la singularización que razonablemente pueda

utilizar el responsable para identificar directa o indirectamente a una persona física. Por lo contrario, si la información no es identificable y no guarda relación con ninguna persona identificada o identificable (o datos convertido en anónimos) no tiene que aplicar los principios de protección de datos y, en consecuencia, no aplican en el reglamento.

> *Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.*

También explicita que el consentimiento debe ser un acto afirmativo claro e inequívoco que refleje la voluntad del interesado, que, además, puede ser revocado. Cuando los datos se recojan debe hacerse de forma trasparente y el interesado debe comprender que, sus datos, han sido recogidos y procesados y que, a su vez, estos deben ser pertinentes y limitados a lo necesario para los fines que se procesan y en su tramitación, por las instituciones y organismos encargados en la UE, deben ser verificado su ejercicio legítimo. Aquellos que gestionan esos datos, además, deben poder demostrar que esa información fue recogida de forma consentida y la persona interesada debe poder identificar a quien gestiona dicha información, asimismo, el consentimiento debe ser libre habiendo gozado el interesado de la capacidad de denegarlo o revocarlo sin prejuicio alguno.

Para evitar el riesgo de elusión, el trato es indiferentes para el tratamiento automatizado de datos como para del tratamiento manual, cuando dichos datos se encuentren en ficheros. Ahora bien, para discernir a cerca de la licitud de operaciones de tratamiento ulterior, siempre que estos sean con fines de interés público, fines de investigación científica e histórica u otros fines estadísticos deben considerarse como operaciones de tratamiento lícito supeditados a garantías adecuadas para los derechos del interesado.

Como no podía ser de otra manera, se les reconoce a los niños una protección especial de sus datos personales, especialmente cuando se recopilan perfiles de personalidad y datos para ofrecer servicios directamente a menores en webs institucionales y organismos de la UE, como servicios de comunicación interpersonal

o venta online de entradas, que, en todo caso, deberán demostrar que la transmisión de estos datos es necesaria para el ejercicio de sus funciones o tiene valor público.

También se protege con especial énfasis aquellos datos que, por su naturaleza sensible podrían entrañar riesgos para los derechos y libertades fundamentales, que no deben, por lo general, ser recogidos, salvo casos especiales definidas en el reglamento, como en el ámbito sanitario en beneficio siempre de las personas físicas y la sociedad en conjunto.

Al regirse por los principios de tratamiento leal y transparente se exige que el interesado sea informado del tratamiento de sus datos, así como facilitar información de la operación y acceso a los datos con el fin de conocer y verificar la licitud, así como aplicar el derecho al olvido si la retención de tales datos infringe el reglamento y derecho de la Unión. El derecho a la supresión debe, además, ampliarse a todos sus efectos de tal modo que le responsable que haya hecho público los datos este obligado a indicar a los responsables del tratamiento todos los espacios donde reside la información y, en consecuencia, suprimir enlaces, copias y réplicas de los datos.

Uno de los mecanismos que se contempla en el Reglamento 2018/1725 para *trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, impedir el acceso de usuarios a esos datos o retirar temporalmente los datos publicados en internet.* En cuanto a aquellos ficheros con funcionamiento automático la limitación al *tratamiento debe realizarse por medios técnicos de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni pueden ser modificados*, permitiendo a los interesados recibir sus datos de una forma estructurada, de uso común, de lectura mecánica e interoperable y que permitan la portabilidad, y transmitirlos a otro responsable de tratamiento sin menoscabar el derecho de supresión o conservación de datos que el interesado haya aportado y sean necesarios para el cumplimiento de un contrato.

Pese que exista un interés público o se esté llevando a cabo el ejercicio de potestades públicas conferidas al responsable del tratamiento, el interesado siempre tendrá derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular, es el responsable quien debe demostrar que seis intereses legítimos imperiosos prevalecen sobre lo s intereses o los derechos del interesado.

El interesado debe tener derecho a nos ser objeto de tratamiento automatizados produzcan efectos jurídicos significativos, como por ejemplo los *servicios de contratación en red en los que no medie intervención humana alguna*, esto incluye la elaboración de perfiles *que evalúe aspectos personales relativos a una persona física, en particular, para analizar o predecir aspectos relacionados con el rendimiento de trabajo*, *situación económica, salud, preferencias o intereses personales, fiabilidad o comportamientos, situación o movimientos (en la medida en la que produzca efectos jurídicos o le afecte de forma significativa),* siempre que no tenga una autorización expresa del derecho de la Unión, siempre *sujeto a las garantías apropiadas, entre lo que se debe incluir la información específica del interesado y el derecho a obtener intervención humana, a expresar su punto de vista, recibir una explicación de la decisión tomada tras la evaluación e impugnarla si es necesario*. La medida no puede afectar a un menor.

El reglamento exige que el responsable de tratamiento debe asegurarse que se utilizan los procedimientos matemáticos y estadísticos necesarios para minimizar el error y se aseguren los datos personales de forma que se reduzcan los riesgos de, entre otras cosas, efectos discriminatorios.

Es preciso señalar que:

> los actos jurídicos adoptados con arreglo a los tratados o a las normas internas adoptadas por instituciones y organismos de la UE, en cuestiones relacionadas con su funcionamiento pueden imponer limitaciones a determinados principios y a los derechos de información, acceso, rectificación o supresión, portabilidad, confidencialidad, comunicación por violación de seguridad y determinadas obligaciones conexa, en la medida en la que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública y la prevención, investigación, enjuiciamiento y ejecución de procesos penales, incluyéndose catástrofes naturales o de origen humano, seguridad interna de las institución es y organismos de la UE y otros objetivos de interés público.

El responsable debe aplicar las medidas oportunas y eficaces, y poder demostrar la conformidad de las actividades e tratamiento del Reglamento, teniendo en cuenta su contexto y los fines de la recogida de datos ya que los riesgos[58] para los derechos y

[58] Algunos ejemplos de riesgos contemplados en el considerando 46 de la ley 2018/1725 son los siguientes, a saber: *en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la*

libertades de las personas físicas en este ámbito pueden magnificarse con bastante celeridad. La probabilidad y gravedad de riesgo debe determinarse con referencia a su naturaleza, alcance, contexto y según los fines del tratamiento, que se ponderará sobre la base de la evaluación objetiva mediante la que se determinará si las operaciones suponen un riesgo. Para proteger a las personas físicas se *exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar le cumplimiento de los requisitos* reglamentarios. *A fin de poder demostrar la conformidad el responsable debe adoptar políticas internas y aplicar medidas que cumplan con los principios de protección de datos, que podrán consistir, por ejemplo, en reducir al máximo el tratamiento de datos personales*, seudomizar con brevedad los datos, dar trasparencia en sus funciones, *permitiendo a los interesados supervisar el tratamiento de sus datos y al responsable del tratamiento crear y mejorar elementos de seguridad*. Por la protección del Dcho. PD como por la responsabilidad de los que tratan los datos, se requiere, desde la normativa, que demuestren el cumplimiento mediante la adhesión a mecanismos de certificación aprobados y requieren también una atribución clara de las responsabilidades de los responsables.

Cuando un responsable encomiende a un encargado actividades de tratamiento debe asegurarse que este último tenga los conocimientos especializados suficientes para ofrecer garantías y fiabilidad en la aplicación de medidas técnicas y organizativas que cumplan los requisitos, incluido la seguridad. Alguna de las maneras que propone el reglamento, en una suerte de sujeción a una *lex artis ad hoc*, para garantizar la diligencia debida, es la adhesión a códigos de conducta aprobados o a mecanismos de certificación aceptados. Sin embargo, teniendo en cuenta el riesgo que supone la gestión de los datos, si el tratamiento se da por un encargado distinto de las instituciones y organismos de la UE deberá fijarse un contrato (a optar entre un contrato individual o cláusulas contractuales tipo

---

seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

adoptadas por la comisión o por el Supervisor Europeo de Protección de Datos[59] (SEPD) y, a posteriori, la comisión) que vincule jurídicamente al encargado con el responsable, donde se fije: naturaleza, fines de tratamiento, objeto, duración y tipo de información a gestionar.

El responsable mantendrá un registro de las actividades de tratamiento bajo su responsabilidad al igual que las categorías de actividades. Las instituciones y organismos de la Unión colaborarán con el Supervisor Europeo de Protección de Datos para proporcionarle dichos registros en calidad de supervisor. En caso de una violación de seguridad de los datos que pudiera entrañar riesgos para las personas físicas, sin dilación indebida y a más tardar 72 horas tras el incidente se deberá notificar al Supervisor Europeo a menos que el responsable pueda demostrar, bajo el principio de responsabilidad proactiva, de la remota improbidad de que la violación suponga riesgos para las personas físicas.
A su vez, el responsable comunicará sin dilación la naturaleza de la violación y las recomendaciones para que la persona física mitigue los efectos adversos potenciales resultantes.

Si una operación de tratamiento de datos implica un alto riesgo se deben establecer mecanismos eficaces para monitorizar estas operaciones, que deben preceder siempre una evaluación del impacto, especialmente cuando se trata de nuevas tecnologías u operaciones de tratamiento inéditas. SI en la evaluación de impacto se revela un alto riesgo que no pueda ser mitigado con medidas razonables el SEPD debe ser consultado previo al inicio de la actividad, su falta de respuesta no impide su posterior intervención dentro de las funciones y poderes que le confiere el reglamento.

[59] Establecido por el Reglamento (CE) nº 45/2001. La función principal del Supervisor Europeo es garantizar que, en el tratamiento de datos personales, las Instituciones y organismos de la UE respeten el derecho de protección de datos de los ciudadanos. En este sentido el SEPD supervisa *el tratamiento, asesora a las instituciones, se ocupa de las reclamaciones, realiza investigaciones, colabora con las autoridades naciones de los países miembros y, además, hace un seguimiento de las nuevas tecnologías para evaluar su incidencia en el campo de la autodeterminación informativa. Si una persona considera que ha sufrido una violación de sus derechos en este campo, hasta llegar al supervisor deberá pasar por los miembros del personal de la UE responsables (Banco Central, Tribunal de cuentas, Comités, Agencias, etc.) Si no se queda satisfecho se puede recurrir al Responsable de la protección de datos, un delegado designado por el propio SEPD, que a su vez colabora con otros delegados que son escogidos en cada uno de los organismos e instituciones de la UE. Si tampoco se soluciona, el interesado puede acudir, tras consumir las vías previas, al SEPD a través de un formulario para que este inicie una investigación e informe de su resultado. En última instancia, si tampoco se ha solucionado la cuestión, el interesado podrá llevar el asunto al Tribunal de Justicia de la UE.*
El supervisor es designado para un mandato renovable de cinco años. Actualmente Wojciech Wiewiórowski ocupa la función de SEPD. (*Supervisor Europeo De Protección De Datos (SEPD)* | *Unión Europea*, n.d.)

El Comité Europeo de Protección de Datos, como ya hemos mencionado, se establece por el Reglamento (UE) 2016/679 y tiene como objetivo la aplicación coherente de la normativa de protección de datos en toda la Unión. La Comisión debe esforzarse por consultar tanto al Supervisor Europeo de Protección de Datos como al Comité Europeo de Protección de Datos para asegurar la coherencia en la protección de los derechos y libertades de las personas físicas, de todas formas, el Delegado de Protección de Datos debe garantizar constantemente que se está aplicando el reglamento correctamente y, a su vez, asesorar a los responsables en el cumplimiento de sus obligaciones.

En cuanto a las transferencias a terceros países y organizaciones internaciones solo pueden llevarse a cabo en plena conformidad con el presente Reglamento y respetando los derechos y libertades fundamentales de la Carta.
En este sentido, la Comisión puede decidir, con arreglo al art. 45 del Reglamento 2016/679 o al art. 36 de la Directiva 2016/680, que en un tercer país, territorio, sector específico o organización internacional ofrece un nivel de protección de datos adecuados. En ausencia de esta decisión el responsable debe tomar las medidas para compensar la falta de protección que pueden consistir en el recurso de cláusulas tipo de protección adoptadas por la comisión o por el SEPD o cláusulas contractuales autorizadas por este último.

Si la transferencia a un tercer país o análogo es necesaria en aras al cumplimiento de un contrato o reclamación y que sea de forma ocasional puede mediar el consentimiento explícito del interesado, independientemente de tratarse de un procedimiento judicial, administrativo o extrajudicial, incluidos los relativos a procedimientos reguladores. También se admiten transferencias en beneficio del interés público o ya previstas por el derecho de la unión, como por ejemplo *transferencias entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, autoridades de supervisión financiera y servicios competentes en materia de seguridad social o sanidad público*. También es lícita cuando se trata de proteger el *interés esencial para los intereses vitales de la persona física, si el interesado no esta en condiciones de dar su consentimiento*.

