TESIS DOCTORAL

2019

VIGENCIA DEL DERECHO EUROPEO DE PROTECCIÓN DE DATOS PERSONALES

CAROLINA MARCELA REYES KAHANSKY

PROGRAMA DE DOCTORADO EN UNIÓN EUROPEA

DIRECTOR: Dr. LUCRECIO REBOLLO DELGADO

A mis padres, mis hermanos y José, que han llenado de vida y riqueza mi pasado y mi presente.

A Lucrecio, que con su paciencia y comprensión infinitas y su sabiduría certera ha sabido llevarme a buen puerto.

ÍNDICE

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
APD	Autoridad de protección de datos
BCR	Normas corporativas vinculantes (por sus siglas en inglés: *Binding corporate rules*)
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CEPD	Comité Europeo de Protección de Datos Personales
CNIL	Comision Nationale de l'Informatique et les Libertés (autoridad francesa de protección de datos)
DUDH	Declaración Universal de los Derechos Humanos
EDPB	Comité Europeo de Protección de Datos Personales (por sus siglas en inglés *European Data Protection Board*)
EEE	Espacio Económico Europeo
G29	Grupo de Trabajo del Art. 29
GPS	Global Positioning System
ICO	Information Comissioner Office (autoridad británica de protección de datos)
IoT	Internet de las Cosas (por sus siglas en inglés: *Internet of things)*

LO 3/2018	Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales
LOPD 15/99	Ley Orgánica 17/1999, de 5 de diciembre, de protección de los datos de carácter personal
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal
PNR	Registros de nombres de pasajeros (por sus siglas en inglés *passengers name records*)
RGPD	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.
SEPD	Supervisor Europeo de Protección de Datos Personales
STC	Sentencia del Tribunal Constitucional Español
TC	Tribunal Constitucional del Reino de España
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TJCE	Tribunal de Justicia de las Comunidades Europeas
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tratado de la Unión Europea
UE	Unión Europea

INTRODUCCIÓN

El objetivo de esta tesis es, como su título lo indica, investigar la vigencia del derecho de protección de datos personales en los entornos en que la investigación se desarrolla: El derecho de la Unión Europea y el español. Vigencia entendida en un sentido amplio, es decir tanto en el aspecto material como en el territorial y, con respecto a determinadas particularidades, en sus aspectos objetivo y subjetivo.

Sin perjuicio de que el enfoque es, como acabamos de expresar, el del sentido amplio de la vigencia, haremos una especial incidencia en el aspecto territorial debido a que la protección de datos personales se diferencia de otras ramas del derecho por las particulares características que presenta, que responden especialmente al hecho de que se trata, en su mayoría, de relaciones jurídicas intermediadas por la tecnología, la informática y las comunicaciones. En otras palabras, es un ámbito del derecho especialmente relacionado con la tecnología que, como tal, cuenta con algunas características que lo diferencian del derecho que llamamos "*tradicional*", que es para nosotros aquél en cuya configuración la tecnología no ejerce una influencia decisiva.

En el derecho tradicional, el factor territorial se halla en la esencia misma de los distintos tipos de normas que componen sus dos grandes vertientes: El nacional y el internacional, que lo presuponen desde su misma definición ya que ambos se basan en la formación jurídico-política del Estado, del cual el territorio es uno de sus elementos esenciales. En este sector del derecho, las *conexiones* que determinan la aplicación de las normas remiten, ya sea en forma directa o indirecta, a un determinado punto geográfico

perfectamente determinado: Nacionalidad, domicilio, residencia, *lugar* de ejecución, *lugar* de celebración, *lugar* de prestación, etc. Por el contrario, en el derecho relacionado con la tecnología, las relaciones jurídicas que constituyen su objeto están compuestas por elementos cuya localización es indiferente e incluso debe ser obviada para que las normas cumplan los objetivos fijados, pues la extensión, facilidad y rapidez de las conexiones hacen que el elemento territorial pierda en este ámbito la importancia que tiene para el resto del derecho.

A su vez, el objeto protegido por la rama jurídica investigada (es decir, los datos personales) son bienes inmateriales que juegan un papel esencial en la protección de la dignidad del ser humano y de otros valores igualmente fundamentales, pero a la vez tienen un alto valor económico para terceros y se pueden comunicar ilimitadamente sin que ninguno de los sujetos que los ha tenido bajo su dominio lo pierda. En otras palabras, estos bienes personalísimos pueden en cierto sentido *desprenderse* de su titular y *tener vida propia*. Una gran parte de esa *vida propia* se desarrolla en un espacio que no está ligado a ningún territorio: El *ciberespacio*, sobre el cual ampliamos información y valoración a lo largo de la tesis.

Las observaciones precedentes provocan la necesidad de determinar las principales características generales del derecho de protección de datos de la Unión Europea, así como las soluciones que éste articula para compensar esa falta de importancia del elemento territorial que puede afectar a los datos personales, de qué manera protege a las personas físicas de una actividad que no tiene territorio y, por lo tanto, tampoco fronteras ni límites jurisdiccionales e, igualmente, si estas soluciones son acertadas.

A pesar de que la Unión Europea surgió como una organización eminentemente económica en cuyas primeras etapas de organización los derechos y libertades fundamentales desempeñaban un rol casi inexistente, en su conformación actual éstos son una parte primordial de su sistema jurídico; y entre esos derechos y libertades la protección de datos personales no juega un papel menor pues, además de ocupar su lugar en la Carta, es una competencia atribuida en virtud de los arts. 39 TUE y 16 TFUE. Esa importancia que ha cobrado la protección de los datos personales como derecho fundamental y a la vez competencia específica de la Unión se debe a que, como hemos expresado, en la actualidad los datos (tanto personales como no personales) poseen un alto valor económico que no es desaprovechado por las empresas y, por ello, forman una parte hoy imprescindible para la vida económica del mercado europeo. A causa justamente de ese valor económico y de la utilización de los datos personales por parte de las empresas para su desarrollo económico, esta rama del derecho consiste en última instancia en la regulación de la limitación de la libertad de empresa a favor de la protección de las personas físicas en relación con los tratamientos de sus datos personales pues si no se limitara esa libertad, los individuos quedarían en situación de grave vulnerabilidad frente a la manipulación de su información personal.

En la Unión Europea se han dictado dos series de regulaciones de derecho derivado de protección de datos: La primera cuya norma principal era la Directiva 95/46, que tuvo el mérito de abrir el camino para la introducción de este derecho en la Unión y, la segunda, formada por el conocido como "paquete de protección de datos", del cual sobresale el RGPD o Reglamento 16/679. Entre la aprobación de la primera y la segunda de las normas citadas habían transcurrido apenas veinte años, tiempo que para el derecho tradicional es un plazo breve, pero los avances tecnológicos provocan que para el derecho

relacionado con este sector sea un lapso en el cual, si las normas no están preparadas para integrar las novedades, queden obsoletas. Eso ocurrió con la Directiva 95/46, motivo que provocó su reemplazo por una norma que está más preparada para abarcar cambios tecnológicos, si bien en algunos aspectos puede ser mejorada, como por ejemplo en cuanto a su eficacia respecto de tratamientos de datos personales realizados por empresas no establecidas en la Unión y a las cuales resulta aplicable; la complejidad y dificultad de aplicación de las disposiciones sobre competencias extraterritoriales de las autoridades de protección de datos; la no aplicación provisional a las comunicaciones electrónicas hasta el dictado de la nueva norma que regule esta materia, y otros que se estudian a lo largo del trabajo.

Por su parte en el derecho español, aunque no está expresamente reconocido en la CE, se considera a la protección de datos personales como un derecho implícito en el art. 18.4 y está regulado por una Ley Orgánica, como corresponde a todo derecho fundamental. Nuestro sistema jurídico ha conocido tres series de regulación de la protección de datos personales: La LORTAD, de 1992, anterior a la Directiva 95/46; la LOPD, de 1999, que transpuso la norma europea al ordenamiento jurídico interno y la LO 3/18, de muy reciente aparición, de adaptación al RGPD. Especialmente con respecto a esta última disposición, a nuestro juicio, el legislador español ha perdido una oportunidad de introducir (dentro del margen que el RGPD permite, cuya estrechez admitimos) disposiciones que incorporen flexibilidad y amplitud a determinados aspectos que en derecho europeo no ha sido posible introducir debido a la dificultad de las negociaciones parlamentarias a causa de la diversidad social y política europea, circunstancia que podía ser superada en el ámbito nacional.

A pesar de las deficiencias que hemos marcado tanto en las disposiciones europeas como internas, ello no quiere decir que la valoración del derecho vigente en estos ámbitos sea negativa; muy por el contrario, la apreciación final es altamente positiva, lo que se debe en parte a las autoridades de protección de datos personales, tanto nacionales como europeas, que realizan una excelente labor como fuentes de interpretación y aplicación del derecho, indispensables para la adaptación de las normas a la realidad social contemporánea.

Finalmente las operaciones en las que se advierte en su mayor magnitud la necesidad de superación de los límites territoriales en derecho de protección de datos personales son las transferencias internacionales, en cuya regulación se aprecia, contradictoriamente, que el factor geográfico estuvo muy presente en la mente del legislador europeo, hecho que quita efectividad a este aspecto pues para proteger los datos personales que son sometidos a estos tratamientos es imperioso pensar en términos de ciberespacio y no de espacio geográfico.

Para el estudio de los aspectos precedentemente destacados la metodología consiste en la exposición de un marco teórico referencial sobre los orígenes, la corta evolución, las definiciones básicas de esta disciplina y su ubicación en el orden jurídico europeo, aspectos indispensables para la comprensión de la necesidad que precedió a su nacimiento como rama específica del derecho y para enmarcar el objetivo de la investigación. Ese marco teórico se distribuye entre el Capítulo I, con los antecedentes cronológicos y lógicos del derecho de la protección de datos personales, así como la naturaleza jurídica de las normas que regulan distintos aspectos de esta especialidad que son relevantes para esta investigación, y en el Capítulo II, en el que se ubica al derecho de protección de datos personales en el contexto del sistema jurídico de la Unión Europea.

En el capítulo III se analiza la principal norma exponente de este derecho en la Unión Europea, el Reglamento General de Protección de Datos Personales, que en la actualidad contiene los principales ingredientes que conforman la especialidad estudiada en el ámbito de la Unión y, en el Capítulo IV, las normas internas de incorporación del derecho europeo al derecho español. Del análisis de los aspectos más generales de estas normas y, especialmente, aquéllos que tienen relación con sus aspectos geográficos, se pretende extraer, a través del método deductivo, las características generales de esta especialidad jurídica y las causas de su especial configuración.

El actual derecho de protección de datos personales en la Unión Europea no puede entenderse sin la existencia y actuación de las autoridades de protección de datos, motivo por el cual dedicamos el Capítulo V a su regulación, a la importancia que tienen para la eficacia de las disposiciones de su aplicación y a las circunstancias que deberían tenerse en cuenta para mejorarla.

En el capítulo VI se expone y analiza la regulación del aspecto que, en la concepción de la autora, más aristas presenta en relación con el objeto de esta investigación: Los flujos internacionales de datos personales, o *transferencias* tal como las denomina el derecho vigente.

En resumen, la investigación se centra sobre la configuración de los aspectos generales del derecho de protección de datos personales de la Unión Europea, que se pueden deducir de las normas positivas anteriores y las actualmente vigentes.

En cuanto a las fuentes utilizadas, para los aspectos más genéricos o teóricos del Capítulo I y el Capítulo II se ha utilizado, principalmente, fuentes doctrinales y análisis del derecho positivo de la Unión, tanto el que está vigente en la actualidad como algunas normas que

si bien ya no están vigentes constituyen antecedentes de interés para el análisis y proyectos de modificación.

Para la investigación en los aspectos más específicos, además de las fuentes jurídicas directas que se han mencionado (el derecho positivo vigente, antecedente y proyectos de modificación) se ha analizado también la jurisprudencia del Tribunal de Justicia de la Unión Europea y, en menor medida, sentencias del Tribunal Europeo de Derechos Humanos y del Tribunal Constitucional español.

Se ha analizado igualmente una fuente jurídica que, si bien no es vinculante, contiene una riqueza excepcional en cuanto a la interpretación de las normas de protección de datos: Los documentos elaborados por los distintos organismos, tanto europeos (Grupo de Trabajo del Art. 29 sobre Protección de Datos, Comité Europeo de Protección de Datos y Supervisor Europeo de Protección de Datos) como español (Agencia Española de Protección de Datos).

Han sido de igual importancia las fuentes doctrinales que, si bien en la materia de la protección de datos son escasas en comparación con otras ramas tradicionales del derecho debido a que su autonomía como rama jurídica y desarrollo es muy reciente, han sido de suma utilidad para la clarificación y valoración de las normas positivas.

Queremos hacer una aclaración muy breve sobre la terminología que utilizaremos en esta tesis, respecto a la diferencia que concebimos en la protección de datos como materia de investigación y conocimiento en el campo de la ciencia jurídica, que denominamos *Derecho de protección de datos personales* y el derecho fundamental y subjetivo que concebimos como *Derecho a la protección de datos personales*. Si bien admitimos que esta es una distinción muy sutil entre ambos, tanto que en algunas ocasiones es imposible

discernir entre uno y otro concepto, intentamos mantener la distinción cada vez que se hace mención a uno u otro.

CAPÍTULO I. DERECHO A LA PROTECCIÓN DE DATOS PERSONALES.

1. Su origen como manifestación del derecho a la vida privada.

Para comprender el origen y contenido del derecho a la protección de datos personales debemos remontarnos, en primer lugar, al derecho a la vida privada o a la intimidad, del cual es una manifestación[1].

El derecho a la intimidad no toma forma como derecho autónomo hasta la última década del Siglo XIX y principios del Siglo XX, aunque algunas de sus manifestaciones, tal como la libertad religiosa, ha tenido algún reconocimiento positivo aislado desde la antigüedad, en el Edicto de Milán del año 313, de los emperadores Constantino y Lucinio. En la Edad Media aparece en la obra de San Agustín y, bajo la forma de "*paz de la casa*" o, como lo llamaríamos hoy, inviolabilidad del domicilio, en algunos textos de las Cortes de Castilla y de León[2].

[1] Rebollo Delgado, L: *Protección de datos en Europa, Origen, evolución y regulación actual*. Ed. Dykinson, Madrid, 2018. Pp. 24-53.

[2] Rebollo Delgado, L.: *Vida privada y protección de datos en la unión europea.* Ed. Dykinson. Madrid, 2008. Pp. 32-33.

Posteriormente, en la Edad Moderna aparecen otras formas, como la libertad de conciencia, la confidencialidad de las comunicaciones y la intimidad corporal[3], si bien estas últimas responden más a la idea de seguridad antes que a la de intimidad[4].

A medida que va evolucionando la sociedad, principalmente en el marco del estado de derecho y la protección del individuo frente al poder del Estado, las expresiones descritas van dando lugar a un nuevo valor digno de protección jurídica: Se trata de un ámbito o esfera de la vida de las personas, en el cual se cuentan los sentimientos religiosos, el domicilio familiar y la correspondencia privada pero también otros elementos respecto a los cuales existe la necesidad de preservar para uno mismo. Ese sentimiento o necesidad evoluciona hasta convertirse en un derecho autónomo en la jurisprudencia norteamericana de principios del Siglo XX[5]: el derecho a la vida privada o a la intimidad, que posteriormente pasa a las declaraciones internacionales de derechos[6]. Instrumentos tales como la Declaración Universal de los Derechos Humanos (en adelante DUDH), de 1948 (art. 12), el Convenio Europeo de Derechos Humanos de 1953 (en adelante CEDH, art. 8), el Pacto de Derechos Civiles y Políticos de 1966 (art. 17), contienen disposiciones que elevan a la categoría de derecho fundamental la protección de la vida privada de las personas.

---

[3] Ibidem, pág- 33.

[4] Rebollo Delgado, L: *El derecho fundamental a la intimidad*. 2ª Edición, Ed. Dykinson, Madrid, 2005. Págs. 85 a 90.

[5] Ibidem, pp. 91-97. Megías, J.J.: "Privacidad en la sociedad de la información". Persona y Derecho, Vol. 59. 2008. Pp. 205-251. Este autor, en la pág. Explica que fue en el año 1873 cuando una sentencia de un tribunal norteamericano utilizó por primera vez la palabra *privacy*, aunque "*Tras una serie de sentencias titubeantes y contradictorias, la dictada en 1905 por la Corte Suprema de Georgia en el caso Pavesick v. New England Life Insurance Company seria decisiva*" para la configuración de la privacidad como un nuevo derecho (pág. 210).

[6] Rebollo Delgado, L: *Vida privada y protección de datos*… cit, pág. 34.

Así, la Declaración Universal de Derechos Humanos garantiza en su art. 12 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*", texto del cual se infiere que los derechos a la inviolabilidad del domicilio, a la confidencialidad de la correspondencia, a la honra y reputación forman parte del derecho a la vida privada en el ámbito de vigencia de este instrumento.

Por su parte el artículo 8 del CEDH en su apartado 1 asegura el respeto a la vida privada y familiar, al domicilio y la correspondencia. En el apartado 2 dirige dicha protección en exclusiva contra la injerencia de las autoridades públicas en dichos ámbitos, que sólo puede efectuarse si está prevista por ley y constituye "*…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 de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*". Es decir, que esté justificada, entre otros motivos, por un listado taxativo de intereses públicos. A pesar de que a priori esta protección esté dirigida exclusivamente contra las injerencias estatales, como no podía ser de otra forma, el Tribunal Europeo de Derechos Humanos (en adelante "TEDH") otorga una interpretación amplia al derecho a la vida privada o privacidad extendiendo la protección a los ataques provenientes de individuos o personas de derecho privado y a algunos elementos relacionados con la identidad de una persona, tales como su nombre y su imagen personal, así como también su integridad física y moral[7]. Tribunal que ha manifestado asimismo que del art. 8 del CEDH se infieren para el Estado obligaciones positivas para adoptar las medidas

[7] Caso *Rubio Dosamantes c/España*, sentencia de 21/02/2017 (apartado 26) y jurisprudencia citada.

necesarias para garantizar la protección de este derecho, entre las cuales se encuentra la de hallar un equilibrio entre el derecho a la intimidad y la libertad de expresión, protegida a través del art. 10 CEDH[8], artículo que a su vez, en su apartado 2, dispone que el Estado puede limitar la libertad de expresión bajo condiciones similares a las que ya hemos transcrito del artículo apartado 2 del art. 8, a los que se suma la de "*impedir la divulgación de informaciones confidenciales*"[9], disposición en la cual el TEDH interpreta que se incluye la protección de la vida privada o la reputación de las personas. El Tribunal Constitucional español también ha tenido ocasión de pronunciarse respecto a este tema, declarando que el derecho a comunicar libremente la información puede verse limitado por el derecho a la intimidad personal y familiar, incluso tratándose de personas públicas[10].

Al igual que muchos de los derechos fundamentales establecidos en éstos y otros instrumentos internacionales, el derecho a la intimidad es un corolario natural del reconocimiento de la dignidad humana y es inescindible del derecho a la formación de la propia personalidad[11].

Según Rolla[12] la evolución que ha transitado la protección constitucional de la privacidad abarca desde la primera etapa en que era considerado un derecho de naturaleza negativa "*estrechamente vinculada al derecho de propiedad o* "*ius excludendi alios*", que se centra en el derecho a no sufrir intromisiones externas, a otro de naturaleza positiva "*que toma*

[8] Ibidem, apartado 27.

[9] Además de la de "garantizar la autoridad y la imparcialidad del poder judicial".

[10] STC 197/1991 de 17 de octubre, de la Sala Segunda, en el recurso de Amparo 492/1989, FJ 4.

[11] Ibidem, FJ 3; vid también Hemann da Rosa, T. y Rigo Ferrari, G.M: "Privacidade, intimidade e proteçào de dados pessoais". Argumenta, nº 21 (2014), pág. 145.

[12] Rolla, G: "El difícil equilibrio entre Derecho a la información y la tutela de dignidad y la vida privada". En Derecho y Persona, nº 44 (2001), Pp. 263-268.

conciencia de la imposibilidad de permanecer ajenos al proceso informativo activado por la impresionante aceleración de las innovaciones tecnológicas…", como la facultad de definir la propia personalidad o identidad por medio del control de la circulación de datos relacionados con uno mismo.

Ahora bien, el contexto en el que comienza a gestarse la preocupación por la protección de los datos personales se inicia a mediados del S. XX, época en la que el avance de la tecnología comienza a dar como resultado los primeros ordenadores y programas de tratamiento de datos de uso civil y comercial, de forma veloz, a gran escala y con efectos predictivos del comportamiento de los individuos, como fueron los pronósticos para las elecciones presidenciales de Estados Unidos de 1950 y 1960. En 1968 la electrónica IBM introduce el primer sistema de gestión de bases de datos, tanto técnicos como personales, cuyo "*tratamiento informático multiplicaba exponencialmente el uso de esa información y como consecuencia, la posible lesión de derechos individuales*" [13].

Así, a finales de la década de los '60 y principios de los '70 del siglo pasado comienza a nacer en la doctrina norteamericana la preocupación por la amenaza que los tratamientos informatizados de datos personales representan para la vida privada de las personas, preocupación que va aumentando a medida que se va desarrollando y extendiendo el uso de la técnica. Relacionadas con esa preocupación comienzan a surgir las primeras normas de protección de datos personales, aunque no en Estados Unidos sino en Europa, con la *Datenschutz* del Land alemán de Hesse en 1970 y la Data Lag de Suecia en 1973, que se referían a ficheros de carácter público debido a que en esos años el uso de la informática

[13] Rebollo Delgado, L: *Vida privada*... cit., pág. 85.

por el sector privado en Europa aún no se había extendido lo suficiente como para constituir una amenaza a los derechos de las personas.

Anteriormente, en 1968, el Consejo de Europa había dictado la Resolución 509 "*que tiene como finalidad poner de manifiesto la posible confrontación entre derechos humanos y los nuevos logros científicos y técnicos*", a la cual en años posteriores le siguen otras dos Resoluciones del Consejo de Ministros del Consejo de Europa[14] que tienen como objetivo recomendar a los Estados miembros "*tomar determinadas precauciones para evitar el uso indebido o abuso de los datos de carácter personal incluidos en bancos de datos…*"[15], tanto en el sector privado como en el público. Es en el seno de esta organización que, a principios de la década de 1980 (concretamente, en 1981) se firma el primer y hasta ahora único instrumento internacional de protección de datos personales: El Convenio 108, que analizaremos en profundidad en el Apartado 2 del Capítulo II de este trabajo.

La tecnología continúa evolucionando en los años siguientes especialmente con respecto a la conexión, a través de la red telefónica, de ordenadores distantes entre sí, por ordenadores individuales en un principio para avanzar luego hacia la formación de redes de ordenadores. Llegamos así al nacimiento de INTERNET a finales de la década de los '80, solapándose con la generalización del uso de los ordenadores personales, no sólo para actividades productivas sino también de comunicación y ocio.

Durante esos años se va haciendo cada vez más evidente que no sólo el tratamiento, sino también la comunicación de los datos personales se va realizando a mayor escala, de

[14] Resoluciones Nº 73, de 26 de septiembre de 1973, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado y Resolución Nº 74 de 20 de septiembre de 1974, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público.

[15] Ambos resaltados en itálicas corresponden a Rebollo Delgado, L: *Vida privada…* cit, pp 86-87.

manera cada vez más veloz y más fácilmente, lo que despierta tanto en la Unión europea como en los Estados miembros la inquietud por la regulación de esta nueva amenaza a los derechos fundamentales. Así, se generaliza la aprobación de normas con ese objetivo, tales como la LORTAD en España y la Directiva 46/95 en la Unión Europea, normas cuyo estudio abordaremos en el próximo capítulo.

En resumen, podemos atribuir a la evolución de la informática, las comunicaciones y, en definitiva, de la tecnología, la formación del derecho a la protección de datos personales a partir del derecho a la vida privada, si bien posteriormente el primero de los derechos mencionados adquiere autonomía al configurarse como garantía para la protección de otros valores fundamentales[16]. Pues se hizo evidente que la generalización, facilitación y aceleración del tratamiento y, especialmente, de la combinación, utilización y comunicación de datos personales por terceras personas permitían a éstas la invasión de la esfera íntima o privada de la vida del individuo, aquella que se quiere reservar sólo para sí, que se desea detraer del conocimiento de las demás personas o de personas ajenas a su círculo más cercano. Por todo ello las operaciones sobre datos personales constituyen verdaderas amenazas a su vida privada, cuya protección constituye un derecho fundamental en Europa, tal como afirma Megías[17]: "… *la persona… tiene también la necesidad de volverse hacia su interior y meterse dentro de sí. No solemos adoptar nuestras decisiones de un modo irreflexivo, instintivamente, sino que éstas suelen ser el resultado de un proceso racional interno en el que han intervenido sentimientos, formas*

[16] Rebollo Delgado, L: *Vida privada...* cit, pág. 100. Rolla, G: Op. cit, pp. 251-285. También De Terwangne, C: "Internet Privacy and the Right to Be Forgotten/Right to Oblivion". En: "VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet" [monograph online]. IDP. Revista de Internet, Derecho y Política. No. 13, pp. 109-121. UOC. http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_eng ISSN 1699-8154

[17] Megías, op. Cit. Pág. 214

de pensar, deseos, anhelos… que normalmente no deseamos revelar a los demás." Esa privacidad o esfera íntima es lo que se protege a través del control de los datos personales pues, como el mismo autor afirma posteriormente, "*… un dato conocido públicamente, pero aislado, puede ser inocuo, pero puesto en conexión con otros datos también públicos puede revelar el perfil íntimo de una persona.*" [18]

2. Concepto y contenido.

En Europa, al igual que ha ocurrido con otros derechos fundamentales, fue la jurisprudencia la que, cuando aún no existían normas específicas, comenzó por considerar a la protección de datos personales como un derecho implícito en el de intimidad y por tanto, protegido por convenios internacionales y constituciones nacionales con el rango de derecho fundamental. Así, tanto la jurisprudencia del Tribunal Europeo de Derechos Humanos como de los Tribunales Constitucionales de los Estados europeos fueron reconociendo la protección de los datos personales como un derecho fundamental, con base en el Artículo 8 del CEDH, que hemos analizado en el apartado anterior.

Ahora bien, tal como hemos visto, al menos hasta mediados del siglo XX el derecho a la intimidad en su versión positiva se manifestaba en la libertad religiosa y de conciencia, la inviolabilidad del domicilio y la confidencialidad de las comunicaciones. No es hasta después de la época indicada que el crecimiento demográfico, la modernización del Estado y de las administraciones públicas y los avances de la técnica comienzan a extender los tratamientos de los datos personales, lo que da nacimiento al derecho a la

[18] Ibidem, pág. 217.

protección de dichos datos o, tal como lo enuncian los instrumentos internacionales y europeos, a la protección de las personas físicas en relación con el tratamiento de sus datos personales.

El derecho a la protección de datos personales consiste en otorgar protección a las personas físicas para que éstas no se vean invadidas de forma no deseada a través de la utilización de sus datos personales[19] o, como lo ha definido el TC: "*... consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso… poderes de disposición y control.. que… se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso...*" [20].

Esta definición del Tribunal Constitucional contiene los elementos esenciales de la protección otorgada por este derecho fundamental al interesado: Conocimiento o información y poderes de control, disposición y oposición, pues además de su aspecto negativo (la exclusión de terceros del ámbito de intimidad del individuo), la protección de datos personales cuenta también con una forma positiva en el denominado derecho a la autodeterminación informativa, que consiste en el control sobre los propios datos o sobre la información generada por una persona[21].

[19] Rebollo Delgado, *Vida privada…* cit,. Pp. 72-73.

[20] STC 292/2000, de 30 de noviembre, FJ 7.

[21] Megías, op. cit, pág. 224.

Cabe remarcar que el sujeto protegido es siempre una persona física, y la protección se extiende a datos que en apariencia no tienen la capacidad de identificarla pero que, si son tratados siguiendo determinadas pautas, podrían invadir la esfera de intimidad personal[22]. En este sentido, el Tribunal de Justicia de la Unión Europea (en adelante, "TJUE") ha declarado que una dirección IP estática constituye un dato personal, ya que permite la identificación del usuario[23]; pero también ha declarado dato personal protegido, en determinadas circunstancias[24], a una dirección IP dinámica. Asimismo ha declarado que los metadatos de las comunicaciones también son datos personales y, por lo tanto, merecen la protección otorgada por los arts. 7 y 8 de la Carta[25].

Es un derecho de los considerados "*restringidos o sometidos al margen de apreciación por los Estados*"[26] al ser susceptible de limitaciones o restricciones establecidas por una norma jurídica o similar, siempre sometidas a determinados requisitos taxativamente determinados y a una interpretación restrictiva, como las establecidas en el art. 8.2 CEDH que ya hemos analizado.

[22] Megías, op. cit, Pág. 211

[23] Sentencia nº C-70/10, de 24 de noviembre de 2011, en el asunto « Scarlet Extended S.A. c/Societé Belge des auteurs, compositeurs et éditeurs (SABAM) », apartado 51.

[24] STJUE de 19 de octubre de 2016, en el asunto C-582/14, "Patrick Breyer c/Bundesrepublik Deutschland". La dirección IP dinámica no es información relativa a una persona física identificada ya que de ésta no se extrae en forma directa la identidad de la persona (apartado 38), sino que es un dato personal que identifica indirectamente a una persona física, susceptible de protección con respecto a un determinado proveedor de servicios de medios en línea, aunque para identificar a la persona usuaria de dicha dirección IP dinámica sea necesaria cierta información adicional que no esté en su poder pero que pueda llegar a estarlo mediante la utilización de determinados procedimientos (apartados 38 - 49).

[25] STJUE (Gran Sala) de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12 "*Digital Rights*". Apartados 26 a 29

[26] Gómez Sánchez, Y: *Constitucionalismo multinivel. Derechos fundamentales*. Ed. Sanz y Torres, Madrid, 2015. Pág. 136.

Por otro lado, el derecho a la protección de datos personales es un derecho de cuarta generación[27] o de la categoría de ciberderechos, como los denominan otros autores[28]. Bustamante Donás[29], además de compartir esta clasificación, define a esta cuarta generación por los elementos que la caracterizan, entre los cuales cita la aparición de nuevos valores, derechos y estructuras sociales (que requieren de un nuevo repertorio de principios éticos), nuevas formas de interrelación humanas a través de la tecnología y nuevas comunidades virtuales que no están aglutinadas por el territorio ni por una lengua común. La protección otorgada por este tipo de derechos que surgen de las nuevas tecnologías se extiende más allá de la intimidad, para abarcar también otros valores fundamentales, como la personalidad, la construcción de la propia identidad[30] o el honor. En un sentido más amplio, también se encuentran protegidas otras libertades tales como la de expresión y la ideológica, así como el ejercicio de los derechos políticos, económicos, educativos y laborales.

El contenido del derecho a la protección de datos personales ha estado distribuido en cuatro generaciones que en mayor o menor medida dependen de las cuatro generaciones en la evolución de los ordenadores, aunque sin coincidir exactamente con ellas[31]. En esas

[27] Gómez Sánchez, Y: Op. Cit, pp. 36-44; Bustamante Donás, J.: Op. cit.

[28] Roig, A: *Derechos fundamentales y tecnologías de la información y de las comunicaciones (TICs)*. Ed. J.M. Bosch, Barcelona, 2010. Bustamante Donás, J: "Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica". *Revista iberoamericana de ciencia, tecnología y sociedad* Nº 1, septiembre-diciembre 2001.

[29] Bustamante Donás, J: Op. Cit.

[30] Rebollo Delgado, L: *Vida privada...* cit, pág. 100. Rolla, G: Op. cit, pp. 251-285. También De Terwangne, C: "Internet Privacy and the Right to Be Forgotten/Right to Oblivion". En: "VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet" [monograph online]. IDP. Revista de Internet, Derecho y Política. No. 13, pp. 109-121. UOC. http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_eng ISSN 1699-8154

[31] Rebollo Delgado, L: *Videa privada…* Cit, pp. 90-95.

cuatro generaciones, el contenido de este derecho varió desde la orientación a la protección frente al uso ilegítimo de los datos personales exclusivamente por parte de los poderes públicos, basada en un aspecto geográficamente localizado y en restricciones al acceso y uso[32], hasta la actual situación en que la protección se dirige tanto a la utilización de los datos personales por parte de los particulares como por parte de organismos públicos y trasciende todo ámbito geográfico.

Al igual que muchos otros derechos fundamentales, la protección de datos personales entra en colisión con otros derechos y libertades: la libertad de expresión y de información, la libertad de empresa y la propiedad intelectual. Colisión para cuya resolución la normativa europea establece algunas reglas básicas, si bien será el derecho y las autoridades de cada Estado parte quienes deben otorgar una solución concreta a los problemas que surjan en la práctica, para lo cual cuentan, además de las disposiciones del Reglamento, con la jurisprudencia del Tribunal de Justicia de la Unión Europea[33].

Como ha ocurrido siempre en la historia del derecho, la norma aparece una vez que se percibe en la sociedad la necesidad de una protección determinada y, en este sentido, la protección de datos personales es un derecho reciente que no surgió hasta que el desarrollo de la tecnología hizo necesaria una especial protección frente a la facilidad y rapidez de la recolección, combinación, utilización y comunicación de información personal sobre los individuos constituyó una intromisión en la esfera más íntima de las personas, lo que no ocurría anteriormente.

[32] Ibidem, pág. 89.

[33] Por ejemplo en los casos Scarlett (apartados 51 a 53), Promusicae (apartados 47 a 54), Satakunnan (apartados 53 a 62) y otros.

Por eso cuando dicha amenaza fue advertida por la doctrina y la jurisprudencia, para dar respuesta a la misma se utilizó la herramienta con que se contaba en ese momento, que era el derecho a la vida privada, del cual la protección de datos personales se constituyó en otra manifestación más tal como lo eran la inviolabilidad del domicilio y de las comunicaciones, entre otras.

Desde su gestación en la doctrina, la jurisprudencia y posteriormente el derecho positivo, la protección de datos personales ha sido un derecho en continua evolución, como lo seguirá siendo mientras siga evolucionando la tecnología y se continúen descubriendo nuevas formas de tratamiento de datos personales.

Podemos poner como ejemplo de esa evolución a las redes sociales, que consideramos que están marcando una nueva generación en la evolución del derecho a la protección de datos personales y, especialmente, en el concepto de vida privada acuñado por las nuevas generaciones, que hacen pública gran parte de su vida al exponerla en blogs y redes sociales[34]. En nuestra opinión, estos comportamientos no son incompatibles con la idea de privacidad sino que la redefinen, pues el deseo de compartir con el público ciertos aspectos de nuestra vida privada no excluye el interés por proteger el ámbito en el cual se producen nuestras decisiones personales, que generalmente si se hace público es de una manera inconsciente y en el que no deseamos que haya injerencias extrañas. Pues, al contrario de lo que expresan Hemann da Rosa y Rigo Ferrari[35], aparentemente existe hoy

[34] Bustamante Donás, J.: "La cuarta generación de derechos humanos en las redes digitales". TELOS. , Vol. 85. .Ed. Fundación Telefónica, Madrid, 2010. Este autor postula en este artículo la redefinición de los derechos clásicos, principalmente el de la privacidad, del que afirma que "*no puede ser entendido en estos tiempos como el derecho a un ámbito privado fuera del escrutinio del ámbito público…*", dado que el sentido de privacidad es radicalmente distinto para las nuevas generaciones de lo que lo ha sido siempre, pues viven la privacidad de una forma distinta, por ejemplo, retransmitiendo sus vidas a través de blogs, videoblogs, tweeters, etc.

[35] Hemann da Rosa, T. y Rigo Ferrari, G.M: "Privacidade, intimidade e proteçâo de dados pessoais/Privacy, intimacy and protection of personal data/Privacidad, confidencialidad y protección de datos personales."

en día una forma, si no de profanar los pensamientos, sí de manipularlos a través de medios en algunas ocasiones legítimos (como la publicidad, especialmente la subliminal) y en otras de dudosa legitimidad (las noticias tendenciosas, falsas o las noticias publicitarias).

Para finalizar este apartado añadiremos que otras formas nuevas de tratamiento de datos relativos a una persona son la inteligencia artificial y el *big data*, que pueden permitir a quienes los utilizan predecir qué decisiones adoptarán los sujetos en determinadas circunstancias, es decir, conocer aspectos de la persona de los cuales ni ella misma es consciente. Estas operaciones de predicción en base a la combinación y análisis de la información producida por un sujeto se denominan *elaboración de perfiles* y están especialmente protegidas en la regulación europea.

Merece una mención especial la tecnología denominada *internet de las cosas*[36], que consiste en "cosas" (juguetes, electrodomésticos, automóviles, etc.) que están conectadas a internet y programadas para realizar tratamientos de datos sin intervención humana. Esos tratamientos pueden incluir la recolección, almacenamiento, clasificación, combinación de datos personales y, lo que es más preocupante, su comunicación a terceros. Esta tecnología merece una especial atención ya que en ella se desdibujan los roles de responsable y encargado de los tratamientos ya que son muchas las personas que intervienen en su fabricación y comercialización y que, a su vez, puede no coincidir con el receptor de los datos que puede realizar con ellos otros tratamientos independientes. Por todo ello las disposiciones de protección de los datos personales deben ser

Revista Argumenta. no. 21 (2014). Pág. 144. Estas autoras consideran que en el ordenamiento jurídico brasileño, la personalidad, más que un derecho está configurada como un valor.

[36] "IoT" por sus siglas en inglés: Internet of Things.

suficientemente abiertas para asegurar que los datos no queden desprotegidos porque el supuesto de hecho no contemple ese tipo de casos. Asimismo deben estar preparados para proteger en el futuro a nuevas tecnologías que puedan llegar a surgir sin que en el presente podamos imaginarlas.

3. Su relación con el derecho internacional y con los aspectos territoriales del derecho.

Coincidimos con Bustamante Donás[37] que con el avance de los entornos virtuales el territorio está perdiendo importancia, no sólo como "*aglutinante de las comunidades*" sino también como "*dimensión*" en la que se plasman las relaciones humanas. En otras palabras el entorno virtual hace que el territorio pierda sentido, las interacciones humanas ya no necesitan de presencia física, lo que se traduce en que "*el territorio se desterritorializa a través del ciberespacio, aunque sea momentáneamente*", ya que vemos que las interacciones en este ámbito se ven influenciadas a la vez que influyen en la dimensión espacial física, lo que le lleva a afirmar que: "*El conocimiento que la informática y las telecomunicaciones extienden por el mundo no es una herramienta de descripción de la realidad, sino de construcción de la misma*".

No obstante, no estamos de acuerdo con este autor en cuanto denomina "*nuevos espacios territoriales*" a las dimensiones relacionales, sociales, culturales y políticas que se engendran en el ciberespacio. No se trata de una nueva forma de "territorialización" o "reterritorialización" sino de nuevas dimensiones carentes de territorio.

[37] Bustamante Donás, J.: "La cuarta generación.." Cit.

El territorio ha sido, históricamente y desde el punto de vista jurídico, el ámbito geográfico en el cual rigen los ordenamientos jurídicos nacionales de Estados independientes, que ejercen el poder dentro de su territorio de forma soberana, excluyendo la injerencia de los demás Estados. Sin perjuicio de ello, existen situaciones intermedias en las cuales los Estados aplican dentro de su territorio el derecho de otro Estado[38], por lo general para casos o situaciones concretas. Las situaciones que caen bajo el ámbito del derecho privado y cuya solución requiere que se trasciendan las normas de un determinado ordenamiento jurídico son objeto del derecho internacional privado, rama del derecho que se aplica a las relaciones jurídicas en las que existen elementos o conexiones, de suficiente intensidad, que la relacionan con más de un ordenamiento jurídico[39] o, dicho de otra forma, cuando un asunto presenta relaciones con los ordenamientos jurídicos vigentes en distintos territorios[40].

La mayor fuente en esta rama del derecho son las normas de conflicto, que son aquellas que dan solución a un caso mediante la elección indeterminada del derecho material nacional o de un derecho material extranjero[41]. Este tipo de normas constan de tres partes: La categoría o descripción de la situación[42], el punto de conexión (que es el elemento elegido para determinar el derecho aplicable) y la consecuencia jurídica, que en este tipo de normas es siempre la aplicación de un determinado ordenamiento jurídico, que puede

[38] Bobbio, N: *Teoría General del Derecho*. Ed. Temis, Bogotá, 1997. Pág. 242. Este autor denomina "*de exclusión recíproca*" a la relación entre los Estados a nivel internacional.

[39] Boggiano, A: *Derecho Internacional Privado*. Sexta Edición, Abeledo Perrot, Buenos Aires, 2011, pp. 12-13.

[40] Ibidem, pág. 35.

[41] Íbidem. Pág. 33

[42] Martínez Bretones, V: "Conflictos de leyes en el espacio. Contribución a su estudio desde la perspectiva de la teoría general del derecho". Pp. 198-199.

resultar la *lex fori* u otro ordenamiento extranjero. Estas normas que ordenan la aplicación de un derecho distinto se denominan normas de reenvío y, a diferencia del derecho material, no resuelven el fondo del asunto sino que remiten a la fuente de donde se debe extraer la norma para su resolución[43].

Dentro del derecho internacional privado encontramos, además de las normas de conflicto, las normas de policía[44], que son aquéllas que excluyen el funcionamiento de las normas de conflicto a los casos que caen bajo el ámbito de aplicación delimitado por el supuesto de hecho descrito, dando a éste una solución de derecho material.

Como veremos en el desarrollo de esta investigación, el derecho de protección de datos contiene disposiciones de derecho internacional tanto público como privado, especialmente en los siguientes aspectos:

a) En tanto que derecho fundamental, forma parte del derecho internacional de los derechos fundamentales, más especialmente desde 1981, a través del Convenio Nº 108 del Consejo de Europa (en adelante "Convenio 108"), de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.
b) El sujeto protegido por las disposiciones de este derecho es una persona física o privada y las relaciones jurídicas que conforman su objeto en una gran cantidad de casos contienen elementos que las relacionan con más de un ordenamiento jurídico, por lo que cae bajo el ámbito del derecho internacional privado.

[43] Íbidem, pp. 254-255.

[44] Sobre las normas de policía, ver Boggiano, A: Op. Cit, Pp. 205 - 215

c) Dado que una protección de los datos personales que se limitara a las conexiones exclusivamente con el territorio de la Unión permitiría el fraude de ley con suma facilidad, algunas normas buscan trascender el ámbito territorial de aplicación de este derecho[45].

Todo lo anteriormente expuesto respecto de la vigencia territorial de los ordenamientos jurídicos y las relaciones entre ellos cobra una dimensión distinta en los derechos derivados de las nuevas tecnologías, entre los cuales se encuentra el de protección de datos personales, ya que la mayoría de los tratamientos de datos personales y de las relaciones jurídicas captadas por el derecho de protección de datos no se desarrollan en un espacio geográfico determinado sino en el *ciberespacio*. O, para decirlo de otra forma, conectar estas situaciones y relaciones con un elemento territorial que es el presupuesto del derecho nacional y de las normas de reenvío no se corresponde con la realidad, debido a la *ubicuidad* de las conexiones electrónicas y a la multiplicidad de elementos con distinta ubicación geográfica que pueden llegar a formar parte de un hecho jurídico *virtual*.

Para comprender cabalmente las cuestiones relacionadas con los aspectos territoriales del ciberderecho es necesario establecer una definición o, al menos, una caracterización del espacio virtual o ciberespacio al que nos hemos referido.

Ciberespacio, según el diccionario de la Real Academia Española, es un "*Ámbito artificial creado por medios informáticos*".

El ciberespacio es una creación intelectual, una entelequia para definir las operaciones realizadas con intermediación de internet o la Red que conecta hoy en día a millones de

[45] Cfr. Capítulo VI de este trabajo, "Transferencias internacionales de datos personales".

dispositivos detrás de los cuales, en la mayoría de los casos pero no siempre, hay personas y que permite (entre otras acciones) encontrar, generar, transmitir, intercambiar y publicar información o datos que se encuentran físicamente en cualquier parte del mundo, desde cualquier otro punto del globo. Para el ciberespacio no existen fronteras[46]. Sin perjuicio de ello, las acciones realizadas en el "espacio virtual" pueden tener efectos (jurídicos o no) sobre la "vida real". Algunos efectos jurídicos de operaciones virtuales son las operaciones bancarias electrónicas, los contratos que se pueden firmar por medios electrónicos (el más frecuente, el de compraventa de mercancías o productos en línea, para que sean enviados al domicilio del comprador) e incluso en actos delictivos como el "ciberacoso", en el que la víctima sufre en la vida real las consecuencias de la actuación de otras personas en el espacio virtual[47].

En el mismo orden de ideas podemos establecer que en el ciberespacio pueden existir trabas, al modo de *fronteras* allí donde no las hay física o geográficamente, como se puede inferir de la voluntad de eliminarlas que forma parte de la estrategia de la Comisión Europea para converger hacia un Mercado Único Digital, que aboga por suprimir las diferencias jurídicas para el comercio electrónico transfronterizo, como son las normas

[46] Sin embargo sí existiría algún tipo de fronteras en el ciberespacio a través de la *geolocalización*, un recurso virtual que permite ofrecer contenidos virtuales diferenciados según el lugar geográfico o país desde el cual se consulte la red. La Unión Europea está desarrollando una estrategia contra la discriminación basada en este recurso, en su camino hacia el mercado digital único.

[47] En la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre "Una estrategia para el mercado único digital de Europa", [COM(2015) 192 final], uno de los pilares en que la Comisión basa su estrategia para el mercado único digital consiste en: "*... que se eliminen rápidamente las diferencias fundamentales entre los mundos en línea y fuera de línea para derribar las barreras a la actividad transfronteriza en línea*" (Pp. 3-4). En relación con este pilar, el 28 de febrero de 2018 se aprobó el Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior, que entra en vigor a los veinte días de su publicación, pero es aplicable a partir del 3 de diciembre de 2018.

contractuales, de protección al consumidor, fiscales y de propiedad intelectual[48], pero también las trabas técnicas, como el geo-bloqueo, para cuya eliminación se ha adoptado el Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) nº 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE.

Por otra parte, el derecho a la protección de los datos personales en tanto que también implica regulación de las nuevas tecnologías, está afectado por la desconexión regulatoria que denuncia Abbot[49], consistente en el hecho de que la ciencia y la tecnología se desarrollan a una velocidad mucho más rápida que la adopción de nuevas regulaciones, si bien es imperativo que los marcos regulatorios sean capaces de igualar esa velocidad[50]. Esta autora postula que desde hace más de dos décadas está cambiando la idea del control de la regulación como una actividad exclusivamente estatal, estamos actualmente en una etapa "*post regulatoria*", en la que actores tales como la industria, las ONGs, las asociaciones de consumidores, asociaciones industriales y las instituciones financieras

[48] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre "Una estrategia para el mercado único digital de Europa", [COM(2015) 192 final], Pág. 5.

[49] Abbot, C.: Op. Cit, pág. 2.

[50] Esta autora destaca que la desconexión regulatoria se puede producir en cualquier momento del ciclo regulatorio, desde que se llega a un consenso hasta después de la puesta en marcha de un nuevo régimen regulatorio. Al respecto nosotros pensamos que la desconexión se debe precisamente al excesivo lapso que transcurre entre esos dos momentos del proceso regulatorio ya que, al menos con respecto a la tecnología, las instituciones políticas tradicionales instauradas en todos los regímenes democráticos han quedado arcaicas. Este tema no puede ser tratado superficialmente sino que necesitaría un profundo debate en la sociedad, pero algunas de sus claves se hallan en la inercia con que se mueven dichas instituciones, que en muchos casos continúan con pautas sociopolíticas nacidas hace décadas (incluso siglos en muchos casos) y, por otro lado, también en su incapacidad para utilizar los adelantos tecnológicos en provecho de los procesos de creación de las fuentes del derecho.

poseen recursos y capacidad que les permiten mejorar el proceso regulatorio y están deseosos de utilizarlos. En este sentido, dejando por un momento de lado el ámbito jurídico, las *reglas* técnicas de uso generalizado (que carecen de implicancias jurídicas o, a lo sumo, sólo con carácter residual) establecidas por personas privadas están ampliamente extendidas por ser indispensables para los avances, muchos de los cuales serían imposibles sin reglas universalmente aceptadas tales como el lenguaje, las normas de construcción y utilización comunes o las normas o cláusulas ISO, que establecen estándares técnicos que son aplicados en todo el mundo.

4. Instrumentos europeos de Derecho Internacional

4.1. El Convenio Nº 108 del Consejo de Europa

El Consejo de Europa adoptó en 1950 el Convenio para la protección de los derechos humanos y de las libertades fundamentales (CEDH) y nueve años después se constituye el Tribunal Europeo de Derechos Humanos (TEDH), que ha realizado una muy ponderable y prolífica labor de garantía del respeto a los derechos fundamentales en Europa.

Es evidente que en la fecha en que se adoptó el CEDH, la informática aún estaba en sus etapas iniciales de desarrollo y, por consiguiente, si bien en el artículo 8 se garantiza el respeto de la vida privada y familiar de las personas, así como las dos vertientes clásicas de este derecho (la inviolabilidad del domicilio y de la correspondencia) con la fórmula: "*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*", no se reconoce explícitamente el derecho a la protección de la persona con respecto al tratamiento de sus datos personales. Aunque, si bien no lo está en

forma expresa, la jurisprudencia del TEDH lo ha considerado implícitamente incluido en el artículo citado, tal como se evidencia por ejemplo en la Sentencia Leander C/Suecia, de 1987[51], en cuyo apartado 48 el TEDH declara que el almacenamiento, la comunicación y la negativa de acceso al interesado (Sr. Leander) a un registro secreto de la policía que contenía datos relativos a su vida privada, constituían una violación del derecho a la privacidad (art. 8.1 CEDH).

No obstante esa incorporación tácita del derecho a la protección de los datos personales (en esta primera etapa, sólo para la protección del derecho a la vida privada) a través de la jurisprudencia del TEDH, la falta de reconocimiento expreso de este derecho se remedió con la adopción del Convenio Nº 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en adelante "Convenio 108"), siendo el primer y, hasta el momento, único instrumento internacional vinculante sobre el derecho fundamental a la protección de los datos personales.

El 8 de noviembre de 2001 se aprobó un Protocolo Adicional al Convenio 108, cuyo objetivo es introducir modificaciones relativas a las autoridades de control y a las transferencias de datos personales hacia estados que no sean Partes, contenidos que analizaremos junto con el texto del Convenio.

El preámbulo del Convenio 108 en la presentación general que realiza de la finalidad de sus disposiciones se refiere específicamente a dos derechos fundamentales que éstas

[51] Sentencia "Leander C/Suecia", de 26 de marzo de 1987. También aparece esta apreciación en la sentencia "S. y Marper C/Reino Unido", de 4 de diciembre de 2008, apartado 67

regularán: El derecho a la privacidad y la libre circulación de la información, que son los que se protegerán y equilibrarán en el texto.

Sin perjuicio de ello, lamentamos que en el texto del Convenio 108 no se haya incluido expresamente ninguna disposición dirigida a respetar la libertad de circulación de la información, más allá de algunas menciones genéricas a las libertades fundamentales en las que ésta se puede considerar incluida[52].

Consecuentemente con la época en la que fue aprobado, en la que el derecho a la protección de los datos personales no había adquirido autonomía, el art. 1 del Convenio 108 establece como objetivo la garantía, en general de "*... sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona*".

Ahora bien, si comparamos los dos instrumentos de derechos humanos adoptados en el seno del Consejo de Europa que hemos mencionado (CEDH y Convenio 108), notaremos que hay una diferencia fundamental en los objetivos de cada uno de ellos, ya que el CEDH tiene como objetivo el *reconocimiento* de los derechos fundamentales de los individuos por parte de los Estados firmantes (que tanto con respecto a los derechos reconocidos como a la jurisdicción del TEDH son los sujetos pasivos), es decir que son los obligados a respetarlos. El instrumento está redactado para ser invocado frente a ellos y así está entendida la competencia del TEDH.

Por el contrario, el objetivo del Convenio 108, o en otras palabras aquello a lo que se obligan las altas partes contratantes no es a *reconocer* los derechos que se enumeran en

[52] Por ejemplo el art. 1 "Objeto y fin", que garantiza el respeto a los derechos y libertades fundamentales de las personas físicas, o el art. 9.2.b), que autoriza la creación de una excepción a los principios básicos de la protección de datos, entre otras circunstancias, para la protección de las libertades de las personas.

el instrumento sino a *garantizar* sus derechos (artículo 1 del Convenio 108), para lo cual se comprometen a adoptar "*…en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos…*" (artículo 4.1. Convenio 108). Esta diferencia es importante en nuestra materia pues mientras la mayor parte de los derechos fundamentales constituyen una garantía para el ciudadano frente al poder del estado, el derecho a la protección de los datos personales no es sólo una garantía o protección ante la acción del estado sino también frente a la de personas o entidades privadas. Esta característica del derecho a la protección de datos personales se evidencia en el artículo 3.1. de la actualización del Convenio (que analizaremos más adelante) mediante el cual las Partes se comprometen a aplicarlo a todo tratamiento de datos que esté sujeto a su jurisdicción, ya sea llevado a cabo en el sector público o en el privado.

En cuanto al ámbito material, el Convenio 108 se aplica a los ficheros y tratamientos automatizados de datos personales, tanto en el sector público como en el privado y, si las partes así lo deciden y lo comunican formalmente, también a los ficheros de datos personales que no estén destinados a ser sometidos a un tratamiento automatizado (art. 3.2.c). La elección del término "automatizado" para definir el ámbito material de aplicación del Convenio 108 nos parece adecuado por ser un término lo suficientemente neutro para incorporar las nuevas técnicas que han surgido y seguirán apareciendo en el futuro, si bien lamentamos que la protección de los datos personales se limite al resguardo del derecho a la vida privada, dejando de lado la mención expresa de otros derechos y libertades fundamentales que se pueden ver amenazados por los tratamientos ilegítimos de ese tipo de datos.

El art. 2.a) da una definición de los datos personales como "*cualquier información relativa a una persona física identificada o identificable*", siendo así susceptible de

incorporar los datos que en principio no aparezcan como personales pero identificados con otros puedan dar lugar a una identificación de la persona. Acertadamente, en el artículo 6 se enumeran algunas categorías de datos especiales respecto de las cuales se prohíbe el tratamiento automatizado, lo que tiene como objetivo la protección de otros derechos fundamentales además de la vida privada, tales como las libertades religiosa, de expresión e ideológica, si bien se advierte la falta de protección para otros bienes jurídicos que pueden verse involucrados, como los derechos sociales y laborales o la protección especial a personas en situación de especial vulnerabilidad, como los menores u otros colectivos. Con posterioridad a la aprobación de este convenio han surgido categorías de datos cuyo tratamiento se ha hecho posible (como por ejemplo los datos genéticos o biométricos) y que no reciben protección especial. Por otra parte, este artículo 6 deja demasiado librada a la voluntad e interpretación de los Estados parte la determinación del carácter "*apropiado*" de las garantías que el derecho interno debe establecer para hacer posible el tratamiento de los datos de las categorías especiales, siendo lo deseable que el artículo establezca, al menos, otro criterio más concreto para el establecimiento de las garantías. Por todo ello se hacía necesaria una actualización de este Convenio, la que ya se ha producido y que analizaremos más adelante.

Con respecto a la vigencia de este instrumento y a la naturaleza de los tratamientos de datos personales que protege, debemos mencionar que su artículo 3. "*Campos de aplicación*" establece un muy complejo sistema de selección, por los estados parte, de listados de tratamientos a los que se amplía o de los que se excluye la aplicación del Convenio, haciendo de esta manera sumamente insegura su vigencia con respecto a los casos concretos, lo que no se condice con el estatus de derecho fundamental del que goza la protección de los datos personales. A su vez, el artículo 11 Convenio 108 prevé la

posibilidad de que las Partes en su derecho interno amplíen la protección otorgada por los principios y los derechos de los interesados, no refiriéndose a los tipos de tratamientos, que ya hemos visto que están regulados en el artículo 3 del Convenio.

En cuanto al espacio de vigencia del Convenio 108, como es lógico a todo tratado internacional, su aplicación se limita en principio a la jurisdicción territorial de las Partes contratantes y adherentes que, al momento de redacción de esta tesis son cuarenta y seis estados miembros del Consejo de Europa, seis estados no miembros del Consejo de Europa cuya adhesión al Convenio fue aceptada de acuerdo al procedimiento establecido en el artículo 23 del mismo y otros tres estados cuya adhesión fue aceptada pero aún no lo han ratificado[53]. También está abierto a la adhesión de la Unión Europea. Más allá de esa vigencia territorial común a los tratados en general, el art. 24 del Convenio 108 dispone que los Estados durante el trámite de adhesión podrán designar territorios a los que se aplica este convenio y aquéllos a los que no, mediante declaración que podrá ser modificada posteriormente, disposición que agrega aún más inseguridad jurídica a la que ya mencionamos al analizar el art. 3.

Como parte de esa aplicación territorial, en el art. 12.1 se denomina flujos transfronterizos a las transmisiones de datos personales desde un estado parte a otro, que se realicen por cualquier medio y siempre para ser sometidos a un tratamiento automatizado, respecto a

[53] Si tenemos en cuenta que entre los veintiocho Estados miembros de la Unión Europea se aplica el derecho de protección de datos vigente en el seno de esta organización, el Convenio 108 se aplica entre cada uno de ellos individualmente y Albania, Andorra, Armenia, Azerbaijan, Bosnia Herzegovina, Georgia, Islandia, Lichtenstein, Macedonia, Moldavia, Mónaco, Montenegro, Noruega, Rusia, San Marino, Serbia, Suiza, Turquía, Ucrania (todos ellos miembros del Consejo de Europa), Cabo Verde, Mauricio, México, Senegal, Túnez y Uruguay (estados no miembros del Consejo de Europa). Cuando se completen los trámites y términos para su entrada en vigor, también incluirá a Argentina, Burkina Faso y Marruecos. La lista de las Partes de este convenio se puede consultar en la siguiente dirección electrónica: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=Pv1WFi41 (visitada por última vez el 06/12/2018).

los cuales se adoptan algunas disposiciones que consideramos anacrónicas dado que se refieren a las "*transmisiones a través de las fronteras nacionales*" (art. 12.1), que como hemos aludido en el primer capítulo en muchos casos será un hecho imposible de determinar con precisión sin perjuicio de lo cual se continúan utilizando en los distintos niveles de fuentes jurídicas.

El art. 12.2) acoge el principio de libertad de circulación de los datos personales al vedar a las partes establecer limitaciones o prohibiciones a las transmisiones de datos "*con destino al territorio de otra Parte*". Esta disposición se basa en la lógica de que, siendo partes firmantes del Convenio, garantizarán en sus territorios una protección homogénea que sea, como mínimo, la exigida por éste. Sin embargo, a pesar de este principio establecido en el segundo apartado, el tercer apartado de este artículo acepta la posibilidad de establecer excepciones a los flujos transfronterizos de datos, en dos subapartados, de los cuales el subapartado b) acierta al autorizarlas para evitar el fraude de ley, pero el subapartado a) las permite sin más motivación que el derecho interno de los Estados partes, sin fijar criterios o motivaciones más estrictos como hubiera sido deseable.

El artículo 13 establece la designación, por cada Parte, de una o más autoridades de aplicación de este Convenio, que tendrán a su cargo la "*cooperación*" y "*asistencia*" mutuas así como la facilitación de información respecto al derecho y prácticas administrativas internos sobre protección de datos personales y, "*solamente a los efectos de la protección de la vida privada*", facilitará información sobre un tratamiento concreto que se realice en su territorio[54]. No obstante, se prohíbe que la información a que nos referimos en último lugar incluya datos personales, sólo podrá comprender el derecho y

[54] Encontramos aquí nuevamente la referencia al *territorio de realización del tratamiento* que, como ya hemos explicado, es de imposible determinación.

la práctica administrativa de la Parte solicitada y detalles fácticos relativos a uno o más tratamientos determinados.

Muy especialmente, el art. 14 dispone que a través de las referidas autoridades se prestará asistencia a las personas que tengan su residencia en el extranjero y a las que su derecho interno faculte para ejercer los derechos de los interesados, adoptados en virtud del artículo 8 del Convenio, lo que en parte suple la excesiva territorialidad de este instrumento al intentar trascender o, al menos, flexibilizar las fronteras geográficas para su aplicación.

Como hemos reseñado al iniciar este apartado, el Convenio 108 fue suscrito en 1981, año en el que la informática estaba en sus primeras etapas de desarrollo, su utilización era muy limitada en relación con la expansión actual y no se conocía aún los efectos de las conexiones entre ordenadores, de INTERNET y de otros avances ocurridos con posterioridad como la computación en la nube, el internet de las cosas y el big data.

Como ya hemos advertido, con posterioridad el derecho a la protección de los datos personales adquirió autonomía con respecto al derecho al respeto de la vida privada y se desligó su protección de la conexión territorial del derecho clásico, hechos que, por la época de su aprobación, no fueron recogidos en el Convenio 108 de forma suficiente para otorgar una protección efectiva. Además, este Convenio está predominantemente dirigido a los tratamientos de datos realizados por el estado, sus órganos y autoridades y, en definitiva, las administraciones públicas, tal como se infiere de las posibilidades que brinda el art. 3 para excluir o ampliar los tratamientos protegidos (que no se justificarían si estuviera dirigido a tratamientos realizados por personas privadas) así como del hecho que no se define a los agentes implicados en los tratamientos (responsables y encargados)

sino a la "*autoridad controladora del fichero*" como "*la persona física o jurídica, autoridad pública, el servicio o cualquier otro organismo…*"[55], lo que se debe a que regula, principal aunque no exclusivamente, la actividad del estado y sus reparticiones.

Por otra parte, así como ha evolucionado la tecnología y las modalidades de tratamientos de datos, ha evolucionado el derecho que las tiene por objeto, incorporando nuevos principios y derechos para los titulares de los datos. Por otra parte, este convenio tiene su mayor desventaja en el hecho de que se trate de un instrumento internacional basado principalmente en el ejercicio de la soberanía territorial de las partes, por lo cual le será imposible trascender ésta para regular eficazmente las relaciones con conexiones territoriales diversas.

Sin perjuicio de todo ello y del desfase que este Convenio significa para el estado actual de la cuestión, el documento bajo análisis tiene los méritos, como ya hemos adelantado, de ser el primer (y hasta ahora el único) instrumento internacional dedicado exclusivamente al derecho a la vida privada a través de la protección contra el tratamiento de los datos personales y de servir de base para los instrumentos legislativos nacionales y regionales posteriores.

Finalizando este apartado, como veremos en el siguiente el Consejo de Europa ha aprobado una actualización de este Protocolo, que ya se hacía necesaria debido a las deficiencias del que acabamos de exponer, concretamente en cuanto a la apertura hacia la protección de otros derechos y libertades fundamentales, a la aparición de nuevas técnicas de tratamientos de datos personales y de amenazas a dichos derechos y libertades, la restricción a las posibilidades de limitar la protección de los datos personales que otorga

[55] Art. 2, "Definiciones", apartado c).

este instrumento y la falta de intención de trascender las divisiones geográficas para que la protección de los datos personales sea un poco más eficaz.

4.2. El Tratado de Reforma del Convenio 108

Después de siete años de trabajo y negociaciones intensas, el 18 de mayo de 2018 el Comité de Ministros del Consejo de Europa, reunido en Elsinore (Dinamarca) en su sesión 128ª ha adoptado el Protocolo de reforma del Convenio para la protección de las personas con respecto al tratamiento automatizado de sus datos personales (Convenio 108), es decir, el protocolo de modernización de este Convenio, que fue anhelado, esperado y trabajado durante muchos años. Protocolo que se someterá a la firma de los Estados Parte del Convenio 108, con la ambición de vincular también a todos aquellos Estados que lo deseen, aunque no formen parte del continente europeo.

Según el mismo Consejo lo explica en su página web[56], esta reforma persigue dos objetivos principales: Afrontar los desafíos que emanan del uso de las nuevas tecnologías de la comunicación y de la información, y reforzar la implementación efectiva del Convenio. Como primera modificación destacable con respecto al actualmente vigente Convenio 108, este nuevo Convenio no se limita a la protección del derecho a la intimidad, sino que trata "*el derecho de la persona al control de sus datos personales y del tratamiento de tales datos*"[57] como derecho autónomo, concepto que se advierte asimismo en su art. 3.1. por el que las partes se obligan a asegurar "*el derecho de todo individuo a la protección de sus datos personales*", resaltando a continuación la necesidad

[56] https://www.coe.int/en/web/data-protection/convention108/cm-decisions

[57] Preámbulo del Convenio.

de garantizar la dignidad humana, la protección de los derechos humanos y las libertades fundamentales y, de forma original, agrega a estos valores el derecho a la autonomía personal. También se reconoce la necesidad de equilibrar este derecho con otros derechos y libertades fundamentales, tal como la libertad de expresión y el derecho de acceso a los documentos oficiales, que se mencionan expresamente en el Preámbulo.

Pasando al articulado del Convenio, el artículo 1 pone como finalidad de la misma la "*protección de toda persona… con respecto al tratamiento de sus datos personales, con el objetivo de hacer respetar sus derechos y libertades fundamentales, y en particular su derecho a la intimidad*"[58].

Es interesante observar que el artículo 2 dedicado a las definiciones, en la correspondiente a los tratamientos de datos, entre los ejemplos de operaciones consideradas tratamientos incluye "*la realización de operaciones lógicas y/o aritméticas sobre tales datos*"[59], lo que remite al procesamiento de datos por medio del big data, problema que está comenzando a visualizarse y que demandará en el futuro soluciones jurídicas más evolucionadas.

Entre las diferencias con respecto al Convenio 108, encontramos que el ámbito de aplicación material de esta Convención no se limita a los tratamientos automatizados de datos personales sino que comprende también los no automatizados "*realizados sobre datos personales dentro de un conjunto estructurados de tales datos a los que se pueda acceder o recuperar de acuerdo a criterios específicos*"[60].

[58] Artículo 1 de la reforma del Convenio, en traducción del inglés realizada por la autora.

[59] Artículo 2.b) de la reforma, aunque esta misma expresión ya se encuentra en el art. 2.c) del vigente Convenio.

[60] Artículo 2.c)

Un gran acierto de esta modificación del Convenio 108 está en su artículo tercero, que se denomina "Ámbito de aplicación"[61], no distinguiendo entre ámbito material y ámbito territorial sino que establece que se aplicará a los tratamientos de datos "*sometidos a la jurisdicción de cada Parte, en el sector público y en el privado*"[62], quedando así su aplicación como un concepto indeterminado cuya determinación, a través de la referencia a la jurisdicción de cada estado Parte, se delega al derecho interno de éstos. Consideramos que esta mención que en principio podría parecer un detalle pequeño consiste en un gran desarrollo para la materia que nos ocupa, ya que al no limitar este ámbito a las fronteras geográficas ni a ciertas materias o criterios de aplicación sino que delega su determinación al ordenamiento jurídico de éstos, permite que definan los elementos que activarán la protección del Convenio y seleccionar los elementos que conectarán los tratamientos con su jurisdicción, otorgando así a los tratamientos frente a los cuales se protegerá a las personas, la necesaria flexibilidad para adaptarse a los cambios que se produzcan en el campo de aplicación, en su mayoría avances tecnológicos pero también jurídicos.

Las partes firmantes, en el art. 4.1. se comprometen a adoptar las medidas necesarias para implementar las disposiciones del Convenio y asegurar su efectiva aplicación. Además, a permitir al Comité que el Convenio crea en su art. 6 (que será un organismo internacional), que evalúe la efectividad de las medidas adoptadas y a contribuir activamente a dicha evaluación (arts. 4.3.a y 4.3.b) lo que consiste en cierta medida, en una cesión de soberanía.

[61] "*Scope*" en inglés en el original, que hemos traducido como "ámbito de aplicación".

[62] Apartado 1. Del art. 3.

Observamos asimismo que se admiten excepciones a algunos principios y derechos de los interesados, siempre que estén establecidos en el derecho interno de las Partes y que las finalidades de los tratamientos sean el archivo en interés público o la investigación con fines históricos o científicos y que no sea previsible que estos tratamientos conculquen los derechos y libertades fundamentales de los interesados (art. 11.2).

Se prevé la posibilidad de que las Partes amplíen la protección otorgada a las personas (art. 13) y, en cuanto a los flujos transfronterizos entre las Partes, el art. 14 establece la prohibición de restringirlo o impedirlo, con dos importantes excepciones:

1. Si existe un serio riesgo de que la transferencia hacia otra Parte o de ésta hacia una jurisdicción que no sea Parte, tenga la finalidad de esquivar la aplicación de la Convención.
2. Si la Parte en cuestión está vinculada por normas de protección compartidas por estados que sean miembros de una organización internacional regional.

Como hemos analizado en el Capítulo I de esta investigación, los derechos fundamentales con que estamos trabajando no son absolutos sino que tienen algunos límites fijados, especialmente los establecidos por la protección de otros derechos y libertades fundamentales, que el legislador pondera al dictar las normas que rigen estas materias. En este aspecto, la libertad de circulación de los datos personales tiene un límite muy claro en las normas de protección de las personas físicas con respecto al tratamiento de este tipo de datos. Las normas de los distintos niveles que rigen en esta materia armonizan ambos valores dando una clara prioridad al segundo (protección de las personas físicas) ya que si no fuera así, la libre circulación de datos personales con ausencia absoluta de límites o condiciones estaría dando una estrategia sumamente fácil de elusión de las normas de protección, dada la facilidad de hacer circular los datos que otorgan las

tecnologías y, en la otra cara, la dificultad para relacionar determinados tratamientos con una conexión territorial certera. Por ello se justifica la preeminencia de todo intento por evitar el fraude a la ley por sobre la libertad de circulación de los datos.

en una clara referencia al derecho de protección de datos de la Unión Europea. Cabe recordar que al momento de aprobarse el Convenio 108 en el ordenamiento de la Unión no existía ninguna norma sobre protección de datos vigente, motivo por el cual éste no podía prever una excepción similar.

Respecto a las transferencias internacionales, que a los efectos de este Convenio podemos definir como las operaciones por medio de las cuales los datos personales pasan a estar sujetos a la jurisdicción de un estado u organización internacional que no sea Parte en la convención, sólo se permiten si se garantiza un nivel de protección apropiado según las disposiciones de éste (art. 14.2), pudiendo asegurarse el nivel de protección a través del derecho vigente en la jurisdicción receptora (art. 14.3.a) o de disposiciones adoptadas por las personas involucradas en la transferencia y en los tratamientos posteriores, en instrumentos vinculantes y ejecutables (art. 14.3.b). Las Partes pueden establecer excepciones a la necesidad del nivel adecuado de protección, los casos en que:

a) El interesado haya dado su consentimiento explícito, específico, libre e informado sobre los riesgos de la falta de protección adecuada (art. 14.4.a);
b) La transferencia es requerida por el interés específico del interesado en un caso concreto (art. 14.4.b)
c) Si el derecho de la Parte prevé la prevalencia de intereses legítimos, en especial intereses públicos importantes, y la transferencia constituye una medida necesaria y proporcionada en una sociedad democrática (art. 14.4c)

d) Constituye una medida necesaria y proporcionada para la libertad de expresión en una sociedad democrática (art. 14.4.d)

5. Su relación con el derecho flexible.

En la actualidad los actores que hemos mencionado en el párrafo final del apartado anterior están utilizando esos recursos y capacidad para la aprobación de normas que, si bien carecen de la obligatoriedad y coercitividad de las de fuente estatal, cuentan con otras características (flexibilidad, mayor agilidad en la adopción, mayores posibilidades de conocimiento y especialización en la tecnología concreta) que le dan un valor añadido con respecto a la regulación estatal. Conforman lo que en inglés se denomina "*soft-law*" y en francés "*droit souple*", cuya traducción literal al castellano sería "*derecho blando*", "*derecho flexible*" o, como lo hace cierta doctrina, *derecho indicativo* como contraposición al *derecho imperativo*[63].

El derecho flexible constituye una fuente del derecho extranacional, presente en relaciones de derecho internacional público, de derecho de la Unión Europea y de comercio internacional[64], en una vertiente que calificamos como *general* por ser de uso generalizado o aceptación universal en los ámbitos mencionados.

[63] Fuente de la traducción: Puntoycoma, Boletín de los traductores españoles, n º 63 /Mayo/junio de 2000. En línea: http://ec.europa.eu/translation/bulletins/puntoycoma/63/pyc633.htm.

[64] Estas normas de derecho flexible se incorporan al derecho comercial internacional en gran medida por medio de lo que tradicionalmente se ha denominado usos y costumbres. Introducimos aquí una breve reflexión sobre las relaciones comerciales internacionales, que tradicionalmente han tratado, en gran medida, sobre la circulación de mercancías, servicios, capitales y personas y a las cuales en la actualidad se le debe adicionar la circulación de datos, tanto personales como no personales, aspecto que se comparte con la materia que analizamos en este trabajo de investigación.

Las notas características de este tipo de normas han sido enumeradas de la siguiente manera: "*1) El diseño o implantación es independiente de la potestad regulatoria de los Estados; 2) Hay una participación voluntaria en la construcción, operación y continuación del mismo. Los participantes pueden adherirse al régimen o no, y no continuar su aplicación; 3) Idealmente, se busca que las decisiones para actuar sean consensuadas y resulten de un diálogo entre actores; y 4) El poder sancionatorio del Estado está ausente*."[65] Sin perjuicio de que no es necesario que estén presentes todas estas notas para la configuración del derecho indicativo[66]. Por otra parte, también se ha caracterizado a este derecho por la integración de tres condiciones acumulativas:

- "*Tiene por objeto modificar u orientar los comportamientos de sus destinatarios suscitando, en la medida de lo posible, su adhesión;*
- *Por si mismo no crean derechos ni obligaciones para sus destinatarios;*
- *Presentan, por su contenido y su modo de elaboración, un grado de formalización y estructuración que las asemeja a las normas de derecho*"[67]

Junto al derecho flexible que hemos calificado como *general* existe otra vertiente que denominamos *particular*, caracterizado por la existencia de sujetos de derecho privado multinacionales o transnacionales[68] que poseen circuitos internos de circulación de datos que trascienden fronteras, tratándose de un único responsable de la circulación de datos a través de distintos ordenamientos jurídicos. Este tipo de sujetos en ocasiones dicta reglas

[65] Garrido Gómez, M.I: *El soft law como fuente del derecho extranacional*. Ed. Dykinson, Madrid, 201. Pp. 13-14.

[66] Ibidem, pág. 56.

[67] Conseil d'État: "Le droit souple". *Les rapports du Conseil d'État*, 2013. Accesible en línea en la página: http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Etude-annuelle-2013-Le-droit-souple (último acceso 18/11/2018). Pág. 61

[68] Garrido Gómez, M.I.: *El soft law…* cit., pág. 128 expone la diferencia entre empresas transnacionales y multinacionales.

de conducta internas para esa circulación de datos, que nacen como una declaración unilateral o corporativa, a las que si se le da publicidad pueden convertirse en obligatorias para quienes pertenecen a la corporación e incorporarse a una relación jurídica al modo de declaraciones unilaterales generadoras de obligaciones para quien las ha pronunciado o quienes se han adherido a ellas.

Otra de las formas de este tipo de normas es la auto regulación, que consiste en un conjunto de normas o código de conducta desarrollados voluntariamente por un grupo de agentes económicos (como empresas de una determinada industria o grupos profesionales) que dirigen el comportamiento, las acciones y los valores de conducta dentro de la actividad regulada. El grupo no sólo los redacta sino que se responsabiliza también por controlar su cumplimiento y penalizar su violación por parte de sus miembros[69].