Es posible que las autoridades competentes de control nacional y el SEPD aprecien una imposibilidad a la hora *de tramitar reclamaciones o realizar investigaciones en actividades desarrolladas fuera de su jurisdicción*, así como en la colaboración

transfronteriza en lo que respecta a las potestades preventivas o correctivas. En consecuencia, es de imperiosa necesidad fomentar la cooperación del SEPD con las autoridades de control nacionales para contribuir el intercambio de información con sus homólogos internacionales.

Toda persona que sufra perjuicios materiales o inmateriales derivados de una infracción del presente reglamento tiene derecho a recibir del responsable una indemnización por dichos daños, por ello mismo, para fortalecer la función supervisora el SEPD está dotado de facultades sancionadoras para imponer multas administrativas, que evitan ser personalísimas y estar dirigidas, principalmente, a las instituciones u organismos de la UE por tal de impedir futuras violaciones y fomentar la cultura del Dcho. PD. El procedimiento administrativo sancionador debe regirse por los principios generales de esta jurisdicción siguiendo la interpretación del Tribunal de justicia.

6. Política de cookies[60]

Antes que nada, las cookies, así como otras tecnologías como los *local shared objects* (flash cookies), son herramientas empleadas por los servidores web para almacenar y recuperar información acerca de sus visitantes, así como ofrecer un correcto funcionamiento del sitio (Ferrer, J., 2022).

Aunque el considerando 30 del RGPD menciona que las personas físicas pueden ser asociadas a identificadores en línea y de sesión (es decir, cookies), al contrario de lo que podríamos pensar, las políticas de cookies no provienen del Reglamento General de Protección de datos, sino de la Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), incorporada a nuestro ordenamiento por trasposición de la Directiva 2000/31/CE del Consejo y del Parlamento Europeo donde se regulan algunas cuestiones de los servicios de la sociedad de la información, especialmente aquellos relativos al comercio electrónico. Importante recalcar que, como se señala en el preámbulo V (*in fine*) Real Decreto-ley 13/2012, este decreto modifica diversos artículos de la ley 34/2002 a fin de adecuar su régimen a la nueva redacción dada por la Directiva 2009/136/CE y la Directiva 2002/58/CE, debiéndose destacar la nueva redacción que se da al artículo 22.2, para:

> exigir el consentimiento del usuario sobre los archivos o programas informáticos (como las cookies) que almacenan información en el equipo usuario y permite que se acceda a ésta; dispositivos que puedan facilitar la navegación por la red pero con cuyo uso pueden desvelarse aspectos de la esfera privada de los usuarios, por lo que es importante la información de los usuarios y que dispongan de mecanismos que les permitan preservar su privacidad.

De la misma manera, el artículo 22 sufrió modificaciones con la entrada en vigor de la nueva ley general de telecomunicaciones con motivo del cumplimiento de su disposición final segunda. Aunque, esta ley está destinada a ser derogada en sustitución de una nueva que abarque los conceptos de la sociedad de la información de forma mucho más transversal, hasta entonces, el artículo 22, así como otros, deberán seguir actualizándose, pues la última actualización es del 2014 y remitiéndose a la Ley Orgánica 15/1999 LOPD.

[60] Para saber más sobre funciones criptográficas y seguridad web ver Anexo III, página 114.

El artículo 22 de la ley 34/2002 trata el derecho de los destinatarios de servicios, los cuales podrán *revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente* (22.1). Para ello;

> *los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Si las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir en la inclusión de una dirección de correo válida donde pueda ejercitarse este derecho, quedando prohibido enviar comunicaciones sin ello indicado* (22.1).

Y es, en este punto del artículo, donde se habla propiamente de lo que conocemos en la cultura popular como *cookies*. El 22.2 empieza diciendo:

> Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se le haya facilitado información clara y completa de su utilización, en particular, sobre los fines de tratamiento de los datos, con arreglo a la Ley/1999 LOPD.

Lo que se traduce en que, generalmente, las empresas que desarrollan y gestionan las páginas web, mediante el uso de esta tecnología permiten al servidor recordar algunos datos concernientes al usuario, como por ejemplo sus preferencias, el nombre de usuario o la contraseña, así como productos que le interesen o el navegador que esta utilizando, etc. con varias finalidades, una de ellas es quela navegación sea más sencilla (como cuando se mantiene la sesión abierta o la página recuerda que ya se ha registrado), pero también con fines puramente mercantilistas y de experiencia como consumidor, como la promoción de diferentes servicios y promociones en función de tu comportamiento online. La función más indirecta, desde la perspectiva del usuario, pero muy importante para los gestores web es la función estadística, que, con las cookies, pueden medir con bastante exactitud cuestiones como el tráfico, el control del progreso y número de, por ejemplo, entradas online (Ferrer, 2022).

Este mismo artículo sigue diciendo que:

> Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento podrá facilitarse mediante el uso de los paramentos adecuados del

navegador y otras aplicaciones, cosa la cual no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida en la que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

No podemos continuar sin advertir a los lectores del porvenir: la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). En su exposición de motivos, en el punto 3.5 nos explica que esta propuesta incluye una clarificación y simplificación de la norma relativa al consentimiento para el uso de cookies y otros identificadores. En el considerando 17 habla sobre la pertinencia y necesidad de los identificadores, siendo estos necesarios para cuestiones como el control del tráfico (ya que un identificador puede interconectar la posición relativa de las personas físicas), cuestión útil desde los ojos de las autoridades públicas u operadores de transporte.

En el considerando 20, a colación del uso de los terminales de los usuarios finales y su utilización, habla de los denominados programa espía, balizas web, identificadores ocultos, cookies de rastreo y otros dispositivos similares de seguimiento no deseados que podrían llegar a introducirse en el equipo terminar del usuario final sin su consentimiento para acceder a datos, archivar información oculta, rastrear actividades. Cuestión que debe estar protegida por la Carta de los Derechos fundamentales de la UE, pues estamos hablando de dispositivos que contienen tal cantidad de información relativa a la esfera más privada que la intromisión ilegítima puede provocar consecuencias insalvables.
En el considerando 25, finalmente, se dice *que el acceso a las redes de comunicaciones electrónicas requiere la emisión periódica de determinados paquetes de datos a fin de descubrir o mantener una conexión con la red u otros dispositivos en la red.* Además a *los dispositivos se les debe asignar una dirección única para que sean identificables*. De igual forma, las normas de telefonía inalámbrica y móvil comportan la emisión de señales activas que contienen identificadores únicos tales como una dirección MAC, IMEI[61], IMSI, etc.

[61] Identidad internacional de estación móvil

En cuanto al programa de Adecuación y Eficacia de la reglamentación de la Comisión Europea (REFIT), el cual tiene por objetivo garantizar que la legislación de la UE cumpla sus objetivos con un coste mínimo de beneficio de los ciudadanos y las empresas (Comisión Europea, s.f.), se tiene en consideración la conclusión a la que llega, donde explican que la Directiva no ha alcanzado plenamente sus objetivos pues su redacción es muy imprecisa en determinadas disposiciones y la ambigüedad de los conceptos jurídicos han puesto en peligro en peligro la armonización. También se pone de manifiesto que algunas disposiciones han impuesto una carga innecesaria, así como la norma relativa al consentimiento, destinada a proteger la confidencialidad de los equipoc terminales, no ha logrado alcanzar sus objetivos por cuanto los usuarios finales pueden acceder a que se les instalen cookies de rastreo sin comprendes lo que ello significa y, en algunos casos, se ven incluso expuestos a cookies instaladas sin su consentimiento.

Otra cuestión tratada en el proyecto fue la consulta pública efectuada por la Comisión con las partes interesadas el 25 de abril y el 5 de julio, y, en relación con lo que nos interesa, se apoyó las soluciones propuestas para la cuestión del consentimiento del uso de cookies siendo estos los resultados exactos:

> el 81,2 % de los ciudadanos y el 63 % de las administraciones públicas abogan por que se imponga a los fabricantes de equipos terminales la obligación de comercializar productos con las opciones de privacidad predeterminadas activadas, mientras que el 58,3 % del sector opta por respaldar la autorregulación o la corregulación.

Así mismo, en la evaluación de impacto, se aboga por la centralización del consentimiento en programas o aplicaciones tales como los navegadores de Internet, incitando a los usuarios a elegir configuración de privacidad y ampliar las excepciones a la norma de consentimiento del uso de las cookies, lo que puede conllevar, por ejemplo, que los anunciantes de publicidad personalizada en línea les puede resultar más difícil obtener el consentimiento si una gran proporción de usuario opta por rechazar las cookies de terceros.

De esta forma se concluía en el 3.5 que debía depararse una protección más eficaz a los ciudadanos contra la publicidad no solicitada añadiendo excepciones a la norma del consentimiento respecto a cookies, además, clarificando y simplificando la norma relativa al consentimiento.

Las cookies pueden ser un instrumento legítimo y útil, pero, habida cuenta la utilización generalizada de las cookies de rastreo y otras técnicas de seguimiento, a los usuarios finales se les pide cada vez más que den su consentimiento para almacenar dichas cookies en sus equipos terminales y, en consecuencia, se ha extendido un agobio relativo a las solicitudes de consentimiento que puede solucionarse estableciendo parámetros transparentes y sencillos.

Una cuestión determinante para las cookies es la que regula el artículo 25 del RGPD, donde se establece los principios de protección de datos desde el diseño por defecto, los cuales deben ser diseñados para proteger los datos personas y las configuraciones predeterminadas deben ser las que ofrezcan mayor protección, es decir, cuando se destacan en la mayoría de los navegadores de forma predeterminada, única y exclusivamente la opción de “acotar todas las cookies” están contraviniendo el Reglamento pues la opción menos lesiva y que más protección tiene es siempre la casilla de “aceptar solo cookies esenciales”. Los proveedores de software deben configurar sus programas para permitir que los usuarios rechacen cookies de tercero haciéndolo siempre con opciones claras e inteligibles, pero, además, debe destacar sino lo mismo, más que la opción de aceptar todas. Los usuarios deben tener la posibilidad de seleccionar desde el nivel de privacidad más alto, que sería "no aceptar nunca cookies", hasta el más bajo, "aceptar siempre cookies", y niveles intermedios. Además, la información proporcionada debe explicar los posibles riesgos de permitir el almacenamiento de cookies de terceros, incluyendo la conservación de registros de historiales de navegación a largo plazo y el uso de esta información para enviar publicidad personalizada.

Por último, mencionaremos los tipos de cookies más relevantes agrupados en cinco grandes grupos: en primer lugar están las cookies analíticas las cuales recogen información del uso que se realiza en la web; las cookies sociales, necesarias para redes sociales externas; cookies de afiliados, que permiten hacer un seguimiento de las vivitas procedentes de otras webs, con las que tienen contrato de afiliación; las cookies de publicidad y comportamentales, que recogen preferencias y elecciones personales; y las cookies técnicas y funcionales que son, estrictamente, las necesarias para el uso del sitio web y la prestación del servicio (Ferrer, J., 2022).

7. Conclusiones

El inexorable avance de las tecnologías (y el acceso a ellas) ha desencadenado la progresiva necesidad de proteger a las personas físicas de ver vulnerado su derecho a la intimidad y autodeterminación informativa. El uso impropio de los sistemas de recogida de datos ha puesto en riesgo el ejercicio de un derecho fundamental y la racional ocupación de los medios informáticos.

La transferencia internacional de información es una realidad, así como la recopilación de datos por parte de entes públicos y privados. En el enfrentamiento perpetuo del principio de disponibilidad, especialmente en la Unión Europea, y los principios de tratamiento leal y transparente, así como los principios análogos a la protección de datos, supone la necesidad de regular con todos los medios disponibles el territorio europeo y, de ser posible, internacional (Gacitúa Espósito, 2014).

Los retos que propone el *right of privacy* exceden las fronteras físicas y políticas instalándose como un problema global en un mundo interdependiente y vinculado esencialmente al desarrollo tecnológico y los instrumentos jurídicos sin fuerza vinculante solo son una referencia, y de allí emana la urgente necesidad de crear textos legislativos con, cada vez, más interés por globalizarse.