Por lo general los cuerpos de reglas a los que nos hemos referido contienen un sistema sancionador, de carácter igualmente *flexible*, que carece de la coercitividad estatal pues es administrado y aplicado por la corporación que las dicta, con sanciones de naturaleza civil y mercantil (como podrían ser condiciones de pertenencia o de participación en el gobierno de la corporación) y laboral.

Como veremos a lo largo de distintos apartados de esta investigación, el derecho europeo incorpora este tipo de normas como complementarias a sus propias disposiciones, que obtienen plena validez y eficacia jurídica mediante su aprobación por parte de las

[69] Abbot, C: "Bridging the Gap – Non-state Actors and the Challenges of Regulating New Technology". Journal of Law and Society. , Vol. 39. 3.Ed. Blackwell Publishing Ltd, Oxford, UK, 2012. Pp. 329-358. doi:10.1111/j.1467-6478.2012.00588.x.

autoridades u órganos nacionales o europeos para lo que es esencial que cuenten con un sistema de control de aplicación entre otras condiciones.

Un ejemplo interesante de este tipo de *derecho indicativo* o *soft law* es el caso de los buscadores de información en internet o "*internet browsers*", de los cuales el caso más destacable es Google, cuya interpretación del "*derecho al olvido*" surgido con posterioridad a la sentencia "*Google Spain*" se ha convertido en muchos casos en una especie de "*doctrina indicativa*" para interpretar los casos en que es procedente la solicitud del interesado de que se borren o eliminen sus datos de la lista de resultados de la búsqueda.

6. Nuestro análisis

En los apartados precedentes hemos expuesto una serie de elementos que forman parte del nacimiento, la evolución y la esencia del derecho de protección de datos personales y que a nuestro entender deben ser ponderados para la elaboración de su regulación a efectos de lograr un equilibrio justo con todos los intereses en juego, que son diversos y en ocasiones opuestos. Quizás uno de los rasgos más predominantes de esta especialidad jurídica consiste en su origen como una expresión concreta del derecho a la vida privada; sin embargo, con posterioridad ha adquirido plena autonomía debido, principalmente, a que a través de los datos personales se protege no sólo la intimidad sino también otros valores igualmente esenciales como son algunos de la personalidad (la propia imagen e identidad), el honor, el patrimonio o la propiedad y los derechos laborales, por no nombrar más que algunos.

En definitiva, el derecho a la protección de datos personales es un derecho de muy reciente aparición y que, por ello, aún está atravesando las primeras etapas de su formación y afianzamiento. El avance de la revolución tecnológica convierte a los medios, programas, dispositivos y servicios informáticos en potenciales amenazas para los datos personales y, a través de éstos, a los derechos y libertades que hemos mencionado, por lo que las disposiciones que se dicten en este ámbito se han convertido en un instrumento de máxima utilidad para la defensa de éstos. La pérdida del elemento territorial que predomina en el entorno virtual hace que muchas de sus disposiciones deban trascender el ámbito de vigencia de un determinado ordenamiento jurídico para lograr que la protección sea eficaz, ya que las normas que ignoren la desterritorialización del espacio virtual serían ineficaces desde el mismo momento de su aprobación.

Hemos visto que con el paso de unos pocos años las normas aprobadas en este ámbito pueden quedar desactualizadas debido a la a constante evolución en que se encuentran todos los ámbitos de la técnica y la tecnología, que provocan que unas normas con conceptos demasiado precisos o rigurosos no sean capaces de abarcar las novedades que van apareciendo. Por ello es necesario que las disposiciones de protección sean abiertas, redactadas con términos amplios y en ocasiones ambiguos para poder aplicarse a los nuevos medios y técnicas de tratamiento que se produzcan en el futuro, que pueden consistir en sistemas hoy inimaginables y frente a los cuales las disposiciones deben estar preparadas para resultar aplicables.

A su vez, el sujeto protegido es el individuo a quien los datos personales identifican, considerado la parte más débil en las relaciones de tratamientos de datos personales y, como tal, digna de protección, puesto que la manipulación de sus datos personales, a menudo indeseada e inesperada, por parte de terceras personas (que pueden ser físicas o

jurídicas, privadas o públicas) lo coloca en una situación de vulnerabilidad que puede resultar en una violación de su esfera íntima, su espacio de privacidad, su identidad o su honor u otros bienes materiales. Ese ataque o amenaza por medio del tratamiento de los datos personales está en gran medida posibilitado por la interacción entre espacio virtual y vida real, que permite que las operaciones que se realizan en el primero, sin conocimiento ni autorización de los individuos a los que perjudican, tengan efectos de distinta naturaleza en la segunda.

Por último, al tratarse de un derecho fundamental aplicable predominantemente en el campo tecnológico es deseable que las normas a través de las cuales se regula trasciendan los límites del derecho tradicional, no sólo en su aspecto geográfico sino también en otros aspectos tales como el ya mencionado de la apertura y falta de concreción y también el del monopolio estatal, admitiéndose la participación de los particulares en la aprobación, control de aplicación y ejecución de nuevos sistemas jurídicos *atenuados* que tienen mayor adaptabilidad y flexibilidad, que les permite garantizar protección en algunos ámbitos tecnológicos, allí donde se producen la mayor parte de los tratamientos de datos personales y en los que el derecho y de las autoridades públicas son de muy difícil y, en algunos casos, imposible penetración.

Por eso aplaudimos y nos inclinamos decididamente por la promoción y facilitación de la participación de las entidades, organizaciones y personas privadas en todos los aspectos de la protección de los datos personales, tanto en el normativo como en el ejecutivo y en el control de su eficacia, para lo cual son valiosas herramientas la difusión de los derechos subjetivos creados por estas normas así como de las funciones de las autoridades públicas y de las obligaciones a cargo de los responsables y encargados, a efectos de que también

las personas protegidas los conozcan y sean capaces de controlar su cumplimiento y respeto por parte de todos los agentes implicados.

CAPÍTULO II. LA UNIÓN EUROPEA Y EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES.

1. Unión Europea: Objetivos, competencias.

El proyecto de la Unión Europea gira, principalmente, en torno a unos objetivos comunes que han fijado los Estados miembros y han concretado como finalidad última de su construcción política, establecida en el artículo 3.1 del Tratado de la Unión Europea (en adelante TUE): "…*la promoción de la paz, sus valores y el bienestar de sus pueblos.*" [70] Dentro de estos objetivos genéricos, Gómez Sánchez incluye en especial el de "... *elaborar y aprobar un catálogo propio de derechos fundamentales…*"[71], objetivo al que dedicaremos especialmente la primera parte de este capítulo de nuestro trabajo.

Entre los medios establecidos para lograr los mentados objetivos, enumerados en los apartados 2 a 5 del artículo 3, se encuentra la creación de un espacio de libertad, seguridad y justicia en todo su territorio (art. 3.2 TUE) y el establecimiento de un mercado interior (art. 3.3 TUE).

En el apartado 6 de la misma disposición se establece que, para dotar a la Unión Europea de los medios necesarios, los Estados miembros le atribuyen competencias o, en otras

[70] Mangas Martín, Araceli y Liñán Nogueras, Diego J: *Instituciones y Derecho de la Unión Europea.* 8ª ed. Tecnos, Madrid, 2014. Pp. 53-54.

[71] Gómez Sánchez, Y: *Constitucionalismo multinivel. Derechos fundamentales*. Ed. Sanz y Torres, Madrid, 2015. Pág. 72

palabras, delegan en sus instituciones y autoridades la facultad de ejercer parte de sus poderes soberanos.

Las competencias soberanas de cada Estado miembro están geográficamente limitadas al ámbito de su territorio[72], por lo tanto el ámbito territorial de ejercicio de las competencias atribuidas a la Unión Europea es el espacio formado por la suma de los territorios de los estados miembros.

Dentro del territorio así delimitado, el Derecho de la Unión Europea convive con el derecho interno de cada Estado miembro, aplicándose este último en los ámbitos de soberanía que no han sido delegados en la Unión, y el derecho de la Unión dentro de los límites de las competencias exclusivas atribuidas, o de las compartidas que la Unión haya decidido ejercer (art. 2 TFUE) con respeto a los principios de subsidiariedad y proporcionalidad (art. 5.1; 5.3 y 5.4 TUE). Así, las competencias derivadas de la soberanía corresponden originariamente a los Estados y, si no han sido atribuidas a la Unión, a ellos les corresponde su ejercicio (art. 5.2). En otras palabras, cada Estado es soberano dentro de su territorio y crea y aplica su propio derecho, excepto en los ámbitos en que (soberanamente) ha decidido delegar sus competencias a la Unión Europea, ámbitos en los que se aplicará exclusiva o preferentemente (según el caso) el derecho de la Unión. Las bases para la determinación y el ejercicio de las competencias atribuidas se delinean en los artículos 3 a 6 del TUE y se establecen más explícitamente en los artículos 2 a 6 del TFUE.

[72] Ramírez Bulla, G: "El ejercicio de la soberanía territorial de acuerdo con los tratados y principios del derecho internacional: el caso colombiano" En Revista Derecho del Estado, 2008, 21. Pp. 121-143, Universidad Externado de Colombia. Si bien este artículo trata sobre la definición, elementos y principios referentes a la concepción tradicional del Territorio, hace una breve referencia al "espectro electromagnético" como una de las manifestaciones de ese territorio, junto al suelo, subsuelo, espacio marítimo, espacio aéreo, etc.

Las competencias atribuidas son funcionales, es decir atribuciones específicas para acciones concretas y determinadas, para las cuales en los tratados se ha predeterminado el alcance, las condiciones y las modalidades de su ejercicio[73].

El espacio de libertad, seguridad y justicia que hemos mencionado anteriormente se encuentra dentro del ámbito de competencias compartidas entre la Unión Europea y los Estados miembros, según el artículo 4.2.j) del TFUE.

Hasta aquí hemos querido realizar una introducción descriptiva de las reglas básicas que configuran la distribución de los poderes que detentan los Estados miembros y la Unión Europea para comprender mejor los temas que siguen y ubicarnos así en el entorno en el que se desarrolla el derecho de los derechos fundamentales en estos ámbitos, para tener una mejor ubicación dentro del entorno que rodea al estudio del derecho fundamental a la protección de los datos personales.

Cabe agregar que en materia penal la Unión sólo tiene facultades para establecer normas de mínimos con respecto a la tipificación de los delitos y a las sanciones, en materias consideradas de especial gravedad, entre los cuales se encuentra la delincuencia informática o ciberdelincuencia[74]. Esta disposición se encuentra ubicada en el título V, dedicado al espacio de libertad, seguridad y justicia y dado que en materia penal la Unión no tiene competencias para dictar derecho sustantivo sino sólo para su armonización, ésta se debe realizar a través de Directivas[74].

[73] Mangas Martín, A. y Liñán Nogueras, D: Op. Cit., pp. 69-72.

[74] Art. 83.1 TFUE

2. Los derechos fundamentales en el derecho primario de la Unión Europea. El derecho a la protección de datos personales.

Como todos los sistemas democráticos, el de la Unión no es ajeno a la idea de "*configurar y proteger una esfera de libertad individual en la que cada persona pueda decidir con plena autonomía, conformar sus opciones vitales…*"[75].

Así, su ordenamiento jurídico es un sistema completo y complejo en cuya cúspide[76] se encuentran actualmente los derechos fundamentales, que no se reconocían expresamente en los tratados fundacionales si bien algunos de ellos se incorporaban de forma indirecta a través de ciertas competencias que se atribuían a las instituciones[77].

La incorporación de los derechos fundamentales al sistema jurídico comunitario comenzó en las décadas de 1960 y 1970 a través de la jurisprudencia del Tribunal de Justicia, bajo la forma de "*principios generales comunes a todos los Estados miembros y como parte de las tradiciones constitucionales comunes a éstos*"[78].

Luego continuaron integrándose progresivamente a los tratados modificativos de los tratados fundacionales, comenzando por algunos derechos e incorporando otros en cada modificación[79]. Pero no se logró un catálogo completo de derechos fundamentales de la

[75] Gómez Sánchez, Y: Op. cit, pág. 34.

[76] El art. 51.1. de la Carta es categórico respecto a la preeminencia de los derechos fundamentales en el ejercicio de las competencias atribuidas a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros en su aplicación del derecho de la Unión, quienes, en la letra de dicha disposición: "… *respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias…*".

[77] Gómez Sánchez, Op. cit, pág. 100.

[78] TJCE, sentencias en los casos Stauder, de 12 de noviembre de 1969; International Handelsgesellschaft, de 17 de diciembre de 1970 y Nold, de 14 de mayo de 1974.

[79] Gómez Sánchez, op. Cit, pág. 86.

Unión hasta diciembre de 2000, con la aprobación de la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, "La Carta") que fue aprobada con el valor de una simple declaración, es decir sin fuerza vinculante hasta el año 2008, en que al ser incorporada al Tratado de Lisboa no sólo adquirió vigencia sino también el valor jurídico de derecho originario, es decir equivalente al de los Tratados[80].

No obstante, en el ámbito competencial atribuido a la Unión al que nos hemos referido en el apartado anterior, es decir, en los artículos 3 a 6 TUE y 2 a 6 TFUE no figuran los derechos fundamentales. Por el contrario, el artículo 6.1 TUE, después de declarar que la Unión reconoce los derechos enunciados en la Carta y otorga a ésta el mismo valor que a los Tratados, establece que sus disposiciones no ampliarán las competencias de la Unión tal como se definen en éstos.

Por ello el art. 51.1 de la Carta ordena a las instituciones, órganos y organismos el respeto de los derechos, la observancia de los principios y la promoción de su aplicación, disposiciones que son completadas por el apartado 2 del mismo artículo que, en el mismo sentido que el art. 6.1 del TUE ya mencionado, prohíbe su interpretación como ampliación de las competencias que los tratados otorgan a la Unión.

Una interpretación armónica de las disposiciones anteriormente mencionadas permite concluir, de acuerdo con el art. 51 de la Carta[81], que los derechos fundamentales no

[80] Ibidem, pág. 76. A pesar de la tardía incorporación de la Carta al derecho primario de la Unión, en la pág. 87 de la misma obra la autora sostiene que "*... los derechos humanos, la democracia y el Estado de Derecho han sido valores básicos de la construcción europea, consagrados en su Tratado fundacional y definitivamente consolidados con la entrada en vigor de la Carta de los Derechos fundamentales…*".

[81] Transcribimos a continuación el contenido textual del art. 51 de la Carta: "*Artículo 51*

Ámbito de aplicación.

1. Las disposiciones de la presente Carta están dirigidas a las instituciones y órganos de la Unión, respetando el principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho

constituyen una competencia autónoma: las disposiciones sobre derechos fundamentales establecidas en la Carta que no constituyan competencias atribuidas en los Tratados deben guiar el desarrollo y ejercicio de las aludidas competencias[82], respetándose en todo momento pues los actos que no los respeten podrán ser declarados nulos por el Tribunal de Justicia de la Unión Europea. Así, el contenido de los derechos fundamentales establecidos en la Carta sirve como directriz de contenido positivo (deber de respetarlos) y de límites de contenido negativo (prohibición de vulnerarlos) para todos los actos emanados de las Instituciones, órganos, organismos y autoridades de la Unión.

Dado que estamos dedicando algunas líneas a los derechos fundamentales en la Unión Europea, haremos algunas consideraciones en torno al concepto de *constitución*, que se puede definir en un sentido formal o en un sentido material. Materialmente, Constitución es el conjunto de normas que en los estados democráticos organizan y limitan el poder y gozan de superioridad jerárquica con respecto al resto de las normas que conforman el ordenamiento jurídico[83]. Conjunto de normas que puede estar escrito y codificado (en cuyo caso coincidirá con la constitución formal) o no escrito y disperso. Formalmente, la constitución es la norma escrita suprema de un determinado ordenamiento jurídico, que puede ser más o menos rígida y no emana del poder legislativo sino directamente de la soberanía popular. Pero, lo que es más importante, la constitución formal no está presente

---

de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias.

2. La presente Carta no crea ninguna competencia ni ninguna misión nuevas para la Comunidad ni para la Unión y no modifica las competencias y misiones definidas por los Tratados."

[82] Linde Paniagua, E: "El ámbito de aplicación: El talón de Aquiles de la Carta de los Derechos Fundamentales de la Unión Europea". Revista de Derecho de la Unión Europea nº 15 - 2º semestre 2008. Pp. 27 a 44.

[83] Azpitarte Sánchez, M: "Del derecho constitucional común europeo a la constitución europea. ¿Cambio de paradigma en la legitimidad de la Unión? En Teoría y Realidad Constitucional, núm. 16, 2005, pp. 343-373.

en todos los ordenamientos jurídicos, como sí lo está la constitución material, ya que todo sistema que se considere *ordenado*, tal como son los sistemas jurídicos, precisan de normas que dispongan ese orden: que por una parte, ordenen el poder político para hacer factible la producción de derecho, la existencia de normas jurídicas y, por la otra, otorguen un orden jerárquico a dichas normas a fin de que exista orden entre ellas.

Recopilando, todo sistema para ser ordenado precisa que haya una determinada jerarquía entre las normas, porque la falta de jerarquía llevaría al caos. Por consiguiente, en todo sistema existe una norma, o un conjunto de normas, jerárquicamente superiores a las demás, aunque dichas normas no estén recogidas en un texto único de rigidez superior al resto. En otras palabras, en todo sistema jurídico democrático existe una constitución *material*, aunque no exista una formal.

Todo lo expresado precedentemente nos permite concluir que en la Unión Europea, si bien no existe una Constitución formal sí existe una Constitución material, formada por las disposiciones sobre la distribución del ejercicio del poder entre las Instituciones, los órganos y organismos y los derechos fundamentales establecidos en la Carta, entre los cuales se encuentra el derecho de protección de datos, que de esta manera forma parte del derecho constitucional europeo[84].

Por último, en el análisis del ordenamiento jurídico europeo no podemos dejar de mencionar que éste no está aislado ni es independiente de los ordenamientos de producción interna de los Estados Miembros; tal como reflexiona Gómez Sánchez, "*Ambos niveles, nacional y europeo, están en permanente interdependencia: las modificaciones de los Tratados llevan aparejada frecuentemente la reforma de las*

[84] Gómez Sánchez, Y: Op. Cit, pág. 81.

constituciones; prácticamente todas las ramas jurídicas internas están afectadas por los Tratados y por el Derecho derivado de la UE y, por lo tanto, se han europeizado. Pero, de igual manera, la producción normativa de la UE se ve influida por la producción normativa de los Estados miembros". Por todo ello esta autora denomina *multinivel* al derecho constitucional actual, expresión que define como "*... un ordenamiento complejo en el que coexisten un número muy elevado de normas de distinta jerarquía, naturaleza, ámbito de aplicación y, especialmente, diferente origen.*"[85]

El derecho de protección de datos no es extraño a este sistema, de ahí que esté constituido por normas de derecho primario y secundario de la Unión Europea, de derecho interno (constitucional, legal e infralegal) y de derecho internacional público. Por ello, su aplicación se realiza en los ámbitos europeo, nacional, internacional y, en algunos casos entre los que se encuentra España también infranacional o regional y asimismo a nivel *transnacional* como veremos más adelante.

En el derecho originario de la Unión aborda el derecho de las personas físicas a la protección de los datos personales en los arts. 39 TUE y 16 TFUE (que analizaremos a continuación), a través de los cuales se otorga competencia a la Unión en esta materia.

El art. 16 TFUE, ubicado en la Primera Parte (que se dedica a los principios de la Unión) y dentro de ella en el Título II, sobre las disposiciones de aplicación general, reafirma en su apartado 1. el derecho a la protección de datos de carácter personal que se garantiza a "*toda persona*". En su apartado 2. establece para el Parlamento Europeo y el Consejo la obligación de dictar, mediante el procedimiento legislativo ordinario de la Unión, "*las normas sobre protección de las personas físicas respecto del tratamiento de datos de*

[85] Gómez Sánchez, Y: Op. cit, pp. 46-47.

carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos".

El artículo que venimos de exponer constituye una norma general con respecto al art. 39 TUE, que ordena al Consejo adoptar una decisión sobre protección de las personas físicas respecto al tratamiento de sus datos personales en relación con las actividades que desarrollen los Estados miembros en el ámbito del capítulo 2 del Título V del tratado, dedicado a la política exterior y de seguridad común, ámbito comprendido en el espacio de libertad, seguridad y justicia instaurado por la Unión, en el que este derecho cobra una especial importancia, especialmente con respecto a la seguridad común, bien jurídico que en muchas ocasiones entra en colisión con el de la protección de datos personales y que, por lo tanto, necesita una regulación especial para la armonización de éstos y de los demás valores jurídicos implicados.

Estos artículos otorgan a las Instituciones que se mencionan la competencia para dictar normas sobre protección de datos personales, que regirán no sólo la actividad de las instituciones, órganos y organismos de la Unión sino también la de los Estados miembros en cuanto apliquen su derecho, siendo ésta una de las competencias compartidas entre la Unión y sus estados miembros en virtud de la cláusula residual del art. 4 TFUE, dado que no está incluida entre las competencias exclusivas del art. 3 ni las de apoyo, coordinación o complemento de la acción de los Estados miembros del art. 6 del referido Tratado. De esta forma, el derecho a la protección de datos personales se diferencia del resto de derechos incorporados a la Carta que, como ya hemos expuesto, no constituyen competencias autónomas.

Las mencionadas competencias fueron ejercidas para la aprobación de un Reglamento de alcance general que estudiaremos en los apartados siguientes, así como de dos Directivas concretamente dirigidas, por un lado, a regular los tratamientos de datos personales realizados por las autoridades competentes en los distintos ámbitos de la persecución y sanción de los delitos[86], y por el otro, a los tratamientos relacionados con los registros de nombres de pasajeros[87] para la prevención, persecución y enjuiciamiento del terrorismo y otros delitos graves[88]. Estas tres normas sobre protección de datos personales constituyen lo que la Comisión denomina "*paquete de protección de datos*"[89]

Por su parte, el artículo 8 de la Carta eleva a la categoría de Derecho Fundamental al derecho a la protección de las personas físicas en relación con el tratamiento de sus datos personales[90], estableciendo las bases sobre las cuales se debe desarrollar el derecho de la Unión en este ámbito y fijando límites claros a la manipulación o tratamiento de esta clase de datos, ya sea por organismos o autoridades públicas o por personas privadas.

Por otra parte, la protección de datos personales se puede considerar desde dos puntos de vista: Como derecho fundamental, que se inserta en el espacio de libertad, seguridad y justicia (apartado 2.j del art. 4 TFUE) y desde el punto de vista económico, como libertad

---

[86] DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[87] PNR por sus siglas en inglés: *passengers names recorder*.

[88] DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

[89] "*The data protection package*" en su original en inglés, en la siguiente dirección electrónica: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (última consulta 14/01/2019).

[90] Que comúnmente se denomina "derecho a la protección de los datos personales" o simplemente "protección de datos personales", como lo haremos indistintamente en el resto del presente trabajo.

de circulación de los datos personales, incluida en el ámbito del mercado interior (art. 4.2.a TFUE).

A modo de reflexión final de este apartado, manifestar que pesar de todo lo expuesto en relación con la protección de datos personales como derecho fundamental, los datos personales tienen la particularidad de que se han convertido en elementos de alto valor económico hoy en día, a tal punto que ha sido calificado como el "*nuevo petróleo del Siglo XXI*"[91].

3. La protección de datos personales en el derecho derivado.

La consolidación y funcionamiento del mercado interior en la Unión Europea ha provocado un aumento considerable de la integración económica y social y, con ellas, también el incremento de los "*flujos transfronterizos de datos personales*"[92], necesarios para ese tipo de integración pero también para la realización del espacio de libertad, seguridad y justicia[93].

Por ello el derecho europeo, además de la protección de las personas físicas frente al tratamiento de sus datos personales tiene asimismo como objetivos la promoción de la libertad de circulación de los mismos[94], como una medida para afianzar el espacio de

[91] Hirsch, D: "The glass house effect: Big data, the new oil, and the power of analogy. Maine Law Review (2014). Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393792.

[92] Considerando 5 del Reglamento.

[93] Considerando 2 del Reglamento.

[94] Artículo 1 del Reglamento, especialmente apartados 1 y 3.

libertad, seguridad y justicia y dar impulso al crecimiento económico y a la integración social.

3.1. Antecedentes: La Directiva 95/46.

3.1.1. Aspectos generales y territoriales.

Para regular y lograr un equilibrio entre esos dos valores, en octubre de 1995 se aprobó la primera norma europea de derecho derivado para la protección de los datos personales, la "*Directiva 95/46 CE del Parlamento Europeo y del Congreso, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*"[95], que fue derogada por el Reglamento actualmente vigente que analizaremos con posterioridad. La referida Directiva regulaba tanto la protección de las personas físicas en lo relativo al tratamiento de sus datos personales como la libre circulación de los mismos. En virtud de ello, en su considerando 56 reconoce que los flujos transfronterizos de datos personales (entendiéndose por tales las comunicaciones de datos en las que el remitente tenga su conexión jurídica principal con el ordenamiento jurídico de un Estado miembro y el receptor, con el de otro Estado miembro diferente, tal como podemos inferir de los considerandos 5, 8 y 56) son beneficiosos para la Unión y que el derecho europeo no se opone a las comunicaciones a países terceros que ofrezcan un nivel apropiado de protección.

[95] Que en adelante llamaremos "La Directiva 95/46".

En virtud de ese doble objetivo de regular la libertad de circulación por un lado y el derecho fundamental por otro, el TJUE en su sentencia Lindqvist[96] ha declarado que la Directiva 95/46 no era una norma de mínimos para desarrollar este último sino que constituía una armonización completa, dado que los mencionados objetivos pueden entrar en conflicto entre sí[97] y que, en consecuencia, está vedado a los Estados ampliar la protección de los datos personales en desmedro de la libertad de circulación de datos, aunque en su legislación de transposición sí pueden ampliar el número de casos cubiertos por la Directiva. Si bien esta norma les dejaba un cierto margen de discrecionalidad en algunas cuestiones, al hacer uso de esa discrecionalidad los Estados miembros debían mantener siempre el equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad tal como venía marcado por la Directiva.

Las líneas generales que marcan la regulación de la Directiva se hallan en sus considerandos, en los que con respecto a los flujos internacionales de datos personales (entendiéndose por tales los flujos entre los Estados miembros y países terceros con respecto a la Unión, tal como se infiere del Capítulo IV de la Directiva), se aboga por restringir las comunicaciones hacia países que no ofrezcan un nivel apropiado de protección de dichos datos, imponiendo ciertos mecanismos que en cierto sentido sustituyan o complementen la baja protección del ordenamiento jurídico de destino, siempre de acuerdo con el derecho interno del país de origen. Los mencionados

[96] Sentencia de 6 de noviembre de 2003 en el Asunto C-101/2001, Caso Proceso Penal contra Bodil Lidqvist (TJCE/2003/368), párrafos 91 a 99.

[97] Ibidem, párrafo 79.

mecanismos son: Garantías suficientes otorgadas por el remitente y el receptor, códigos de conducta y normas corporativas vinculantes[98].

En los considerandos 63 a 65 se establece la necesidad de la designación de autoridades independientes de protección de datos personales por parte de los Estados miembros, de que dichas autoridades cuenten con mecanismos de coordinación entre ellas para garantizar el respeto a las normas de su competencia en el territorio de toda la Unión y de que exista asimismo un órgano a nivel europeo con competencias de asesoramiento a las Instituciones en este ámbito, que contribuya además a lograr una aplicación uniforme del derecho comunitario.

Introduciéndonos en el articulado de esta norma, su artículo 1.2 garantiza, tal como lo hemos adelantado, la búsqueda del equilibrio entre protección de las personas respecto al tratamiento de sus datos personales y la libre circulación de dichos datos en el territorio de la Unión.

Con respecto a la vigencia territorial de la Directiva, al carecer ésta de aplicación directa, en ella no se establece un ámbito territorial propio sino que se delega este aspecto en las normas internas que dicten los Estados miembros para su aplicación, disponiendo en el artículo 4, bajo el título "Derecho nacional aplicable", dos criterios para determinar el ámbito territorial de aplicación.

En primer lugar, el criterio de: "*el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro*"[99] o en un lugar en el

[98] Cfr. considerandos 59, 60 y 61 de la Directiva.

[99] Art. 4.1.a) de la Directiva 95/46.

que, en virtud del Derecho Internacional Público, se aplique el derecho de un estado miembro[100].

Queremos realizar una mención expresa a la última frase del art. 4.1.a), que prevé que, si un responsable cuenta con establecimientos en varios Estados miembros, "*deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable*", disposición que con la intensificación de las relaciones comerciales y la expansión de las empresas transfronterizas se tornó en una carga administrativa realmente pesada para muchas de estas empresas, que era uno de los motivos por los que se hacía necesaria una modificación de esta Directiva que establezca una mayor homologación del derecho aplicable a todos los Estados miembros así como una simplificación de la carga administrativa para impulsar la eficacia y la agilidad de procedimientos que permita dirigir los recursos dedicados a esta diferencia de derechos y de criterios administrativos hacia otras actividades más productivas.

El segundo criterio se aplicaba cuando el responsable no estaba establecido en la Comunidad y el tratamiento se realizara con la utilización de medios ubicados en un estado miembro, en cuyo caso se aplicaría el derecho de ese estado, excepto que los mencionados medios se utilicen exclusivamente para fines de tránsito por el territorio de la Comunidad[101], debiendo el responsable designar un representante en el estado donde se encuentren los medios[102].

[100] Art. 4.1.b) de la Directiva.

[101] Cfr. art. 4.1.c) de la Directiva.

[102] Art. 4.2 Directiva 95/46.

Como se puede observar, el primero de los criterios se centra exclusivamente en el establecimiento del responsable del tratamiento, dejando de lado al encargado, que sólo tendrá relevancia en cuanto fije en el territorio de la Unión el lugar de ubicación de los medios utilizados para los tratamientos que se realicen fuera del territorio de la Unión. La falta de amplitud y flexibilidad de estos criterios que les permitiera adaptarse a la evolución de los tratamientos fue otro de los motivos que hacía imperioso un cambio en la legislación, por un lado debido a que se hacía evidente que en muchos casos las actuaciones del tratamiento realizadas por el encargado comprometían los datos personales en mayor medida que las realizadas por el responsable y, por lo tanto, la necesidad de que la ubicación del establecimiento del primero en cuyo ámbito se llevaran a cabo las operaciones del tratamiento fuera tan decisivo para la determinación del derecho aplicable como la ubicación del establecimiento del responsable del tratamiento. Por otro lado, el criterio de la ubicación de los medios que servían para la realización del tratamiento careció prácticamente de aplicación debido a la imposibilidad e inutilidad que ya hemos apuntado, para muchos casos, de determinar la localización del medio por el cual se realizan una o más operaciones de tratamiento, entre otros motivos porque éstas pueden realizarse "en la nube", mediante servidores de ubicación desconocida o porque para una misma operación de tratamiento, pueden existir medios o recursos establecidos en distintas localizaciones en todo el mundo y no existían parámetros para decidir cuál de todas esas localizaciones se consideraría decisiva para conectar la ubicación de los medios a que se refiere el art. 4.1.c) de la Directiva.

3.1.2. Autoridades y vías internas de reclamación.

El Capítulo VI de la Directiva y, especialmente, su art. 28, ordena a los Estados miembros el establecimiento de una o más autoridades públicas para encargarse de vigilar la aplicación de las normas de transposición de la misma, cuya actuación tendría una base exclusivamente territorial.

Dichas autoridades debían ejercer con total independencia las funciones que se enumeran en el mismo artículo examinado, las que están diseñadas para ser ejercidas exclusivamente en el ámbito territorial del Estado de designación, con excepción de la conformación del Grupo del artículo 29 que analizaremos más adelante. No se halla en los considerandos ni en el articulado de esta Directiva ninguna disposición que haga referencia a actuaciones de las autoridades de control ni del mencionado Grupo fuera del ámbito geográfico de la Unión, otra de las características que hacían de esta Directiva una norma demasiado rígida y limitada para poder comprender y regular a una gran parte de los tratamientos de datos personales realizados por medios electrónicos, para los que ya hemos expuesto que en ocasiones desconocen o prescinden de las fronteras geográficas.

Otra de las autoridades que crea el artículo 29 de esta Directiva es un "Grupo de protección de las personas en lo que respecta al tratamiento de datos personales"[103], que estará compuesto por: Un representante de la(s) autoridad(es) de control de cada Estado miembro, un representante de la(s) autoridad(es) creadas por las instituciones y organismos comunitarios y un representante de la Comisión. Tendrá carácter consultivo e independiente.

[103] Que en lo sucesivo denominaremos "Grupo de trabajo del artículo 29" o "G29".

Las funciones de este Grupo están definidas en el artículo 30[104] y son, en general, de estudio de la aplicación de la Directiva 95/46 en los diferentes Estados miembros (Art. 30.1.a), en la Comunidad en su conjunto y en países terceros (Art. 30.6); funciones de asesoramiento de la Comisión (apartados b), c); 2. y 3. del art. 30) y la formulación de dictámenes y recomendaciones sobre cualquier asunto relacionado con la protección de los datos personales, a iniciativa propia (apartados 3; 4. y 5. del art. 30 Directiva 95/46).

Si bien analizaremos más en profundidad la composición y naturaleza de este órgano en el Capítulo V de este trabajo, adelantamos aquí que, quizás porque este análisis se realiza retrospectivamente y con una realidad muy diferente a la del momento en que se aprobó la Directiva 95/46, pero este Grupo, aunque la Directiva 95/46 le dedica sólo dos artículos (lo que parece indicar que el legislador europeo ha querido darle una función menor), ha ocupado una posición sumamente relevante en la protección de datos personales en la Unión, realizando una magnífica labor de difusión, interpretación y aplicación del derecho europeo de protección de datos y no sólo de la Directiva 95/46, permitiendo la flexibilización y adaptación de esta disposición a las circunstancias cambiantes de los tratamiento para evitar que la evolución de la tecnología la convierta en una norma de aplicación imposible.

Respecto a las vías internas de reclamación, el art. 22 dispone en primer término que los Estados miembros preverán en sus legislaciones internas un recurso judicial a disposición de los interesados que consideren que se ha cometido una violación de sus derechos. El

[104] El artículo 15 apartado 3 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) agrega una tarea a las contenidas en el artículo 30 de la Directiva 95/46, cual es la de garantizar la protección de los derechos y libertades fundamentales y de los intereses legítimos en el sector de las comunicaciones electrónicas.

art. 23 ordena garantizar el derecho a obtener una indemnización por los perjuicios sufridos como consecuencia de una violación de la Directiva por parte del responsable del tratamiento, permitiéndose eximir de esta obligación al responsable que acredite que el hecho que ha provocado el daño no le puede ser imputado.

En este aspecto sí se trata de disposiciones de mínimos dado que cada Estado miembro sigue siendo soberano para establecer sus vías de reclamación y procedimientos internos, tanto administrativos como judiciales limitándose la Directiva en este aspecto a disponer los mínimos requeridos.

Afortunadamente muchos Estados miembros han hecho uso de estas facultades soberanas, adicionando vías de reclamaciones administrativas a las establecidas como preceptivas por la Directiva, ya que éstas sumadas al resto de funciones de las autoridades de aplicación y control de protección de datos fueron el verdadero alimento que nutrió al G29 en su actividad. En este sentido destacan especialmente la Agencia Española de Protección de Datos, así como la británica Information Comissioner Office (ICO) o la francesa Comission Nationale de l'Informatique et des Libertés (CNIL)

3.1.3. Las transferencias internacionales de datos personales.

La Directiva 95/4 regula las transferencias internacionales de datos personales, en tanto que modalidad específica de tratamiento, en su Capítulo IV, artículos 25 y 26, si bien no da una definición de este tipo de tratamientos[105].

[105] Cfr. Sentencia Lindqvist, apartado 56.

La primera consideración que debemos verter sobre esta regulación es que, siendo esta materia una de las más complicadas (si no la más) para la protección de los datos personales, la regulación se nos aparece muy escueta y, en consecuencia, incompleta y complicada de

El apartado 1 del primero de dichos artículos delimita los ámbitos de aplicación de estas disposiciones: Materialmente se aplicará a las trasferencias de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia y, en su alcance territorial, serán aquellas que se dirijan a un país tercero entendiéndose por "país tercero" todo país en el cual no sea aplicable el derecho del Espacio Económico Europeo.

Así, quedarían hipotéticamente excluidas del control previo de los Estados las transmisiones de datos que no impliquen ninguna forma de tratamiento por parte del receptor. Decimos "hipotéticamente" pues es imposible pensar que se realizará una comunicación de datos personales que no estén destinados a ser sometidos a un tratamiento dado que el sólo hecho de su recepción ya es un tratamiento y, luego de ésta, tanto su mantenimiento en poder del receptor (es decir archivo o almacenamiento) o su eliminación son distintas formas de tratamiento, por lo tanto es imposible que los datos sean transmitidos para no ser sometidos a ningún tratamiento.

También hipotéticamente quedarían fuera del ámbito de aplicación las transferencias de datos que no estén incluidos en un fichero y que se realicen por medios no automatizados, ya que esto se reduce a las comunicaciones de datos personales realizadas a un país tercero por medio de cartas enviadas por el correo terrestre tradicional y que incluya datos personales aislados. Este tipo de comunicaciones o tratamientos de datos personales

queda fuera del ámbito material de aplicación de la Directiva 95/46, por lo tanto su inclusión en estas disposiciones es redundante.

El sistema de protección de los datos personales que van a ser transferidos a un país tercero con respecto al Espacio Económico Europeo es un tanto complicado, pues se basa en tres supuestos:

Principio General: Los Estados miembros deben disponer en su derecho nacional que sólo se podrán realizar transferencias internacionales de datos personales cuando el país de destino de los datos personales "*garantice un nivel de protección adecuado*"[106]. La adecuación (o falta de ella) del ordenamiento jurídico de un país tercero debe ser evaluada y constatada por la Comisión a través de una decisión adoptada de conformidad con el procedimiento del apartado 2 del artículo 31[107]. Los Estados miembros y la Comisión deberán informarse recíprocamente los casos en que consideren que un país no ofrece un nivel de protección adecuado, con arreglo al apartado 2 del artículo 25[108]. En caso de que sea la Comisión quien compruebe que un país tercero no ofrece el adecuado nivel de protección y así lo haga constar, los Estados miembros deberán adoptar las medidas necesarias para impedir las transferencias de datos personales hacia ese país[109].

Excepciones: basadas en el consentimiento del interesado o en el fundamento jurídico del tratamiento, establecidos en los distintos subapartados del art. 26.1 de la Directiva 95/46.

Autorización. Otorgada por las autoridades nacionales de protección de datos, en forma expresa, habiendo verificado previamente que la falta de protección otorgada por el

[106] Art. 25.1 Directiva 95/46.

[107] Apartado 6 del art. 25, Directiva 95/46.

[108] Art. 25.3 Directiva 95/46.

[109] Art. 25.4 Directiva 95/46.

ordenamiento jurídico del país receptor esté compensada por garantías suficientes otorgadas por el responsable del tratamiento, para "*la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos*", según el apartado 2 del Art. 26 de la Directiva 95/46 que, si bien sólo menciona a las "*cláusulas contractuales apropiadas*" para otorgar dichas garantías, esta mención no se hace con un sentido de *animus clausus* sino meramente ejemplificador, lo que ha dado pie a que en la práctica además de las *cláusulas contractuales tipo* también se acepten las garantías establecidas en normas corporativas vinculantes (*CBR* por sus iniciales en inglés, correspondientes a *corporate binding rules*) así como en las certificaciones y los códigos de conducta elementos que analizaremos en profundidad en el apartado relativo a su configuración bajo la normativa actual.

En opinión del G29 la facultad de autorizar transferencias debe ejercerse con cuidado dado que el hecho de que una transferencia en particular no ofrezca riesgos no significa que otras transferencias a ese país serán seguras; aparte de ello, uno de los problemas fundamentales de la autorización de la transferencia merced a la utilización de las cláusulas contractuales tipo radica en que el interesado no será parte del contrato y, en carácter de tercero, será muy difícil el ejercicio de los derechos que en su favor disponen dichas cláusulas[110].

Cuando otorguen autorizaciones bajo las condiciones establecidas en los párrafos anteriores, los Estados miembros deberán informar a la Comisión y a los otros Estados miembros. Como resultado de esa información los demás Estados o la Comisión pueden ejercer oposición a la autorización, por motivos derivados de la protección de la vida

[110] First orientations on transfers of personal data to third countries – Possible ways forward in assessing adequacy (WP4 – XV D/5020/97). Grupo de Trabajo del Art. 29, Bruselas, 26/06/1997, pp. 4 – 7.

privada y demás derechos y libertades fundamentales, en cuyo caso la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31[111].

Para comprender el procedimiento establecido en el artículo 31, apartado 2 (al que remiten estos artículos), es necesario mencionar que el artículo 31 en su apartado 1 crea un Comité que asistirá a la Comisión en las medidas de ejecución referentes a la protección de los datos personales.

El procedimiento establecido en el apartado 2 consiste en que la Comisión presentará a dicho Comité los proyectos de medidas cuya adopción se haya previsto y el Comité, dentro del plazo que su Presidente determine al efecto, emitirá un dictamen con la mayoría establecida en el artículo 148, apartado 2 del Tratado[112].

Debemos agregar que tanto la Directiva como el Grupo de Trabajo fueron incorporados al derecho vigente en el Espacio Económico Europeo (en adelante, EEE)[113], por la

[111] Art. 26.3 Directiva 95/46.

[112] Este artículo definía la composición de la mayoría cualificada con la cual el Consejo debía adoptar sus acuerdos cuando así estuviera exigido por los Tratados. Pasó a ser el número 205 con la modificación introducida por el Tratado de Ámsterdam, numeración que conservó en el Tratado de Niza. El Tratado de Lisboa, al sustituir el Tratado Constitutivo de la Comunidad Europea por el Tratado de Funcionamiento de la Unión Europea, derogó los apartados 2 y 4 del antiguo artículo 205. Estos artículos fueron sustituidos por el artículo 16, apartados 4 y 5 del Tratado de la Unión Europea y el artículo 238, apartado 2 del Tratado de Funcionamiento de la Unión Europea, cuya vigencia se producirá a partir del 1 de noviembre de 2014 y que definen la mayoría cualificada del Consejo como un mínimo del 55 % de sus miembros que incluya al menos a quince de ellos y represente a Estados miembros que reúnan como mínimo el 65 % de la población de la Unión. Se establece una minoría de bloqueo en el voto en este sentido de 4 miembros.

El régimen transitorio vigente hasta el 31 de octubre de 2014 se establece en el Protocolo (n 36) sobre las disposiciones transitorias, que en su artículo 3 "Disposiciones relativas a la mayoría cualificada", apartado 3, define la mayoría cualificada del Consejo Europeo o del Consejo, estableciendo una ponderación fija del voto de cada país. De los votos así ponderados, la mayoría cualificada estará formada por 255 votos favorables que representen la mayoría o dos tercios de los miembros, según el caso.

[113] Actualmente, el Espacio Económico Europeo está formado por los 28 Estados Miembros de la Unión Europea y además Islandia, Liechtenstein y Noruega.

Decisión n° 83/1999 del Comité Mixto del Espacio Económico Europeo, de 25 de junio de 1999, por la que se modifica el Protocolo 37 y el anexo XI (Servicios de telecomunicaciones) del Acuerdo EEE que agrega la Directiva 95/46 al Anexo mencionado y el Grupo de Trabajo del artículo 29 de la Directiva a la lista de organismos incluida en el Protocolo 37.

Para dar una apreciación final de la Directiva 95/46, mencionar que desde la perspectiva del estado actual de esta materia esta norma presenta un número importante de deficiencias o desactualizaciones, que parten desde el tratamiento de la protección de datos personales como un derecho instrumental, pasando por las amplias diferencias que amparaba en la regulación interna de esta materia en cada Estados miembro, causante de una gran inseguridad jurídica para las empresas transnacionales, la poca importancia otorgada al Grupo de Trabajo del Art. 29 y finalizando con la rigidez de algunas de las disposiciones que no permitía su adaptación a tecnologías o modalidades de tratamiento surgidas con posterioridad a su aprobación. Sin embargo, si analizamos esta Directiva desde la perspectiva del año en que fue aprobada y no desde el punto de vista actual, son muchos los méritos de una norma que fue pionera en la materia regulada ya que anteriormente no existía una norma similar en Europa, es decir que tuvo que abrir un camino que hoy en día nos permite asegurar que en la Unión Europea la protección de la información personal de los individuos es un derecho fundamental consolidado.

3.2. Los tratamientos de datos personales realizados por las Instituciones y Organismos de la Unión.

Junto a la Directiva 95/46 y el Reglamento que la ha sustituido y que examinaremos más adelante, que son las normas de aplicación general sobre protección de datos en la Unión, han existido y existen otras normas especiales que regulan los tratamientos de datos personales en sectores específicos, como era el caso del Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[114], hoy derogado por el 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[115].

El Reglamento 2018/1725 tiene el objetivo de adecuar la regulación de los tratamientos de datos personales que realizan las instituciones, autoridades y organismos de la Unión a las disposiciones del RGPD, ya que el anterior Reglamento 45/2001 se había aprobado durante la vigencia de la Directiva 95/46 y, por lo tanto, muchas de sus disposiciones adolecían de los mismos defectos que ésta.

En su denominación queda definido el ámbito de aplicación de este Reglamento, que tiene una base material de aplicación (los tratamientos de datos personales) careciendo de base territorial para, en su lugar, establecer una funcional: Aquellos tratamientos que son

[114] Al que en adelante nos referiremos como "Reglamento 45/2001".

[115] En adelante, "el Reglamento 18/1725".

realizados por las instituciones, autoridades y organismos comunitarios en las actividades que se enmarquen en el Derecho Comunitario (arts. 1.1 y 2 Reglamento 18/1725).

Este Reglamento comienza tratando al derecho de protección de datos personales como un derecho autónomo en su art. 1.2, que textualmente establece que su objetivo es la protección de "*los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales*".

Por otra parte, no sólo regula la protección de las personas físicas con respecto a los tratamientos de sus datos personales, sino también la libre circulación de estos datos dentro de un ámbito definido por distintos elementos de los cuales uno es geográfico, junto a otro que podríamos definir como *funcional* u *orgánico*: La circulación de datos personales entre las instituciones y organismos de la Unión o entre éstos y destinatarios "*establecidos en la Unión*"[116], afirmación que a nuestro entender se debe interpretar como destinatarios a quienes se les aplique el derecho de la Unión en virtud de su establecimiento en el territorio de ésta. Observamos que sólo se refiere a la *libre* circulación en este ámbito[117], pues veremos en los próximos párrafos que la circulación de datos personales entre las Instituciones y organismos de la Unión y entidades que no estén sujetas al derecho europeo no se establece como una libertad sino que está sometida a determinadas condiciones y limitaciones.

Sin embargo, en lo que a nuestro parecer es paradójico, la comunicación de datos personales a destinatarios distintos de las instituciones y organismos de la Unión que estén

[116] Art. 1.1. Reglamento 18/1725.

[117] Sin perjuicio de que en el art. 9 del Reglamento 18/1725 se establecen dos fundamentos jurídicos específicos para la comunicación de datos personales a destinatarios distintos de las instituciones y organismos de la Unión que estén sujetos al derecho europeo, es decir, que en cierto sentido también se establecen condiciones específicas para estas comunicaciones de datos.

sujetos al derecho europeo se somete a una gran limitación en el art. 9 del Reglamento 18/1725, que establece con carácter taxativo dos únicos fundamentos jurídicos para este tipo de comunicaciones, es decir, que en cierto sentido también se establecen condiciones limitativas para las mismas, lo que consideramos que es una limitación excesiva de la libertad de circulación de los datos personales en la Unión.

Coincidentemente con lo que hemos venido sosteniendo en esta tesis, este Reglamento (al igual que todas las normas que regulan tratamientos de datos) también establece su ámbito de aplicación principalmente en los tratamientos automatizados, que son los tratamientos realizados por medios mecánicos o informáticos, entre los cuales se incluyen aquéllos llevados a cabo con alguna intervención del entorno virtual.

El art. 3.1) del Reglamento 18/1725, dedicado a las definiciones, integre en el concepto de datos personales a la noción de "*identificador*", para cuya determinación realiza una enumeración abierta o flexible de algunos elementos que se considerarán tales, como el nombre, un número de identificación, un identificador en línea pero también, lo que queremos destacar, los "*datos de localización*". Es dable comentar que en el estado actual de desarrollo de la técnica estos datos de localización se han convertido en un dato personal que está siendo captado y tratado por numerosas aplicaciones electrónicas a través del *Sistema de Posicionamiento Global*[118]*,* del cual vienen dotados un gran número de dispositivos y elementos diversos, desde vehículos hasta relojes, pasando por supuesto por móviles y ordenadores. Sin perjuicio de que por localización no debe entenderse sólo la geográfica, sino también la *virtual* determinada por los *sitios de la Red* que se visitan, es decir por la *ubicación virtual*. Por todo ello es importante la inclusión de este elemento

[118] GPS, por sus siglas en inglés correspondientes a Global Positioning System.

como identificador sin perjuicio de que, si no se lo hubiera incluido explícitamente, su consideración como identificador surge de la definición amplia que se da de "*datos personales*", pero de esta forma se hace más evidente y despeja dudas.

Otro identificador nombrado explícitamente en este artículo son los elementos propios de la identidad psíquica, que también son profusamente tratados en la elaboración de perfiles, especialmente con fines de marketing y de la concreción de determinados contratos, especialmente con empresas financieras y aseguradoras.

En el apartado 8) de este artículo 3 encontramos que, de acuerdo al ámbito de aplicación que hemos definido como *funcional,* sólo se definen como *responsables del tratamiento* a las instituciones, autoridades, organismos y órganos de la Unión.

En su adaptación al RGPD, este Reglamento designa como autoridad independiente para el control de su aplicación al Supervisor Europeo de Protección de Datos[119], autoridad sobre la que nos detendremos en el Capítulo V de este trabajo.

Los artículos 46 a 50 del Reglamento 18/1725 regulan las denominadas *transferencias internacionales de datos personales*, que es como se denomina en esta norma a la comunicación de datos personales desde un órgano u organismo de la Unión hacia un país tercero o una organización internacional, es decir, las comunicaciones realizadas a una persona o entidad que no esté sometida al derecho de la Unión. Trataremos el contenido de estos artículos en el Capítulo VI de este trabajo, dedicado específicamente a las transferencias internacionales de datos personales.

[119] En adelante, SEPD. Esto se evidencia desde el considerando 2 del Reglamento 18/1725, así como en los considerandos 51 a 61 y en algunos otros, también en el art. 1.3. de esta norma y, principalmente, en el Capítulo VI, arts. 52 a 62 que es donde se regula esta autoridad.

Encontramos que la definición del ámbito de aplicación de este Reglamento, es decir los tratamientos realizados por las Instituciones y organismos de la Unión, una definición que hemos calificado de *funcional*, es más acertada y adaptada a la realidad del entorno virtual de realización de muchos de los tratamientos, que una definición basada en un elemento geográfico, que sería extremadamente difícil de concretar en muchos casos.

Por otra parte, si bien este Reglamento entró en vigor menos de seis meses después del Reglamento 16/679, hay que recordar que este último se elevó como propuesta de la Comisión en el año 2012 y fue aprobado como Reglamento de la Unión en abril de 2016, es decir que a pesar de que su entrada en vigor es reciente, su andadura legislativa cuenta ya con varios años. Por el contrario, el Reglamento 18/1725 surgió como propuesta poco tiempo después del RGPD y se aprobó en octubre de 2018, lo que se traduce en algunos avances con respecto a la normativa general, que en algunas cuestiones (afortunadamente pocas) ya ha quedado obsoleta. Es lo observado, por ejemplo, en el apartado de las definiciones.

3.3. Norma en etapa de modificación: La Directiva 2002/58 (Directiva de la e-privacidad) y su propuesta de modificación.

A nivel de la Unión Europea, los tratamientos de datos personales en el sector de las comunicaciones electrónicas están regulados por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, que ha sido modificada por las Directivas 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo (declarada inválida

por Sentencia del Tribunal de Justicia en el caso "*Digital Rights Ireland*") y 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre.

Esta Directiva y sus modificaciones han sido aprobadas durante la vigencia de la Directiva 1995/46, a cuyas disposiciones están adaptadas e incluso se remiten a ella, como por ejemplo en el art. 1.2 y en el art. 2, al regular algunas definiciones como, concretamente, la de "*consentimiento*", o el art. 4.1. bis, que remite a la Directiva 95/46 respecto a la seguridad de los tratamientos y, muy especialmente, el art. 15, dedicado a la "*Aplicación de determinadas disposiciones de la Directiva 95/46/CE*". Por ello la primera observación que realizamos es que, al igual que ocurre con todas las normas de esta etapa, que no trata el derecho a la protección de datos personales como autónomo sino que define su objetivo como la protección de otros derechos y libertades, particularmente, los de intimidad y confidencialidad de las comunicaciones.

Su ámbito de aplicación comprende los tratamientos de datos personales efectuados en el sector de los servicios de las comunicaciones electrónicas para proteger, en general, las libertades y los derechos fundamentales, con especial incidencia en los derechos a la intimidad y a la confidencialidad de las comunicaciones, así como a la libre circulación de los datos y de los equipos y servicios, todo ello en el mismo sector de las comunicaciones electrónicas, extendiéndose algunos aspectos de su ámbito de regulación a la protección de las personas jurídicas (art. 1 apartados 1 y 2 y art. 3), a diferencia de la regulación general de protección de datos personales, que sólo protege a las personas físicas.

Al tratarse de una Directiva su objetivo es armonizar el derecho de los Estados miembros, que deben adoptar normas internas incorporando y desarrollando sus disposiciones. Por

ello la directiva no tiene aplicación o vigencia directa (salvo algunas excepciones), ya que el derecho vigente será el que adopten los Estados miembros que, como ya sabemos, es un derecho de base territorial, limitado al territorio geográfico de éstos.

Por esos motivos, el art. 1.1 de esta Directiva 2002/58 sólo se refiere a su aplicación a los tratamientos de datos personales "*en el sector de las comunicaciones*" y a la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas "*en la Comunidad*"[120]. A su vez, el subapartado 2 de este artículo dispone que las disposiciones de esta Directiva "*especifican y completan la Directiva 95/46/CE*[121] *...*".

El art. 3 apartado 1, en forma similar al art. 1.1, establece su aplicación a los tratamientos de datos personales "*en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones* de la Comunidad[122]".

En otras palabras, la aplicación territorial de esta Directiva se delega en la legislación interna de los Estados miembros, aunque se precisa que debe estar materialmente conectada con las redes públicas de comunicaciones de la Unión.

Aclaramos que por *comunicaciones* se entienden, según el art. 2.d), cualquier información intercambiada o conducida a través de los servicios o redes de comunicaciones electrónicas públicas, pero que a su vez estén dirigidas a un número determinado de abonados o usuarios que, interpretando la frase final *a sensu contrario*, deben ser identificables. Si tenemos en cuenta la gran difusión y extensión de los dispositivos

[120] Hoy Unión Europea.

[121] Hoy RGPD.

[122] El subrayado en texto normal es de la autora.

conectados hoy en día, tanto entre sí como en la red, el número de comunicaciones que se producen es astronómico, por lo que esta Directiva tiene una importancia crucial para la protección de los datos personales.

El art. 5 de la Directiva de la e-Privacidad ordena a los Estados miembros que garanticen, en su derecho interno, la confidencialidad de las comunicaciones que se realicen a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles para el público. Las medidas concretas que los Estados miembros deben adoptar para hacer efectiva esa protección son, como mínimo, la prohibición de las escuchas, grabaciones, almacenamiento y cualquier otro tipo de intervención o vigilancia tanto de las comunicaciones como de los datos de tráfico asociados a ellas, con las siguientes excepciones:

a) Cuando el interesado ha dado su consentimiento informado y de acuerdo a la Directiva 95/46 (art. 5.3);

b) Se permiten el acceso y el almacenamiento técnicos necesarios para la realización de una comunicación o la prestación de un servicio solicitado por el interesado, que deben hacerse respetando el principio de confidencialidad (arts. 5.1 y 5.3), debiendo eliminarse los datos de tráfico almacenados cuando ya no sean necesarios a tales fines (art. 6.1);

c) Se permiten las grabaciones de comunicaciones y de los tráficos asociados a ellas, cuando se realicen con el fin de acreditar una transacción o una comunicación comercial en cuyo marco se desarrollen, todo ello de conformidad con el derecho aplicable;

d) Los datos de tráfico podrán ser tratados en la medida en que sean necesarios para la facturación y pago de los servicios prestados. Una vez expirado el plazo legalmente establecido para la impugnación de la factura y la exigencia del pago, deberán eliminarse (art. 6.2).

e) Se permite a los Estados miembros limitar el alcance de los derechos protegidos por esta Directiva cuando "*... tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional… la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos…*" (art. 15.1) Todo ello conforme al Derecho de la Unión.

Esta Directiva no contiene ninguna disposición relativa a la autoridad que se encargará de su aplicación a nivel estatal, lo que por lo tanto ha quedado librado a las normas de transposición, pero sí encarga al Grupo de Trabajo del Art. 29 de la Directiva 1995/46 el ejercicio de las funciones que esta última directiva le encomienda, también en el ámbito de la Directiva de la e-Privacidad.

Por lo demás contiene disposiciones referentes a la seguridad en las comunicaciones y a algunos servicios y productos complementarios, en un lenguaje neutro y amplio que es el adecuado para una norma de la naturaleza de una Directiva y que además no impide la incorporación de nuevas tecnologías.

Como hemos expuesto, esta Directiva se basa en el concepto de *consentimiento* de la Directiva 95/46; por lo demás, quedó sumamente desactualizada al regular las comunicaciones electrónicas casi exclusivamente de terminal a terminal (como es el caso de las comunicaciones telefónicas), dejando fuera de su regulación algunos aspectos de

los terminales utilizados por los usuarios para realizar sus comunicaciones así como algunos servicios de comunicaciones que se difundieron con posterioridad a la aprobación de esta norma, como los servicios de mensajería instantánea, redes sociales, servicios de correo electrónico basados en la web y servicios de voz sobre IP. Por otra parte, existen algunas tecnologías y soportes que son utilizados para las comunicaciones y que quedan fuera del campo de aplicación de esta Directiva, como los navegadores de internet.

Introducimos aquí un punto y aparte para referirnos a algunos programas de software que tienen capacidad de intervenir o de acceder a las comunicaciones y cuyas funciones pueden interferir en éstas o recoger y someter a tratamiento datos de los usuarios que aunque en sí mismos no constituyan una intervención o accesos ilegítimos ni un atentado contra los derechos y libertades fundamentales de los interesados, si son combinados con otros datos que, generalmente, están a disposición de los responsables por medio de otros métodos, pueden permitirle la violación de los mencionados derechos y libertades. Nos referimos específicamente a las *cookies* o programas espías, que actualmente son instalados en los dispositivos de los usuarios por la práctica totalidad de las páginas de internet, así como a los programas o tecnologías de características similares que puedan surgir en el futuro. Este tipo de programas o aplicaciones electrónicas que en la actualidad infestan los dispositivos con capacidad de acceso a la red, están deficientemente regulados en esta Directiva debido a su obsolescencia, por ello es imperativo que se produzca su urgente modificación.

La Directiva 2002/58 ya ha comenzado a recorrer el camino de su modificación, a través de una propuesta de la Comisión presentada el 10 de enero de 2017 y que está siendo debatida para su adopción (por lo que el texto analizado en este trabajo puede cambiar

antes de su aprobación), para lo cual cuenta ya con el informe del Supervisor Europeo de Protección de Datos y del Comité Económico y Social Europeo.

Dicha propuesta consiste en un Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (COM(2017) 10 final), en cuya exposición de motivos (apartado 1.2) destaca que la propuesta constituirá una norma especial con respecto al RGPD, aplicable sólo a los datos personales implicados en las comunicaciones electrónicas y, por otra parte, se basa en algunas de las disposiciones de la Propuesta de Directiva para un Código Europeo de las Comunicaciones Electrónicas[123].

Se observa que, al igual que ha ocurrido con la norma de aplicación general (el RGPD), se ha elegido para actualizar la norma la forma de Reglamento, para lograr una máxima unificación del derecho vigente en la Unión en estas materias.

Pasando a su articulado vemos en primer lugar que esta propuesta de Reglamento, tal como ocurre con todas las normas de reciente aprobación que hemos analizado, considera la protección de los datos personales como un derecho autónomo, en este caso equiparándolo en su artículo 1.1 a los derechos a la privacidad y a la confidencialidad de las comunicaciones, que son los tres derechos regulados por esta norma y que consideramos de suma importancia en el desarrollo de la vida actual por lo que esperamos que las Instituciones involucradas en la redacción y aprobación de este Reglamento se tomen el tiempo que merezca su estudio y profundización. Por otra parte, el ámbito de aplicación material de este Reglamento es más amplio en un aspecto, ya que al aplicarse

[123] Propuesta de la Comisión relativa a una Directiva del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas (refundición) [COM/2016/0590 final - 2016/0288 (COD)].

fundamentalmente a la confidencialidad en la prestación y utilización de servicios de comunicaciones electrónicas, protege los datos personales y no personales y a las personas tanto físicas como jurídicas, pero es más reducido en lo que respecta a la protección de datos personales ya que, en este aspecto, constituye una norma específica con respecto al RGPD, comprendiendo sólo la libertad de circulación y los tratamientos de datos personales relacionados con las comunicaciones electrónicas y los servicios vinculados con éstas[124].

El nexo de conexión seleccionado para relacionar esta norma con el territorio de la Unión[125] es personal, concretamente la ubicación geográfica del usuario final, ya sea de los servicios de comunicaciones electrónicas o del equipo terminal utilizado para dichas comunicaciones, mientras permanezca en la Unión. Los proveedores de servicios de comunicaciones electrónicas para usuarios finales que estén en la Unión, si no poseen establecimiento en su territorio, deberán designar un representante.

El art. 4.3.a) define como "*datos de comunicaciones electrónicas*" no sólo al contenido de éstas sino también a los metadatos generados por las mismas, a los que en el apartado c) del mismo artículo define como aquéllos "*... datos tratados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas*", entre los cuales se incluyen los datos "*... utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del dispositivo generado en el contexto de la prestación de servicios de comunicaciones electrónicas, así como la fecha, la hora, la duración y el tipo de*

[124] Ámbito de aplicación material, art. 2 de la Propuesta.

[125] Establecido en el art. 3 apartado 1 de la Propuesta.

comunicación". Sobre este tipo de datos, cabe añadir que si bien en principio podrían parecer no personales o anónimos, pueden dar una gran cantidad de detalles sobre vida y hábitos sociales, laborales y familiares de los interesados si se combinan con otros, que en muchas ocasiones están al alcance de entidades interesadas en conseguirlos. Por este motivo la Sentencia *Digital Rights* los considera datos personales, declarando que su conservación constituye una injerencia en los derechos reconocidos en los arts. 7 y 8 de la Carta[126].

Al igual que la vigente Directiva, la Propuesta de Reglamento de e-Privacidad garantiza la confidencialidad de los datos relacionados con las comunicaciones electrónicas, prohibiendo todo tipo de tratamiento sobre ellos (art. 5), excepto los que realicen los proveedores de redes y servicios de comunicaciones electrónicas en las circunstancias que mencionamos a continuación:

a) los datos necesarios para la transmisión, mantenimiento, restablecimiento de la seguridad o la detección de fallos técnicos en las comunicaciones electrónicas podrán ser tratados por el tiempo que sea necesario para la finalidad del tratamiento (arts. 6.1. a) y b).

b) Los metadatos necesarios para cumplir las obligaciones del derecho de la Unión en materia de calidad del servicio (art. 6.2.c), cuando sea necesario para calcular las tarifas, la facturación, detectar o impedir la utilización abusiva o fraudulenta de este tipo de servicios (art. 6.2.d), o cuando el usuario final haya dado su consentimiento, siempre que el fin o los fines de que se trate no puedan alcanzarse mediante el tratamiento de datos anonimizados (art. 6.2.e).

[126] Apartados 26 a 29.

c) El contenido de las comunicaciones electrónicas podrá ser tratado:

1. Con el fin exclusivo de prestar a un usuario final un servicio específico para el cual sea indispensable tratar el contenido de las comunicaciones y siempre que el o los usuarios finales hayan dado su consentimiento para el tratamiento de dicho contenido (art. 6.3.a).

2. Previa consulta a la autoridad de control de conformidad con el artículo 36, apartados 2 y 3 del RGPD, con uno o más fines que no puedan ser alcanzados con el tratamiento de datos anonimizados y cuando todos los usuarios finales hayan dado su consentimiento para los fines de que se trate (art. 6.3.b).

El proveedor de los servicios de comunicación electrónica debe eliminar o anonimizar el contenido y los metadatos de las comunicaciones una vez que los haya recibido su destinatario y ya no sean necesarios para la transmisión de la comunicación concernida, con las excepciones que hemos visto precedentemente. Los usuarios finales o un tercero encargado por ellos podrán registrar, almacenar o tratar de cualquier otra forma los datos objeto de esta propuesta, de conformidad con el RGPD (arts. 7.1 y 7.2).

Cuando los metadatos sean utilizados para el cálculo de las tarifas o la facturación de los servicios de comunicación electrónica, el prestador podrá conservarlos hasta que expire el plazo legal para impugnarlas o para exigir su pago (art. 7.3).

Respecto a las *cookies* o programas espías cuya regulación constituye una de las mayores deficiencias de la actual Directiva de la e-privacidad, la propuesta de reglamento las regula en su art. 10, definiéndolas como programas informáticos comerciales que permitan comunicaciones electrónicas, que como es lógico, puede ser originario de cualquier parte del mundo. Concretamente, les exige que en el momento de su instalación

informen al usuario final sobre las opciones para la configuración de la privacidad y solicitar al usuario su consentimiento para una configuración determinada.

Los arts. 18 y 19 de esta Propuesta delegan en las autoridades de protección de datos y en el Comité Europeo de Protección de Datos regulados en el RGPD también el control de la aplicación de este futuro Reglamento, para lo cual se adaptarán las mismas competencias, funciones y poderes que establece el RGPD, incluyendo los mecanismos de cooperación y coherencia y, para el Comité, las funciones de asesoramiento relacionadas con el Reglamento sobre privacidad en las comunicaciones electrónicas.

3.4. Jurisprudencia.

Hemos manifestado que la Directiva 95/46 apenas contiene disposiciones dedicadas a su aplicación extraterritorial, hecho que constituyó una carencia grave de esta norma y que en el transcurso del tiempo que estuvo vigente fue paliada por la interpretación jurisprudencial tanto de órganos jurisdiccionales nacionales como del Tribunal de Justicia de la entonces Comunidad Europea, hoy Unión Europea.

Sin perjuicio de que en el desarrollo de los distintos puntos de este trabajo incluiremos referencias a la jurisprudencia del Tribunal de Justicia, queremos hacer mención expresa a algunos de sus pronunciamientos que son de especial relevancia para nuestra investigación, si bien sólo como manifestación de las etapas atravesadas en su evolución ya que la mayoría de las interpretaciones realizadas por la jurisprudencia, no sólo de la Directiva como norma positiva vigente sino también de los principios generales del derecho a la protección de los datos personales han sido acogidos en las normas

recientemente modificadas y en los proyectos de modificación, por lo que sus pronunciamientos serán valorados conjuntamente con éstos.

3.4.1. Sentencia Lindqvist (2003)

Comenzaremos con el caso Lindqvist[127] caso del que, además del interés que ofrece por su importancia para el estudio de la vigencia del derecho europeo de protección de datos, es digno de mención una de las principales cuestiones que en él se plantearon: si algunas medidas contenidas en la Directiva (concretamente el consentimiento previo para el tratamiento de datos personales, la comunicación previa a una autoridad de control o la prohibición de tratamiento de datos personales delicados) excedían la proporcionalidad y eran contrarias a otros derechos y libertades reconocidos por el derecho de la Unión, tal como la libertad de expresión. La defensa de la acusada en el asunto principal cuestiona también la validez misma de la protección de datos personales como garantía del derecho a la intimidad, ya que hechos tales como: "…*citar nominalmente a una persona física, divulgar sus datos telefónicos y sus condiciones de trabajo, proporcionar información sobre su estado de salud y sus aficiones*…" constituye información pública, notoria y trivial, que por sí no vulnera el derecho a la intimidad y su restricción constituye, por lo tanto, una medida desproporcionada[128].

Este cuestionamiento de la parte acusada en los asuntos principales surge como una consecuencia de la consideración de la protección de datos personales como un derecho instrumental, útil sólo para la protección del derecho al cual custodiaba en el momento en que se dictó esta sentencia, que era el derecho a la intimidad. En el momento presente, en

[127] Sentencia del TJCE de 6 de noviembre de 2003.

[128] Sent. Lindqvist, apartado 74.

que el derecho de protección de datos es considerado un derecho autónomo y no al servicio de otro, este cuestionamiento no tiene cabida.

El Tribunal de Justicia, tras un análisis de la Directiva 95/46, de los valores que la inspiraban y de la realidad de los tratamientos de datos personales en Europa[129], expresa que dicha Directiva intenta proteger tanto la libertad de circulación de datos personales como el derecho de las personas físicas a la protección frente al tratamiento ilícito de éstos, y que en virtud de ello es una norma flexible y en ocasiones abierta, a efectos de que sean los Estados miembros los que, al transponerla, elijan soluciones más concretas. Y, lo que es más importante, nada en sus disposiciones permite concluir que éstas sean, por si mismas, contrarias a los principios generales del derecho comunitario y, en particular, a los derechos fundamentales[130]. Tanto el derecho a la protección de la intimidad como la libertad de expresión están protegidos por el ordenamiento comunitario y en virtud de las disposiciones de la Directiva 95/46 deben ser los estados los que ponderen los intereses en juego en cada caso, decidiéndose por el mejor equilibrio entre ellos[131]. En definitiva, las disposiciones de la Directiva no son, *per se*, desproporcionadas ni atentan contra el derecho y, en los casos concretos, son los Estados los encargados de ponderar los derechos en juego para garantizar que exista un equilibrio entre ellos.

Es éste el primer caso en el que se planteó una cuestión íntimamente relacionada con la falta de correlación con un espacio geográfico y, a la vez, ubicuidad del *ciberespacio*: si la difusión de datos personales en una página web, accesible desde cualquier país del mundo constituye una transferencia de datos a un país tercero, aún cuando no se haya

[129] Sent. Lindqvist, apartados 79 a 81.

[130] Sent. Lindqvist, apartados 82 a 84.

[131] Íbidem, apartados 85 a 87.

acreditado que un nacional de un país tercero ha accedido a dicha página, o cuando no se pueda determinar si esto ha sucedido.

El Tribunal de Justicia, teniendo en cuenta la naturaleza técnica de las operaciones efectuadas y la regulación de las transferencias en la Directiva 95/46 (más específicamente, su art. 25), decide esta cuestión teniendo en consideración que, a priori, la ubicuidad de internet hace imposible localizar geográficamente los datos subidos a un sitio web, dado que tanto las personas como los medios tecnológicos que intervienen en el proceso de publicación de la información en la Red pueden hallarse en distintos países del globo e, incluso, es posible que no se pueda determinar con exactitud la ubicación de uno o más de estos elementos. De la misma forma, el receptor de dichos datos (quien accede a la página) puede hallarse en cualquier otro país[132].

Sin embargo, la publicación de información en internet no consiste en una transferencia directa de datos, porque una página con las características de la de este caso no contiene los mecanismos técnicos necesarios para enviar la información a otra persona y por ello no se puede considerar que realice una transferencia directa sino que quien quiera consultar dicha información debe en primer lugar conectarse y luego realizar un número de operaciones técnicas para acceder a la misma, es decir que es el internauta quien la recoge de allí donde la ha ubicado el creador de la página y no éste quien la envía[133].

A continuación realiza un análisis del contenido del Capítulo IV de la Directiva y, especialmente, su artículo 25[134], concluyendo[135] que en el mismo no se hace ninguna

[132] Sentencia Lindqvist, apartados 58 y 59.

[133] Sent. Lindqvist, apartados 60 y 61.

[134] Sent. Lindqvist, apartados 62 a 69.

[135] En los apartados 70 y 71 de la Sent. Lindqvist.

referencia a la publicación de información en internet, que en el momento de redacción de la Directiva ya se encontraba en estado bastante avanzado como para que el legislador, si la hubiera querido incluir en esta regulación, podría haberlo hecho. Pero muy especialmente tiene en cuenta el Tribunal de Justicia que, si se entendiera que la publicación de información en internet constituye una transferencia internacional de datos personales según el art. 25 de la Directiva y dado el régimen de control por parte de las autoridades de aplicación que prevé ese artículo, éstas se convertirían prácticamente en órganos de censura al verse en la obligación de controlar toda publicación en una página web a efectos de no permitir la publicación de datos personales en los casos en que el acceso a la página de que se trate pudiera hacerse desde cualquier país del mundo, incluidos aquéllos que no ofrecen un nivel adecuado, lo que sucede en la gran mayoría de las páginas de internet.

Por todo ello el Tribunal concluye que operaciones como las efectuadas por la Sra. Lindqvist no constituyen transferencias de datos personales a un país tercero (apartado 71).

Como comentario final a esta sentencia, resaltar que si bien en algunos párrafos, como el 88, el TJUE se refiere a las sanciones contra los tratamientos ilegítimos de los datos personales como requisitos necesarios para la tutela de la intimidad, en los párrafos 81 y 82 trata a la protección de datos personales como un auténtico derecho autónomo, al expresar que: "… *las personas afectadas por el tratamiento de datos personales reclaman con razón que dichos datos se protejan de manera eficaz*" (párrafo 81), ya que no se relaciona esa protección con la de la vida privada; y en el párrafo siguiente, al reconocer que la Directiva 95/46 establece la licitud de los tratamientos en base a la ponderación de diferentes derechos e intereses.

3.4.2. Sentencia Promusicae (2008)

En este caso el Tribunal de Justicia de la Comunidad Europea se pronunció, entre otras cuestiones, en el sentido de que el artículo 13 de la Directiva 95/46, al permitir a los Estados miembros limitar los derechos de los interesados para salvaguardar los derechos y libertades de otras personas [art. 13.1.g) Directiva 95/46], no restringe esa posibilidad a determinados derechos, permitiendo así la inclusión de la preparación de una acción civil entre los motivos que habilitan esa limitación; por lo tanto, es conforme con el derecho comunitario una norma interna que obligue al responsable a ceder los datos personales a un tercero con la finalidad de la preparación de acciones civiles[136]. Sin embargo, ni la mencionada Directiva ni otras normas comunitarias obligan a los Estados miembros a imponer a los responsables de tratamiento de datos personales la obligación de comunicar los datos a terceros con motivo de acciones civiles; pues el derecho europeo sólo les exige que a la hora de transponer distintas Directivas a su derecho interno, "*procuren basarse en una interpretación de éstas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario*" y que "*en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también no basarse en una interpretación de éstas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad*."[137]

[136] Sentencia *Promusicae*, párrafo 54.

[137] Sentencia *Promusicae*, párrafo 70.

Más allá del contexto y de su significación precisa, estas normas establecen algunas bases por las que se debe guiar no sólo el legislador de los Estados miembros, sino todos quienes aplican e interpretan el derecho europeo en los casos en que haya un enfrentamiento entre dos o más derechos y libertades fundamentales: Se debe lograr un equilibrio entre todos los derechos y libertades en juego, es decir que ninguno de ellos prevalezca sobre los otros sin fundamentación legítima; que la normativa interna sea interpretada de una manera compatible con los derechos fundamentales y con los principios generales del Derecho europeo.

3.4.3. Sentencia Digital Rights (2014)

En esta sentencia el Tribunal de Justicia de la Unión Europea pondera el equilibrio o prevalencia entre el derecho a la protección de datos, el derecho a la intimidad o a la vida privada y otros derechos fundamentales.