El Reglamento General de Protección de Datos a supuesto un importante avance respecto a la Directiva 95/46/CE, gracias también a su prolongada gestación que, sin embargo, ha resultado ser un arma de doble filo en un mundo donde la curva de progreso es cada vez más pronunciada. La puesta en vigor en el año 2016 conllevó poner en término una norma que, desde su día de salida, estaba ciertamente desfasada. En un mundo de estas características la ley debe procurar predecir las diferentes dificultades que puedan confrontar la seguridad jurídica y, aunque en cierta medida, el RGPD prevé de manera relativamente abstracta la probabilidad de que el tratamiento contenga riesgos para los derechos y libertades (art. 24, 25, 30, 32, 33, 34, etc.) derivado, principalmente, de tecnologías incipientes, como el art. 35 RGPD, no coarta verdaderamente la empleabilidad de muchas técnicas informáticas.

El consentimiento es la piedra angular bajo la cual orbitan, en su gran mayoría de veces, el articulado del Reglamento europeo y la ley orgánica y, por ese motivo, es imperativo su blindaje, anulando la probabilidad de la elusión conceptual. Un ejemplo

para ilustrarlo lo hallamos en el 7.3 RGPD in fine, donde alude a la máxima siguiente: El interesado podrá retirar su consentimiento en cualquier momento y retirarlo será tan fácil como darlo.
Tras más de un lustro desde la entrada en vigor del RGPD podemos afirmar que esto es rotundamente falso. Ni siquiera en las grandes corporaciones tecnológicas han sabido aplicar este artículo con la rigurosidad necesaria como para garantizar la intencionalidad preventiva del mismo.

Otra consideración, traída de la mano de la Agencia Española de Protección de Datos, en relación con el artículo 8 del Reglamento y su homónimo artículo 7 de la LOPD, es la consideración de que los menores de edad, pero mayores de catorce años, se les considera con las aptitudes propias de la madurez para consentir por sí mismos el tratamiento automatizado de sus datos de carácter personal. Deducción, que como ya hemos adelantado antes, se fundamenta en la resolución tercera de la Dirección General de Registros del 89 y en cuestiones específicas del Derecho Civil, aterrizando en un *reductio ad absurdum* con delirios pragmáticos y tropezar en la, esperemos, involuntariamente en la *falacia ad populum*,

En cuanto a la imposición de multas administrativas (art. 83.4 y 5), parece ser un buen avance respecto a la Directiva, así como el acceso a indemnización y responsabilidad, como también las acciones de repetición del 82.5. Empero, a nivel nacional, el art. 78, cuenta con plazos de prescripción excesivamente cortos, aun teniendo la posibilidad de interrumpirse por iniciación, dando expectativas evasoras.

Otro gran problema, que evoca irremediablemente a la inseguridad jurídica son los conceptos indeterminados presentes en el RGPD, que no tan solo son gravantes para los interesados por la elusión jurídica a la que puede desembocar, sino que permiten el excesivo relativismo normativo. Ejemplo de ello es el art. 91, que acota parcialmente el concepto al decir que las operaciones de tratamiento a gran escala persiguen tratar una “cantidad considerable de datos personales” a nivel regional, nacional o supranacional que podrían afectar a un gran número de interesados, donde incluso el Grupo de trabajo del artículo 29 se adelantaron estableciendo criterios orientativos y, a pesar de ello, el RGPD no define que se entiende por tratamiento a gran escala, cuestión que el propio grupo a calificado como indeterminable[62] (Ribas, X., 2021). En España sucede algo parecido con el art. 34,

[62] Algunos de los criterios presentados por el grupo de trabajo: El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente; el

que carece de rigor jurídico, optando por obligar a 17 entidades, sin filtro alguno, a designar un delegado de protección de datos. Johannes Caspar, responsable de protección de datos en Hamburgo, ha denunciado en Bloomberg algunos fracasos del RGPD, de su crítica ratificamos hechos como que la Comisión de protección de Datos Irlandesa, burlando el RGPD, se ha convertido en el principal dique de contención (Aguiar, A. R., 2021), como el caso de Meta con Facebook, caso en el que se estima una emigración de 1.500 millones de cuentas de usuario cambiando, simplemente, los términos y condiciones de uso (B.T, El Mundo, 2018), número que se suma a los 500 millones de usuarios filtrados en una brecha de seguridad en la misma compañía en la que Europa no ha tenido competencias y ha presionado desde la Comisión. Otra critica es la inoperatividad del Comité Europeo de Protección de Datos del art. 68 RGPD, donde Caspar nos recuerda la dificultad que representa que 30 autoridades lleguen a un consenso (Aguiar, A. R. 2021).

Finalmente, vemos necesario la previsión normativa del reglamento en tres cuestiones primarias. En primer lugar, entender la cesión de consentimiento desde la comprensión de que el uso de los servicios en el ámbito informático es infinitamente fluido y fugaz, tanto que, en cuestión de minutos, puedes haber hecho uso, casi accidentalmente, de decenas de servicios que han comportado el consentimiento de uso de datos y cookies. Ante esta realidad, la baliza a la que debemos dirigirnos es a la máxima protección de datos de forma estandarizada, debiendo cederlos intencionalmente aquellos que no son estrictamente necesarios para el uso del servicio. En segundo lugar, acotar la inteligencia artificial, en primer lugar, reconociéndola como una plausible tratante de datos y, en segundo, limitando su uso, advirtiendo a las autoridades pertinentes, y adhiriéndose a modelos que presenten, imperativamente, homologaciones de seguridad y, en tercer y último lugar, el Big Data al que se asocia con el riesgo de la predictibilidad preventiva lo que implica el establecimiento de patrones de conducta que permiten catalogar a las personas de forma cada vez más eficaz, lo que puede conducir a la discriminación y a la toma de decisiones preventivas basadas en predicciones (Martínez, R. 2017).

volumen de datos o la variedad de elementos de datos que son objeto de tratamiento; la duración, o permanencia, de la actividad de tratamiento de datos y ell alcance geográfico de la actividad de tratamiento (Ribas, 2021).

8. Bibliografía

8.1. Jurisprudencia

- STEDH-12, 4451/70 CASO GOLDER de 21 de febrero de 1975.

- STEDH. Caso Klass y otros. Sentencia de 6 de septiembre de 1978. Recuperado del archivo de la Universidad de Navarra. https://revistas.unav.edu/index.php/persona-y-derecho/article/view/34198

- STEDH 10581/83. CASO NORRIS CONTRA IRLANDA Artículo 8 (La condición de víctima y la injerencia en la vida privada para la protección de la moral) Sentencia de 26 de octubre de 1988.

- STEDH 8691/79. Caso Malone. Sentencia de 2 de agosto de 1984. Registro policial de conversaciones telefónicas (Arts. 8 y 13 del Convenio Europeo) https://hudoc.echr.coe.int/eng?i=001-165112

- . TEDH 12433/86. Caso Lüdi. Sentencia de 15 de junio de 1992.

- STEDH 16798/90. CASE OF LÓPEZ OSTRA v. SPAIN. The European Court of Human Rights. Sentencia de 9 de diciembre de 1994. https://hudoc.echr.coe.int/eng?i=001-57905

- STJUE (Sala Sexta) de 11 de enero de 2001. Asunto C-403/98, caso Azienda Agricola Monte Arcosu Srl.

- STJUE (6 de noviembre de 2003) asunto C-101/01, caso Bodil Lindqvist. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2003%3A596

- STJUE (2014, mayo 13). Asunto C-131/12. Caso Google y AEPD. https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

- STJUE (2015, 6 octubre). Asunto C-362/14. Caso Maximillian Schrems y Data Protection Commissioner. A petición de decisión perjudicial planteada por la High Court (Irlanda). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62014CJ0362b

- Tribunal Constitucional. Sala Primera. Sentencia número 110/1984, de 26 de noviembre. Recurso de amparo número 575/1983.

- Tribunal Constitucional. Sección Cuarta. Auto 642/1986, de 23 de julio de 1986. Recurso de amparo 1.135/1985. Acordando la inadmisión a trámite del recurso de amparo 1.135/1985.

- Tribunal Constitucional. Sala Segunda. Sentencia 231/1988, de 2 de diciembre. Recurso de amparo 1.247/1986. https://www.boe.es/buscar/doc.php?id=BOE-T-1988-29203

- Tribunal Constitucional. Sala Primera. Sentencia 37/1989, de 15 de febrero, recurso de amparo seguido con el núm. 235/87.

- Tribunal constitucional. Sala Primera. Sentencia nº 254/1993, de 20 de julio. Sala primera, Recurso de amparo 1827-1990.

- Tribunal Constitucional. Sala Primera. Sentencia 7/1994, de 17 de enero de 1994. Recurso de amparo 1407/1992.

- Tribunal Constitucional. Sala Segunda. Sentencia 117/1994, de 25 de abril de 1994. Recurso de amparo 2.016/1990.

- Tribunal Constitucional. Sentencia 127/1994, de 5 de mayo de 1994. Pleno. Recursos de inconstitucionalidad 1363-1988, 1364-1988, 1412-1988, 1430-1988 (acumulados).

- Tribunal Constitucional. Sala Primera. Sentencia 143/1994, de 9 de mayo. Recurso de amparo núm. 3.192/92.

- Tribunal Constitucional. Sala Segunda, Sentencia 175/1997, de 27 de noviembre de 1997.

- Tribunal Constitucional. Sala Segunda. STC 151/1997, 29 de septiembre. ponente Don carles Viver i Pi-Sunyer. https://www.congreso.es/constitucion/ficheros/sentencias/stc_151_1997.pd

- Tribunal Constitucional. Sala Segunda. Sentencia 94/1998, de 4 de mayo. recurso de amparo núm. 840/95.

- Tribunal Constitucional. Pleno. Sentencia 49/1999, de 5 de abril, recursos de amparo acumulados núms. 195/95, 254/95, 255/95, 256/95, 257/95 y 260/95, avocados al Pleno.

- Tribunal Constitucional. Sala Segunda. Sentencia 94/1998, de 4 de mayo. recurso de amparo núm. 840/95.

- Tribunal Constitucional. Sala Segunda. Sentencia 95/1999, de 31 de mayo de 1999. Recurso de amparo 1.167/1999.

- Tribunal Constitucional. Sala Primera. Sentencia 134/1999, de 15 de julio de 1999. Recurso de amparo 209/1996.

- Tribunal Constitucional. Sala Primera. Sentencia 166/1999, de 27 de septiembre, recursos de amparo acumulados núms. 3.918/95 y 3.948/95.

- Tribunal Constitucional. Sala Segunda. Sentencia 171/1999, de 27 de septiembre, recurso de amparo núm. 3.759/96.

- Tribunal Constitucional. Sala Primera. Sentencia 98/2000, de 10 de abril de 2000. Recurso de amparo 4.015/96.

- Tribunal Constitucional. Sala Segunda. Sentencia 115/2000, de 10 de mayo de 2000. Recurso de amparo 640/97.

- Tribunal Constitucional. Sala Primera. Sentencia 186/2000, de 10 de julio. Recurso de amparo 2.662/1997.

- Tribunal Constitucional. Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000.

- Tribunal Constitucional. Sala Segunda. Sentencia 299/2000, de 11 de diciembre, recurso de amparo núm. 3290/97.

- Tribunal Constitucional. Sala Segunda. Sentencia 14/2001, de 29 de enero, recurso de amparo núm. 873/97.

- Tribunal Constitucional. Sala Segunda. Sentencia 138/2001, de 18 de junio (BOE núm. 170, de 17 de julio de 2001), Recurso de amparo núm. 2855/97.

- Tribunal Constitucional. Sala Primera. Sentencia 83/2002, de 22 de abril de 2002. Recurso de amparo 182/98

- Tribunal Constitucional. Sala primera. Sentencia 196/2004, de 21 diciembre 2004. Recurso de amparo núm. 1322-2000.

- Tribunal Supremo. Sentencia 569/2013, 26 de junio de 2013. Ponente Perfecto Agustín Andrés Ibáñez

- Tribunal Supremo (15 de octubre de 2015). Sentencia nº. 545/2015. Sala 1ª. rec. 2772/2013, (Pte: Sarazá Jimena, Rafael).

8.2. Ley

Derecho Internacional

- Pacto Internacional de Derechos Civiles y Políticos del 19 de diciembre de 1966 de Nueva York. https://www.boe.es/buscar/doc.php?id=BOE-A-1977-10733

- *Carta de los Derechos Fundamentales de la Unión Europea. (2000/C 364/01)*

- Declaración Universal de Derechos Humanos proclamada el 10 de diciembre de 1948. https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf

- Versión Consolidada del Tratado De Funcionamiento de la Unión Europea (30 de marzo de 2010) C83/47.

- Convenio para la protección de los derechos humanos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950.

- Convenio 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.

- Convención Internacional sobre los derechos del Niño, adoptada por la Asamblea General de las naciones Unidas el 20 de noviembre de 1989. https://www.boe.es/buscar/doc.php?id=BOE-A-1990-31312

- *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).* (n.d.). https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

- *Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE.* (n.d.). https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-81849

- *Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).* (2000, junio 8). https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295

- Consejo de Estado (aprobado en 2017, 10 octubre). Número de expediente: 757/2017 con motivo del Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal. BOE. https://www.boe.es/buscar/doc.php?id=CE-D-2017-757

- Resoluciones aprobadas por la asamblea general durante el 45° período de sesiones. A/RES/45/95 de 14 de diciembre de 1990. Principios rectores

sobre la reglamentación de los ficheros computadorizados de datos personales.

Legislación nacional

- Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 28/2006, de 18 de julio, de Agencias estatales para la mejora de los servicios públicos.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.
- Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista.

8.3. Bibliografía

- Know How *¿Qué es un servidor?* (2020, 15 septiembre). IONOS Digital Guide. Recuperado 11 de diciembre de 2022, de https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/
- AEPD (2022, 14 julio) *Derecho de supresión ("al olvido"): buscadores de internet*. Agencia Española de Protección de datos. https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido

- AEPD. (s. f.). Guía del Reglamento General de Protección de Datos para responsables de tratamiento. En *Agencia Española de Protección de Datos*. https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf

- Agencia Española de Protección de Datos. (s. f.). Consentimiento otorgado por menores de edad. https://www.aepd.es/es/documento/2000-9905.pdf

- Aguiar, A. R. (2021, June 25). Uno de los mayores expertos de Europa denuncia que el RGPD no funciona. *Business Insider España*. https://www.businessinsider.es/mayores-expertos-europa-denuncia-rgpd-no-funciona-888997

- Amazon. (s. f.). ¿Qué es un VPS? - Servidor virtual privado - AWS. Amazon Web Services, Inc. Recuperado 11 de diciembre de 2022, de https://aws.amazon.com/es/what-is/vps/

- Art. 29 Data Protection Working Party (2009, 01 december). *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

- B.T., El Mundo, Tecnología (2018, April 20). *Facebook burla la nueva normativa europea al mover su sede de Irlanda a EEUU*. ELMUNDO. https://www.elmundo.es/tecnologia/2018/04/20/5ad9bc9a46163f4f248b45b6.html

- Blain Escalona, LS., & Vázquez Inclán, IL. (2012). Funciones resúmenes o hash. Telematica, 10 (1). https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/52

- BOE.es - Derechos Fundamentales. (s. f.). Agencia Estatal Boletín Oficial del Estado. Recuperado 15 de julio de 2022, de https://www.boe.es/legislacion/derechos_fundamentales.php

- *BOE.es - DOUE-L-2003-80730 Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas [notificada con el número C(2003) 1422].* https://www.boe.es/buscar/doc.php?id=DOUE-L-2003-80730ç

- Comisión Europea. *REFIT – Por una la legislación de la UE más sencilla, económica y con garantías de futuro*. (n.d.). Comisión Europea. https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof_es

- Commission Of The European Communities on the protection of individuals with regard to the processing of personal data and on the free movement of such data (presented by the Commission pursuant to Article 149 (3) of the EEC Treaty) COM (92) 422 final - SYN 287 Brussels, 15 October 1992.
- *Concepto de fichero — Fundamentos de Programación en C++*. (2020). https://www2.eii.uva.es/fund_inf/cpp/temas/10_ficheros/concepto_fichero.html

- Cuervo, J. *(17 de febrero de 1015), Sentencia de 15 de diciembre 1983., Ley del Censo. Derecho a la personalidad y dignidad humana. Informática Jurídica*. https://www.informatica-juridica.com/sentencia/sentencia-de-15-de-diciembre-1983-ley-del-censo-derecho-la-personalidad-y-dignidad-humana/

- Dans, E. (2011, July 9). Capítulo 13. La evolución de la tecnología: del ordenador a la nube | Todo va a cambiar |. https://www.todovaacambiar.com/capitulo-13-la-evolucion-de-la-tecnologia-del-ordenador-a-la-nube

- De Franceschi, A., Schulze, R., Graziadei, M., Pollicino, O., Riente, F., Sica, S., & Sirena, P. (2019). *Digital Revolution - New Challenges for Law: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*.

- Diccionario de siglas y abreviaturas utilizadas en libros jurídicos españoles, Colegio Universitario de Estudios Financieros (CUNEF) (centro en proceso

de desadscripción de la UCM), Recuperado el 15 diciembre de 2022, https://biblioteca.cunef.edu/files/docs/abreviaturaslegislacion.pdf

- Diccionario panhispánico del español jurídico (2022), Siglas jurídicas, recuperado el 16 de julio de 2022, de https://dpej.rae.es/contenido/siglas-jur%C3%ADdicas

- Donohue, B. (2021, 11 marzo). ¿Qué Es Un Hash Y Cómo Funciona? Blog oficial de Kaspersky. https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

- Eeva Pavy (2023) *El principio de subsidiariedad | Fichas temáticas sobre la Unión Europea | Parlamento Europeo*. https://www.europarl.europa.eu/factsheets/es/sheet/7/el-principio-de-subsidiariedad

- Euroestat Statistics Explained (2020). *Archive: Estadísticas sobre sociedad y economía digital.* https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals/es&oldid=510151

- Europäische Kommission (2008). Flash Eurobarometer 225 (Data Protection - General Public). *GESIS Data Archive, Cologne. ZA4736 Data file Version 1.0.0, https://doi.org/10.4232/1.4736*.

- Ferrer, J. (junio 30, 2022). *Política de Cookies*. Weyketing. https://www.weyketing.com/politica-de-cookies/

- Gacitúa Espósito, A. L. (2014). *El derecho fundamental a la Protección de Datos Personales en el ámbito de la prevención y represión penal europea*. Universidad Autònoma de Barcelona.

- Gómez, R. M. (2016). Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016) *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha*, (6), 243-280.

- Grupo de trabajo del artículo 29. (2009). Dictamen 4/2007 sobre el concepto de datos personales. Grupo de trabajo creado virtud del art. 29 de la Directiva 95/46/CE.

- *Heredero Higueras, M. (1983). La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población. Documentación Adminsitrativa, 198(1983), 139–159. https://revistasonline.inap.es/index.php/DA/article/view/4687/4741*

- Kelsey, J., Chang, S., & Perlner, R. (2016, 22 diciembre). SP 800-185, SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, ParallelHash | CSRC. NIST. https://csrc.nist.gov/publications/detail/sp/800-185/final

- López, A. (2022, 20 julio). Criptografía: Qué son los algoritmos hash y para qué se utilizan. RedesZone. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-hash/

- López, O., & Arauz, T. (s. f.). Uso de hash enfocadas en la búsqueda de datos y seguridad informática [IEEE Conference Paper Template]. Universidad Tecnológica de Panamá.

- Mañas, J. L. P. (2016). Reglamento general de protección de datos. Revista del Consejo General de la Abogacía, (98), 26-29.

- Martínez Rodríguez, N. (diciembre 2018) Crónica de legislación de la protección de datos y derechos digitales. Ars Iuris Salmanticensis, vol. 7, Junio 2019, 254-259, eISSN: 2340-5155. Ediciones Universidad de Salamanca.

- Martínez, R. M. (2017). Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos. *Dilemata*, (24), 151-164.

- *Murillo De La Cueva, P. L., & Piñar Mañas, J. L. (2009). El derecho a la autodeterminación informativa. Fundación Coloquio Jurídico Europeo.*

- *Murillo De La Cueva, P.L. (Recep.:2004, 30 agosto). El derecho a la autodeterminación informativa y la protección de datos personales. Core. Acep.: 17 de octubre de 2008. https://core.ac.uk/download/pdf/11501784.pdf*

- Murillo De La Cueva, P. L. La Construcción del Derecho a la Autodeterminación Informativa. (1999). *Revista de Estudios Políticos (Nueva Época)*, *104* (abril-junio), 35–60. https://helvia.uco.es/bitstream/handle/10396/2238/REPNE_104_037.pdf?sequence=1&isAllowed=y

- National Institute of Standards and Technology. (2017, 4 enero). Hash Functions | CSRC. NIST | CSRC. https://csrc.nist.gov/projects/hash-functions (actualizado el 19 de diciembre de 2022)

- News Center Microsoft Latinoamérica. (2023, 8 febrero). *Una nueva investigación de Microsoft ilustra los riesgos en línea y el valor de las herramientas de seguridad para mantener a los niños más seguros en el entorno digital - News Center Latinoamérica*. https://news.microsoft.com/es-xl/una-nueva-investigacion-de-microsoft-ilustra-los-riesgos-en-linea-y-el-valor-de-las-herramientas-de-seguridad-para-mantener-a-los-ninos-mas-seguros-en-el-entorno-digital/

- Niño Camazón, J. (2010, 1 de mayo). Servidores de aplicaciones web [Ebook]. En Aplicaciones web. Editorial Editex S.A. https://play.google.com/books/reader?id=5c7hAwAAQBAJ&pg=GBS.PA39&hl=es

- *Normativa aplicable en materia de protección de datos de carácter personal tanto en la legislación específica como en la sectorial*. (2022, 28 marzo). Agencia Española de Protección de Datos. Recuperado el 14 de julio de 2022, de https://www.aepd.es/es/informes-y-resoluciones/normativa-y-circulares

- *Protección de datos de carácter personal. (2022, 11 julio). Senado de España. Recuperado 31 de julio de 2022, de*

https://www.senado.es/web/relacionesciudadanos/atencionciudadano/proteccion datos/index.html

- Rallo Lombarte, A. (2019). El nuevo derecho de protección de datos. *Revista Española de Derecho Constitucional*, 116, 45-74. doi: https://doi.org/10.18042/cepc/redc.116.02
- Ramiro, M. A. (2015). *Artemi Rallo Lombarte (Ed.). El derecho al olvido en Internet. Google*. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=5289834

- Raphaël Gellert, (2018) Understanding the notion of risk in the General Data Protection Regulation, Computer Law & Security Review, Volume 34, Issue 2, Pages 279-288, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.12.003. (https://www.sciencedirect.com/science/article/pii/S0267364917302698)

- Real Academia de Jurisprudencia y Legislación. (2016). Diccionario jurídico (1ª edición).

- Ribas, X. (2021, September 14). *El tratamiento a gran escala como concepto jurídico indeterminado*. Xavier Ribas. https://xribas.com/2021/08/25/el-tratamiento-a-gran-escala-como-concepto-juridico-ineterminado/

- Ruiz, C. (1992). *La configuración constitucional del derecho a la intimidad,* Universidad Complutense de Madrid. https://eprints.ucm.es/id/eprint/2164/1/T17616.pdf

- Schwabe, J. (2009). Jurisprudencia del Tribunal Constitucional Federal Alemán - Compilación de los extractos de sentencias más relevantes [Compilación de las sentencias más relevantes del Tribunal Constitucional Federal Alemán]. Konrad-Adenauer-Stiftung e. V. Programa Estado de Derecho para Latinoamérica.

- Silva, JM; Ragués i Vallès, R; Castiñeira, MT; Robles, R; Felip, D; Benlloch, G; Pastor, N; Ortiz, I; Montaner, R; Llobet, M; Estrada, A; Coca, I. (Atelier) (2019). *Lecciones de Derecho Penal Parte Especial*, (6ª edición)

- Sinopsis artículo 18 CE realizada por: Ascensión Elvira Perales, Profesora Titular. Universidad Carlos III. Diciembre 2003 y Actualizada por Ángeles González Escudero, Letrada de las Cortes Generales, en enero de 2011. https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2

- Unión Europea. (s. f.). Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea. Eur-Lex. El acceso al derecho de la Unión Europea. Recuperado 4 de noviembre de 2010, de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0609&from=EN

- Universitat de València. (s. f.). *Extracto STC 143/1994*. Universitat de València, Servicio de Informática. Recuperado 5 de agosto de 2022, de https://www.uv.es/uvweb/servicio-informatica/es/normativa-procedimientos/recursos/jurisprudencia/stc-143/1994-1285902043770.html

- Xataka (2019, December 31). La historia del ordenador desde la experiencia de nueve profesionales. Territorio Intel. https://territoriointel.xataka.com/historia-ordenador-experiencia-nueve-profesionales-ambitos-muy-dispares/

9. Anexos

9.1. Anexo I

Sistemas gestores de bases de datos:

Son programas informáticos que sirven para manejar bases de datos. Existen sistemas gestores libres y no libres.
Uno de los sistemas más utilizados en aplicaciones web es MySQL; se distribuye bajo dos licencias. Los usuarios pueden elegir entre usar el *software* MySQL como producto con licencia propietaria o como *Open Source* bajo los términos de la licencia GNU *General Public License*. Se puede instalar en plataformas Linux, Windows, Mac OS, Solaris, etc., es compatible con servidores web como Apache, IIS, etc. (Niño Camazón, 2010)

Commission of the European Communities on the protection of individuals with regard to the processing of personal data and on the free movement of such data (presented by the Commission pursuant to Article 149(3) of the EEC Treaty) COM (92) 422 final - SYN 287 Brussels, 15 October 1992 – Art. 2

Article 2
Definitions
This Article defines the main concepts used in the Directive. The definitions are taken from the Council of Europe Convention, but have been adapted and clarified to ensure equivalent protection at a high level in the Community.