Así, en el párrafo 51, el Tribunal de Justicia declara que a pesar de que la lucha contra la delincuencia grave, especialmente la delincuencia organizada y el terrorismo es de vital importancia, la protección de los datos personales es un derecho fundamental y, por lo tanto, las excepciones y restricciones a este derecho aunque se motiven en la lucha contra esos tipos de delitos no deben sobrepasar los límites de lo estrictamente necesario, con reglas claras y precisas[138], en especial cuando los datos personales se sometan a un tratamiento automático y el riesgo de acceso ilícito a los mismos sea elevado[139].

Con esos fundamentos en esta Sentencia el Tribunal declara inválida la Directiva 2006/24, porque establecía una obligación de conservación de los metadatos generados por todas

[138] Sentencia Digital Rights, párrafo 54.

[139] Ibídem, párrafo 55.

las comunicaciones electrónicas (es decir, todo tipo de datos relativos a éstas con excepción de su contenido), de entre seis y veinticuatro meses, sin ningún tipo de distinción ni limitación con respecto a los interesados a los que afecta (comprende a todos los usuarios y abonados de todos los medios de comunicación electrónica) ni a los tipos de datos, ni exige que las comunicaciones afectadas tengan alguna relación con los delitos graves[140]. En otras palabras, la medida que consiste en la conservación de los metadatos generados por todas las comunicaciones electrónicas de la población europea en general, sin ningún tipo de límite ni criterio de aplicación selectiva, no constituye una medida proporcionada, por lo que se declara inválida.

Este caso consiste en una aplicación concreta de las normas de equilibrio entre dos valores fundamentales de la Unión Europea: Por un lado la protección de datos personales y el derecho a la vida privada, y por otro el interés por la persecución de la delincuencia grave. La conclusión que podemos extraer es que, si bien los derechos fundamentales a la protección de datos personales y a la vida privada pueden ceder frente al interés público por la persecución de la delincuencia grave, esa cesión no puede ser ilimitada sino que tiene que responder a criterios objetivos y límites claros.

3.4.4. Sentencia Google Spain (2014)

La Sentencia *Google Spain* (o simplemente *Google*) es una de las más trascendentales para la doctrina en el campo de la protección de datos porque fue la que introdujo en una fuente de derecho europeo el conocido como *derecho al olvido*, del que hasta ese

[140] Párrafos 57 y 58.

momento sólo se conocían algunas manifestaciones en el campo doctrinal[141]; y ello a pesar de que este derecho sólo se menciona un par de veces[142] y sólo en citas de escritos de las partes: las preguntas de las cuestiones previas en la primera ocasión, y los escritos de una de las partes y de dos gobiernos europeos que apoyan su postura, en la segunda. Es decir, que el Tribunal de Justicia no se refiere a esta especial aplicación del derecho a la eliminación de datos personales con ese nombre.

Más allá de eso, la importancia de esta sentencia viene dada también por el hecho de que el Tribunal de Justicia se pronuncia sobre algunos aspectos esenciales en el derecho europeo de protección de datos que le dan parte de su configuración actual, tales como la calificación como "tratamiento de datos personales" de las actividades de los buscadores de internet, la calificación de éstos como responsables de dichos tratamientos[143] y, finalmente, la introducción de la expresión "*elaboración de un perfil*", sobre la que se expresa en los siguientes términos: "…*un tratamiento de datos personales… efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no*

[141] En de Terwangne, C: *Privacidad en Internet y el derecho a ser olvidado/derecho al olvido*, en: IDP, Revista de los Estudios de Derecho y Ciencia Política de la UOC, Número 13 (Febrero 2012), la autora realiza una completa exposición del derecho al olvido en sus tres facetas, un par de años antes de la sentencia Google.

[142] En los párrafos 20.3) y 91.

[143] Sent. Google Spain, apartado 41.

se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate[144]. Esta es una noción fundamental en el derecho de protección de datos personales y también íntimamente relacionada con el entorno tecnológico en el que se inserta este derecho puesto que sólo ese entorno permite a cualquier persona el acceso a una cantidad ingente de información con un coste muy bajo tanto de tiempo como de recursos, lo que facilita sobremanera la *elaboración de perfiles*.

Pero la mayor importancia de esta sentencia para nuestro objeto de investigación radica en el pronunciamiento respecto al art. 4.1.a) de la Directiva 95/46 y, más precisamente, a las expresiones "establecimiento" y "marco de las actividades" de dicho establecimiento. La discusión sobre estos aspectos surgía a causa de que Google Inc (casa matriz de Google, establecida en los Estados Unidos) así como su filial en España (Google Spain) rechazaban que les resulte aplicable el derecho europeo de protección de datos dado que las actividades de tratamiento de datos personales que eran objeto del asunto principal no se realizaban en España sino en la casa matriz, es decir en un país tercero. La filial española sólo llevaba a cabo la promoción y venta de la publicidad en su página web. El TJUE resuelve que si un establecimiento en un Estado miembro se dedica a la promoción y venta en dicho Estado de los espacios de publicidad que permiten la explotación económica de los servicios que presta un establecimiento en un estado tercero, que incluyen el tratamiento de datos personales, procede declarar que dicho tratamiento de datos se realiza en el marco de las actividades del establecimiento en la Unión (apartado

[144] Sent. Google Spain, apartado 80.

55). Y ello porque las actividades de ambos establecimientos, principal y filial, están "*indisociablemente ligadas*"[145]

Este pronunciamiento es fundamental para algunos de los aspectos del derecho de protección de datos personales que estamos destacando en este trabajo, cuales son los de su calificación como derecho tecnológico y el hecho de que una gran cantidad de los tratamientos se realizan en el espacio virtual, del que las actividades de los motores de búsqueda son, qué duda cabe, un claro exponente. Por ello el punto de conexión elegido por la Directiva 95/46 y mantenido por el RGPD tal como veremos en el capítulo siguiente, que está compuesto por un elemento físico que lo relaciona con el territorio de la Unión (un establecimiento situado en un Estado miembro) y otro elemento que denominamos *contextual* y que permite conectarlo con el ciberespacio, "el marco de las actividades", cuya abstracción (cualidad que puede llegar a resultar antijurídica en otros campos) es necesaria en este ámbito del derecho, tal como lo expresa el mismo Tribunal en los apartados 53 y 54 de esta Sentencia:

"*…visto el objetivo de la Directiva 95/46 de garantizar una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales, esta expresión no puede ser objeto de una interpretación restrictiva (véase, por analogía, la sentencia L'Oréal y otros, C-324/09, EU:C:2011:474, apartados 62 y 63).*

54. En este marco, cabe señalar que se desprende, concretamente de los considerandos 18 a 20 y del artículo 4 de la Directiva 95/46, que el legislador de la Unión pretendió evitar que una persona se viera excluida de la protección garantizada por ella y que se

[145] Sent. Google Spain, apartado 56.

eludiera esta protección, estableciendo un ámbito de aplicación territorial particularmente extenso."

Y que "…*no se puede aceptar que el tratamiento de datos personales llevado a cabo para el funcionamiento del mencionado motor de búsqueda se sustraiga a las obligaciones y a las garantías previstas por la Directiva 95/46, lo que menoscabaría su efecto útil y la protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas que tiene por objeto garantizar (véase, por analogía, la sentencia L'Oréal y otros, EU:C:2011:474, apartados 62 y 63)*…"[146]. Este aspecto de la elaboración de perfiles realizada a través de los motores de búsqueda es una característica de los tratamientos de datos realizados en el ciberespacio, que permite la disponibilidad de éstos para cualquier persona, desde cualquier parte del mundo, a través de una operación muy sencilla, de coste muy bajo y de acceso universal.

En este pronunciamiento el TJUE, al declarar a Google Inc responsable por el tratamiento de datos personales que realiza el motor de búsqueda, de forma autónoma respecto a los titulares de las páginas web que el motor indiza (que solo son responsables por los tratamientos que realizan en éstas) declaró que también son autónomas las obligaciones respecto a los derechos de los interesados, en el sentido de que una página puede realizar tratamientos de datos personales que se consideren lícitos y, sin embargo, el tratamiento realizado por los motores de búsqueda al incluir esa página en un listado de direcciones de internet que aparezcan como resultado de una determinada búsqueda puede ser ilegítimo.

[146] Sent. Google Spain, apartado 58.

Eso puede ocurrir porque pueden diferir los intereses legítimos que justifican ambos tratamientos, como sucede en el asunto original de esta cuestión prejudicial, en el cual el tratamiento originario (el realizado por la página web) estaba legitimado por la libertad de prensa, mientras que no ocurría lo mismo con la actividad del motor de búsqueda, que no puede considerarse una mera reproducción de la página originaria sino que, al incluirla en un listado junto con otras, permite realizar un perfil del interesado[147], con lo cual difieren también las consecuencias que uno y otro tratamiento tienen sobre el interesado.

Finalmente, esta Sentencia decide también sobre el equilibrio entre el derecho a la protección de datos del interesado (arts. 7 y 8 de la CDFUE) y el derecho de los internautas de acceso a la información a través de los motores de búsqueda, aspecto sobre el cual decide que tanto con carácter general como en este caso concreto debe prevalecer el derecho a la protección de datos personales, sin perjuicio de que la preponderancia de uno u otro derecho puede variar dependiendo de "*... la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública.*"[148]

3.4.5. Sentencia Schrems (2014)

En el asunto principal de esta cuestión prejudicial un ciudadano austríaco, el Sr. Schrems, solicitaba que se impida a la sociedad que explota la red social Facebook la transferencia de sus datos personales hacia su matriz, Facebook Inc., ubicada en los Estados Unidos, sosteniendo que el mencionado país tercero no contaba con un nivel adecuado de

[147] Sent. Google Spain, apartados 81, 85 y 88.

[148] Sent. Google Spain, apartado 81.

protección de datos personales, conforme al standard europeo. Ahora bien, las transferencias de datos personales de Facebook Ireland hacia su matriz en Estados Unidos estaban cubiertas por la Decisión 2000/520, conocida como los "*Principios de Puerto Seguro*", por lo que en definitiva solicitaba la declaración de nulidad de esta Decisión.

El Sr. Schrems en su petición, dirigida en primer lugar a la autoridad irlandesa de protección de datos, que llegó al TJUE en el curso de un recurso judicial de revisión de sus actos por la justicia irlandesa, refleja la relación entre las operaciones electrónicas ejecutadas en el espacio virtual y su manifestación en la vida real de las personas, sobre la que hemos expuesto brevemente en la Introducción de este trabajo, ya que cuando los usuarios introducen sus datos personales en la red social Facebook, desde cualquier parte del mundo, los mismos quedan a disposición de la sociedad matriz, Facebook Inc., con sede social en los Estados Unidos; incluso dentro de ese extenso país, la ubicación concreta es desconocida ya que se mantiene secreta por motivos de seguridad. En este marco, el derecho de la Unión Europea, correctamente interpretado y aplicado por el Tribunal de Justicia, desplegó sus efectos para proteger a los ciudadanos frente al tratamiento de sus datos personales, incluso ante una Decisión de la Comisión que había quedado vacía de contenido merced a información hecha pública con posterioridad a su adopción.

El ciudadano austríaco que hemos mencionado, luego de que Edward Snowden revelara que el gobierno de los Estados Unidos monitoreaba datos personales de distintas categorías y naturaleza a través de diversos órganos y agencias federales, consideró que estos hechos no habían sido tenidos en cuenta al adoptarse la Decisión 2000/520 por parte de la Comisión y que ésta por lo tanto había quedado vacía de contenido.

El Tribunal de Justicia declara la nulidad de la Decisión 2000/520[149], debido a que considera constatado que las autoridades estadounidenses podían tener acceso a los datos personales de ciudadanos europeos que habían sido transmitidos y tratarlos de manera incompatible con las finalidades de esa transferencia, en especial de forma desproporcional e indiscriminada[150].

Agregar que la Decisión 2000/520 había sido adoptada por la Comisión para permitir el flujo de datos personales entre Europa y Estados Unidos, que tal como ya hemos comentado ha adquirido una importancia económica fundamental para las economías de ambas regiones y, en consecuencia, si se veía impedido u obstaculizado hubiera conducido a pérdidas económicas significativas para muchas empresas de ambos continentes. En este contexto, la sentencia del TJUE significo un claro aviso para las Instituciones de que la economía no debe primar sobre la protección de los derechos fundamentales, que se puede y se debe buscar fórmulas de consenso que constituyan un equilibrio entre ambos valores.

3.4.6. Sentencia Weltimmo (2015)

En esta sentencia el TJUE analiza nuevamente el concepto de "*establecimiento*" contenido en la Directiva 95/46, al que da un contenido distinto en derecho de Sociedades que en el derecho de protección de datos[151].

[149] Sentencia Schrems, apartado 106.

[150] Sentencia Schrems, apartado 90 y 93 a 95. Sin perjuicio de que en los apartados 99 a 104 también se invalida el art. 3 de dicha Decisión debido a que el Tribunal considera que la Comisión, al restringir las facultades que la Directiva 95/46 concedía a las autoridades nacionales de control, se excedía de sus competencias.

[151] Sentencia Weltimmo, apartado 17.

Por ello, basándose en gran medida en la Sentencia Google Spain[152] y analizando el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en el establecimiento del Estado miembro de que se trate (parámetros que declara especialmente aplicables a las empresas que ofrecen servicios exclusivamente a través de internet[153]), declara que: "*la presencia de un único representante puede bastar, en determinadas circunstancias, para constituir una instalación estable si actúa con un grado de estabilidad suficiente a través de los medios necesarios para la prestación de los servicios concretos de los que se trate en el Estado miembro en cuestión*"[154]. En el asunto principal, una sociedad registrada en un Estado miembro, a través de una página web redactada exclusivamente en el idioma de otro Estado miembro, gestiona inmuebles en este último Estado, en el cual tiene un representante estable y ha abierto una cuenta bancaria para los pagos que reciba por los servicios prestados en los inmuebles que gestiona.

Por todo ello el TJUE declara que el tratamiento de datos personales en cuestión se realiza en el marco de las actividades del establecimiento en ese Estado miembro y, por lo tanto, se le puede aplicar la ley local[155], independientemente de que el registro y, por lo tanto, el "establecimiento" a los efectos mercantiles (que no se analizan en este caso) se haya efectuado en un Estado miembro distinto.

El caso Weltimmo es un claro exponente de un hecho sobre el que llamaremos la atención en más de una oportunidad en este trabajo de investigación: La utilización del espacio

[152] Sent. Weltimmo, apartados 25 a 28

[153] Sent. Weltimmo, apartado 29.

[154] Sent. Weltimmo, ap. 30.

[155] Sent. Weltimmo, ap. 39.

virtual o de la facilidad que dan las conexiones electrónicas para eludir una conexión geográfica a efectos de actuar en fraude de ley o de terceros. En este caso, el TJUE acertadamente consideró que la inscripción en el Registro de un Estado miembro carece de relevancia en el derecho de protección de datos si los efectos de las actividades de tratamiento por las cuales es responsable la sociedad se producen en otro Estado.

3.4.7. Sentencia Tele 2 Sverige (2017)

En este caso se juzga la validez, frente al derecho europeo, de las normas sueca y británica de transposición de la Directiva 2002/58 que, al igual que ésta, disponían la obligación de los prestadores de servicios de comunicación de conservar por largos períodos de tiempo todos los metadatos, datos de tráfico, de localización y otros, relativos a las comunicaciones realizadas por todos los usuarios a los que prestaban servicios. El Tribunal opina que la conservación de tales datos puede ser una herramienta valiosa para la lucha contra la delincuencia grave; pero también constituye una excepción a la confidencialidad de las comunicaciones[156] y por ello es necesario que la normativa que la imponga fije criterios objetivos a cumplir por los interesados o los datos que deban ser conservados, y también requisitos para el acceso de las autoridades a dichos datos, todo lo cual en mérito al principio de proporcionalidad se debe limitar a lo estrictamente necesario, lo que implica tener al menos una relación indirecta con los fines perseguidos por la normativa[157]. El acceso de las autoridades a los datos conservados debería estar sujeto a un control jurisdiccional previo (salvo casos excepcionales) pues la normativa

[156] Sent. Tele 2 Sverige, apartado 115.

[157] Sent. Tele 2 Sverige, apartado 119.

que permita a las autoridades un acceso generalizado y sin restricciones convierte en regla general lo que debería ser la excepción.

Por otra parte, el TJUE encuentra que la conservación indiscriminada y masiva de los datos de los usuarios, sin obligación de informar, que disponían las normativas examinadas podía crear en los usuarios la idea de una vigilancia constante de sus comunicaciones, lo que según el Tribunal finalizaría por afectar a su libertad de expresión[158]. Esta injerencia masiva e indiscriminada en la mencionada libertad, así como en los derechos a la vida privada y a la protección de los datos personales de los interesados no está justificada y, por lo tanto, la normativa es contraria a los artículos 7, 8, 11 y 52, apartado 1 de la Carta[159].

Resumiendo, el TJUE encuentra que una normativa que no ponga límites a la conservación de los datos ni requisitos objetivos para el acceso de las autoridades, ni sujete estas operaciones al control judicial o de las autoridades de protección de datos personales, es contraria al derecho europeo[160].

Nuevamente nos encontramos en este caso con la aplicación concreta de las reglas de armonización entre distintos valores fundamentales del sistema jurídico de la Unión Europea: Por un lado el interés público por la persecución de la delincuencia grave y por otro, la libertad de expresión, el derecho de protección de datos personales y la confidencialidad de las comunicaciones. El TJUE decide que si bien, tal como las normas europeas de protección de los derechos y libertades mencionados en el segundo grupo lo establecen, éstos pueden encontrar ciertos límites en mérito al interés público del primer

[158] Sent. Tele 2 Sverige, apartado 101.

[159] Sent. Tele 2 Sverige, apartado 112.

[160] Sent. Tele 2 Sverige, apartado 125.

término, pero dichos límites deben establecerse como excepciones y respetar el principio de proporcionalidad. Toda excepción o limitación a la protección de los derechos y libertades fundamentales que no cumpla con estos requisitos es contraria al derecho europeo.

CAPÍTULO III. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES (RGPD)

1. Aspectos generales y comparación con la Directiva 95/46.

Actualmente, la disposición general sobre protección de datos personales vigente en el derecho derivado de la Unión es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[161].

El Reglamento es la norma de aplicación general para los tratamientos de datos personales vinculados a la Unión[162], pero no la única. Conjuntamente con él, en abril de 2016, se aprobaron otras dos normas en este ámbito: La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo ("Directiva 2016/680") y la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros

[161] Que en adelante denominaremos indistintamente "El Reglamento" o "RGPD".

[162] Sin perjuicio de que continuemos refiriendo a la vigencia de esta norma en la Unión, debemos aclarar que la misma fue incorporada al Acuerdo del EEE a través de la Decisión 154/2018 del Comité Mixto del EEE, adoptada en Brusela el 6 de julio de 2018.

(PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave ("Directiva 2016/681"). Existen asimismo otras normas que regulan otros aspectos de la misma materia, como los ya mencionados 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, y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[163]. Esta última norma también regula derechos fundamentales como los de la intimidad y el honor, pero su ámbito objetivo de aplicación no se limita a la protección de datos ya que abarca en general la privacidad en las comunicaciones electrónicas, de ahí que se la denomine "Directiva de la e-privacidad".

Cabe mencionar que el RGPD tiene carácter internacionalmente imperativo y está sometido a una conexión autónoma establecida en su artículo 3 que estudiaremos más adelante. Ello implica que esta norma debe ser obligatoriamente aplicada por los tribunales europeos e internos de los Estados miembros, incluso en casos relacionados

[163] Actualmente esta Directiva está en etapa de reforma, habiéndose aprobado por la Comisión un borrador de Reglamento para su sustitución, titulado: COM (2017) 10: 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), que se encuentra en etapa de discusión en el Consejo. La intención de la Comisión es que este Reglamento se apruebe con el tiempo suficiente para que entre en vigor en la misma fecha del Reglamento General del Protección de Datos, es decir el 258 de mayo de 2018. En adelante nos referiremos a este proyecto de Reglamento como el "Proyecto de Reglamento de e-privacidad".

con contratos internacionales regidos por el derecho de un estado tercero con respecto a la Unión, según lo dispuesto por el art. 9.2 del Reglamento Roma I[164].

Respecto a la finalidad del Reglamento y tal como su título lo indica, no es sólo la de proteger a las personas físicas en cuanto al tratamiento de sus datos personales, sino también garantizar la libre circulación de éstos dentro del territorio de la Unión.

El Reglamento desarrolla el derecho originario de protección de datos como derecho de fondo, designando a las autoridades nacionales como los principales órganos ejecutivos de aplicación del mismo, con una serie de reglas de determinación de la autoridad nacional que tendrá competencia prioritaria en el caso concreto, cuando se encuentren involucrados elementos que podrían determinar la competencia de diferentes autoridades nacionales. A través de un Reglamento se intenta mantener la seguridad jurídica y práctica para las personas[165].

La sustitución de la Directiva por un Reglamento responde en gran medida a que los objetivos de este derecho sólo se pueden cumplir cabalmente si la protección de los datos personales, tanto formal como en la práctica, es homogénea en todo el territorio de la Unión, ya que el anterior sistema basado en una directiva dejaba un margen de autonomía demasiado amplio a los Estados miembros, y las diferencias tanto formales como prácticas han constituido trabas para la integración económica y social[166].

---

[164] De Miguel Asensio, P.A: *Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea*. Revista Española de Derecho Internacional, Vol. 69 Tomo I, 2017. Pág. 104.

[165] RGPD, Considerando 7.

[166] Troncoso Reigada, A: *Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una*. Revista d'internet, dret i política, número 15, noviembre 2012, pp. 61-75. En línea en <http://idp.uoc.edu/ojs/index.php/idp/article/view/n15-troncoso/n15-troncoso-es>.

Un nivel equivalente de protección de datos personales en los estados miembros facilita la libertad de circulación de los datos. Para ello, el Reglamento General de Protección de Datos, en varios de sus artículos[167] y, especialmente, en las disposiciones relativas al mecanismo de coherencia para su aplicación, establece la obligación para las autoridades de control, de contribuir a la aplicación coherente del Reglamento en el territorio de toda la Unión. Específicamente, en los arts. 60 a 64, se establecen mecanismos de coordinación y cooperación entre las autoridades de control.

En la concepción del legislador europeo, manifestada en el considerando 4 del Reglamento, el derecho a la protección de datos debe estar concebido para servir a la humanidad y, por lo tanto, no es un derecho absoluto, sino que debe ejercerse en armonía con otros derechos fundamentales y está sometido al principio de proporcionalidad. De acuerdo con lo expuesto en el Capítulo I de este trabajo, a través del RGPD se pretende brindar protección a otros derechos fundamentales, tales como el derecho a la intimidad, el respeto de la vida privada y familiar, del domicilio y de las comunicaciones[168], el derecho al honor y a la propia personalidad. Por otro lado, la protección de datos personales, en tanto que derecho-garantía, entra en colisión con otros derechos y libertades fundamentales, entre los cuales destacan la libertad de circulación de esos datos, la libertad de expresión, libertad de acceso y de difusión de la información, de culto, de las artes y las ciencias y de cátedra por poner sólo algunos ejemplos. Y, en lo que respecta a la Unión Europea, formando parte de su riqueza social, la protección de

[167] Por ejemplo, arts. 28.8; 35.6; 46.4; 47.1; 51.3, etc. Pero, especialmente, el Capítulo VII, "*Cooperación y coherencia*", Secciones 1 y 2, artículos 60 a 67.

[168] Troncoso Reigada, A: Op. cit.

los datos personales es también protección de su diversidad cultural, religiosa y lingüística.

Por todo ello, tanto la protección de los datos personales como el respeto de la privacidad y la libertad de circulación de dichos datos son valores necesarios para el crecimiento social y económico, especialmente en un entorno de integración y eliminación de barreras sociales, económicas y culturales tal como es la Unión Europea. Protección de datos personales y libertad de circulación de los mismos son dos hechos que se retroalimentan, se fortalecen recíprocamente y son interdependientes.

Hemos mencionado ya que la Directiva 95/46 había quedado obsoleta por el desarrollo tecnológico y porque, durante los años en que estuvo vigente, se hizo patente que este tipo de actos legislativos europeos, que deben ser interpretados por cada Estado y adaptados a las particularidades de cada uno de ellos para su transposición, no establecen reglas claras ni protección uniforme en todo el territorio de la Unión.

Como toda Directiva, la 95/46 requería la aplicación de los derechos nacionales o, dicho de otra forma, del derecho de la Unión a través de las normas de transposición de la propia Directiva, cuestión que genera desigualdad en el territorio de la Unión, siendo fuente de inseguridad jurídica y como tal fue tratada por el Tribunal de Justicia en distintas sentencias, entre ellas las conocidas como "Google Spain"[169] y "Weltimmo"[170] que hemos examinado en el capítulo anterior.

[169] Sentencia del TJUE (Gran Sala), de 13 de mayo de 2014, En el asunto C 131/12, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Audiencia Nacional, mediante auto de 27 de febrero de 2012, recibido en el Tribunal de Justicia el 9 de marzo de 2012, en el procedimiento entre Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González (ECLI:EU:C:2014:317).

[170] Sentencia del TJUE, (Sala Tercera), de 1 de octubre de 2015 C 230/14, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Kúria [Tribunal Supremo] (Hungría), mediante resolución de 22 de abril de 2014, recibida en el Tribunal de Justicia el 12 de mayo

Al hilo de estas consideraciones cabe recordar que el ámbito de aplicación territorial de la Directiva se basaba en un establecimiento del responsable y, si un responsable contaba con establecimientos en varios Estados miembros debía garantizar, en cada uno de esos establecimientos, el respeto a la legislación nacional sobre protección de datos (considerando 19 de la Directiva), disposición ésta que deja en evidencia la carga administrativa que la Directiva implicaba para las empresas con establecimientos en varios Estados miembros y también la falta de homogeneidad que la propia norma estaba recogiendo. Por ello la definición del ámbito de aplicación territorial en la Directiva (art. 4) se dirigía hacia el derecho del Estado miembro que resultara aplicable, mientras que el art. 3 del RGPD define su propio ámbito de aplicación territorial, en calidad de norma aplicable en forma directa[171].

Para solventar los problemas de regulación que habían surgido con motivo de la interpretación de la Directiva tanto por las autoridades nacionales de aplicación (administrativas y judiciales) como por las autoridades comunitarias y, a su vez, para adaptar el derecho europeo de protección de datos a los adelantos tecnológicos, se optó por un Reglamento que, al tener vigencia directa en todos los Estados, elimina las desigualdades creadas por las normas de transposición necesarias para las Directivas, que constituyen obstáculos para la libre circulación de datos y, con ello, también al ejercicio de las actividades económicas en la Unión[172]. Una protección uniforme garantiza una

---

de 2014, en el procedimiento entre Weltimmo s. r. o. y Nemzeti Adatvédelmi és Információszabadság Hatóság (Autoridad húngara de protección de datos) (ECLI:EU:C:2015:639).

[171] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Comité Europeo de Protección de Datos, adoptada el 16 de noviembre de 2018, Pág. 3. Accesible desde el sitio web: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en (último acceso 07/04/2019).

[172] Considerando 9 del Reglamento.

mayor libertad de circulación de los datos personales. Al mismo tiempo, se deja un margen de maniobra a los Estados miembros para que especifiquen las normas del Reglamento[173], si bien se trata de un margen mucho menor que el de la Directiva.

En base al objetivo fijado para esta investigación, se analizarán en especial las disposiciones del RGPD destinadas a regular la libertad de circulación de los datos personales y de regulación de competencias estatales en el interior del ámbito de aplicación territorial del derecho de la Unión así como también a las disposiciones que regulan la continuidad de la protección de los datos personales que han sido tratados en el territorio de la Unión Europea y se transfieren hacia otros Estados para ser sometidos a tratamiento. Es decir, los casos en que los datos abandonan el ámbito de vigencia territorial del derecho de la Unión para ingresar en el ámbito de vigencia de otro sistema normativo, a pesar de lo cual, según las disposiciones del Derecho Europeo, los datos personales deben gozar de una protección similar a la otorgada por el derecho de la Unión, aún al entrar en el ámbito de vigencia de un sistema jurídico distinto.

En lo que consiste en un hecho original del derecho europeo, en dichos casos no se trata de que las normas sobre protección de datos personales que forman parte de éste extiendan su vigencia más allá del territorio de la Unión, sino de que éstos no se desprendan de la protección que, a modo de coraza, se han adherido a los datos al estar sometidos al derecho de la Unión. Esa continuidad de la protección se logra mediante dos métodos: En virtud del primero, las autoridades de la Unión verifican que, allí donde los datos se dirigen, el derecho vigente les otorgue un nivel de protección similar al de la Unión y, por medio del segundo, la protección es otorgada por previsiones de derecho

[173] Considerandos 9 y 10 del Reglamento.

flexible o contractuales entre las partes, también aprobadas por las autoridades europeas o nacionales. En otras palabras, los datos no pueden abandonar el derecho de la Unión sin que sus autoridades hayan aprobado el nivel de protección que continuarán teniendo.

Cabe mencionar que con la Directiva 95/46 el planteamiento era similar aunque con algunas diferencias, puesto que un Reglamento, al tener aplicación directa, no es una norma de mínimos sino una norma íntegra que sólo necesita de normas complementarias que la desarrollen y la completen en los aspectos que se delegan a la regulación estatal.

Otra diferencia digna de remarcar entre ambas normas es que la obligación de las empresas establecidas en varios estados miembros de cumplir con los requisitos de la norma de transposición de cada uno de los estados donde tuviera presencia, que imponía una carga administrativa excesiva para las empresas o entidades con presencia en varios estados miembros, se sustituyó en el RGPD por el mecanismo de ventanilla única o, en su denominación original en inglés, “one stop shop”, tal como veremos más adelante.

2. La libertad de circulación de datos personales.

El RGPD, en su artículo 1 establece que sus objetivos son, por un lado (apartado 2), la protección de las personas físicas en cuanto al tratamiento de los datos personales y, por el otro (apartado 3), la libre circulación de tales datos en la Unión.

La libertad de circulación de datos en la Unión Europea merece un comentario especial, ya que se establece en calidad de actividad económica y social, en el marco de la

integración y del funcionamiento del mercado interior[174] y constituye una de las libertades básicas de la Economía de Datos Europea[175] y del Mercado Único Digital, que la Comisión planifica establecer con un valor similar al de las libertades básicas que conforman el Mercado Único Europeo, esto es la circulación de personas, mercancías, servicios y capitales establecidos en el art. 26.2 TFUE.

Esta libertad se refiere a dos tipos de datos perfectamente diferenciados: Los datos personales y los no personales. Respecto de estos últimos, existe actualmente una propuesta de reglamento sobre cuyo texto la Comisión, el Parlamento y el Consejo han llegado a un acuerdo el 19 de junio de 2018[176], que tiene como objetivos garantizar: a) La libertad de circulación de los datos no personales en el interior del Mercado Único Digital; b) El libre acceso de las autoridades públicas de cualquier Estado miembro a los datos almacenados, aunque estén jurídicamente sometidos a la regulación de otro Estado miembro; c) Incentivar la creación de códigos de conducta para los servicios en la nube.

La libertad de circulación de los datos personales, tal como ya hemos explicado, está regulada por el RGPD, aunque en muchas ocasiones queda eclipsada por la protección que se otorga a los mencionados datos. Por ello vale la pena destacar algunos pronunciamientos del TJUE recordando o afirmando el lugar de este objetivo, que han

---

[174] Observaciones presentadas por la Comisión Europea ante al Tribunal de Justicia de la Unión Europea en el caso Lindqvist, citadas en el fundamento 35 de la sentencia.

[175] Los fundamentos y acciones para la Economía Europea de los Datos se pueden consultar en: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy. También en la *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones*. Bruselas, 25/04/2018, COM(2018)232 final. Accesible en castellano en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0232&from=EN

[176] European Commission Press release: "Digital Single Market: EU negotiators reach a political agreement on free flow of non-personal data". Bruselas, 19 de junio de 2018, accesible desde la dirección: http://europa.eu/rapid/press-release_IP-18-4227_en.htm. Información que se puede consultar también en la página web: https://ec.europa.eu/digital-single-market/en/news/eu-negotiators-reach-political-agreement-free-flow-non-personal-data.

tenido lugar durante la vigencia de la Directiva 95/46. En primer lugar, en la sentencia Lindqvist, el Tribunal declara que la referida Directiva no constituye una armonización mínima de las legislaciones nacionales sino una armonización completa (FJ 96) y que su objetivo consiste en "*... mantener el equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad.*" (FJ 97). Debido a eso las normas de transposición adoptadas por los Estados miembros no pueden excederse en uno de estos objetivos en detrimento del otro y pueden extender el alcance de sus normas internas más allá de los supuestos regulados por la Directiva 95/46, "*... siempre que ninguna otra norma de Derecho comunitario se oponga a ello.*" (FJ 99). En un sentido similar, ordena a las autoridades nacionales de control respetar siempre ese equilibrio entre "*el respeto del derecho fundamental a la vida privada y los intereses que exigen la libre circulación de datos personales…*"[177] para garantizar la protección frente al tratamiento ilícito de los datos personales.

En definitiva, libertad de circulación y protección de los datos personales son dos caras de un mismo fenómeno, que pueden interferir entre sí por lo que su regulación es necesaria a efectos de que no se bloqueen mutuamente. Por ello el legislador Europeo mantiene el principio de la libertad de su circulación, no sólo dentro del territorio de la Unión sino, como hemos visto en el Capítulo anterior, también a nivel internacional entre los Estados que son parte en el Convenio 108 del Consejo de Europa.

Pero la libertad de circulación de los datos personales no es absoluta sino que está sometida a las condiciones que el Reglamento establece para permitirla; es decir libertad sí, pero no ilimitada sino regulada. Los requisitos que deben reunir los tratamientos a los

[177] Sentencias Comisión C/Alemania, C-518/07, apartado 25; Comisión C/Hungría, C-288/12, apartado 48; Schrems, C-362/14, apartado 42.

que son sometidos los datos personales se regulan a través de todo el Reglamento, tal como estudiaremos a lo largo de este capítulo y los siguientes.

Finalmente, con respecto a la circulación de datos en el interior del territorio de la Unión, el apartado 23) del art. 4 RGPD se refiere a esos casos como "tratamiento transfronterizo", determinando que se entenderán por tales los tratamientos que:

a) Se realicen por encargados o responsables que estén establecidos en más de un estado miembro, y en el contexto de las actividades de establecimientos en distintos estados miembros.
b) Se realicen en el contexto de las actividades de un establecimiento de un encargado o responsable en un único estado miembro, pero que afecte sustancialmente o sea probable que afecte sustancialmente a interesados en más de un Estado miembro.

Para esta circulación también dispone el RGPD que no se podrán interponer obstáculos.

3. Ámbitos objetivo y subjetivo de aplicación.

Antes de analizar los aspectos territoriales o espaciales que pretende abarcar el Reglamento, definiremos los ámbitos objetivo y subjetivo de aplicación, establecido por algunas definiciones básicas que contiene el RGPD, que son: a) El concepto de datos personales; b) El concepto de tratamiento; c) Los agentes intervinientes en la relación de datos personales: responsable y encargado e interesado.

a) Datos personales

Corresponde en primer lugar dar una definición de qué son datos personales para el Reglamento, definición que obtendremos del apartado 1) de su artículo 4, que los define como "*toda información sobre una persona física identificada o identificable ('el interesado')*". El mismo apartado enumera luego algunos datos a los que caracteriza de "*identificador*" de la persona física: "*nombre, número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*".

Cabe agregar que en el año 2014 el TJCE en la sentencia "*Digital Rights*"[178] va más allá de los datos identificativos clásicos al incluir en esta definición a los conocidos como *metadatos* o aquéllos que son generados por los interesados en el uso de sus dispositivos de comunicación, tales como la identificación de un equipo de usuario, la localización del inicio y del destino de una llamada, su duración, el equipo, números de teléfono y dirección IP.

La calificación de dichos datos como datos personales es hoy en día ya no sólo acertada sino necesaria puesto que la cantidad de metadatos generados por las comunicaciones, aún excluyendo su contenido, puede permitir extraer conclusiones muy precisas sobre la vida privada de las personas como por ejemplo: El seguimiento de los datos de localización de una persona durante un cierto período de tiempo permite conocer sus hábitos de vida cotidiana, lugares de residencia permanentes o temporales, sus desplazamientos habituales y sus actividades; la identificación de los receptores o emisores de sus comunicaciones permiten conocer sus relaciones sociales y familiares; y su huella digital permite conocer sus preferencias e inclinaciones más íntimas. Todos

[178] Apartados 26 a 29.

estos son datos cuyo conocimiento y utilización por parte de terceras personas (aunque sean autoridades públicas) y, sobre todo, la realización de perfiles, constituye una injerencia grave en los derechos fundamentales protegidos por los artículos 7 y 8 de la Carta puesto que quienes los manipulen pueden llegar a conocer aspectos de la vida privada de las personas a quienes dichos datos identifican, sin que ella lo sepa, que constituirán en muchos casos detalles que la persona no desea hacer públicos.

b) Tratamientos de datos personales.

Una vez definido qué entendemos por datos personales, podemos avanzar en el ámbito objetivo o material de aplicación del RGPD, que está definido en el apartado 1 de su art. 2 como el "*tratamiento total o parcialmente automatizado de datos personales*", así como el "*tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*". El apartado 2 de este artículo excluye varias situaciones de tratamientos, entre las cuales cabe destacar los "*efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*".

En otras palabras, el reglamento se aplica a los tratamientos de datos personales total o parcialmente automatizados o aquéllos que no sean automatizados pero estén incluidos o destinados a ser incluidos en un fichero.