(a) "Personal data". The amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual (amendment No 12). A person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.). The definition would also cover data such as appearance, voice, fingerprints or genetic characteristics. –

"Depersonalized" data are not defined: the term is not used in the Directive. This means that whether or not data are depersonalized no longer depends on the cost of determining the data subject's identity (amendment No 13). However, in the specific case where data are compiled in the form of statistics, it has been considered appropriate to state that they cannot be considered to be personal data where the data subjects can no longer reasonably be identified.

(b) "Processing of personal data" ("processing"). The definition given here is likewise an extensive one, the better to ensure that individuals are protected (amendment No 15), as it covers everything from the collection to the erasure of data, including organization, use, consultation, disclosure by transmission, dissemination or otherwise making available (amendment No 16), comparison and suppression.

(c) "Personal data file" ("file"). This definition, which covers both automatic and non-automatic files, is now clarified. In the case of non-automatic processing it allows the scope of the Directive to be confined to sets of data which are structured so as to facilitate access and searches for data on individuals. Personal data which are not organized so that they can be used with reference to the data subjects themselves are thus excluded. In practice data of this kind do not present the same dangers for individuals, and it is more realistic not to subject them to the same obligations.

To ensure that individuals are properly protected the criteria for access must have the "object or effect" of facilitating the use or comparison of data. This means that the data subject has does not have to prove intention, something which might have made it difficult to apply the national legislation.

The word "comparison" has been preferred to "combination" because it is appropriate both to automatic processing and to files kept on paper.

(d) "Controller". The definition is borrowed from the definition of the "controller of the file" in the Council of Europe Convention.

But as the Directive sets out to regulate the use of data in the light of the object being pursued, it is preferable to speak of the "controller", and to drop any reference to a "file" or to "data".

The controller is the person ultimately reponsible for the choices governing the design and operation of the processing carried out (usually a chief executive of the company), rather than anyone who carries out processing in accordance with the controller s instructions. That is why the definition stipulates that the controller decides the "objective" of the processing. This is in line with Parliament's amendment No 17. The controller may process data himself, or have them processed by members of his staff or by an outside processor, a legally separate person acting on his behalf. -life)

(e) "Processor". This is a useful definition proposed by Parliament (amendment No 18).

(f) "Third party". This definition is taken from one of Parliament's amendments (No 134); it has been reworded in the amended proposal in order to make it clear that third parties do not include the data subject, the controller, or any person authorized to process the data under the controller's direct authority or on his behalf, as is the case with the processor.

Thus persons working for another organization, even if it belongs to the same group or holding company, will generally be third parties.

On the other hand, branches of a bank processing customers' accounts under the direct authority of their headquarters would not be third parties. The same would apply to the employees of insurance companies; in the case of insurance brokers, on the other hand, the position may vary from case to case.

(g) "The data subject's consent". In the initial proposal the definition of a person's consent to the processing of data concerning him was given in Article 12, dealing with the rights of data subjects.

This caused some confusion; some interested parties drew the conclusion that all processing required the prior consent of the data subject, whereas consent was only one of the possible grounds making processing lawful.

It seems more logical, therefore, to put the rules on consent in Article 2, with a few changes of wording so as to cast them in the form of a definition.

The reference to consent being "express" has been removed, lest it be interpreted as requiring written consent (a procedure confined to sensitive data in Article 8 of the amended proposal). It has been replaced by the concept of an "express indication of his wishes", something which may be either oral or in writing.

The amended proposal makes it clear that consent must be "freely given", in cases where pressure might be brought to bear on the data subject (the case of a wage-earner and his employer, for example).

To enable the data subject to make an assessment of the advantages and disadvantages of the processing of data concerning him, and to exercise his rights under Article 13 of the proposal (rectification, erasure and suppression), the consent given must be informed consent.
The controller must supply the data subject with the information he needs, such as the name and address of the controller and of his representative if any (see Article 4(2)), the purpose of the processing, the data recorded, etc.

The data subject's consent must be "specific", meaning that it must relate to a particular data processing oper ı Ion concerning the data subject carried out by a particular controller and for particular purposes.

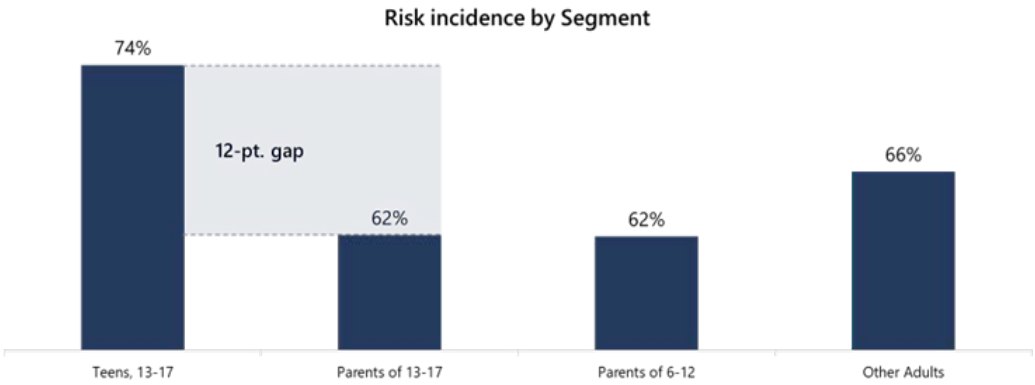
The data subject may withdraw his consent at any time. But this withdrawal has no retrospective effects; otherwise a processing operation which was lawful when carried out might become unlawful retroactively.

Three definitions in the original proposal have been deleted:

- the definition of the supervisory authority, which is covered by Article 32 of the amended proposal;

- the public and private sectors, as the provisions dealing with the two sectors have been merged (Chapter II of the amended proposal).

Riesgo de incidencia por segmento relativo al contacto de un riesgo en línea



La jerarquía de Datos

Podemos establecer una jerarquía para los distintos tipos de **datos**, organizándolos en diferentes niveles:

- **Bit**: Su valor es **0** o **1**. Es la unidad mínima de información.
- **Byte**: 8 bits: Pueden usarse para almacenar caracteres o números pequeños
- **Campo**: Grupo de bytes con un significado, por ejemplo, un nombre de persona, un entero, un real
- **Registro**: Un grupo de campos relacionados. Por ejemplo, los campos nombre, apellidos, edad y DNI pueden ser un registro para describir a una persona en un contexto determinado. En C++, un registro se programa con una **clase**, *class*.
- **Fichero**: Un grupo de campos o registros relacionados.
- **Base de datos**: Un grupo de ficheros relacionados.

Fuente:

Concepto de fichero — Fundamentos de Programación en C++. (n.d.). https://www2.eii.uva.es/fund_inf/cpp/temas/10_ficheros/concepto_fichero.html

Anexo II

Abreviaturas

- **APD**: Agencia de Protección de Datos
- **BOE**: Boletín Oficial del Estado
- **BVerfGE**: Bundesverfassungsgericht (Tribunal Constitucional Federal)
- **CE**: Constitución Española
- **CP**: Código Penal
- **DP**: Datos personales
- **DPO / DPD**: Delegado de Protección de Datos
- **DchoPD**: Derecho de Protección de Datos
- **DUDH / DUDDHH**: Declaración Universal de los Derechos Humanos
- **EEE**: Espacio Económico Europeo
- **EEMM**: Estados Miembros
- **F**. **Hash**: Función Hash
- **LO**: Ley Orgánica
- **LOPD / LOPDCP / LOPDGDD**: Ley Orgánica de Protección de Datos / Ley Orgánica de Protección de Datos de Carácter Personal / Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- **LSSI**: Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- **PD**: Protección de Datos
- **RD**: Real Decreto
- **RGPG**: Reglamento General de Protección de Datos
- **STC**: Sentencia Tribunal Constitucional
- **STS**: Sentencia del Tribunal Supremo
- **STJUE**: Sentencia del Tribunal de Justicia de la Unión Europea
- **STEDH**: Sentencia del Tribunal Europeo de Derechos Humanos
- **TFUE**: Tratado de Funcionameinto de la Unión Europea
- **TUE**: Tratado de la Unión Europea
- **TL**: Tratado de Lisboa
- **TEDH**: Tribunal Europeo de Derechos Humanos
- **UE**: Unión Europea

Anexo III – Contexto histórico

Contexto histórico hasta la entrada en vigor de la LOPD

Como ya hemos puesto de manifiesto en páginas anteriores, así como se ha expresado en múltiples ocasiones por nuestros tribunales, sirva de ejemplo la STC 94/1998, de 4 de mayo que, haciéndose eco de las STC 254/1993[63] (que declaró que la garantía de la intimidad adoptaba un entendimiento positivo que se traducía en el derecho de control sobre los datos relativos de cada individuo, aludiendo a la libertad informática como el derecho a controlar el uso de los datos insertos en el *habeas data,* así como la capacidad del ciudadano a oponerse a la utilización de determinados datos personales para fines distintitos de aquel que legítimamente justificó su obtención) y 143/1994 (que especificaba que la autorización de la recogida de datos con fines legítimos que no incluyera garantías adecuadas frente al uso potencialmente invasor de la vida privada a través de un tratamiento técnico era, también, una vulneración al derecho a la intimidad), en el fundamento jurídico 4º, precisaba que el ATC 642/1989 en su FJ. 3º, insinuaba que el uso de datos suministrados a través de medios informatizados más allá de lo legalmente autorizado podría constituir un grave atentado a los derechos fundamentales de la persona y ser objeto de la correspondiente demanda de amparo.

Más tarde, en la sentencia 292/2000, de 30 de noviembre, se apreció la doctrina previa que desarrollaba este novedoso concepto acuñado primeramente en España como "libertad informática" y lo acotó en términos de derecho fundamental autónomo (véase FJ. 2º y 5º 2º párrafo) dado el amplio alcance que sostenía el "tratamiento mecanizado de datos" en la garantía de la vida privada de la persona y que su integración, así como protección, era crucial dada la nueva dimensión positiva que rebasaba, incluso, el derecho a la intimidad, con quien comparte objetivo de ofrecer una eficaz protección constitucional de la vida personal uy familiar, pero necesario a la hora de atribuir al titular un haz de facultades consistentes, en gran parte, en el poder jurídico de imponer a terceros la realización y omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, limitando así el uso de la informática, desarrollando el derecho fundamental a la protección de datos o regulando su ejercicio (53.1 CE).

[63] Sentencia vanguardista en defensa del 18.4 CE donde el Gobierno Civil de Guipúzcoa denegó a un ciudadano información relativa a la posesión de sus datos personales, aquilatando su contenido en sentencias posteriores en ámbitos como las normas reguladoras del número de identificación fiscal o la libertad sindical.

Podría tacharse como un derecho subsidiario o complementario al de la intimidad en cuanto a que ambos protegen el ámbito personal y familiar de intromisiones no legítimas, sin embargo, el derecho a la protección de datos persigue *garantizar a esa persona un poder de control* (y disposición) *sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal* (SSTC 134/1999, de 15 de julio, F.J. 5; 144/1999, F.J. 8; 98/2000, de 10 de abril, F.J. 5; 115/2000, de 10 de mayo, F.J. 4)*, es decir, el poder de resguardar su vida privada de una publicidad no querida*. De ahí la particular singularidad del *right of privacy*, pues su objeto de estudio es más amplio, inclusive, que el derecho a la intimidad, ya que extiende, a entendimiento del TC, su garantía a la intimidad, a la "esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, F.J. 4)", como al derecho al honor y, sobre todo al ejercicio y protección de cualquier dato personal, ya sea de índole más íntima o no.

También se extiende dicha garantía a una imposición a los poderes públicos de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de dicha información, ahora bien, y como trataremos más adelante de forma más amplia, el poder de disposición no es efectivo ni real cuando el afectado desconoce qué datos son los que se poseen por terceros y con qué fin, ya que es necesario para hacerse operativo, el reconocimiento del derecho a ser informado de tales hechos y a poder oponerse a su posesión, accediendo, si es oportuno, a los registros y asientos, observar el destino que han tenido, el alcance a posibles cesionarios y, en su caso, requerirle para su rectificación o cancelación.

Principios rectores para la reglamentación de los ficheros computadorizados de datos personales. Adopción: Asamblea General de la ONU - Resolución 45/95, 14 de diciembre de 1990.

El contenido de este derecho se ajusta a los diferentes instrumentos internacionales, como en el caso de la Resolución 45/95 de la Asamblea General de las Naciones Unidas donde se recogen los principios relativos a las garantías mínimas que deberían preverse en la legislación nacional, así como también su aplicación en los ficheros de las organizaciones internacionales gubernamentales que contienen datos personales, en la que quisiera detenerme para repasarlo en profundidad.

Esta resolución de extensión más bien breve cuenta con dos principales bloques: Las garantías mínimas que deberían preverse en la legislación nacional, que establece diez principios y la aplicación de estos en los ficheros de las organizaciones internacionales gubernamentales.

Este primer punto empieza con el principio de la licitud y lealtad, por el cual la información de las personas debe ajustarse a los requerimientos, propósitos y principios de la Carta de las Naciones Unidas, prohibiendo los procedimientos que fueran desleales o ilícitos.
Le sigue el principio de exactitud por el cual se obliga a las personas encargadas de la creación o funcionamiento de un fichero la verificación de la exactitud y pertenencia de los datos registrados con el objetivo de cerciorarse de la no comisión de errores u omisiones, actualizando los mismos periódicamente.

En tercer lugar, el principio de finalidad, siendo imperativo la especificación y justificación, en el momento de creación de ficheros, de la finalidad y funcionalidad de los datos recabados, poniéndose en conocimiento del interesado a fin de que ulteriormente sea posible asegurarse de que a) todos los datos siguen siendo pertinentes a la finalidad; b) que ninguno de esos datos pueda ser utilizado y revelado sin el consentimiento del usuario (con un propósito incompatible al especificado); c) que el período de conservación de los datos no exceda del necesario para alcanzar la finalidad con la que se registraron.

En cuarto lugar, se encuentra el principio de acceso de la persona interesada, por el cual se específica que cualquiera que documente y demuestre su identidad tiene derecho a saber si se está procesando información personal, conseguir una comunicación inteligible, sin demoras o gastos excesivos, y obtener rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos, además de conocer los destinatarios cuando la información es comunicada. Así mismo se exige, en conformidad con el octavo principio, que se prevea una vía de recurso ante la autoridad competente (convenientemente para todas las personas que se encuentren en la región) que, en caso de rectificación, el costo deberá sufragarlo el responsable del fichero.

En quinto lugar, hallamos el principio de no discriminación, que, a excepción, del criterio limitativo (que veremos a continuación), expone que no deben registrarse datos que puedan originar discriminación ilícita o arbitraria, especialmente sobre el

origen racial o ético, vía sexual, opiniones políticas, convicciones religiosas, filosóficas o participación y afiliación en asociaciones o sindicatos.

Seguidamente se encuentra el sexto subapartado correspondiente a la facultad de establecer excepciones a los cuatro primeros principios supeditado a la necesidad de proteger la seguridad nacional, orden público, salud o moral públicas y, en particular, derechos y libertades de los demás, especialmente de personas y grupos perseguidos (cláusula humanitaria) con reserva de una ley o reglamento equivalente que lo prevea en conformidad con el sistema jurídico nacional. En cuanto a las excepciones del quinto principio deberá estar sujeto a las mismas garantías antes establecidas y solo podrán ser autorizadas dentro de los límites previstos por la Carta Internacional de Derechos Humanos y demás instrumentos de protección y lucha contra la discriminación.

El principio de seguridad, como séptimo apartado, trata de prever posibles riesgos para los ficheros como son riesgos naturales, la perdida accidental o la destrucción por siniestro y otros riesgos humanos como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático.

En octavo punto se dedica al control y a las sanciones ya que cada legislación deberá designar a una autoridad que se encargue de controlar el respeto de los principios anteriormente enunciados, ofreciendo garantías de imparcialidad, independencia y competencia técnica. Así pues, en caso de violar las disposiciones legislativas internas deberán preverse sanciones penales, así como recursos individuales apropiados. Es por todo ello que en España se escogió el modelo de Agencias estatales (Ley 28/2006) para llevar a cabo estas funciones, pues, así como indica su ley reguladora en la exposición de motivos I. la fórmula organizativa general se caracteriza por estar dotadas de mayor nivel de autonomía e independencia funcional respecto de la AGE, flexibilidad en la gestión, refuerzo de los mecanismos de control de eficacia y promoción de la cultura de la responsabilización de los resultados. De igual manera, en el art. 2 de la mencionada ley, continúa detallando su naturaleza y régimen jurídico, como es la personalidad jurídica pública, patrimonio propio y autonomía en su gestión. Se rigen por esta ley y un estatuto propio, además de, supletoriamente, por las normas aplicables a las entidades de derecho público vinculadas o dependientes de la AGE.

El noveno punto precisa el flujo de datos a través de las fronteras que, cuando se trate de dos países con garantías comparables en cuanto a la protección de la vida privada se refiere, la información puede circular tan libremente como en el interior de casa uno de los territorios, no obstante, cuando no exista dicha garantía, no se podrán imponer limitaciones injustificadas a dicha circulación, solo en la medida que aso lo exija la protección de la vida personal.

En décimo lugar está el campo de aplicación que serán ni más ni menos que todos los ficheros computadorizados, tanto públicos como privados y, por extensión facultativa y a reserva de las adaptaciones pertinentes, a los ficheros manuales. Podrán extenderse total o parcialmente estos principios a las personas cuando contengan en parte información sobre personas físicas.

Respecto al segundo bloque, hace imperativo que los principios rectores sean aplicables a los ficheros de las organizaciones internacionales gubernamentales que contengan datos personales, a reserva de las adaptaciones necesarias teniendo en cuenta las posibles diferencias con los ficheros con fines internos, como los relativos a la gestión personal y los ficheros con fines externos relativos a terceras personas relacionadas con la organización. Cada organización deberá asignar a la autoridad que estatutariamente sea competente para velar por la correcta aplicación de estos principios.

Se debe tener la previsión de una cláusula humanitaria por la cual se puedan excepcionar estos principios en virtud de la protección de los derechos humanos y las libertades fundamentales, así como en la prestación asistencia humanitaria.
Por último, la legislación nacional deberá contener una excepción análoga para las organizaciones internacionales gubernamentales en cuyo convenio sobre la sede no se hubiera excluido la aplicación de dicha legislación nacional, asó como para las organizaciones internacionales no gubernamentales
en las que sea aplicable ducha legislación.

Dejando de lado el ámbito internacional y centrándonos en el europeo encontramos el Convenio para la protección de las personas respecto al Tratamiento Automatizado de Datos de Carácter Personal hecho en Estrasburgo el 28 de enero de 1981, ratificado por Alemania, España, Noruega y Suecia y aprobado por Francia, el cual tiene por fin garantizar a cualquier persona física, en territorio de las partes, independientemente de su nacionalidad o residencia, el respeto del derecho a la

vida privada con respecto al tratamiento automatizados de datos de carácter personal. El mérito más remarcable del Convenio residía en su artículo octavo, como advierte la STC 254/1993, FJ. 4, puesto que dotaba a las personas el poder conocer la existencia de un fichero automatizado de datos personales, sus finalidades, así como ser informado de la identidad y la residencia habitual del establecimiento principal de la autoridad controladora, así mismo como obtener la confirmación de la existencia del fichero y la comunicación de estos, además del poder de rectificación de dichos datos o la supresión de los mimos cuando se trate de una infracción de las disposiciones del derecho interno y disponer de un recurso si no se ha atendido a una petición de confirmación, comunicación, rectificación o borrado.

Retomando la evolución legislativa del derecho fundamental de protección de datos de carácter personal en el estado español, podemos remontarnos hasta la Ley orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida por su acrónimo LORTAD, que fue reemplazada por su sucesora normativa, la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, con el fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que tuvo la oportunidad de complementarse con abundante jurisprudencia civil y contencioso-administrativa (LO 3/2018, Preámbulo I *in fine*) y que estableció un hito en la historia de este derecho consagrando dos de las más antiguas ambiciones del proceso de integración europea: la protección del derecho fundamental a la protección de datos y la realización del mercado interior, es decir, la libre circulación de datos personales, objetivos los cuales, siguen teniendo vigencia, al igual que los principios consagrados en dicha directiva.

Sin embargo, la precipitada evolución tecnológica y la globalización han modificado el entorno y han lanzado nuevos problemas en esta materia. Actualmente, la tecnología permite un intercambio feroz de información de toda índole, tanto a los ciudadanos, como organizaciones, instituciones y personas jurídicas, y hacerla mundialmente pública. Las redes sociales evidencian este fenómeno, al igual que la computación en la nube, que permite guardar datos en servidores[64] remotos ajenos sin tener que disponer de extensas memorias internas, como por ejemplo los VPS[65].

[64] El termino servidor aglutina dos significados en el ámbito informático, el primero, también conocido como "*host*", hace referencia al *hardware*, es decir, una máquina física integrada en una red informática, en la que, además de su Sistema Operativo, funcionan uno o varios servidores basados en *software*, que es, precisamente, la segunda definición. Un servidor basado en *software* es un programa que ofrece un servicio especial que otros programas denominados clientes pueden

Estos fenómenos plantean nuevos retos en materia de derecho de protección de datos, puesto que implica perder el control de la información personal, parte de la cual es potencialmente sensible. Las herramientas empleadas para la recogida de datos cada vez son más sofisticadas y permiten a los agentes económicos obtener información más precisa y detallada de sus targets, como la geolocalización y determinación de la ubicación de un individuo y su/s residencia/s, el registro de comportamientos virtuales, la monitorización de pagos o cribaje de intereses más frecuentes.

Estas consideraciones suscitan inevitablemente si la legislación internacional y nacional será capaz de hacer frente plena y eficazmente a estos sucesos y, por ello, a principios de la primera década de los 2000, se fueron adoptando distintas instancias internacionales, propuestas para la reforma del marco vigente, en aras a una regulación más uniforme del derecho, hasta que, la Comisión Europea lanzó el 4 de noviembre de 2010 una comunicación (al Parlamento Europea, al Consejo, al Comité Económico y Social y al Comité de las Regiones) titulada «Un enfoque global de la protección de los datos personales en la Unión Europea» que planteaba, primeramente, los nuevos retos en materia de Protección de Datos, precedida de un examen del marco jurídico vigente hasta entonces y una consulta pública en 2009, asimismo como diversos estudios, que, a ojos de la Comisión, validaron los principios fundamentales que la Directiva instauró anteriormente aunque, a su vez, identificaron diversos problemas, a destacar: el impacto de las nuevas tecnologías (que se resolvió de forma muy parcial en la Directiva 2002/58/CE completando la Directiva 95/46/CE y modificada por la Directiva 2009/136/CE), la necesidad de

---

usar a nivel local o a través de la red y su servicio variará en función del propio tipo de software que se trate. La base de la comunicación es el modelo cliente-servidor y, en lo que concierne al intercambio de datos, entran en acción los protocolos específicos del servicio (Digital Guide Ionos, ¿Qué es un servidor?, 2020).
Siendo más específicos, cuando hablamos de páginas web (servidores web), en palabras de Jesús Niño Camazón, nos referimos a un programa que implementa el protocolo HTTP (*HyperText Transfer Protocol*); un protocolo diseñado para transferir paginas HTML. Son servidores que se ejecutan continuamente en un ordenador y atienden a las peticiones que hacen los clientes desde sus navegadores. Algunos ejemplos de servidores web serían: Apache, un software de código abierto que funciona en multitud de plataformas (Windows, Linux, etc.); IIS, un conjunto de servicios que convierten un ordenador en un servidor web y el tipo de licencia es propietaria; y Lighttpd, un servidor seguro, rápido y flexible, tiene licencia BSD (berkley Software Distribution) y funcioan en Linux (Niño Camazón, J. 2010)

[65] Termino que proviene de las siglas en inglés para abreviar el término *vitual private server*, una máquina que aloja el software y los datos necesarios para ejecutar una aplicación o sitio web. Se le denomina virtual por su capacidad de consumir una parte de los recursos físicos subyacentes del servidor que esta administrado por un proveedor externo. Sus funciones principales serían: lanzamiento y ejecución de aplicaciones web, creación de entornos de prueba y almacenamiento secundario de archivos (Amazon s. f.).

reforzar la dimisión de mercado interior de la protección de datos (por la insuficiente armonización de las legislaciones nacionales de los Estados miembros a pesar del marco común y que incrementaba la inseguridad jurídica, las cargas administrativas y no garantizaba la igualdad de condiciones en los diferentes agentes económicos), hacer frente a la globalización y mejorar las trasferencias internacionales de datos (el incremento de la subcontratación del tratamiento fuera de las fronteras de la UE acrecentaba los problemas de aplicación legislativa y de atribución de responsabilidades civiles y penales, además, se recomendaba la revisión y racionalización de las transferencias en aras a su agilización), consolidar las disposiciones institucionales para la aplicación efectiva de las normas sobre PD (conveniencia de reforzar el papel de las autoridades nacionales encargadas de la regulación del DchoPD) y mejorar la coherencia del marco jurídico que regula la PD.