El artículo 4, sobre *Definiciones*, apartado 2, define los *tratamientos* como todo tipo de operaciones que pueden ser realizadas sobre los datos personales, exponiendo a continuación una enumeración ejemplificativa de operaciones que se consideran tratamientos, que incluye la recogida, registro, organización, conservación, comunicación, difusión y la habilitación de acceso. Dado que, como ya hemos afirmado, la enumeración es ejemplificativa, existen otras operaciones que no se han mencionado,

como las transferencias internacionales de datos personales, las operaciones lógicas, aritméticas[179] o similares que se realicen sobre ellos y, dentro de las operaciones de difusión, se debe interpretar comprendida toda referencia a datos personales que se haga en una página web, tal como lo decidió el Tribunal de Justicia de las Comunidades Europeas en la Sentencia Lindqvist[180].

También es aplicable a estas definiciones el caso Google Spain, en el que el TJUE debió dilucidar, entre otras cuestiones, si la actividad de proveedor de contenidos realizada por un motor de búsqueda debe ser considerada un tratamiento de datos personales, a lo que contestó afirmativamente, destacando que "… *el gestor de un motor de búsqueda 'recoge' tales datos* (personales) *que 'extrae', 'registra' y 'organiza'..., 'conserva'... 'comunica' y 'facilita el acceso'...*" , operaciones todas que están recogidas en el artículo 2.b) de la Directiva 95/46 como tratamientos de datos. En consecuencia, la actividad realizada por el motor de búsqueda se debe considerar tratamiento de datos personales[181].

Consideramos que la combinación entre el ámbito material de aplicación y la definición de tratamiento nos permite realizar una delimitación genérica y a la vez sencilla y breve de la aplicación objetiva del RGPD: Todas las operaciones total o parcialmente automatizadas a que son sometidos los datos personales, así como los datos personales destinados a ser incluidos en un fichero de forma no automatizada, excluyendo las operaciones que se realizan en el ámbito exclusivamente doméstico.

A su vez el tratamiento de datos personales puede descomponerse en distintas *actividades de tratamiento*, concepto que no se define en el artículo 4 sino que se desprende del

[179] Art. 2.b) del Convenio de reforma del Convenio 108 del Consejo de Europa.

[180] Sentencia del TJCE de 6 de noviembre de 2003 en los asuntos C 101/01, EU:C:2003:596, apartado 25.

[181] Sentencia Google Spain (2014), apartado 28.

articulado del RGPD, como por ejemplo el art. 3.2); el art. 24.2) y 28.4), de los cuales se puede colegir que este concepto no se corresponde con el de *operaciones* sino más bien con distintos conjuntos o cadenas de operaciones en los que es posible dividir un tratamiento y que componen un aspecto lógicamente completo del tratamiento principal.

El ámbito material de aplicación del Reglamento no son los datos en sí (independientemente de que éstos son los destinatarios de una gran parte de la regulación del RGPD) sino los tratamientos que se realizan sobre tales datos o, lo que es lo mismo, las operaciones que, en su mayoría, se realizan directamente sobre datos personales pero en algunos casos pueden realizarse sobre aspectos relacionados con tales datos, como la habilitación de acceso y las operaciones de seguridad de los datos que se realizan sobre los medios o soportes que los contienen o almacenan.

c) Responsables y encargados.

El artículo 4.7) define el "*responsable del tratamiento*" o simplemente "*responsable*" como "*... la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento…*" Siguiendo esta definición, encontramos que el responsable puede ser una persona física o jurídica, y ser privada o pública. En los casos en que son más de una persona las que deciden los fines y medios del tratamiento, el artículo 26 del Reglamento los denomina "*corresponsables*" y establece que deben determinar de modo transparente y de mutuo acuerdo sus respectivas responsabilidades y funciones. La práctica totalidad de las obligaciones impuestas por el RGPD están dirigidas a este sujeto, cuyo elemento determinante es la organización y dirección intelectual del tratamiento, si bien hay una gran parte que son compartidas con el encargado del tratamiento.

A su vez el encargado del tratamiento es, según el art. 4.8), "*... la persona física o jurídica* (o) *autoridad pública… que trate datos personales por cuenta del responsable del tratamiento.*" Es decir, aquí el elemento determinante es que sea una persona (ya sea física o jurídica, privada, pública o autoridad) distinto del responsable y que realice el tratamiento por cuenta de éste; en otras palabras, a quien el responsable haya *encargado* la ejecución material del tratamiento y que actúe bajo sus órdenes e instrucciones. En este sentido, si el encargado actúa excediendo las órdenes o instrucciones del responsable, será considerado corresponsable (art. 28.10 RGPD).

El encargado puede delegar en otro encargado (art. 28.2 y 28.4 RGPD), que en su caso será denominado subencargado.

d) Interesado.

Interpretando el apartado 1) del artículo 4 RGPD, podemos definir al interesado como la persona a la cual los datos identifican.

Según el considerando 7 RGPD, esa persona debe tener el control sobre los datos que la identifican; es el destinatario de la protección y de las garantías de este derecho fundamental y, como se desprende de todo su articulado, debe ser capaz de decidir libremente los tratamientos a los que desee que dichos datos sean sometidos.

En las relaciones de tratamiento de datos personales el interesado puede denominarse también *titular* de los datos, puesto que estos constituyen bienes personalísimos de los cuales el interesado es titular; especialmente algunos atributos de la personalidad tales como el nombre, la imagen o el número de identificación nacional. El carácter de bienes personalísimos que damos a los datos personales surge de su propia naturaleza que es la de formar parte de la personalidad del individuo al que identifican, lo que les otorga el

carácter de abstractamente intransmisibles e irrenunciables[182], sin perjuicio de que se pueda renunciar a alguna de sus manifestaciones concretas, lo que ocurre por ejemplo con el consentimiento para los tratamientos de los datos personales propios.

Por el contrario el concepto de *propietario* de los datos personales no se utiliza en esta rama del derecho, por un lado porque en nuestra opinión se refiere más especialmente a los datos en su calidad de bienes económicos que no es deseable cuando estamos tratando su aspecto de derecho fundamental, y por otro porque en su mayoría no son objetos materiales (aunque sí puede serlo el soporte en que se hallan) por lo que el concepto de propietario puede inducir a muchas confusiones.

4. Ámbito territorial de aplicación.

4.1. Regla general.

Está claro que, en su calidad de norma europea, el ámbito de aplicación territorial del Reglamento es el territorio de la Unión, es decir, la adición de los territorios de los Estados Miembros y aquéllos donde en virtud de las normas de derecho internacional se aplica el derecho de uno de éstos, tal como hemos explicado en el Capítulo I de esta investigación; y el ámbito positivo[183] de aplicación material del Reglamento se refiere a los *tratamientos*,

[182] Cfr. Art. 469 del Código Civil y el preámbulo de la Ley Orgánica 1/1982, de 5 de mayo.

[183] El artículo 2.2. contiene unas normas que excluyen la aplicación del Reglamento, es decir que definen el ámbito negativo de su aplicación, constituidos por los tratamientos:

- Realizados en un ámbito en el que no sea aplicable el derecho de la Unión,
- Realizados por los Estados miembros cuando llevan a cabo actividades comprendidas en el Capítulo 2 del Título V del TFUE;
- Efectuados por las personas físicas en el ejercicio de actividades exclusivamente personales o domésticas;

cuya definición hemos expuesto en el apartado anterior. No obstante, el ámbito para su aplicación territorial no se define en base al aspecto objetivo de su aplicación (es decir, en base a los tratamientos) ni usando una conexión directa como sería la localización de los datos o del tratamiento[184], sino que se utiliza como conexión geográfica principal (junto a otras) un grupo de elementos que conforman un nexo complejo, uno de los cuales tiene un componente geográfico: un establecimiento del responsable o del encargado del tratamiento ubicado dentro del ámbito territorial de vigencia del Reglamento, es decir, dentro del espacio geográfico de la Unión Europea, siendo indistinto que dicho establecimiento esté directamente relacionado con las operaciones de tratamiento.

Ello es así pues la localización geográfica de los tratamientos sobre datos total o parcialmente automatizados, especialmente si se realizan a través de medios conectados, constituye un problema de difícil solución en tanto que, como operaciones digitales que son, en muchas ocasiones su ubicación física tanto a los efectos jurídicos como prácticos es de muy difícil o imposible determinación, dado que los distintos elementos físicos relacionados con ellas pueden estar en lugares donde se apliquen ordenamientos jurídicos distintos, como por ejemplo las personas intervinientes (no sólo responsables y encargados, sino las personas físicas que realizan efectivamente las operaciones de tratamiento bajo órdenes de éstos) pueden estar situados en territorios de distintos Estados y los medios técnicos con los que se efectúa el tratamiento (por ejemplo, el almacenamiento de los datos), en el territorio de otro país, en "*la nube*" o en "*el*

- Llevados a cabo por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y prevención de la seguridad pública.

[184] Como explicamos a lo largo de este trabajo y, especialmente, de este Capítulo, es imposible determinar el lugar donde se realizan, o *localizar* los tratamientos.

ciberespacio", cuya localización geográfica puede ser desconocida y el o los proveedores de estos medios (que también pueden tener participación como responsables o encargados), en otros territorios.

De ahí que el legislador de la Unión, en un intento por asociar los tratamientos a una ubicación geográfica determinada, ha establecido como principal la mencionada conexión que permite, por un lado proteger los datos que presenten una determinada conexión con el territorio de la Unión y, por otro, relacionar los tratamientos con la aplicación del derecho de la Unión, independientemente de la localización geográfica (o falta de ella) de los distintos factores relacionados con el tratamiento. El ámbito de aplicación geográfica del Reglamento así definido es de carácter imperativo[185].

Por otra parte, teniendo en cuenta la facilidad de comunicación de los datos digitalizados, si el ámbito de aplicación territorial se circunscribiera, por ejemplo, al lugar físico donde el tratamiento es realizado, sería sumamente sencillo cometer fraude a la norma.

Así, la primera y genérica disposición sobre el ámbito geográfico de aplicación del RGPD se halla en el artículo 3.1 del Reglamento que transcribimos a continuación:

"*El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.*"

Se trata ésta de una norma cuya redacción especifica territorialmente el ámbito material, con un alto grado de ambigüedad que roza casi con la abstracción, al asociar la aplicación del Reglamento a todo tratamiento de datos que se realice *en el contexto de las actividades*

[185] De Miguel Asensio, P.A: Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea. Revista Española de Derecho Internacional, Vol. 69 Tomo 1. Pág. 104

de un *establecimiento* de la persona responsable o encargada de dicho tratamiento, que se ubique en la Unión Europea. Al referirnos a esta norma como ambigua y abstracta no es nuestra intención realizar una crítica negativa de la misma, ya que consideramos que las normas jurídicas destinadas a regular relaciones que se desarrollan en el espacio virtual o en el ámbito tecnológico deben tener necesariamente términos amplios para relacionar ese espacio o ámbito con las conductas que tengan sus efectos en el espacio geográfico, al menos en la etapa actual que está atravesando este derecho que consideramos que es aún incipiente, tomando en cuenta que el derecho que regula las relaciones "reales" (por contraposición a "virtuales") lleva milenios de desarrollo y, el que regula las conductas que se desarrollan en el espacio virtual, lleva apenas unas pocas décadas.

Regresando al art. 3.1 RGPD, como la propia disposición establece, es indiferente que el tratamiento se realice en este territorio o fuera de él.

Esta disposición es esencialmente idéntica a la de la anterior Directiva 95/46, las únicas diferencias se refieren a la aplicación de cada una de las normas: Está dirigida a la aplicación territorial de la ley nacional de cada Estado miembro en la Directiva, mientras el Reglamento se refiere a su aplicación en el territorio de la Unión. En este último se agrega que el titular del establecimiento puede ser el responsable o el encargado[186].

Este artículo debe ser complementado con el considerando 22 del Reglamento, que además de reiterar la delimitación geográfica ya expuesta, define un concepto muy

[186] Existe una pequeña diferencia de vocabulario, que no de concepto, en las versiones en castellano de cada uno de los documentos: La Directiva se refiere a los tratamientos realizados en el *marco* de las actividades de un establecimiento, mientras que el Reglamento se refiere a los realizados en el *contexto* de las actividades de un establecimiento. Esta diferencia desaparece en la versión en inglés, que utiliza la palabra *context* (contexto) en ambos casos.

flexible y no formalista[187] de establecimiento, al considerar como tal al ejercicio de una actividad, de manera efectiva y real y estable en el tiempo, independientemente de su forma jurídica[188].

El diccionario de la lengua española de la Real Academia Española define *contexto* en su segunda acepción como: "*Entorno físico o de situación, político, histórico, cultural o de cualquier otra índole, en el que se considera un hecho*", definición que consideramos aplicable al concepto que estamos analizando, siendo el término "*entorno*" un sinónimo de "*contexto*" a los efectos del RGPD, al igual que lo es el término "*marco*" que se utilizó en la traducción de la Directiva 95/46.

Como se observa a primera vista, el único elemento geográfico de conexión es la ubicación del establecimiento en cuyo *contexto* se realiza el tratamiento, siendo indiferente la ubicación del interesado, la del lugar donde se recogen los datos y la de realización del tratamiento.

De acuerdo con de Hert y Czerniawski[189], este criterio del *marco de las actividades de un establecimiento*[190] se fija sobre la base de un test de dos pasos: El primero, consiste en determinar si el responsable tiene un establecimiento en un Estado miembro y, segundo,

---

[187] Sentencia del Tribunal de Justicia (Sala Tercera) de 1 de octubre de 2015 en el asunto C-230/14 Weltimmo, S.R.O. y Nemzeti Adatvédelmi és Információszabadság Hatóság (en adelante "Sentencia Weltimmo"). Apartado 29.

[188] El considerando 36 y otros artículos del Reglamento distinguen entre establecimiento principal y secundarios, pero esta distinción no tiene importancia a los efectos del ámbito geográfico de aplicación del Reglamento sino con respecto a la determinación de la autoridad de aplicación principal y las autoridades interesadas, tema que desarrollaremos más adelante.

[189] De Hert, P., Czerniawski, M.: "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context." International Data Privacy Law, Vol. 6. 3., 2016. Pp. 233-234.

[190] Estos autores se refieren al *marco* de las actividades debido a la diferencia en la traducción al español que hemos expuesto en la nota 186. Igualmente limitan el test sólo a la ubicación del establecimiento del responsable dado que la Directiva 95/46 sólo se refería a éste, excluyendo el establecimiento del encargado.

si una determinada operación de un tratamiento se realiza en el ámbito de las actividades de dicho establecimiento[191].

El primero de dichos pasos (determinación de la existencia de un establecimiento), es equiparado en el considerando 19[192] de la Directiva 95/46 a la realización de una actividad que cuente con tres requisitos: Que sea efectiva, que sea real y que sea estable, si bien el TJUE en la sentencia Weltimmo[193] aclara que en ciertos casos (concretamente, en el caso de empresas que se dedican a ofrecer servicios exclusivamente a través de internet) se debe realizar una interpretación amplia del término *establecimiento*, no limitándolo al sitio donde está registrada la persona jurídica sino que, para determinar si una empresa tiene un establecimiento en un Estado miembro, cabe analizar tanto el grado de estabilidad de la instalación como la realidad del desarrollo de actividades en ese Estado tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios real y efectivamente ejercidas (FJ 29). Se pronuncia expresamente en el sentido de que, según las circunstancias del caso, la sola existencia de un único representante, si tiene estabilidad suficiente, puede constituir una instalación estable (FJ 30), aún con una actividad mínima (FJ 31)[194]. En definitiva, *establecimiento* puede quedar reducido a una persona que actúe por cuenta o en nombre del responsable,

[191] El Comité Europeo de Protección de Datos también estima necesarias estas dos operaciones de análisis "*in concreto*", en su documento "Guidelins 3/2018…" ya citado, págs.. 5-6.

[192] En el mismo sentido el Considerando 22 RGPD.

[193] Sentencia Weltimmo. Cabe tener en cuenta que en este caso, se juzgaba a la empresa "Weltimmo", con domicilio social en Eslovaquia, por sus actividades de tratamiento de datos en Hungría, país en el que gestionaba una página de Internet con anuncios de inmuebles ubicados allí, exclusivamente en húngaro, donde además contaba con un representante.

[194] El Comité Europeo de Protección de Datos avala esta interpretación de la Corte de Justicia, incluyéndola en la Directiva 3/2018, apartado 1.a).

siempre que cuente con una relativa *estabilidad*[195] y las *actividades* no necesitan ser permanentes ni continuadas sino que pueden quedar reducidas a su mínima expresión.

Como ha quedado expuesto, la relación con el territorio de la Unión viene dada por el establecimiento de la persona responsable o encargada del tratamiento, con cuyas actividades esté relacionado el tratamiento y no por el lugar físico donde éste efectivamente se realice, que puede ser en el territorio de la Unión o fuera de él. Tampoco se requiere que el tratamiento sea llevado a cabo *por* el establecimiento, sino *en el marco de las actividades* del establecimiento[196].

De Miguel se refiere a este elemento como una "*situación*"[197], nosotros preferimos referirnos a él como el elemento *contextual*: El marco de las actividades.

En el caso Google Spain, el Tribunal interpretó este *elemento contextual* que define el ámbito geográfico de una manera muy abierta, declarando que un tratamiento realizado en un lugar no determinado, del cual es responsable una sociedad radicada en Estados Unidos se considera realizado "*dentro del marco de las actividades de un establecimiento del responsable en el Estado miembro de que se trate*" si el responsable posee un establecimiento en un Estado miembro que se dedica a la promoción y comercialización de la publicidad relacionada con ese tratamiento, ya que estas actividades son las que hacen redituable el tratamiento para el responsable. Si bien este fallo se refiere a la

[195] Comité Europeo de Protección de Datos: Guidelines 3/2018…, cit., pág. 5

[196] Google Spain, fj. 52. De las declaraciones de los párrafos subsiguientes de la Sentencia Google Spain, se puede extraer como principio general que si una empresa domiciliada en un país tercero cuenta con un establecimiento en un estado miembro que está destinado a la promoción y venta de productos que sirvan para rentabilizar la actividad principal de la empresa matriz, el tratamiento de datos que constituye parte de la actividad principal de la matriz está indisociablemente ligado a las actividades del establecimiento del Estado miembro y por tanto se puede considerar realizado en el marco de las actividades de éste.

[197] De Miguel Asensio, Op Cit, pág. 76..

Directiva 95/46 que estaba en vigor en ese momento, resulta de aplicación también a las previsiones del Reglamento. En definitiva, también se da una interpretación amplia al concepto de *marco de las actividades*.

Para De Hert y Czerniawski[198], la decisión de la Corte en el caso Google Spain se puede considerar una forma de forzar a los responsables de tratamientos cuya empresa matriz no se encuentre establecida en un estado miembro, a que cumplan con el derecho europeo de protección de datos; valoración con la que nosotros disentimos en cuanto al término *forzar* dado que el país de establecimiento o registro de una empresa es totalmente intrascendente a los efectos de los tratamientos de datos. La importancia en este sentido la otorgan los tratamientos, por lo tanto es indiferente el lugar de registro o establecimiento a los efectos mercantiles, siendo sólo trascendente las operaciones de tratamientos de datos que la empresa realice.

Finalmente, los tratamientos pueden también efectuarse *en el contexto de las actividades* de varios establecimientos del responsable o del encargado que se encuentren en distintos Estados Miembros, o bien el tratamiento realizado en el contexto de las actividades de un único Estado miembro puede afectar significativamente a interesados que se encuentren en distintos Estados miembros. Ambos casos, que son denominados *tratamientos transfronterizos* por el artículo 4.23) del Reglamento, son una muestra más de la dificultad de relacionar actividades (tratamientos u operaciones) realizadas en el ciberespacio con una ubicación geográfica determinada.

Como ya habíamos avanzado, en una gran cantidad de casos la conexión de los tratamientos que se realizan en un entorno tecnológico y conectado con un elemento que

[198] De Hert y Czerniawski, Op. Cit, pág. 233.

los vincule al sistema jurídico de la Unión es algo sumamente complejo que ha sido resuelto por parte del legislador europeo mediante la elección de dos elementos de conexión, uno de ellos *geográfico* y otro *contextual*; y por parte del TJUE, mediante la interpretación sumamente amplia de los conceptos y de algunos factores accesorios tales como *establecimiento, actividades* y *marco*.

Nosotros consideramos que, tanto la regulación de la vinculación de los tratamientos de datos personales con el derecho europeo como la interpretación jurisprudencial de esas disposiciones son acertadas. La laxitud o abstracción de los términos así como la amplitud de su interpretación constituyen una característica de los ámbitos del derecho relacionados con la tecnología, que se diferencia de los campos jurídicos clásicos, estrechamente relacionados con elementos concretos de conexión física que tienen su origen en los límites geográficos de ejercicio de la soberanía. Con respecto al derecho relacionado con la tecnología, la facultad soberana de dictar el derecho sigue teniendo una base geográfica pero no ocurre lo mismo con su aplicación cuando tiene que tener lugar en un entorno virtual o en el ciberespacio, en el cual no se pueden mantener los lazos físicos concretos que conforman las conexiones en derecho clásico sino que son no sólo admisibles sino necesarios los conceptos abstractos y las interpretaciones difusas para no hacer del ciberespacio un espacio sin derecho.

4.2. Reglas especiales: El criterio del objetivo o finalidad.

Hemos mencionado que el art. 3.1. del Reglamento establece el principio general para la aplicación territorial de éste, cuyo nexo de conexión tiene relación directa con el responsable o el encargado; ahora bien, en el art. 3.2. se establecen un par de casos especiales en los que el Reglamento resulta aplicable a pesar de que ni el encargado ni el

responsable tengan establecimientos en el territorio de la Unión[199], ya que el nexo de conexión se basa en dos elementos distintos de éste: por un lado, la presencia de los interesados en dicho territorio y, por otro, por el objetivo del tratamiento[200].

Comenzaremos por mencionar que en este aspecto el Reglamento se aparta del art. 4.1.c) de la Directiva, que extendía su aplicación a los tratamientos realizados por un responsable o encargado no establecido en el territorio de la Unión pero que recurra para el tratamiento a medios, automatizados o no, establecidos en el territorio de un estado miembro, salvo que la utilización de dichos medios tenga como finalidad únicamente la transmisión o tránsito de los datos por el territorio de la Unión. Esta disposición por un lado quedó obsoleta debido a la absoluta falta de trascendencia de la ubicación física de los medios para la realización de los tratamientos y, por otro, podía conducir a la aplicación del derecho del estado miembro a situaciones que no tenían una vinculación real con la Unión[201] por lo que fue eliminada en el Reglamento, que también extiende su aplicación a tratamientos realizados por responsables o encargados que no tengan ningún establecimiento en la Unión, pero en base a otros criterios que resultan de mayor importancia y aplicación que el determinado en la Directiva.

Volviendo al Reglamento y tal como hemos visto, en la norma general el nexo de conexión territorial es complejo ya que la determinación no es directa entre el ámbito material de aplicación del Reglamento (el tratamiento) y su localización geográfica, sino que dicho nexo está compuesto por los distintos elementos:

---

[199] Al igual que en el principio general que acabamos de analizar, también es indiferente el lugar de realización del tratamiento.

[200] Por la palabra en inglés "*target*", tal como lo define el CEPD en sus "Guidelines 3/2018…" cit, pág. 3.

[201] De Miguel Asensio, op. Cit., Pp. 80-81.

- Localización física de un establecimiento del responsable o encargado dentro del territorio de la Unión;
- Actividades reales llevadas a cabo por dicho establecimiento;
- Tratamiento que se realice en el marco de las mencionadas actividades.

Con respecto a los casos especiales establecidos en el artículo 3.2, el nexo de conexión también es complejo y en él la localización del establecimiento se vuelve un elemento presente en los dos casos en su forma negativa o, en otras palabras, *ausente* en ambos casos: Que no haya establecimiento del responsable o el encargado en la Unión.

El segundo elemento que relaciona los tratamientos con el territorio de la Unión lo constituye la localización física de los interesados que deben encontrarse en su territorio[202].

Los otros elementos son diferentes para cada caso, si bien se insertan dentro del aspecto del objetivo del tratamiento:

- El primer caso especial se refiere a la oferta de bienes y servicios, que debe estar destinada a los interesados que se encuentren en la Unión;
- El segundo caso al control del comportamiento de los interesados, que debe tener lugar en el territorio de la Unión.

Este apartado se aplica a tratamientos que sean exclusivamente realizados en el ámbito de las actividades de encargados y responsables que no tengan ningún establecimiento en la Unión, pero cuyo objeto sean datos relacionados con la oferta de bienes o servicios dirigida específicamente a *personas que se encuentren* en la Unión o la observación de

[202] En el texto original del RGPD se establecía que los interesados debían *residir* en el territorio de la Unión, pero la corrección de errores del 19 de abril de 2018 del Consejo cambió acertadamente el verbo por la expresión "*interesados que se encuentren en la Unión*".

conductas *que se desarrollen en la Unión*. A los tratamientos que se encuentran dentro del espectro de aplicación de estos artículos no les son aplicables las normas de ventanilla única o de selección de la autoridad de control principal[203], tal como veremos en el Capítulo correspondiente a las autoridades de control.

Estas normas, a través de los complejos nexos de conexión, encuentran un equilibrio entre la flexibilidad del ámbito territorial, necesario en la era digital para que el derecho de protección de datos sea efectivo, y la seguridad jurídica para las empresas establecidas fuera de la Unión, que traten datos personales de los individuos en la Unión Europea. Por otra parte, De Hert y Czerniawski opinan que están basadas en una lógica directa ("straightforward") que formulan en lo que se podría traducir como: "podrás ser el blanco del derecho de la Unión sólo si apuntas a ella"[204], criterio que no es absoluto y al cual el artículo 3.2 impone límites precisos.

Hemos expuesto anteriormente que el ámbito material de aplicación del Reglamento son los *tratamientos de datos*; lo que implica que no se aplica a la oferta de bienes o servicios en sí ni a la observación de las conductas en la Unión, sino a los tratamientos de datos personales que estén relacionados con dichas actividades, lo que excluiría, en un ejemplo muy hipotético, la observación de conductas si en ella no se recogen datos personales, es decir si la observación de la conducta se realiza de forma totalmente anónima, no registrando los datos que identifiquen a la persona.

[203] Comité Europeo de Protección de Datos: "Guidelines 3/2018…" cit., pág. 12.

[204] La traducción es de la autora, la expresión original en inglés es la siguiente: "you might be targeted by EU law only if you target". De Hert y Czerniawski, op. Cit, pág. 238.

De Hert y Czerniawski[205] critican el alcance del artículo 3.2.a) que acabamos de ver, porque en su interpretación puede dar lugar a que se entiendan alcanzadas por el mismo compañías que no estén establecidas en la Unión, que ofrezcan sus productos o servicios globalmente, sin apuntar especialmente a la Unión y en las situaciones en que todos los elementos del contrato (el servicio, el pago, la localización del proveedor) se ubican fuera de la Unión, poniendo el ejemplo de una persona que desde un Estado miembro reserva una habitación en un hotel de California a través de una agencia de viajes norteamericana, caso en el cual, según la interpretación que estos autores realizan de las normas que acabamos de exponer la operación entraría en el ámbito jurisdiccional de la Unión, lo que para los autores no debería ocurrir, teniendo en cuenta que en este caso es el interesado-consumidor quien elige el servicio fuera de la Unión. Opinan que cuando se imponen sanciones por medio de la extraterritorialidad de las normas de un determinado sistema se pueden afectar negativamente los derechos de una persona, sea física o jurídica, comenzando por el derecho a la seguridad jurídica y el principio de legalidad, fundamental en el caso de sanciones administrativas. Pero también el derecho al juez natural (ante lo cual preconizan el desarrollo e incentivación de normas transnacionales sobre la elección del foro), la libertad de circulación, de establecimiento (particularmente dentro de la UE), el derecho al debido proceso y el principio *ne bis in ídem*, derechos que no se ven afectados mediante el nexo del "*establecimiento*" que, incluso cuando se interpreta en su sentido más amplio, permite un grado de seguridad jurídica relativamente alto[206].

[205] Op. Cit., pág. 239.

[206] Ibidem, pág. 243.

Nosotros pensamos que los casos en que el servicio/producto no está *concretamente* dirigido a la Unión Europea y no es el responsable o encargado quien dirige su oferta a ese mercado sino el consumidor quien elige dicho servicio o producto, si aplicamos los criterios de orientación delineados en el considerando 23 del Reglamento, el caso no caería bajo el ámbito del RGPD, si bien estos autores están en lo cierto en cuanto al respeto al principio de la legalidad para las sanciones administrativas. En consonancia con nuestra opinión, el CEPD[207] pone como ejemplo de tratamiento que no entraría dentro del campo de aplicación del RGPD una cadena de hoteles en Sudáfrica que ofrezca paquetes vacacionales a través de su página web en inglés, francés, alemán y español y que no posea ninguna oficina, representación ni ninguna otra forma de establecimiento estable en la Unión Europea. En todo caso, será la jurisprudencia la que deba determinarlo en el futuro, para lo cual se necesitará la elaboración y aplicación de normas interpretativas especiales tal como ha ocurrido en los casos *Google Spain* y *Weltimmo*. Todo ello independientemente de que la existencia de una decisión de adecuación de la Comisión o, en el caso de los Estados Unidos, la cobertura del *Privacy Shield* permitirían realizar estos tratamientos con total seguridad.

A continuación analizaremos un poco más detenidamente los dos casos.

a) *Oferta de bienes o servicios dirigida a personas que estén en el territorio de la Unión.*

El considerando 23 complementa esta disposición estableciendo que la relación entre el tratamiento y la oferta de bienes o servicios se debe determinar teniendo en cuenta la

[207] "Guidelines 3/2018…" cit., pp. 7-8.

intención del responsable o encargado del tratamiento de realizar su oferta dentro del territorio de la Unión, para lo que no será suficiente la mera accesibilidad a la página web de oferta de bienes o servicios desde la Unión, sino que se necesitarán otros indicios como por ejemplo la oferta en idiomas que no coincidan con el del país tercero en el que resida el responsable y que sean propios de uno o más estados miembros de la Unión, o que ésta se realice en monedas de uno o más estados miembros. En la opinión del legislador reflejada en este considerando queda claro que el ejemplo mencionado más arriba que ponen De Hert y Czerniawski quedaría fuera del ámbito de aplicación del Reglamento.

Destacar finalmente que es indiferente si los bienes y servicios que se ofrecen son de pago o gratuitos, a tenor de lo establecido en el art. 3.2.a) RGPD.

b) Control del comportamiento que se desarrolle en el territorio de la Unión.

En este caso, la orientación que da el Considerando 24 del RGPD para determinar si hay una actividad de tratamiento por medio de la cual se controlen comportamientos que tengan lugar en la Unión, consiste en evaluar si las personas físicas son objeto de un seguimiento en internet, especialmente si los datos recogidos mediante ese control o seguimiento son utilizados para la elaboración de un perfil de la persona física, ya sea con el fin de adoptar decisiones sobre ella o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

En virtud de la finalidad u objetivo de estas reglas especiales, el control debe estar específicamente dirigido a personas que se encuentren en la Unión ya que no entrarán dentro de esta norma la observación de conductas de un grupo de personas que no se

encuentran en la Unión, algunas de las cuales se desplacen temporalmente al territorio Unión sin conocimiento del responsable del tratamiento.

Si bien esta norma es altamente eficaz para la protección de los datos personales, consideramos que la evolución de la tecnología ha causado su insuficiencia en el tiempo transcurrido desde la aprobación del RGPD, pues a día de hoy conocemos que principalmente la combinación de la inteligencia artificial con el big data permiten no sólo controlar sino predeterminar la conducta de las personas cuyos datos personales se someten a tratamiento, por lo que hubiera sido deseable que, además del control, se incluyan otras acciones como el ejercicio de influencia sobre la conducta de personas que transcurra en la Unión, o bien dejar un concepto abierto en el que se pueda en el futuro incluir otras formas de tratamiento.

Si bien el caso no está resuelto en el Reglamento, consideramos que en el caso de los tratamientos a los cuales se aplica el Reglamento a pesar de que el responsable o encargado respectivo no cuenta con un establecimiento en la Unión, la autoridad principal será la del Estado en que esté domiciliado el representante del responsable o del encargado, en caso de que éste haya sido designado. Si el responsable o el encargado no establecidos en la Unión no hubieran designado representante, será autoridad principal la del estado con mayor número de interesados afectados por el tratamiento o, si fuera imposible determinar cuál es el estado con mayor número de interesados lo será la primera que haya entendido en el asunto, si el número de interesados que se encuentren en su estado de designación es significativo.

4.3. Excepciones a las reglas especiales.

El artículo 27.2 exceptúa de la aplicación extraterritorial del Reglamento a los tratamientos realizados por las autoridades u organismos públicos y a los realizados por entidades privadas que cumplan acumulativamente con los siguientes requisitos:

- Que sean ocasionales;
- Que no incluya el manejo a gran escala de datos especialmente protegidos por el art. 9.1 o de datos referentes a condenas e infracciones penales según el art. 10;
- Que sea improbable que entrañen un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento.

Es decir, el Reglamento se aplicará a los tratamientos que se realicen en el contexto de las actividades de establecimientos no ubicados en la Unión, cuando sean ocasionales pero incluyan el manejo a gran escala de datos especialmente protegidos, de datos relativos a condenas o infracciones penales o que supongan un riesgo para los derechos y libertades de las personas.

4.4. Representantes.

Cuando el Reglamento sea de aplicación a personas privadas que sean responsables o encargados de tratamientos de datos y no posean establecimientos en la Unión, el artículo 27 de esta norma establece para ellos la obligatoriedad de designar por escrito un representante en la Unión.

El representante debe estar establecido en uno de los Estados en cuyo territorio se encuentren interesados a quienes se dirige la oferta de bienes o servicios o cuyo

comportamiento se controla. La principal función de este representante será la de representar al encargado o al responsable frente a los interesados o a las autoridades de control, a fin de garantizar el cumplimiento de las disposiciones del Reglamento.

La designación de un representante en ningún modo exime de responsabilidad al responsable o encargado del tratamiento, contra quienes se deberán dirigir las acciones y/o reclamaciones; aunque las notificaciones se dirigirán al domicilio del representante (art. 27.5 RGPD).

Consideramos que esta disposición es de difícil aplicación pues será muy complicado hacer efectiva la responsabilidad de una persona que no posea ningún establecimiento en la Unión y que realice tratamientos de datos personales a los cuales les sea aplicable el RGPD a tenor de lo dispuesto por su art. 3.2, tanto si ha designado representante como si no lo ha designado. En concreto, la aplicación de sanciones (especialmente las pecuniarias) podrá volverse en muchos casos ilusoria debido a la imposibilidad de hacerlas efectivas en una jurisdicción distinta de la Unión. Ante un incumplimiento de las disposiciones del RGPD en estos casos, se deberá aplicar en primer lugar la regla del art. 27.3 RGPD para la designación de la autoridad de control principal o interesada[208] y las sanciones a aplicar serán, preferentemente, las que vayan dirigidas a limitar o evitar el tratamiento de datos personales en cuanto ello sea posible.

[208] Es decir, se designará la autoridad del Estado miembro "… en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado." (art. 27.3 RGPD).

5. Relación con el derecho interno.

Si bien, como ya hemos establecido, el Reglamento es una norma íntegra y autónoma que se aplicará en forma directa en todo el territorio del Espacio Económico Europeo[209], cada Estado Miembro tiene cierto margen de autonomía para desarrollarlo mediante uno o más actos internos que deben respetar los límites de derecho imperativo que fija, de entre los cuales destacan especialmente los que sean necesarios para establecer la autoridad o las autoridades de control de aplicación del reglamento.

Ahora bien, dentro de los distintos actos internos de desarrollo del Reglamento, el derecho aplicable a los tratamientos transfronterizos se determinará por el mismo grupo de disposiciones que designan a la autoridad de control principal, es decir, se les aplicará la norma de desarrollo del Reglamento que esté vigente en el lugar donde se ubique el establecimiento principal a los fines del tratamiento, del responsable o del encargado. En otras palabras, aunque un tratamiento afecte a interesados o se dirija a la oferta de bienes o servicios a potenciales clientes en distintos Estados Miembros, además del RGPD se le aplicará el acto interno del Estado de designación de la autoridad de control principal para ese tratamiento, que es el sentido de la instauración de este tipo de autoridades: Que las empresas que tengan establecimientos en distintos Estados miembros, en cuyos contextos se realicen actividades de tratamiento de datos personales, no tengan que cumplir con la normativa de cada uno de ellos, sino que se entienda conforme con el derecho europeo el cumplimiento con el derecho de uno de los Estados Miembros[210].

[209] En adelante, "EEE".

[210] A diferencia de lo que acontecía durante la vigencia de la Directiva, en que los responsables que tuvieran establecimientos en distintos estados miembros debían cumplir con el acto de internalización de la

6. Ámbitos materiales específicos de aplicación.

Como hemos desarrollado al inicio de este trabajo, la protección de las personas físicas con respecto al tratamiento de sus datos personales es un derecho fundamental que, como tal, se inserta dentro de un sistema que responde a una determinada jerarquía de valores, en la cual en ocasiones se producen conflictos que es necesario resolver jurídicamente.

Respecto a la relación entre el derecho a la protección de los datos personales y otros derechos fundamentales con los que puede colisionar, el TJUE se ha pronunciado en diversas ocasiones (Sentenecias Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, apartado 68; Google Spain y Google, C-131/12, apartado 68; Ryneš, C-212/13, apartado 29; Schrems, C362/14, apartado 38) en el sentido de que las disposiciones que regulan "*... el tratamiento de datos personales, que puede vulnerar las libertades fundamentales y, en particular, el derecho al respeto de la vida privada, deben ser necesariamente interpretadas a la luz de los derechos fundamentales protegidos por la Carta*"[211].

En concreto, el derecho a la protección de los datos personales tiene relación con determinados derechos y libertades fundamentales, tales como las libertades de expresión, de información, de pensamiento, de empresa, de las artes y de las ciencias, así como los derechos al honor, a la propia imagen y a la personalidad. Con el objetivo de equilibrar la

Directiva en cada uno de ellos. Por el contrario, en los Estados en los cuales no se encontraba ubicado ningún establecimiento del responsable no había obligación de cumplir con su normativa, aunque el tratamiento afectara a interesados en dicho Estado.

[211] Sentencia Schrems, apartado 38.

relación entre la protección de datos personales y algunos de dichos derechos y libertades, el Reglamento dedica su Capítulo IX a la resolución de algunas de esas situaciones, mediante las disposiciones que analizaremos a continuación.

6.1. Libertad de expresión y de información.

En primer lugar el art. 85 del Reglamento, en consonancia con el Considerando 153, impone a los Estados la obligación (y a su vez también el derecho) de conciliar el derecho a la protección de los datos personales con los derechos a la libertad de expresión y de información (art. 11 de la Carta), lo que debe hacerse mediante una disposición con rango de ley[212] teniendo especial consideración hacia los tratamientos con fines periodísticos y de expresión académica, artística o literaria (art. 13 de la Carta), tratamientos para los cuales se habilita a los Estados miembros a establecer exenciones o excepciones a las disposiciones de los Capítulos II a VII y a este mismo capítulo IX del Reglamento, Capítulos que tratan sobre los principios que deben cumplir los tratamientos de datos personales (Capítulo II), los derechos de los interesados (Capítulo III), las obligaciones del responsable y del encargado del Tratamiento (Capítulo IV), las transferencias internacionales de datos personales (Capítulo V), las disposiciones aplicables a las autoridades de protección de datos (Capítulo VI), los mecanismos de cooperación y coherencia (Capítulo VII) y las disposiciones que analizamos en este apartado.

El Considerando 153, si bien no es vinculante, contiene una afirmación que, lamentablemente, no se ha incluido en el artículo que aquí analizamos: "... *Si dichas*

[212] Rebollo Delgado, L: *Protección de datos...* Pág. 169 y, en España, por regular derechos fundamentales, debe tratarse de una Ley Orgánica.

exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento." Adoptando esta norma como disposición vinculante en el texto del artículo, se evitarían cargas jurídico-administrativas innecesarias a los responsables que realicen tratamientos de datos para estas finalidades, lo que en la redacción final del artículo 85 queda indeterminado y deberá ser interpretado, si no por el derecho de los Estados miembros, sí por las autoridades de protección de datos o por las autoridades judiciales.

Los Estados miembros al igual que con toda otra disposición legal adoptada en virtud del Reglamento, deben notificar a la Comisión también respecto a las excepciones que se adopten en virtud de este capítulo.

En virtud de las disposiciones de los arts. 8 y 10 del CEDH, es obligación de los Estados adoptar las medidas necesarias para el respeto y la protección de estos dos derechos (derecho a la protección de los datos personales y libertad de expresión), así como abstenerse de adoptar medidas que los restrinjan ilegítimamente y, por consiguiente, también de regular el equilibrio entre ambos, pudiendo limitarlos respectivamente con la finalidad de conservar dicho equilibrio, en base a las disposiciones del apartado segundo de cada uno de los artículos citados. En este sentido se ha pronunciado el TEDH, si bien en referencia al art. 8 del CEDH que no se refiere específicamente al derecho a la protección de datos personales sino al más amplio de la vida privada[213].

Las libertades mencionadas en este artículo están íntimamente ligadas con la escala de valores que, a su vez, responden a la idiosincrasia y factores sociológicos, históricos,

[213] Caso *Rubio Dosamantes*… citado, apartados 27 y 28.

económicos, políticos y religiosos de cada Estado miembro, por lo que es un acierto que el equilibrio entre ellos se haya dejado librado al derecho interno.

Por otro lado, siendo la protección de datos personales uno de los valores más recientes dentro de la escala propia de cada Estado miembro, se hacía necesaria una disposición imperativa y directamente aplicable de nivel europeo que establezca que este nuevo valor, dentro del sistema de derechos y libertades fundamentales de cada Estado miembro debe estar, al igual que en el de la Unión Europea, en un estado de equilibrio y no de subordinación ni de superioridad respecto al resto de derechos y libertades fundamentales.

6.2. Tratamientos de datos personales en los documentos oficiales con relación al acceso del público a dichos documentos.

El art. 86 del Reglamento autoriza[214] a las autoridades y organismos públicos, así como a las entidades privadas en el cumplimiento de una misión en interés público, a comunicar los datos personales que figuren en documentos oficiales a efectos de conciliar el derecho de acceso público a este tipo de documentos con la protección de datos personales, siempre que se haga de conformidad con el Derecho de la Unión o de los Estados miembros.

Este artículo por un lado dispone la licitud de la comunicación de los datos personales que se realice para permitir el acceso del público a documentos oficiales, pero por otro

[214] Rebollo Delgado (*Protección de datos…*, pág. 170) resalta la diferencia del tratamiento con respecto a la libertad de expresión e información, en que es obligación de los Estados dictar las disposiciones para conciliar ambos derechos, mientras que en el acceso público a los documentos, que forma parte de la transparencia en los documentos públicos, elípticamente se *permite* o *autoriza* a los Estados miembros a dictar normas para conciliar ambos derechos.

lado condiciona esa licitud a que el derecho aplicable (ya sea de la Unión o de los Estados miembros) concilie dicho acceso con la protección de datos personales.

Es decir, que ninguno de ambos derechos podrá tener primacía sino que las distintas fuentes deberán disponer la conciliación entre ambos.

6.3. Tratamiento del número nacional de identificación.

Con respecto a otro las tratamiento específico de datos realizados por entidades públicas o por entidades privadas en cumplimiento de obligaciones legales o de interés público, el artículo 87 habilita a los Estados miembros a disponer en su derecho interno las condiciones específicas para establecer un medio de identificación general para sus ciudadanos, especialmente un número nacional de identificación, los que serán utilizados únicamente con las garantías adecuadas para el respeto de los derechos y libertades de los interesados.

Si tenemos en cuenta que el art. 4.1) RGPD equipara los datos personales con un *identificador* de una persona física, el número nacional de identificación es uno de los datos más representativos en este aspecto. Pero, a los efectos de su organización cívica, política y económica, es una prerrogativa innegable del Estado la instauración y organización de un método de identificación de sus ciudadanos, por lo que esta facultad estatal no puede ceder ante el derecho fundamental a la protección de datos. Por ello se otorga al Estado la facultad, pero también la obligación, de establecer las bases para la organización de este sistema, que debe contar con normas especiales que permitan los tratamientos de datos personales a estos efectos, por parte de organismos o autoridades públicas y entidades privadas que actúen en cumplimiento de una misión de interés

público, pero también que sometan dichos tratamientos a requisitos más estrictos, especialmente de seguridad y confidencialidad.

6.4. Tratamientos en el ámbito laboral.

La relación laboral constituye una relación específica que trasciende los límites de la celebración y ejecución de cualquier otro tipo de contrato de tracto sucesivo, en especial debido al desequilibrio existente entre las partes[215] y, por otra parte, en el desarrollo de una relación laboral es necesario tratar algunos datos sensibles[216], como aquéllos relativos a la salud, a la familia, a la discapacidad, datos sindicales, etc., por todo lo cual los tratamientos de datos en la relación laboral se deben regular de manera particular, que bien puede ser a través de los convenios colectivos[217].

El Reglamento también contiene algunas disposiciones específicas para los tratamientos que se efectúen en el contexto de una relación laboral, como el artículo 9.2.b) (y, para algunos aspectos concretos de la relación laboral, también el artículo 9.2.h), que levanta la prohibición de someter a tratamiento las categorías especiales de datos personales cuando se llevan a cabo en el ámbito del derecho laboral, o el artículo 88, que está íntegramente dedicado a los tratamientos en este ámbito.

Dado que el objetivo de la regulación específica en este ámbito es la protección de los derechos y libertades del trabajador en su calidad de parte más débil en la relación, el artículo mencionado en su apartado 1 dispone que con esa finalidad los Estados miembros podrán adoptar normas legislativas o convenios colectivos que garantizarán la dignidad

[215] Considerando 43 RGPD.

[216] Considerando 52 RGPD.

[217] Considerando 155 RGPD.

humana y prestarán especial atención a las situaciones susceptibles de poner en riesgo los derechos y libertades del trabajador, como la transferencia de datos personales entre las empresas que sean miembros de un grupo empresarial, los sistemas de supervisión en el lugar de trabajo y la transparencia en el tratamiento (art. 88.2)[218].

El 8 de junio de 2017 el Grupo de Trabajo del Art. 29 adoptó una Opinión sobre el tratamiento de datos en el ámbito laboral[219], en la que el órgano opina que el hecho de que el empleador posea la propiedad de los medios electrónicos no significa que los empleados se vean privados del derecho al secreto de sus comunicaciones[220] y que la posición de dependencia económica de los empleados con respecto al empleador, en la mayoría de los casos no les permitirá otorgar, rechazar o revocar el consentimiento con libertad. Algo similar ocurre con el interés legítimo del empleador, que en muchos casos puede colisionar con los derechos y libertades del empleado, por lo que esta base legal no se debería invocar a menos que el tratamiento sea estrictamente necesario para una finalidad legítima y respete los principios de proporcionalidad y subsidiariedad[221].

Otros aspectos de los tratamientos de datos personales en el ámbito laboral que se deben respetar escrupulosamente e interpretar de manera amplia son los principios de minimización de datos y de transparencia[222].

Sobre un aspecto concreto de los tratamientos de datos personales en el ámbito laboral y su relación con la transparencia, concretamente la supervisión de las comunicaciones del

[218] Rebollo Delgado, L: *Protección de datos…*, pp. 170-171.

[219] Article 29 Data Protection Party: Opinion 2/2017 on data processing at work, adopted on 8 June 2017.

[220] Opinión 2/2017 citada, apartado 6.1., pág. 22.

[221] Ibidem, apartado 6.2. pág. 23.

[222] Ibid, apartados 6.4 y 6.4, pág. 23.

trabajador, se ha pronunciado la Corte Europea de Derechos Humanos en su sentencia "*Barbulescu c/Rumanía*", de 5 de septiembre de 2017, sentencia en la cual además del artículo 8 del Convenio Europeo de Derechos Humanos y el Convenio 108 del Consejo de Europa, también se toman en consideración los artículos 7 y 8 de la Carta y los artículos aplicables tanto de la Directiva 95/46 como del RGPD (que al momento de dictarse sentencia ya estaba vigente aunque no era aplicable). La Corte sostiene que "*... las instrucciones de un empleador no pueden reducir a cero la vida social privada en el lugar de trabajo. El respeto a la vida privada y a la intimidad continúan existiendo, aunque puedan restringirse en la medida necesaria*"[223]. La decisión incluye el pronunciamiento de que la supervisión e interceptación de las comunicaciones en el lugar de trabajo, aunque se realicen con los medios técnicos suministrados por el empleador, constituye una violación al art. 8 del CEDH si previamente no se ha notificado al empleado de la existencia y alcance de dicha supervisión e intercepción (si ésta abarca sólo el flujo de comunicaciones o también su contenido), incluido el grado de intrusión en sus comunicaciones[224]. No es suficiente con la notificación de que el uso de los medios técnicos de la empresa para usos privados está prohibido; además, debe ser notificado de que se controlará la correspondencia y otras comunicaciones.

La armonización de los intereses del empleador con los derechos fundamentales del trabajador es un asunto altamente complicado y rico en casuística, así como lo es la relación laboral en su conjunto. Por ello más allá de la regulación que pueda existir en el derecho interno, en este ámbito es necesario el trabajo conjunto de la administración pública laboral con las APD, que deberán tender a proteger al trabajador, por ser la parte

[223] Sentencia "Barbulescu c/Rumanía", apartado 80, pág. 29.

[224] Sentencia "Barbulescu c/Rumanía", apartado 121 pp. 36-37.

cuyo derecho fundamental a la protección de datos personales se encuentra en juego, aunque sin por ello ignorar los legítimos intereses del empleador, que por ser meros intereses (aunque plenamente legítimos) nunca podrán tener supremacía frente a los derechos fundamentales del trabajador.

En definitiva, en este aspecto de la relación de tratamiento de datos personales, tendrán tanta importancia las normas como las decisiones adoptadas por las autoridades de aplicación, tanto judiciales como administrativas, en los dos ámbitos de su confluencia; El derecho social y el de protección de datos personales.

6.5. Tratamientos con fines de archivo en interés público, de investigación científica o histórica y fines estadísticos.

Los tratamientos realizados con fines de archivo, investigación científica o histórica y estadísticos tienen un alto interés público, por lo que este hecho debe ser tenido en cuenta por los Estados miembros al regularlos pero no por ello deben dispensarse las garantías establecidas en el Reglamento (art. 89.1 RGPD). Sin embargo, estas finalidades se pueden alcanzar, en un gran número de los casos, mediante el tratamiento de datos anonimizados o aplicando el principio de minimización de los datos de forma estricta.

Por esos motivos el art. 89.1 establece la obligatoriedad de que los datos que se sometan a tratamientos con estos fines estén anonimizados siempre que ello sea posible y que deben disponerse las medidas técnicas y organizativas necesarias para garantizar el respeto al principio de minimización de datos, incluida especialmente la seudonimización.

En los tratamientos que se realicen con las finalidades de investigación histórica o científica o estadística, el art. 89.2 autoriza a que el derecho de la Unión o el de los Estados miembros establezca excepciones a los derechos de acceso (art. 15 RGPD), de rectificación (art. 16), a solicitar la limitación del tratamiento (art. 18 RGPD) y a la oposición de los interesados (art. 21 RGPD), cuando sea probable que el ejercicio de esos derechos imposibiliten u obstaculicen gravemente el logro de los fines perseguidos y en la medida en que resulte necesario para lograrlos. Cuando la finalidad del tratamiento sea de archivo en interés público, además de dichas excepciones se podrán establecer éstas también para el derecho a la portabilidad de los datos (art. 20 RGPD) y para la obligación de notificar la supresión o rectificación de los datos (art. 19 RGPD), siempre con las mismas limitaciones[225].

Como corresponde a toda excepción a las garantías de los derechos fundamentales, las precedentes se deben interpretar restrictivamente.

Aquí también nos encontramos frente a un interés legítimo (el de los fines de archivo, estadística e investigación científica) si bien en este caso se trata de un interés público y no de un interés privado. Por ese motivo en este caso es procedente otorgar prioridad a este interés frente a algunos derechos de los interesados, aunque ello no puede de ninguna manera conducir al desconocimiento o eliminación del derecho a la protección de datos personales.

[225] Rebollo Delgado, L: *Protección de datos…*, pp. 171-172.

6.6. Obligaciones de secreto.

Hay ciertas profesiones o situaciones en que determinados responsables y encargados de tratamiento están obligados por normas legales a guardar secreto respecto a ciertos datos (como por ejemplo los sacerdotes, profesionales de la medicina, abogados, periodistas, etc.) Para estos casos, el art. 90 del RGPD faculta a los Estados miembros a adoptar normas específicas que modifiquen los poderes de las autoridades de control establecidos en el art. 58.1, e) y f), esto es obtener del responsable o del encargado el acceso a todos los datos que están siendo objeto de tratamiento, así como a todos los locales, equipos y medios para los tratamientos, sólo para aquellos datos o actividades que estén cubiertos por el deber de secreto.

La obligación de secreto de algunas profesiones es un elemento fundamental para resguardar ciertos valores esenciales para el ser humano como pueden ser sus derechos, su salud física, psicológica o espiritual, sus intereses económicos y algunas libertades como la libertad de empresa. Por todo ello es justificado e incluso necesario que el secreto profesional tenga prioridad frente a los poderes y facultades de las APD, así como lo tiene en general frente a las funciones y poderes del Estado, en especial la administración de justicia, ya que permitir lo contrario podría socavar los cimientos sobre los que se asienta gran parte del sistema de respeto a los derechos fundamentales.

6.7. Tratamientos de datos realizados por iglesias y asociaciones religiosas.

El apartado 1 del artículo 91, dedicado a las iglesias y asociaciones religiosas que realicen tratamientos de datos, interpretado a *sensu contrario*, ordena que las normas sobre protección de datos que regulen dichos tratamientos se adapten al RGPD[226].

El apartado 2 de dicho artículo habilita a los Estados miembros a establecer autoridades de supervisión independientes para estas entidades, que pueden ser distintas de las autoridades nacionales con competencia genérica, siempre que respeten las disposiciones del RGPD referentes a dichas autoridades.

Este artículo viene a aclarar que las entidades y autoridades religiosas, que en algunos Estados miembros gozan de ciertos privilegios frente a algunas funciones del Estado, no los tienen frente a la regulación del derecho de protección de datos personales.

6.8. Los tratamientos realizados en el marco de la prestación de servicios públicos de comunicaciones electrónicas.

Tal como lo hemos tratado en otro apartado de esta investigación[227], existe en el derecho derivado europeo una Directiva para garantizar la confidencialidad de las comunicaciones electrónicas (Directiva 2002/58/CE o Directiva de la E-Privacidad), que regula entre otros aspectos también los tratamientos de datos personales relacionados con las comunicaciones electrónicas. Norma que está atravesando actualmente un proceso de modificación.

---

[226] Esta excepción fue introducida por Alemania, con el fin de que sus asociaciones religiosas conservaran su normativa propia. Rebollo Delgado, L: *Protección de datos…*, pág. 173.

[227] Apartado 3.3. del Capítulo III.

Dicha directiva, a través de la regulación de las capacidades de tratamiento y almacenamiento de la información en los dispositivos de los usuarios finales, así como del acceso a dicha información, legisla sobre los conocidos programas "espías" o *cookies*, presentes en la gran mayoría de las páginas de internet y aplicaciones informáticas que, a través de estos mecanismos, consiguen acceso a una gran cantidad de datos personales y a otros que, aunque en sí no son personales, se pueden combinar con otros (que están comúnmente a disposición de las entidades que lo deseen) que sí permiten identificar a un usuario individual o a un grupo de usuarios, para realizar perfiles en muchos aspectos su vida tales como el social, familiar, laboral y de salud.

Por ello hubiera sido preferible que el RGPD tuviera una norma transitoria de aplicación hasta la aprobación del nuevo Reglamento de la E-Privacidad, para los tratamientos de datos personales en las comunicaciones electrónicas (una parte muy significativa de los tratamientos de datos en un mundo hiperconectado). En lugar de eso, el art. 95 de esta norma aclara que éste no impone obligaciones adicionales a los responsables o encargados de tratamientos de datos en el marco de la prestación de servicios públicos de comunicaciones electrónicas que estén sujetos a la Directiva de la E-Privacidad, con lo cual continúa aplicándose esta norma que otorga un nivel mucho menor que el del RGPD en cuanto a garantías para la protección de los datos personales.

Es de esperar por lo tanto, que el Reglamento de la E-Privacidad se apruebe cuanto antes a fin de que los usuarios e interesados no estén desprotegidos con respecto a los tratamientos de sus datos personales que se realicen en este ámbito, como lo están en la actualidad.

CAPÍTULO IV. LA PROTECCIÓN DE DATOS PERSONALES EN EL DERECHO NACIONAL

1. Disposiciones constitucionales.

En 1977, año en que fue redactada la Constitución Española[228], la tecnología y, especialmente, la informática ya estaba en la segunda etapa de su desarrollo, lo que le permite incluir, en el artículo 18 dedicado a la protección de la intimidad, una referencia a la informática y a la necesidad de limitación de su uso para proteger la vida íntima personal y familiar, así como el derecho al honor y el pleno ejercicio de los derechos (apartado 4 del mencionado artículo).

En el resto de apartados, dicho artículo reconoce expresamente "*el derecho al honor, a la intimidad personal y familiar y a la propia imagen*" (apartado 1), la inviolabilidad del domicilio (apartado 2), y garantiza el secreto de las comunicaciones (apartado 3).

El derecho a la intimidad ha sido definido por el Tribunal Constitucional como uno de los derechos *"...reconocidos en el art. 18 de la C.E... estrictamente vinculados a la propia personalidad, derivados sin duda de la «dignidad de la persona», que reconoce el art. 10 de la C.E., y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario - según las pautas de nuestra cultura- para*

[228] En adelante, "CE".

mantener una calidad mínima de la vida humana. Se muestran así esos derechos como personalísimos y ligados a la misma existencia del individuo."[229]

Siguiendo el desarrollo general del derecho de protección de datos como una rama del derecho a la intimidad, tal como hemos analizado en los capítulos anteriores, a partir de esa definición de derecho a la intimidad el Tribunal Constitucional Español extrae posteriormente el derecho a la protección de datos como implícito en los arts. 18.1 y 18.4 de la Constitución ya citados.

La primera sentencia del Tribunal Constitucional que reconoce el derecho a la protección de los datos personales data de 1993[230] y decide sobre unos hechos ocurridos con anterioridad a la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, pero durante la vigencia del Convenio 108 del Consejo de Europa sobre Protección de Datos personales, de 1981.

En la citada Sentencia el Tribunal concede el amparo solicitado, reconociendo el derecho a la protección de datos personales con base en el art. 18 CE y en el Convenio 108 del Consejo de Europa, como una garantía de otros derechos, concretamente a la intimidad y al honor, para los cuales se configura como una facultad positiva del interesado (FJ 7) pero también nos parece muy importante destacar que el TC admite la protección de datos personales como un derecho independiente (FJ 6), y ello a pesar de que no fue hasta la aprobación del RGPD, en 2016, que una norma jurídica reconoció dicha independencia.

[229] Entre otras, STC 196/2004, de 15 de noviembre, FJ 2; STC 186/2000, de 10 de julio, FJ 5 y STC 207/1996, de 16 de diciembre, FJ 3 B**.**

[230] Sentencia 254/1993, de 20 de julio de 1993 de la sala primera. Recurso de amparo 1.827/1990. Contra denegación presunta por parte del Gobernador Civil de Guipúzcoa y del Ministro del Interior de solicitud de información de los datos de carácter personal existentes en ficheros automatizados de la Administración del Estado, confirmada en la vía contencioso- administrativa. Vulneración del derecho a la intimidad personal.

Así, la sentencia declara que el Estado tiene ciertas obligaciones con respecto a los administrados y ellas no dependen de que los datos que las administraciones conservan sean, real o presuntamente, susceptibles de lesionar la privacidad del interesado (FJ 8), sino que, en tanto que derecho independiente que configura una esfera positiva de actuación para el interesado, las administraciones están obligadas a suministrar a los interesados, siempre que lo soliciten, la información relativa a sus datos personales que éstas almacenen y sometan a tratamiento.

En cuanto a la regulación legal de la protección de datos, por orden cronológico en España se ha dictado en primer lugar la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal[231]. Unos años después, una vez que en la Unión Europea se había aprobado la Directiva 95/46, su transposición se realizó en España a través de la Ley Orgánica 15/1999, de 5 de diciembre, de protección de los datos de carácter personal[232], que también ha sido derogada por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[233].

2. Ley Orgánica de Protección de Datos 15/1999

Tal como ya hemos comentado, la LOPD 15/99 era la norma de transposición de la Directiva 95/46, por lo cual en muchos de sus artículos no hacía más que reproducir las

[231] En adelante, "LORTAD".

[232] En adelante, "LOPD 15/99" o "Ley Orgánica 15/99" indistintamente.

[233] En adelante, "LO 3/18"

disposiciones de ésta (como se advierte en los distintos apartados del artículo 2, que regulan el ámbito material de aplicación) si bien adaptadas al ámbito territorial nacional, tal como analizaremos seguidamente.

Esta ley orgánica, como es natural, no contenía la noción de lo que en el momento de su aprobación se entendía por derecho a la protección de datos personales, aunque dicha noción se puede inferir de su art. 1 que instaura como "*Objeto*" la protección de distintos derechos y libertades fundamentales "*y especialmente* (el) *honor e intimidad personal y familiar*"[234]; es decir se concibe al derecho a la protección de los datos personales como un derecho instrumental para la protección de otros derechos y libertades.

El ámbito de aplicación material general de la LOPD 15/99, establecido en su art. 2.1, estaba constituido por los datos personales registrados en soporte físico y toda modalidad de uso de dichos datos, ya sea por entidades públicas o privadas. Apreciamos aquí cómo a pesar de que la tecnología y, especialmente, la informática ya estaba en pleno desarrollo, esta norma se decanta por una elección del ámbito material de aplicación que no se correspondía con el mencionado desarrollo y que fue después superado por la aparición de nuevos entornos virtuales o digitales, tales como la computación en la nube, las redes sociales y otros sistemas similares que no responden a la concepción de un soporte físico. Afortunadamente la aplicación de esta norma no se vio limitada por un concepto restrictivo del concepto de "soporte físico".

El ámbito territorial de su aplicación se define en los tres apartados del mismo artículo 2, siendo necesario antes de pasar a su análisis recordar que tratándose de una ley estatal, este ámbito está constituido por la combinación de los supuestos que constituyen el

[234] Art. 1 LOPD 15/99.

ámbito material de aplicación más la jurisdicción territorial del estado del cual emana la norma.

Así, el apartado a) del artículo 2.1. disponía que se aplicaría en primer lugar a todo tratamiento que se realice en el territorio español, en el marco de las actividades de un establecimiento del responsable del tratamiento. Vemos aquí que se incorpora el elemento de conexión complejo que está presente en las normas europeas, pero se le añade el nexo de conexión física o geográfica del lugar de realización del tratamiento, elección que en la actualidad resulta desacertada y que puede dar lugar a una gran inseguridad jurídica debido a que en muchos casos es imposible determinar con exactitud cuál es el lugar de realización del tratamiento. De todos modos, para el contexto en el que fue aprobada la LOPD 15/99 y el ámbito de aplicación material elegido, esta disposición resulta congruente.

En el apartado b) del artículo 2.1. se añaden los casos en los cuales, a pesar de no hallarse en territorio español, al responsable del tratamiento le es aplicable el derecho de este Estado en virtud de las normas de derecho internacional público. Entendemos que al seleccionar el derecho aplicable al responsable esta disposición se está refiriendo al establecimiento del responsable en cuyo marco de actividades se realiza el tratamiento.

En el apartado c) de esta disposición (que era transposición del artículo 4.1.c de la Directiva 95/46) se ampliaba el ámbito geográfico de aplicación de la LOPD 15/99 a los responsables que no estuvieran establecidos en el territorio de la Unión pero que utilicen para el tratamiento medios situados en territorio español, excepto si la función de éstos es meramente de tránsito. Debido a la dificultad a la que ya hemos hecho referencia, de otorgar una ubicación determinada a los medios utilizados en el tratamiento de los datos,

esta disposición (que tuvo muy poca aplicación) ha sido descartada en el Reglamento 679/16 y las normas que lo desarrollan.

El artículo 2.2. describe los ámbitos de los cuales se excluye la aplicación de la LOPD 15/99, encabezando la enumeración los ficheros mantenidos por personas físicas para ser usados en el ámbito exclusivamente personal o doméstico. El resto de ámbitos enumerados son aquéllos donde se aplican normas particulares y que, por tanto, derogan a la que estamos analizando, de carácter general, si bien es de destacar que las materias para las que se excluye la aplicación de esta ley orgánica según el apartado 3 del art. 2 son las referidas al régimen electoral, a la función estadística pública, al régimen del personal de las fuerzas armadas, a los Registros Civil y al Central de penados y rebeldes, y a la función de vigilancia a través de videocámaras ejercida por las fuerzas y cuerpos de seguridad del Estado, lo que podemos interpretar como que en cuanto entran en juego este tipo de intereses y el derecho a la protección de datos personales de las personas físicas, el legislador justificó la limitación de este segundo. Hablamos de limitación y no de supresión, ya que esta disposición no implica que en esos ámbitos no se protejan los datos personales, sino que ese aplica la legislación especial (que posiblemente contendrá algunas limitaciones con respecto a la general) y no la LOPD 15/99. Por ello, en los arts. 22 a 24 de esta ley orgánica se establecen algunas de las limitaciones de la protección, relacionadas con los tratamientos realizados por las fuerzas y cuerpos de seguridad del Estado en materia de seguridad pública, de defensa nacional y de persecución de delitos, por las administraciones públicas en sus funciones de control y verificación y de persecución de infracciones administrativas (en especial se menciona la Hacienda pública en relación con los deberes tributarios de los ciudadanos).

Es interesante destacar que según el artículo 11.1 de esta Ley Orgánica, los datos sólo podían ser cedidos contando con el consentimiento del interesado, con algunas excepciones enumeradas en el apartado 2 de este artículo. Si bien esta disposición tenía el objetivo de limitar la apropiación de datos por parte de los responsables de los tratamientos, adoleció del gran error de implícitamente admitir el consentimiento tácito y condicionado, por lo que en la práctica quedó vacía de contenido ya que, al menos en el entorno virtual, en la totalidad de situaciones en que se requería el consentimiento, éste era condición imprescindible para acceder a los servicios para los que se requería, al igual que aún hoy ocurre con las cookies.

Continuando con el análisis de la normativa, no se consideraba comunicación de datos (según el artículo 12.1) el acceso de un tercero a los datos, cuando dicho acceso, realizado por una persona (el encargado del tratamiento), cuando dicho acceso sea imprescindible para la prestación de un servicio al responsable del tratamiento y siempre que medie un contrato en el cual se establezcan, entre otros asuntos, las instrucciones precisas para el tratamiento, así como el compromiso del encargado de no transgredir tales instrucciones en el uso, aplicación ni en la comunicación de los datos, bajo apercibimiento de ser considerado responsable del tratamiento y debiendo responder como tal. Esta disposición puede entrar en contradicción con los arts. 33 y 34 de la LOPD 15/99, que analizamos a continuación, dado que el encargado del tratamiento de los datos, cuyo acceso a los mismos no se consideraba comunicación, podía encontrarse domiciliado en un estado tercero, a cuyo ordenamiento jurídico estará sometido. Consideramos que estos casos eran verdaderas transferencias internacionales de datos personales y, por consiguiente, tenía prevalencia la prohibición de realizarlas del art. 33, con las excepciones que se verán a continuación.

Los artículos 33 y 34 de esta norma estaban destinados a los movimientos internacionales de datos, los que no podían realizarse sino bajo algunas condiciones específicas, de las cuales mencionaremos las siguientes por tener interés para esta investigación:

- Que el nivel de protección de los datos personales del país al que éstos van destinados sea equiparable al nivel de protección otorgado por la LOPD 15/99. Para realizar la evaluación y determinar cuándo un nivel de protección es adecuado se facultaba a la Agencia Española de Protección de Datos.
- En defecto de nivel de protección adecuado, se necesitaría la autorización de la Agencia.
- Que exista un tratado o convenio en el que sea parte España y en cuya virtud se realice la transferencia;
- Que el afectado haya dado su consentimiento inequívoco a la transferencia.

El artículo 32 LOPD 15/99 admite la creación por parte de sectores de actividad, empresas o de las administraciones públicas, de códigos de conducta o deontológicos que denomina *códigos tipos*, que consisten en normas de autorregulación en materia de tratamientos de datos personales, que debían respetar las disposiciones de la LOPD 15/99 y ser inscritos en la Agencia Española de Protección de Datos y, a tenor de la letra de la norma que estamos estudiando, no tenían ninguna influencia con respecto a la autorización de las transferencias internacionales de datos personales por parte del Director de la AEPD.

Por último, el sistema de protección de datos de la LOPD 15/99 se basaba en un registro de los tratamientos de datos personales que era llevado por al AEPD, integrado por las comunicaciones de dichos tratamientos que todos los responsables estaban obligados a realizar. Este método ponía la carga genérica de la protección y el control bajo la

responsabilidad de la Agencia de protección de datos, lo que implícitamente limitaba el poder de control de los interesados.

Hasta aquí las disposiciones que definen la vigencia de la LOPD 15/99, cuyo estudio no consideramos necesario profundizar, porque esta norma ya fue derogada por la actual Ley Orgánica que analizamos a continuación. A pesar de ello sí mencionaremos que las disposiciones precedentemente expuestas estaban excesivamente limitadas al ámbito geográfico y resultaban demasiado rígidas para cubrir las tecnologías y aplicaciones que surgieron con posterioridad a su aprobación, todo lo cual, si sus intérpretes y aplicadores no la hubieran interpretado de un modo amplio, hubiera restringido su vigencia.

Tal como veremos a continuación, la actual ley orgánica de protección de datos personales no incluye disposiciones de delimitación del ámbito geográfico de vigencia (entendiéndose por ello que este aspecto está regulado exclusivamente por el RGPD) y en cuanto al ámbito material de aplicación, se divide entre los tratamientos que entran bajo el ámbito de aplicación del RGPD (art. 2.1 LO 3/18) y aquellos que en principio no entran bajo su ámbito de aplicación, a los que según el art. 2, apartados 2; 3 y 4 LO 3/18 se aplica en primer lugar la legislación específica si la hubiere y, supletoriamente, el RGPD.

3. Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LO 3/18).

Con posterioridad a la publicación del RGPD y a efectos de adaptar la regulación española a esta norma, las Cortes han aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de

Protección de Datos Personales y garantía de los derechos digitales[235], publicada en el BOE de 6 de diciembre de 2018.

Como el mismo artículo 1.a) establece, la finalidad de la LO 3/18 es la adaptación del derecho español al RGPD, por lo que el art. 2.1. de la mencionada Ley Orgánica describe un ámbito de aplicación de la mayor parte de su articulado (se excluyen los arts. 79 a 88 y 95 a 97) que coincide con el del art. 2.1 RGPD.

El apartado 2.a) del mismo artículo expresamente excluye "*los tratamientos excluidos del ámbito de aplicación del* (RGPD) *por su artículo 2.2…*" y el apartado b) excluye a los tratamientos de las personas fallecidas que se regulan en el artículo 3 de la LO 3/18, que analizaremos más adelante.

El apartado c) del art. 2.2. de la LO 3/18 excluye de su aplicación a los tratamientos regulados por las normas sobre protección de materias clasificadas.

El apartado 3 del artículo 2 de la LO 3/18 es interesante ya que cubre lo que podría haber sido un vacío legal, al disponer que "*Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea*…", se regirán por su regulación específica si la hay y, de no haberla, por las disposiciones del RGPD y de la LO 3/18. A continuación se enumeran de forma ejemplificativa tres ámbitos de tratamientos de datos personales que se encuentran en esta situación: Los relacionados con el régimen electoral general, con las instituciones penitenciarias y con los Registros públicos (Civil, de la Propiedad y Mercantiles). La aplicación supletoria del régimen general de los tratamientos de datos personales es una solución que transitoriamente consideramos

[235] En adelante, LOPD 3/18 o LO 3/18.

adecuada, pero no creemos que deba transformarse en solución definitiva, al menos en todos los ámbitos, pues en algunos de ellos, dada su especificidad (como es el ámbito, por ejemplo, de las instituciones penitenciarias y del Registro Civil) es necesario que se dicte una norma específica que contemple todas sus particularidades. El apartado 4 se refiere específicamente a los tratamientos realizados por los órganos judiciales en ejercicio de su función jurisdiccional y, aunque con una formulación distinta, el resultado es el mismo: Se aplican con preferencia las disposiciones específicas de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en lo no previsto por éstas se aplicará el RGPD y la LO 3/18.

Con respecto al art. 3 de esta Ley Orgánica 3/18, aprovecharemos su comentario para incluir otra reflexión respecto a la interrelación entre el ámbito virtual y la vida real, pues cuando una persona fallece en el ciberespacio continúan circulando datos personales y datos no personales de los cuales era titular, muchos de ellos protegidos por contraseñas que sólo eran conocidas por él o ella. Esta situación merece una solución legal, pues los mencionados datos son aún dignos de protección para el resguardo de la memoria del difunto, que es un interés jurídicamente relevante para sus familiares y allegados y que puede incluso tener importancia económica para sus derechohabientes. Estas consideraciones han sido advertidas por el legislador, que ha regulado los datos de las personas fallecidas en el art. 3 LO 3/18, aunque la habilitación genérica a "*…las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos…*", a los que se podrán sumar las personas o entidades que el causante haya designado específicamente al efecto, para solicitar al responsable o encargado del tratamiento el acceso, rectificación y supresión de los datos, puede ser fuente de conflictos entre todas las personas mencionadas, que pueden llegar a ser un grupo numeroso, con ideas distintas

acerca del destino de los datos. Por ello habrá que esperar el reglamento de este artículo de la ley, así como el real decreto en el que según el apartado 2 de este artículo se delegará la reglamentación de "*... los requisitos y condiciones para acreditar la validez y vigencia de...* (los) *mandatos e instrucciones...*" de las personas fallecidas respecto de sus datos personales para que se establezca un orden de preferencia de todas las personas habilitadas o, de forma similar, se establezcan las soluciones para las controversias que surjan entre ellas.

El apartado 2 del art. 3 se refiere a los "*mandatos e instrucciones*" que el causante haya dejado para la gestión de su legado digital, lo que se conoce como el testamento digital, una figura que ha surgido en los últimos años y está adquiriendo cada vez más importancia para estas cuestiones.

En relación con la protección de otros derechos fundamentales a través de la protección de datos personales, los artículos 9 y 10 LO 3/18 se refieren, respectivamente, a las categorías especiales de datos personales y a los datos de naturaleza penal, reglamentando los arts. 9 y 10 RGPD, prohibiendo el solo consentimiento como fundamento legal del tratamiento de los datos relativos a la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico y restringiendo la base jurídica para los tratamientos de los datos de naturaleza penal las establecidas por el derecho de la Unión o por normas internas de rango legal.

Con respecto a los tratamientos de datos personales en situaciones determinadas, complementando el RGPD que los regula en los arts. 85 a 91[236], la LO 3/18 regula los tratamientos de datos de contacto de empresarios individuales y de profesionales liberales

[236] Que analizamos en el apartado 6 del Capítulo III de este trabajo.

(art. 19), los sistemas de información crediticia (art. 20), de las operaciones mercantiles que incluyan comunicación de datos (art. 21), los de videovigilancia (art. 22), los sistemas de exclusión publicitaria (art. 23), los de denuncias internas (art. 24) y los que se realicen en el ámbito de la función estadística (art. 25) o con fines de archivo (art. 26) en ámbitos públicos.