La consecución de estos retos empezó con el Tratado de Lisboa (en adelante TL) que proporcionó los medios suplementarios, reconociendo los principios enunciados en la Carta de los Derechos fundamentales de la Unión Europea, con el valor jurídico de Tratados (antiguo art. 6 TUE), con su artículo octavo, constituyendo normativamente la protección de datos de carácter personal como derecho autónomo y jurídicamente vinculante para los estados miembros de la UE.

El objetivo seguía siendo, desde la Directiva 95/46, proteger los derechos fundamentales de las personas físicas *y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento su de datos personales* (STJUE C-101/01, Bodil Lindqvist), prohibiendo, el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicados o datos relativos a la salud o sexualidad (art.8, Directiva 95/46 CE).

Reanudando con el Comunicado de la Comisión Europea para la consecución de los objetivos esenciales del enfoque global de la PD en la UE, se debía, en primer lugar, garantizar a las personas una protección adecuada en cualquier circunstancia, para ello se fijaba el alcance de diversos términos, primeramente, el de “datos personales”, basándose, en el alcance proyectado en la Directiva; «*toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica,*

económica, cultural o social» (Directiva 95/45/CE y apartado 2.1.1 Bruselas, 4.11.2010 COM (2010) 609 final), que, a su vez, para determinar si este era identificable se debía *considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona* (Considerando 26 de la Directiva 95/46/CE), permitiendo aplicarlo en distintos casos, previendo también posibles evoluciones que afectan al derecho fundamental y, sobre todo, *con el fin de incluir toda la información referente a una persona identificable* (COM (92) 422 final de 28.10.1992, p. 10 (comentario sobre el artículo 2)[66]), incluido los que no eran previsibles en el momento de aprobación de la Directiva, aunque con varios defectos: el primero discernir en qué casos debía aplicarse el DchoPDCP o el cumplimiento de las obligaciones impuestas por la Directiva a los responsables de tratamiento[67] (2.11 Bruselas, 4.11.2010 COM (2010) 609 final).

Debemos señalar que, la Directiva, necesita que la información se refiera a una persona física "identificada o identificable, a lo que al grupo de trabajo del art. 29, en el Dictamen 4/2007 le suscita las siguientes consideraciones:
Por lo general se considera identificada a una persona física cuando es posible distinguirla de entre un grupo de personas, ergo, es identificable cuando, aun no habiéndose identificado todavía, sea posible hacerlo (como indica el sufijo "ble"). Ello se puede lograr con datos concretos que (el grupo de trabajo del art.29, 2007) denomina como "identificadores", que se caracterizan por tener una relación privilegiada y cercana respecto a un determinado individuo[68].

> *Artículo 2º de la Directiva 95/45/CE*
> *A efectos de la presente Directiva, se entenderá por:*
>
> *a) «datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad fisica, fisiológica, psíquica, económica, cultural o social;*

[66] Véase el artículo 2 original de la "*Commission Of The European Communities on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (*presented by the Commission pursuant to Article 149(3) of the EEC Treaty*) COM(92) 422 final - SYN 287 Brussels, 15 October 1992", en el Anexo I.
[67] Véase, por ejemplo, el caso de las direcciones IP, examinado en el Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 sobre el concepto de datos personales (documento WP 136) y presidido por Peter Schaar.
[68] Son ejemplos de identificadores: la altura, el color del cabello, la ropa, u etc. o una cualidad de la persona que no se puede percibir de forma inmediata como su profesión, cargo que desempeña, nombre, etc. (Grupo de trabajo del artículo 29, 2007)

b) (…)

Siguiendo el hilo conductor del Dictamen 4/2007, cuando se declara en el artículo segundo de la directiva que se considera *identificable toda persona cuya identidad pueda determinarse, directa o indirectamente*, se afirma, en palabras, que una persona puede ser identificada directamente por su nombre y apellidos o indirectamente por un número de teléfono, matrícula, número de la seguridad social, núm. de pasaporte o por una combinación de criterios significativos (..). También depende del contexto de la situación pues, un apellido muy común no bastará para identificar a un ciudadano de entre un país, mientras que sí se podrá como alumno de entre una clase.

Cuando se mencionaba el término *"indirectamente" identificadas o identificables*, se refiere en general al fenómeno de las "combinaciones únicas", sean estas pequeñas o grandes. Aun no pudiendo utilizar, a primera vista, los identificadores para singularizar a una persona, aun cabe que pueda ser identificada gracias a la combinación de dicha información con otros datos. Entra en juego lo que la Directiva se refiere como *elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social* y algunas son tan únicas que permitirían identificar a una persona de manera autónoma, igualmente, una combinación de detalles puede ser lo bastante concluyente, es especial si tiene acceso a información adicional.

Cabe añadir que, aun siendo algunos identificadores los más comunes para distinguir a una persona del resto, estos no son necesarios a día de hoy puesto que, sin conocer, por ejemplo, el nombre de un usuario concreto, podremos distinguirlo a través de ficheros informatizados de datos personales que suele asignar identificadores únicos a las personas registradas para evitar cualquier confusión que pueda darse entre dos personas incluidas en el fichero. Igualmente, en la red existen herramientas de control de tráfico con el mismo cometido, identificar al individuo que está detrás de la computadora por tal de atribuirle determinadas decisiones y que, en palabras del Tribunal de Justicia de las Comunidades Europeas, en el caso Lindqvist, hacerlo *constituye un tratamiento (…) de datos personales en el sentido del artículo 3, apartado 1, de la Directiva 95/46*, y, por lo tanto, sujeta a Ley.
En este sentido, desarrollar técnicas para evitar la identificación del interesado aun persiguiendo una finalidad en el tratamiento de sus datos es vital, por ello se adoptan medidas para protegerla teniendo en cuenta el conjunto de medios que

puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, requisito necesario para que la información no se considere como datos personales y su tratamiento no estuviera sujeta a la Directiva. Utilizar seudónimos o la *seudonimización*, se emplea para ocultar identidades y, a su vez, poder recopilar más datos sobre un mismo individuo sin necesidad de conocer su identidad. Se suele realizar de forma que quede un vínculo entre el seudónimo y la identidad a la que corresponde utilizando listas de correspondencias o algoritmos criptográficos bidireccionales. También puede realizarse sin dejar rastro alguno utilizando criptografía unidireccional, capaz de crear datos anónimos.

A efectos de la Directiva, es posible puntualizar diversas cuestiones, la primera es que se protegían a las personas físicas, así lo concluía el considerando 2º de la misma, el artículo 6 de la DUDDHH, afirmaba que todo ser humano tiene derecho al reconocimiento de su personalidad jurídica. A efectos prácticos, en la Directiva 2002/58/CE, que completaba la Directiva 95/46/CE en lo respectivo al primer apartado, se aplicaba, directamente, a las personas jurídicas y, subsidiariamente, a los intereses legítimos de los abonados que sean personas jurídicas. Además, el Tribunal de justicia de las Comunidades Europeas aclaró que cada Estado miembro podía extender el alcance de la normativa establecida por trasposición a situaciones que no están comprendidas en la propia Directiva, siempre y cuando no se oponga al Derecho comunitario, cuestión de la que se aprovecharon países como Luxemburgo, Italia o Austria por tal de extender el alcance de la protección a personas jurídicas.

Respecto a las personas fallecidas no se consideraban pues estos dejaban de ser personas físicas para el derecho civil, empero aún podían recibir indirectamente cierta protección puesto que: 1. sus datos pueden contener información de otras personas, 2. El responsable de los datos quizá no tiene medios para determinar si alguien ha fallecido, por lo que debería optar por aplicarlo siempre, 3. La información de estas personas puede estar sujeta a protección mediante lo que algunos denominan como personalidad pretérita (este hecho puede darse, por ejemplo, en la legislación nacional sobre el derecho a la propia imagen y al honor) y, por último, e igual que en el caso de las personas jurídicas, los estados pueden extender el alcance legislativo nacional a situaciones que no comprende el ámbito de aplicación de la norma comunitaria (grupo de trabajo del art.29, 2007).

Otro de los grandes retos de la Comunicación de la Comisión era la de aumentar la transparencia para los afectados, debiendo informar los responsables a los ciudadanos de una forma correcta y clara, además de garantizar un acceso fácil a la información, que, a su vez, debe ser fácil de entender, con un lenguaje sencillo. Realmente, hasta entonces, la transparencia no había sido uno de los puntos fuertes de la Directiva debido a que, en multitud de ocasiones, el usuario no era consciente de si se recogía información y con que finalidad. El ejemplo más palpable era la introducción de la publicidad personalizada, basada en el comportamiento on-line.

Así mismo también se apreció el creciente uso de la informática por parte de los niños y adolescentes[69], por lo que era necesaria introducir medidas de protección particular.
En este sentido se estudió la forma de introducir un principio general que imponga el tratamiento trasparente en los datos personales y también un paquete de obligaciones específicas para los responsables del tratamiento de datos y cómo deben ser comunicados, además de establecer modalidades de la forma y modo de esta comunicación, teniendo en cuenta que los ciudadanos deben ser informador cuando los datos que les conciernen sean objeto de destrucción accidental o ilícita, perdida, alteración, o acceso a personas no autorizadas o revelación a tales personas.

Debido a que la notificación obligatoria de las violaciones de datos solo se protegía en el ámbito de las telecomunicaciones y, por aquel entonces, la revisión que se había hecho a la Directiva quería extenderla inmediatamente al sector financiero la comisión tomó nota para dotar este campo de protección normativa.

Para reforzar el control sobre los propios datos, la comunicación de la comisión alentaba a regirse por el principio de minimización de los datos, pues su recopilación

[69] Tanto en un estudio cualitativo que elaboró la UE, donde se reveló que los niños de entre 9 y 14 años tienden a subestimar los riesgos vinculados a la utilización de Internet y a minimizar las consecuencias de sus comportamientos, así como una investigación de Microsoft de 2023 donde se mostraba como el 69% de las personas habían experimentado un riesgo, pero en el caso de los adolescentes ascendía a un 74% (cuando solo un 62% de sus padres declararon creer que su hijo había encontrado un riesgo y que además subestimaban los riesgos sobre todo en brechas como el discurso de odio, las amenaza de violencia exposición a contenido suicida, de ciberacoso o abuso). *El 39% de los adolescentes informaron haber experimentado discursos de odio en línea, mientras que solo el 29% de los padres informaron que sus hijos adolescentes tuvieron esa experiencia. Alrededor del 19% de los adolescentes experimentaron una amenaza de violencia, mientras que solo el 11% de los padres informaron lo mismo* (News Center Microsoft Latinoamérica, 2023) (Ver anexo I).

debe limitarse únicamente a su propósito. Así como el derecho a acceder, rectificar, suprimir o bloquear, salvo reservas legítimas de ley, principios actualmente presentes en la Ley Orgánica 3/2018 y en el Reglamento 2016/679 del Parlamento Europeo y del Consejo, específicamente en los artículos 12 al 18 del Capítulo II de la primera ley y del art. 13 al 21 de la segunda donde se reconoce el derecho al ejercicio directo o mediante representante legal o voluntario el Derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y de oposición (sobre los cuales ahondaremos más adelante).

En definitiva, la comisión pretendía estudiar e implementar el principio de minimización de datos, mejorar cualitativamente las condiciones de un verdadero ejercicio de los derechos de acceso, rectificación, supresión y bloqueo", asimismo garantizar la portabilidad de los datos", en otros términos, conferir al interesado el derecho explícito a retirar sus datos de una aplicación o servicio.

Otra cuestión relevante que tuvo en cuenta el Grupo de trabajo era la sensibilización de la protección de los datos personales. En 2008 se realizado un sondeo de Eurobarómetro (que puso de manifiesto que la mayoría de los habitantes de los Estados no estaban sensibilizados ante esta nueva realidad por lo que proponían cofinanciar acciones de sensibilización en los estados miembros con ayuda del presupuesto de la UE, así como un marco jurídico que obligara realizar estas acciones.

También se tuvo en cuenta la garantía del consentimiento libre e informado, así como la consideración de que datos eran necesarios proteger por su naturaleza sensible, es decir, que puedas revelar datos que descubran el origen racial, étnico, datos de opinión política, convicciones o de asociación, así como datos relativos a la genética[70] y salud[71].
De igual forma se iniciaron acciones en aras a reforzar la eficacia de las vías de recursos y sanciones estudiando la posibilidad de ampliar el poder de recurrir a los

[70] En el RGPD se establece como datos genéticos (art. 4.13) aquellos relativos a características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona, y, en el mismo sentido, existen los datos biométricos (4.14) que son aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

[71] De igual forma el reglamento general europeo de protección de datos define en su artículo 4.15 los datos relativos a la salud como DP que revelen la salud física y mental, incluida la prestación de servicios de atención sanitaria de forma que se revele información sobre su estado de salud.

órganos jurisdiccionales nacionales y evaluar la necesidad de endurecer las disposiciones que regulaban las sanciones.

Un hecho que se refleja en la comunicación “Un enfoque global de la protección de los datos personales en la Unión Europea” y que empaparía toda la normativa relativa a la protección de datos es la dimensión de mercado interior, la voluntad de avalar la libre circulación de datos entre los estados de la unión en el mercado interior y, por consiguiente, la armonización por la Directiva de las legislaciones nacionales que no se limite a pautas mínimas sino a una uniformización general completa (STJUE C-101/01, Bodil Lindqvist), dejando un pequeño margen de maniobra en algunos ámbitos, autorizándolos para introducir regímenes especiales para situaciones específicas. Ahora bien, para llevarlo a cabo exige la prudencia que se reduzca la carga administrativa, en este caso, simplificando y armonizando el actual sistema de notificación, incluida la opción de la existencia de un formulario de registro uniforme válido en toda la unión. Pero la simplificación administrativa no debe entenderse como un reducción general del nivel de responsabilidad de los gestores de datos, sino también una clara definición del marco jurídico en lo referente a los mecanismos de control interno y cooperación de las autoridades de control de datos.

No obstante, la susodicha armonización del mercado interior, en conjunto con la simplificación administrativa debe ir acompañada de una sustancial clarificación de las normas relativas a la legislación aplicable y al estado miembro responsable ya que desde el primer informe (2003) de la Comisión había indicios de que la aplicación del artículo 4 de la D 95/46/CE al derecho aplicable era “deficiente (…) lo que puede provocar conflictos jurídicos”, lo que, con el tiempo, ha ido complicándose todavía más debido a las complejidades que nos presenta el creciente globalismo tecnológico, habiéndose normalizado que los responsables del tratamiento de datos estén fuera del Espacio Económico Europeo con todas las dificultades que conlleva.

La comisión también estudió la viabilidad del fomento de las iniciativas en materia de autorregulación y la examinación de la posibilidad de instaurar regímenes europeos de certificación (pone el ejemplo de un “distintivo de protección de la intimidad”) para los procesos, tecnologías, productos y servicios que sean conformes a las normas de protección de la intimidad.

Un aspecto que estudio el Grupo de trabajo del artículo 29 y que tiene gran relevancia es la dimensión mundial de la protección de datos. Puesto que la transferencia fuera de la UE y del espacio EEE es una realidad que se va a dar requerimos que dicha transmisión este supeditada a la comprobación de la existencia de un nivel de protección de datos adecuado determinado, por ejemplo, por la Comisión y EEMM.
Con la normativa anterior existía el riesgo de que el nivel de protección de los dos interesados previstos en un tercer país se juzgara diferentemente en un estado miembro a otro, que, además, las cláusulas modelo de la comisión de entonces no concebían situaciones extracontractuales y no podían, por ejemplo, aplicarse a transferencias entre Administraciones Públicas. Habida cuenta de los problemas que destacaban, era preciso mejorar los mecanismos existentes de transferencia internacional de datos, clarificar su procedimiento de evaluación del carácter adecuado del nivel de protección, así como sus criterios y condiciones y definir los elementos esenciales en materia de Dcho. PD.
Con todo lo puesto en relieve la Comisión fijó presentar en 2011 las propuestas legislativas destinadas a revisar el marco jurídico de este derecho y, en segundo lugar, evaluar la necesidad de adaptar otros instrumentos jurídicos prosiguiendo, entre de otras cuestiones, una política activa de represión de las infracciones.

Como es sabido, tanto la Directiva 95/46/CE como la Directiva 2016/680 fueron derogadas, el 27 de abril de 2016, con la entrada del Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Este nuevo Reglamento sigue muchas de las finalidades que se estudiaron la comisión y, con una vocación muy predominante, la armonizadora.

Para ello cambiar de acto legislativo era clave puesto que las Directivas establecen objetivos a seguir por los EEMM, pudiendo estos elaborar sus propias leyes y dando como resultado un despliegue normativo irregular encarado a los intereses particulares de cada Estado, aun teniendo un nexo común, suelen tener poca capacidad conjuntiva, el Reglamento, sin embargo debe aplicarse en su integridad en toda la Unión permitiendo que, en un derecho tan empapado por las circunstancias de la globalización y que, naturalmente, tiende a la universalidad, pueda compenetrarse y funcionar en todos los países sin que choquen entre sí los diferentes cuerpos del mosaico normativo.

El RGPD aborda nuevos retos como el aumento de los flujos transfronterizos de datos que se derivan de la rápida evolución tecnológica que ha comportado que los datos personales sea una pieza clave en la sociedad de la información, tanto a nivel social, como con las redes sociales, como a nivel económico, como por ejemplo con la publicidad personalizada y, si bien esta información de carácter personal puede tener aspectos positivos como la mejora de los servicios, conlleva riesgos difusos en cuanto a su magnitud ya que es de difícil control en cuanto a su destino y uso. Así pues el Reglamento pretende reforzar la seguridad jurídica y la transparencia estableciendo una normativa recia que, por razones de coherencia, sea extrapolable a todas las disposiciones nacionales. Para ello es necesario que los EEMM integren el ordenamiento europeo de una manera clara y publica y elimine situaciones de incertidumbre derivadas de normas nacionales incompatibles que deben ser eliminadas a tenor del principio de seguridad jurídica. Su adoptación se llevó a cabo el 25 de mayo de 2018 siendo obligatorio en todos sus elementos para los Estados de la Unión, así como establece su art.99.
Por ello mismo era necesario la elaboración de una nueva ley orgánica que sustituyese la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La ley que vamos a analizar consta de noventa y siete artículos indexados en diez títulos y veintidós disposiciones adicionales, seis transitorias, una derogatoria y dieciséis finales.

Criptografía y funciones algorítmicas hash.

Es necesario detenerme en el funcionamiento técnico, por lo menos de forma elemental, de la criptografía, con especial énfasis en la que tiene que ver con la encriptación de información web. Es vital su explicación pues de nada sirve asegurar la legalidad establecida de un derecho fundamental si este no se garantiza frente a los fraudes que, por el contexto en el que se desarrolla dicho derecho, son muy frecuentes y sobradamente evasivos, en muchos de los casos, respecto a los poderes facticos de seguridad y control.

Primeramente, y para situarnos, podemos decir que la criptografía es una de las tantas ramas que constituyen, en la actualidad, las matemáticas. Esta variable se ha empleado en múltiples campos, pero destacan el de la informática y telemática pues es donde, precisamente, se puede aprovechar de forma pragmática los algoritmos

desarrollados para cifrar y proteger archivos y mensajes. A esto se le conoce como criptosistemas y permite asegurar la confidencialidad, la integridad del mensaje y la autenticidad del emisor (Blain Escalona, LS., & Vázquez Inclán, IL., 2012).

Hay diversas maneras de hacerlo, una de ellas es la función hash, de la que podemos distinguir diversos algoritmos, algunos de los más utilizados en la historia son el SHA-1[72], junto con SHA-2 (algoritmo hash seguro especificado por la FIPS (Federal Information Processing Standard)) y MD5[73] (Donohue, 2021). Tambien se diferencian funciones como el hashing por residuo, por cuadrado medio, por pliegue, etc. (López & Arauz, s. f.).

Siendo generalistas, la f. hash es un algoritmo matemático capaz de transformar un bloque de datos de longitud arbitraria o una cadena binaria entrante en una nueva serie de caracteres de salida con una longitud fija (National Institute of Standards and Technology, 2017) (o variable dependiendo del tipo de hash empleado), en este caso 40, independientemente de la extensión de la serie que se esté encriptando.

El uso del hash es diverso (emisión de certificados, firmas digitales…), pero una de las funciones vitales es la encriptación de contraseñas. Este aspecto no es menor ya que garantizar la protección de las contraseñas frente a la piratería y los ciberdelincuentes es imprescindible por tal de que los datos personales no queden al descubierto y, en consecuencia, no se puedan, en una gran mayoría de casos, ni tan siquiera rastrear.

Los servicios en línea legítimos no almacenan las contraseñas en texto claro/plano, sino que lo hacen bajo el valor hash de estas, por ello mismo, cuando debes recuperar una contraseña olvidada, la página en cuestión no puede enviártela y debe rastrearte bajo un código de recuperación y, normalmente, el uso del mail de usuario u otro alternativo.

Esta herramienta también se utiliza para la detección de malwares o virus informático o la integridad de los mensajes. Este algoritmo nos protege doblemente,

[72] NIST desaprobó el uso de SHA-1 (https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/archive/2015-11-06) en 2011 y prohibió su uso para firmas digitales a fines de 2013, según Wang et. al ataque y el potencial de ataque de fuerza bruta. En diciembre de 2022, NIST publicó el plan de transición del uso limitado actual del SHA-1 (https://csrc.nist.gov/news/2022/nist-transitioning-away-from-sha-1-for-all-apps). (National Institute of Standards and Technology, 2017)

[73] desarrollado por Ron Rivest en el 92, mejora respecto al MD4 y MD2 (1990), es más lento pero con mayor nivel de seguridad. Resumen de 128 bits. Aunque está obsoleto desde 2005 su algoritmo constituye la base de otras funciones.

en primer lugar, cifran nuestros datos de cara al receptor que los almacena en una base de datos, por lo que no tendrá conocimiento directo del contenido, y, en segundo lugar, en caso de una exposición o vulneración de la base de datos, los cibercriminales solo tendrían acceso a las contraseñas “hasheadas”. Ahora bien, es necesario que la contraseña introducida en texto plano sea segura, es decir, una clave robusta, ya que el hash que ira asociada a ella no será desencriptadle, sin embargo, si introducimos una débil, ejemplo: “123456” o “contraseña”, los hashes que tienen asignados suelen estar incorporados en los sistemas de crackeo de hashes en línea (López, A. 2022).

Como hemos indicado, no solo existen funciones hash de longitud fija, también las hay de salida ampliable, como las cuatro funciones derivadas de SHA-3: cSHAKE, KMAC, TupleHash y ParellHash, que, a diferencia del resto admiten salidas de longitud variable (Kelsey et al., 2016).

A modo de conclusión diremos que la fortaleza de la función hash, además de la encriptación de la contraseña y detección de virus, es la creación de una firma digital, denominada también como función resumen o huella digital. Este hecho imposibilita la falsificación y, por lo tanto, garantiza la integridad de la información. No obstante, hay que tener en cuenta que pueden darse lo que se denominan como colisiones, que, de una manera sencilla y simplificada podemos entenderlo como la existencia de dos ficheros con el mismo resumen criptográfico (Blain Escalona, LS., & Vázquez Inclán, IL., 2012), este hecho y otros muchos son los que empujan a seguir desarrollando algoritmos criptográficos que den seguridad a nuestros datos frente a una delincuencia cada vez más adaptada.