No se encuentran más disposiciones que incidan en la vigencia de esta norma hasta su artículo 30, dedicado a los representantes de los responsables o encargados no establecidos en la Unión Europea, que otorga competencia a la Agencia Española de Protección de datos o, en su caso, a las agencias autonómicas, para entender en los casos que se refieran a afectados que se hallen en España. Lo que más llama la atención de esta disposición es que se habilita a imponer al representante, de manera personal, las medidas establecidas en el RGPD (principalmente las correctivas y sancionadoras), dejando a salvo la posible corresponsabilidad de responsable y encargado (con quienes responderá de forma solidaria) así como el derecho de repetición del representante. Si bien esta disposición es perfectamente comprensible con respecto a algunas de las medidas correctivas, como las de hacer o no hacer establecidas en el art. 58.2 RGPD, es de más difícil aplicación con respecto a las multas que requieren una especial atribución de responsabilidad o imputabilidad de la persona sancionada.

El artículo citado viene a complementar el artículo 27.3 del RGPD, por lo tanto por "afectados que se hallen en España" se debe entender las personas a quienes va dirigida la oferta de bienes o servicios o aquéllas cuyo comportamiento esté siendo controlado. Las disposiciones sobre la acción de repetición que el representante tendrá contra el responsable o el encargado, así como la solidaridad en la responsabilidad de responsable, encargado y representante son innovaciones de la LO 3/18 con respecto al RGPD. Por su

parte, también se debe relacionar este artículo con los arts. 73.h) y 73.i) de esta Ley Orgánica, que declara infracciones graves (que, por lo tanto, prescriben a los dos años):

- la falta de designación de un representante por parte de los responsables o encargados que realicen los tratamientos descritos en el art. 3.2.a) y b) del Reglamento, establecida en su artículo 27.
- la falta de atención a las solicitudes de la AEPD o de los afectados, por el representante en la Unión del responsable o encargado del tratamiento.

También tienen cabida en la LO 3/18 las normas de derecho flexible, a las que se dedica el artículo 38 bajo la forma de códigos de conducta y certificación. El apartado 1 de este artículo establece que estos códigos serán vinculantes para quienes se adhieran a ellos, que podrán ser, además de las asociaciones y organismos a que se refiere el art. 41 del RGPD, las empresas o grupos de empresas y los organismos enumerados en el art. 77.1 de la LO 3/18, que son en general las administraciones y corporaciones públicas y entidades relacionadas con ellas. Teniendo en cuenta que esta Ley Orgánica no contiene ninguna previsión respecto al marco de condiciones necesarias para la validez de estos códigos, se deberán considerar aplicables en este ámbito los artículos 40 y 41 RGPD. Por el contrario, sí se regulan algunos detalles referentes a los organismos de supervisión de los códigos de conducta, que de hecho funcionan como una especie de extensión de la autoridad de protección en cuanto a la supervisión del cumplimiento de las normas por parte de los responsables y encargados implicados, motivo por el cual es necesario que la ley interna de desarrollo del RGPD contenga algunas disposiciones sobre su funcionamiento. Respecto a las acreditaciones, el único artículo dedicado a ellas (el art. 39 LO 3/18) sólo dispone que serán gestionadas por la Entidad Nacional de Acreditación (ENAC), que debe comunicar a la AEPD y a las autoridades autonómicas, en su caso, las

concesiones, denegaciones o revocaciones de las acreditaciones, incluyendo la motivación de la respectiva decisión.

En el Título VI de la LOPD 3/18 (arts. 40 a 43) se regulan las transferencias internacionales de datos que, recordemos, en principio no necesitarán autorización de la Agencia Española de Protección de Datos sino que estarán prohibidas a menos que se cumpla alguna de las condiciones de validez o garantía establecidas en los arts. 44 a 46 RGPD.

En el artículo 40 se menciona por primera vez lo que constituye una nueva fuente del derecho, al menos para el caso de las transferencias internacionales de datos: Las Circulares de la AEPD y de las autoridades autonómicas, que se enumeran en este artículo en cuarto lugar después del RGPD, la LOPD 3/18 y sus normas de desarrollo.

A diferencia de la anterior Directiva y la anterior LOPD 15/99, en que la intervención de la AEPD era, en principio, preceptiva en todos las transferencias (que debían contar, al menos, con su conocimiento), en la regulación que estamos estudiando ésta sólo interviene (también en principio) en supuestos tasados: al adoptar las cláusulas contractuales tipo (art. 46.2.c del RGPD) o las normas corporativas vinculantes (art. 47 RGPD), en los supuestos sometidos a información previa a la AEPD (art. 49.1 del RGPD) y en casos que podríamos llamar residuales, cuando el país de destino no haya obtenido la decisión de adecuación de la Comisión y la transferencia no cuente con ninguna de las garantías establecidas en los artículos 47 y 48 RGPD, la realización de la transferencia necesitará de la autorización previa de la AEPD. Estos supuestos están debidamente enumerados y acotados en el apartado 1 del art. 42, y sólo se permiten cuando se dé alguna de las siguientes situaciones, alternativamente:

- Que la transferencia se garantice mediante cláusulas que no se correspondan con las cláusulas tipo del art. 46.2 del RGPD;
- Que el responsable o encargado que la ordene sea alguna de las entidades enumeradas en el art. 77.1 LOPD 3/18.

En la disposición adicional quinta, esta ley orgánica contiene una norma específica para prevenir situaciones como la que originó el procedimiento que culminó con la sentencia Schrems: El ámbito de aplicación son las transferencias internacionales de datos personales, y dentro de éstas, aquéllas que estén amparadas por una decisión de adecuación, por las cláusulas tipo o por un código de conducta aprobados por la Comisión. En los casos en que exista un procedimiento que tramite ante la AEPD cuyo objeto sea una o una serie de transferencias internacionales amparadas por una decisión de la Comisión que la autoridad nacional considere que vulnera las disposiciones del RGPD, la disposición adicional quinta de la LOPD 3/18 la autoriza para suspender preventivamente el procedimiento del que las transferencias amparadas por esa Decisión sean objeto y plantear la validez de ésta ante una autoridad judicial, que en el mismo acuerdo de admisión o inadmisión a trámite de la solicitud debe confirmar, modificar o levantar la suspensión del procedimiento decidida por la AEPD. Esta disposición responde a las consideraciones vertidas por el TJUE en el asunto Schrems, que analizamos a lo largo de este trabajo.

4. Consideraciones finales

Como hemos visto a lo largo de este capítulo, la breve mención en el art. 18.4 CE de la necesidad de regular los usos de la informática para proteger la privacidad de las personas ha sido una base fundamental para el posterior desarrollo del derecho de protección de datos personales, tanto a nivel legal como jurisprudencial y de la práctica administrativa.

En cuanto a la norma positiva que mayor plazo de vigencia ha tenido en España, debemos recordar que debía ceñirse a las disposiciones de la Directiva 95/46, hecho que determinó que, si bien al momento de su aprobación contenía las previsiones jurídicamente más avanzadas con respecto a lo que el conocimiento, desarrollo y la práctica administrativa dictaban para ese momento, en unos años quedó superada por los desarrollos tecnológicos, desfase que no podía solucionarse por vía administrativa debido al lastre al que estaba sujeta por la mencionada directiva.

Concretamente, nos referimos a la concepción del derecho a la protección de los datos personales como un derecho instrumental, la aceptación del consentimiento tácito y condicionado, la delegación de la mayor parte de los poderes de control y supervisión en la APD y la rigidez de las normas de autorización, control y supervisión ejercidas por ésta, así como a la normal desactualización que han sufrido los conceptos y términos relacionados con la tecnología, causada por la vertiginosa evolución de ésta.

En cuanto a la flamante Ley Orgánica 3/2018, aplaudimos el fiel seguimiento que realiza del RGPD y, aunque consideramos positiva la regulación de los derechos digitales contenidos en su Título X, no nos parece adecuado incluirlos en la misma norma que trata el derecho a la protección de datos personales, principalmente por tratarse éste de un derecho fundamental cuya regulación se debe llevar a cabo mediante ley orgánica (art. 81.1 CE) y por contrapartida, el resto de los derechos digitales pueden no serlo, lo que

significar una mayor dificultad para su modificación y adaptación a las realidades cambiantes de los avances tecnológicos.

CAPÍTULO V. AUTORIDADES CON COMPETENCIAS EN EL ÁMBITO DE PROTECCIÓN DE DATOS

1. Autoridades Europeas.

1.1. El Comité Europeo de Protección de Datos.

Antes de comenzar el análisis del Comité Europeo de Protección de Datos, nuevo órgano creado por el Reglamento, cabe realizar unas consideraciones respecto al Grupo de Trabajo del Artículo 29, denominación que tenía este mismo órgano bajo la vigencia de la Directiva 95/46, que lo creó en su artículo 29, y en el artículo 30 estableció un puñado de funciones, la mayor parte no preceptivas ni vinculantes, de entre las que destaca la formulación de recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Unión, que se ejercerá a iniciativa propia del grupo. A este órgano la Directiva 95/46 sólo le dedica un par de disposiciones que establecen su creación y funcionamiento, sin perjuicio de lo cual el Grupo de Trabajo del Art. 29 se ha convertido en un órgano fundamental para el derecho de protección de datos en la Unión y los documentos que elabora (directrices, opiniones, informes y notas de prensa) son instrumentos de consulta obligada para los intérpretes y aplicadores de las normas europeas de protección de datos, si bien es muy importante aclarar que, como hemos adelantado, sus opiniones no son vinculantes.

Desde la aprobación del RGPD, el Grupo de Trabajo del Art. 29 ha elaborado un abundante número de documentos de interpretación del Reglamento, bajo la forma de

"Directrices" (o, en su palabra original en lengua inglesa, "Guidelines"), de las que destacamos las que tratan los siguientes temas:

- La identificación de la autoridad principal para responsables o encargados;
- Los Delegados de protección de datos;
- El derecho a la portabilidad de los datos;
- Las evaluaciones de impacto relativas a la protección de datos;
- La imposición de las sanciones administrativas establecidas en el Reglamento (dirigidas a las autoridades de control);
- Decisiones individuales automatizadas;
- La elaboración de perfiles;
- Las notificaciones de las brechas de seguridad

En el RGPD, el legislador europeo otorga a este órgano una importancia y un lugar más acorde con los que se merece dentro del capítulo VII dedicado a la cooperación y coherencia, en la Sección 3ª y con una extensión de nueve artículos (más otros dos en la sección anterior, los artículos 64 y 65), en los que se han desarrollado la estructura y funciones del Comité Europeo de Protección de Datos (nombre bajo el que desde el 25 de mayo de 2018 funciona el antiguo Grupo del Artículo 29), que está compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos, está representado por su Presidente y en sus reuniones tendrá derecho a participar, con voz pero sin voto, un representante designado por la Comisión.

Este órgano tendrá personalidad jurídica[237] y desarrollará toda su actividad de manera totalmente independiente y tiene prohibido recibir instrucciones de ningún tipo[238].

En general, su actividad se dirige al asesoramiento y la emisión de informes, directrices, recomendaciones y buenas prácticas en todos los aspectos relacionados con la protección de datos en la Unión, de entre los cuales destacamos algunos que se mencionan en el Reglamento, tales como:

- Las normas corporativas vinculantes
- Situaciones de excepción para el otorgamiento de garantías ante una transferencia internacional de datos personales
- Decisiones automáticas basadas en perfiles creados a partir del análisis de datos personales.
- Violaciones de la seguridad de los datos personales y su notificación.
- Asesoramiento a las autoridades de control, en general y especialmente en lo relativo a los poderes de investigación y a la imposición de sanciones.

Tal como se infiere del capítulo en el cual se incluye, entre las principales funciones del Comité está la de garantizar la aplicación coherente del Reglamento, unificando su interpretación y aplicación en algunos casos de trascendencia transfronteriza, tal como se establece en los artículos 64 y 65 del Reglamento. Con esta finalidad el art. 65 enumera ciertos aspectos de la aplicación del RGPD, para los cuales las APD deben consultar al

[237] Art. 68.1 RGPD.

[238] Arts. 69.1 y 69.2RGPD.

Comité antes de adoptar una decisión, en cuyo caso el Comité debe emitir un dictamen que será obligatorio.

También deberá asesorar a la Comisión en todo asunto relacionado con la protección de datos personales en la Unión y, especialmente, en lo que respecta a la modificación del Reglamento. Asimismo, examinará a iniciativa propia o a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del Reglamento, emitiendo directrices, recomendaciones y buenas prácticas a fin de promover su aplicación coherente.

El artículo 71 le otorga la tarea de elaborar informes anuales sobre la protección de las personas físicas en lo que respeta al tratamiento de sus datos personales, tanto en la Unión como en terceros países y organizaciones internacionales si procede, estando también facultado [en el apartado s) del artículo 70] para evaluar si ese tercer país, territorio, uno o varios sectores específicos del mismo o una organización internacional, ya no garantizan un nivel de protección adecuado.

Llama la atención que no se establezca expresamente la necesidad, ni siquiera la conveniencia de un informe o dictamen del Comité previo a la adopción de las decisiones de adecuación que adopte la Comisión. Pero en realidad tampoco se excluye expresamente esta posibilidad y, dado que el Comité puede emitir sus directrices y recomendaciones tanto a iniciativa propia como ajena, es deseable que se convierta en buena práctica la solicitud al Comité, por parte de la Comisión, de un informe previo a la adopción de tales decisiones.

Los documentos elaborados por el Comité serán públicos, excepto en los casos en que su publicidad afecte negativamente los derechos y libertades de las personas.

El Comité ha celebrado su primera sesión plenaria el mismo día en que comenzó la aplicación del RGPD, el 25 de mayo (durante la cual aprobó una declaración sobre la e-privacidad), y su segunda sesión plenaria los días 4 y 5 de julio de 2018. A la fecha de redacción de este trabajo ha emitido seis Directrices (cuatro en 2018 y 2 en lo que va de 2019), de las cuales a lo largo de este trabajo consultaremos principalmente dos: Las "Directrices 2/2018 sobre las excepciones del Artículo 49 del Reglamento 2016/679"[239] y "Directrices 3/2018 sobre el ámbito de aplicación territorial del RGPD (artículo 3)"[240].

1.2. El Supervisor Europeo de Protección de Datos[241]

Los tratamientos de datos personales llevados a cabo por las Instituciones, órganos y organismos de la Unión Europea no están regulados por la norma general (es decir, actualmente, por el RGPD) sino por el Reglamento 18/1725 que hemos estudiado en el Capítulo II de esta tesis, norma en la que se regula la organización, funciones, facultades y poderes del Supervisor Europeo de Protección de Datos como autoridad independiente encargada de velar por la correcta aplicación de este Reglamento por parte de los organismos mencionados, así como de coordinar, junto con el CEPD (del cual forma parte[242] y de cuya Secretaría está a cargo[243]) y las APD, que la aplicación de esta norma

[239] "*EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*" en el original en ingles, citadas en el próximo Capítulo de esta tesis.

[240] "*EDPG Guidelines 3/2018 on the territorial scope of the GDPR (article 3)*" en su título original en ingles, citada en el capítulo III de esta tesis.

[241] En adelante, "SEPD".

[242] Art. 68.3 RGPD.

[243] Art. 75.1 RGPD.

sea coherente con las demás normas europeas sobre protección de datos personales, especialmente con el RGPD[244].

Esta autoridad no tiene atribuido un ámbito geográfico de competencia ya que ésta es exclusivamente material: Supervisa las actividades de las Instituciones, órganos y organismos de la Unión, en todo lo relacionado con los tratamientos de datos personales, el derecho de las personas físicas a su protección y, en un sentido amplio, también la protección de los derechos fundamentales relacionados con los datos personales.

El SEPD no fue creado por el Reglamento 18/1725 sino por la norma que anteriormente regulaba la protección de los datos personales en el mismo sector, el Reglamento 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[245].

Desde su creación, la función principal de este órgano ha sido la de controlar que los tratamientos de datos personales realizados por las instituciones, órganos y organismos de la Unión respeten los derechos y libertades fundamentales de las personas (principalmente el derecho a la protección de datos personales)[246], así como también asesorar a las mismas entidades y a los interesados en todas las cuestiones relacionadas con los tratamientos de datos personales.

[244] Art. 62 Reglamento 18/1725.

[245] En adelante, "Reglamento 45/01".

[246] Art. 52, apartados 2) y 3), Reglamento 18/1725.

El artículo 55 del Reglamento 18/1725 asegura la independencia del SEPD, que no podrá tener influencias externas ni recibir instrucciones de ninguna otra persona[247] o entidad, ni podrá tener ninguna otra actividad profesional aparte de la propia de este cargo[248].

Además de las actividades propias del control de la aplicación del Reglamento 18/1725[249] y de las de difusión y promoción del respeto a los derechos fundamentales (principalmente, el derecho a la protección de datos personales) entre los organismos e Instituciones de la UE[250] así como entre la ciudadanía en general[251], el SEPD es el órgano encargado de recibir, gestionar, investigar y decidir acerca de las reclamaciones de los interesados[252] que consideren que un tratamiento de datos personales realizado por una Institución u organismo de la Unión Europea infringe el Reglamento 18/1725, ya la haya presentado el interesado frente al SEPD[253] o una entidad, organización o asociación en su representación[254].

También tiene potestades de investigación[255], correctivas y sancionadoras[256] con respecto a las Instituciones y organismos de la Unión, quienes merced a estas potestades tienen la obligación de obedecer las decisiones del SEPD, sin perjuicio de que éstas están

[247] Apartado 2 del Art. 55 Reglamento 18/1725.

[248] Apartado 3 art. 55 Reglamento 18/1725.

[249] Si bien ninguna de las funciones que el Reglamento 18/1725 establece para el SEPD se limita a uno solo de los aspectos señalados, en esta nota y en las dos siguientes citaremos las que más parecen referirse a los aspectos particulares. La aplicación en general del Reglamento 18/1725 predomina en las disposiciones del Art. 57.1, apartados a); f) i); j); n) o) y p) de la citada norma.

[250] Art. 57.1 apartados a); c) y g) del Reglamento 18/1725.

[251] Art. 57.1, apartados b) y d) Reglamento 18/1725; los aspectos de sus funciones relacionados en la anterior nota al pie y en esta, también se encuentran presentes en el art. 58.3 del Reglamento 18/1725.

[252] Art. 57.1.e) Reglamento 18/1725.

[253] Art. 63.1) Reglamento 18/1725.

[254] Art. 67 Reglamento 18/1725.

[255] Art. 58.1 Reglamento 18/1725.

[256] Arts. 58.2 y 66 Reglamento 18/1725.

sometidas al control jurisdiccional del Tribunal de Justicia de la Unión Europea[257], jurisdicción ante la cual el SEPD también tiene la potestad de someter los asuntos que considere procedentes[258].

1.3. El Comité Consultivo de Convenio 108 del Consejo de Europa.

El artículo 18 del Convenio 108 dispone la creación de un Comité Consultivo formado por un representante por cada Parte en el Convenio, en el que pueden estar representados a través de un observador los Estados que sean miembros del Consejo de Europa y no sean Parte del Convenio 108. También podrá estar representado por un observador cualquier Estado que no sea miembro del Consejo de Europea ni sea Parte, al que el Comité invite a hacerlo.

Las funciones de este Comité son de consulta y asesoramiento con respecto a la mejora y facilitación de la aplicación del Convenio así como de cualquier proyecto de reforma, respecto a los cuales tendrá también la facultad de proponerlo al Comité de Ministros del Consejo de Europa.

El Protocolo de reforma de esta Convención, en su Capítulo VI (arts. 22 a 24) mantiene el funcionamiento de este Comité, con una composición, funciones y especialidades básicamente idénticas a las que hemos visto.

[257] Arts. 58.5 y 64 Reglamento 18/1725.

[258] Art. 58.4 Reglamento 18/1725.

2. Autoridades nacionales.

2.1. Regulación en el RGPD.

Las autoridades nacionales de aplicación o de control comenzaron a funcionar durante la vigencia de la Directiva 95/46, si no antes como es el caso de la Agencia Española de Protección de Datos, creada por medio de la LORTAD de 1992 y conformada definitivamente mediante Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Al igual que ocurre con los demás aspectos del derecho a la protección de datos, la Directiva 95/46 dedica unas pocas disposiciones a las autoridades nacionales de aplicación, contenidas en el artículo 28, que está incluido junto al art. 29 (dedicado al Grupo de Protección de las personas con respecto al tratamiento de sus Datos Personales) en el capítulo VI de la norma. De entre las características mínimas exigidas por la Directiva para dichas autoridades, podemos destacar la independencia en cuanto a su naturaleza, la atribución de funciones de carácter consultivo así como de poderes de investigación y de adopción de medidas preventivas y resolutivas[259], las que estaban sometidas a control judicial, para lo cual la Directiva 95/46 les atribuía capacidad para comparecer en juicio.

[259] En la Unión Europea existen Estados miembros cuyo ordenamiento jurídico no permite que las autoridades administrativas impongan sanciones administrativas, que están reservadas a los órganos judiciales. Por ese motivo la Directiva 95/46 no imponía estas funciones a las APD. El RGPD por el contrario sí las atribuye por lo que en la norma interna que se apruebe para la adaptación a este Reglamento, los Estados miembros deben adoptar las medidas necesarias para permitir esas facultades.

Por su parte el RGPD (que en este aspecto es, al igual que en el resto de los aspectos analizados, una norma evidentemente más desarrollada y efectiva que la anterior Directiva) regula las autoridades de control en sus Capítulos VI y VII, individualmente consideradas en el primero de ellos y en relación a su interacción mutua en el segundo.

El Capítulo VI del RGPD ya en su título las califica de "*independientes*", requisito al que dedica el título de la Sección I del capítulo y los seis apartados del artículo 52, característica en la que se advierte la decisiva influencia del TJUE, que en su sentencia Schrems declara que: "*La creación en los Estados miembros de autoridades de control independientes constituye, pues, un elemento esencial de la protección de las personas frente al tratamiento de datos personales…*" y su independencia es una garantía que "*se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades.*[260]"

Es más, el Tribunal de Justicia proclama que las autoridades nacionales de control, en su función de protección de los derechos y libertades de las personas, gozan de independencia incluso con respecto a la Comisión, al resolver que tienen poderes para investigar si una transferencia internacional de datos personales cumple con los requisitos instaurados en la Directiva 95/46, incluso cuando existe una Decisión de la Comisión sobre la adecuación del nivel de protección otorgado por el derecho del estado receptor[261]. Si bien no tienen la facultad de declarar inválidas (lo que sólo compete al Tribunal de Justicia[262]) o dejar de aplicar las decisiones de la Comisión sino que, por el contrario, deben adoptar las medidas necesarias para que sean de aplicación en el Estado que las ha

[260] Sentencia Schrems, párrafo 41.

[261] Párrafos 54 a 59 de la Sentencia Schrems, especialmente este último

[262] Párrafo 61 Sent. Schrems.

designado[263], cuando consideren que una decisión de la Comisión (u otro acto de las Instituciones) puede vulnerar los derechos y libertades de una persona, deben emplear su capacidad para comparecer en juicio para impugnar, ante los tribunales nacionales, el mencionado acto[264].

Siguiendo la doctrina sentada por la jurisprudencia citada, el art. 51 del RGPD luego de ordenar el establecimiento en cada Estado miembro de una autoridad de control, delinea las funciones centrales de ésta: Supervisar la aplicación del RGPD, proteger los derechos y libertades fundamentales de las personas en relación con el tratamiento de datos personales, facilitar la libertad de circulación de este tipo de datos en la Unión y contribuir a la aplicación coherente del Reglamento a través de la cooperación entre sí y con la Comisión.

2.2. Ámbito territorial de actuación

Según el artículo 54 del RGPD tanto el establecimiento de la autoridad de supervisión como el estatuto y condiciones de sus miembros se deben establecer por ley, lo que indica que, en líneas generales y tal como lo ratifican el considerando 122 y el art. 55.1, la competencia de ésta tiene la misma base territorial de vigencia, es decir, el territorio del Estado miembro que la aprueba.

En su propio Estado, las autoridades ejercen todos los poderes y funciones otorgados por el RGPD y por el derecho interno, entre los cuales se incluyen amplios poderes de investigación en el territorio en el que ejerce sus competencias, aun cuando para el

[263] Párrafos 51 y 52 sentencia Schrems

[264] Párrafo 65 Sent. Schrems.

responsable o el encargado del tratamiento bajo investigación sea otra la autoridad principal designada y siempre en coordinación con ésta[265].

Pero además el RGPD, en calidad de norma europea, confiere a dichas autoridades un buen número de facultades, funciones y poderes que hacen que los límites territoriales de sus competencias se difuminen, extendiéndose potencialmente hacia todo el territorio de la Unión. Esta extensión de las competencias tiene excepciones en el caso de los tratamientos efectuados por autoridades públicas u organismos privados que actúen en virtud del art. 6.1. c) y e) del RGPD (esto es, en cumplimiento de una obligación legal, de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento), en los cuales la autoridad competente es la del Estado miembro de que se trate, y no se aplicará el art. 56, es decir la ampliación del ámbito geográfico de sus competencias[266]. En ningún caso las autoridades de control podrán supervisar los tratamientos llevados a cabo por órganos jurisdiccionales en ejercicio de su función judicial[267].

En este orden de ideas, en el listado de funciones y poderes enumerados en los artículos 57 y 58 del RGPD, podemos encontrar algunos que sobrepasan las fronteras del Estado miembro de designación, cuales son: cooperar con otras autoridades de control, prestarles asistencia y, en especial, solicitar la cooperación y asistencia de las autoridades de otros Estados miembros, investigar los incumplimientos en otros estados miembros, adoptar cláusulas tipo que surtirán efecto en toda la Unión, dictaminar y aprobar códigos de

[265] Considerando 130 del Reglamento.

[266] Art. 55.2 RGPD.

[267] Art. 55.3 RGPD.

conducta para tratamientos transfronterizos, autorizar cláusulas contractuales y aprobar normas corporativas vinculantes con el mismo alcance territorial.

La extensión de la competencia de las autoridades de control más allá de los límites del Estado miembro de designación se produce asimismo en los mecanismos de contribución a la aplicación coherente del Reglamento[268].

2.3. Modificaciones introducidas por el RGPD a la competencia territorial.

2.3.1. Autoridad de control principal.

El Reglamento dispone que para los responsables o encargados que realicen tratamientos de datos personales transfronterizos se asignará una autoridad de control única, denominada *autoridad principal*[269]*,* con el objetivo de impedir que las entidades se vean obligadas a adaptarse a normas estatales distintas o a diferentes interpretaciones del Reglamento en cada Estado afectado por el tratamiento.

Sin embargo, los tratamientos realizados por las autoridades públicas o por organismos privados pero en interés público constituyen una excepción a estas disposiciones, ya que para ellos no tendrán aplicación las normas de extraterritorialidad de las competencias de las autoridades de control. En dichos casos, sólo actuará la autoridad de control designada por el Estado al que pertenezca la autoridad pública o en cuyo interés se realice el tratamiento.

[268] Art. 51.2 RGPD.

[269] Considerando 124 y art. 56 RGPD.

Con respecto a tratamientos realizados por entidades privadas en interés privado pueden darse los siguientes casos:

a) Tratamientos realizados en el ámbito de actividades de un único establecimiento del responsable o del encargado y que afecten a interesados de forma sustancial en distintos estados miembros.

b) Tratamientos realizados en el ámbito de las actividades de distintos establecimientos del responsable o del encargado, que afecten sustancialmente a interesados en más de un estado miembro.

c) Tratamientos realizados en el ámbito de las actividades de distintos establecimientos del responsable o del encargado, ubicados en más de un estado miembro y que, sin embargo, ya sea el tratamiento en sí o uno o más aspectos del mismo sólo afecten sustancialmente a interesados en un único estado miembro (que puede coincidir con el estado del establecimiento o no).

Tal como hemos visto, los casos de los puntos a) y b) son denominados en el Reglamento *tratamientos transfronterizos* y la mayor parte de los diferentes aspectos de estos tratamientos caen bajo la competencia de una autoridad de control a la que se otorga el título de *principal*, que puede no ser la única autoridad actuante ya que en muchos casos puede ser necesaria la colaboración de otras autoridades de control, denominadas *autoridades interesadas* que analizaremos posteriormente.

A los casos como el descrito en el apartado c) los denominaremos *tratamientos de efectos restringidos* y tienen una solución peculiar que analizaremos más adelante.

La autoridad principal será la del Estado miembro donde esté ubicado el único establecimiento o el establecimiento principal a los fines del tratamiento, según el caso.

Podemos encontrar la definición de establecimiento principal en el artículo 4.16) RGPD, que realiza una distinción entre el establecimiento principal del responsable y el del encargado, en la que el primero es el lugar de su administración central en la Unión o el establecimiento donde se adopten las decisiones sobre los fines y los medios del tratamiento, si fuera distinto de la administración central.

Con respecto al establecimiento principal del encargado, será aquél de su administración central en la Unión o, si careciera de ésta, se toma nuevamente la conexión territorial *contextual*, es decir se refiere al establecimiento en cuyo contexto de actividades se ejecuten las principales actividades de tratamiento en este caso del encargado en la Unión, siempre que al realizarlas el encargado en cuestión esté sometido al Reglamento. Volvemos a encontrarnos en esta definición con la ubicuidad del derecho tecnológico, dado que en el caso en que un encargado de tratamiento de datos posea establecimientos en distintos Estados miembros pero su administración central se encuentre en un país tercero, es posible que el o los tratamientos de datos se realicen *en el contexto de las actividades* de varios (si no de todos los) establecimientos, por lo tanto para determinar la autoridad principal habrá que emplear otro nexo de conexión, por ejemplo la existencia de interesados especialmente afectados en uno de los Estados miembros.

Según lo describe el considerando 36, el establecimiento principal debe ser un lugar en donde se ejerzan de modo efectivo, real y de forma estable[270] actividades de gestión y donde se adopten las principales decisiones en cuanto a los fines y medios del tratamiento, no siendo necesario que su ubicación coincida con el lugar donde se ubiquen los medios técnicos y tecnologías para el tratamiento de datos personales ni con el lugar donde se

[270] Tal como ya hemos visto, estas características de la actividad han sido establecidas por la Sentencia Google del TJUE.

realice el tratamiento (entendemos que esta última expresión se refiere al lugar donde se encuentren las personas que realicen el tratamiento).

El establecimiento principal así descrito puede no coincidir con el establecimiento principal en el sentido mercantil de la entidad, ya que habrá coincidencia entre ambos sólo cuando el establecimiento principal en sentido mercantil sea el centro donde se adoptan las principales decisiones en cuanto a fines y medios del tratamiento.

2.3.2. Autoridades de control interesadas. Mecanismos de coordinación y cooperación.

Si bien, tal como hemos visto, en principio la competencia de la autoridad de control se ejerce dentro de los límites territoriales del Estado de designación, el considerando 134 y los artículos 60 a 63 del Reglamento las autorizan a actuar coordinadamente cuando el tratamiento sea considerado transfronterizo, es decir que cada autoridad de control tiene ciertas facultades para trascender el nivel nacional y actuar a nivel europeo.

Las competencias a nivel europeo se advierten especialmente en la letra del considerando 135, relativo al mecanismo de coherencia, que describe un contexto en el cual una autoridad de control puede adoptar una medida con efectos jurídicos sobre operaciones de tratamientos transfronterizos, casos en los cuales junto a la autoridad principal actuarán otras autoridades (aunque no frente al agente, para quien la autoridad principal es la única), que el Reglamento denomina interesadas, que se presentarán en los siguientes casos[271]:

[271] Artículo 4.22) del Reglamento.

- Cuando el responsable o encargado posean establecimientos en más de un Estado miembro;
- Cuando el tratamiento efectuado en el contexto de las actividades de un único establecimiento afecte sustancialmente a interesados que se encuentren en otros Estados miembros;
- Cuando un interesado presente una reclamación ante una autoridad de control que no sea la principal, respecto a un tratamiento cuyos efectos trasciendan el ámbito geográfico del Estado miembro donde se presenta la reclamación[272].

En los casos en que la autoridad principal del responsable sea distinta de la del encargado, se considerará autoridad principal la que corresponda al responsable y autoridad de control interesada la correspondiente al encargado, excepto que el proyecto de decisión sobre el tratamiento afecte únicamente al responsable[273], caso en el cual para ese tratamiento concreto no existirá autoridad interesada.

Quitando los casos en que la Resolución consista en el rechazo total o parcial de una reclamación presentada por un interesado ante otra autoridad[274] (que trataremos más adelante), la autoridad de control principal debe adoptar las decisiones que impliquen al responsable o encargado, coordinando la participación de las demás autoridades en el proceso de adopción de la decisión, de acuerdo a las directrices que mencionamos a continuación.

[272] Pues si la reclamación se refiere a un tratamiento realizado exclusivamente por un determinado establecimiento del responsable en el Estado de la reclamación, o que afecte significativamente sólo a personas que se encuentren en dicho estado, se activará el mecanismo que analizamos en el apartado siguiente.

[273] Considerando 36 del Reglamento.

[274] Considerando 125 del Reglamento.

Esta necesaria interactividad entre las autoridades de diferentes jurisdicciones se regula en el Reglamento bajo la denominación de mecanismos de cooperación y de coherencia, para cuya coordinación se faculta al Comité de Protección de Datos de la Unión Europea.

2.3.3. Autoridad de control interesada competente.

En los casos en que el responsable o encargado está establecido en más de un estado miembro y ante una autoridad de control que no sea la principal se presente una reclamación relativa a un tratamiento que se realice exclusivamente en el contexto de un establecimiento en el Estado miembro de designación de esa autoridad o afecte solamente a interesados en el Estado en cuestión, la autoridad de control receptora de la reclamación (que en este caso es interesada) informará sobre todas las circunstancias del caso a la autoridad de control principal, que deberá decidir si trata el asunto o lo delega en la autoridad interesada[275]. Estos procedimientos se regulan en los apartados 2 a 6 del artículo 56 y, por remisión de éstos, se aplicarán los artículos 60, 61 y 62.

Cuando la decisión sobre la avocación al asunto sea positiva, sin perjuicio de la aplicación de los mecanismos de coordinación que veremos a continuación, la autoridad interesada debe tener la posibilidad de presentar un proyecto de decisión, que la autoridad principal deberá tener en cuenta en la mayor medida posible al preparar su proyecto de decisión[276].

Si la autoridad principal decide dejar la decisión a la autoridad interesada, ésta se convertirá en *autoridad interesada competente* y el caso tramitará de acuerdo a los artículos 61 y 62 del Reglamento, teniendo en cuenta que la autoridad principal siempre

[275] Art. 56.3.

[276] Art. 56.4.

actuará como interlocutora con respecto al responsable correspondiente[277]; en otras palabras, será la encargada de notificar la decisión al responsable y recibir los posteriores escritos o recursos que procedan.

Del juego de disposiciones que hemos expuesto en este subapartado, que son las destinadas a determinar la autoridad que tendrá competencia en los casos con elementos de conexión territorial relacionados con distintos estados miembros, podemos inferir que los elementos que determinan la competencia de una autoridad pueden ser:

- La ubicación en el estado de designación de un establecimiento del responsable o del encargado en cuyo contexto se llevan a cabo tratamientos de datos personales. Por ello, el límite geográfico de las competencias de las autoridades de supervisión no se determina por la ubicación de medios físicos o de personas, sino por otro elemento de conexión territorial, que en este caso es, tal como lo hemos denominado, contextual o abstracto, cual es el contexto de las actividades de un establecimiento.
- La existencia de interesados sustancialmente afectados (o que puedan estarlo) por el tratamiento, siempre que se encuentren en uno o más estados diferentes. En este caso el elemento de conexión territorial no se refiere al ámbito material de aplicación del Reglamento (los tratamientos de datos personales) sino a otro totalmente autónomo: La existencia de interesados que estén *afectados* por el tratamiento.
- La presentación de una reclamación de un interesado ante una determinada autoridad de control.

[277] Art. 56.6.

- La presencia de interesados a quienes esté dirigido el tratamiento, cuando el encargado o el responsable no están establecidos en la Unión.

2.4. Situaciones especiales: impugnación de sus decisiones

El RGPD en su artículo 78 regula el derecho a la tutela judicial efectiva contra las decisiones de las autoridades de control, es decir el derecho a impugnar judicialmente sus resoluciones, por parte los distintos sujetos (responsables, encargados e interesados). Este asunto plantea situaciones complejas creadas por la restricción de la competencia territorial de los órganos jurisdiccionales, dado que en virtud de la organización jurisdiccional y administrativa de los Estados miembros, los órganos judiciales no tienen competencia para juzgar las decisiones adoptadas por órganos administrativos de otros Estados miembros, sólo están habilitados para juzgar las decisiones o resoluciones de los órganos y autoridades administrativas establecidos en el Estado miembro de que se trate.

Por ello el Reglamento introduce varias disposiciones que tienen como finalidad permitir el control jurisdiccional de las autoridades de control, cuya solución depende del sujeto perjudicado por la resolución, que en tal calidad debe estar habilitado para impugnarla.

a) *Por los responsables y encargados*.

Hemos visto que la autoridad principal para los responsables y encargados es la competente en el Estado miembro donde tienen su establecimiento principal a los efectos del tratamiento o su establecimiento único. Esta regla de la autoridad principal también determina la competencia jurisdiccional sobre sus decisiones, es decir que para impugnar las resoluciones de las autoridades principales (que además son el único interlocutor válido para los correspondientes responsables y encargados) que les perjudican, tienen

competencia los juzgados del mismo Estado de establecimiento, lo que facilita el acceso a la justicia de responsables y encargados.

b) *Por los interesados*.

Es un derecho fundamental de los interesados establecido en el art. 77 del Reglamento, el de presentar reclamaciones ante una autoridad de control. Si bien en principio la habilitación de la competencia de cada autoridad deberá estar establecida en la ley de creación, el Reglamento en el artículo citado habilita la competencia, como mínimo, de la autoridad del Estado miembro en que el interesado tenga su residencia, su lugar habitual de trabajo o donde considere que se haya cometido una infracción al Reglamento[278]. La redacción de este apartado deja margen a los Estados para establecer otras normas de habilitación.

Según el apartado 8 del art. 60, cuando la resolución final sea de rechazo de las pretensiones del interesado, será adoptada y notificada por la autoridad ante la que éste haya presentado la reclamación, a los efectos de habilitar la competencia jurisdiccional del mismo estado para la impugnación de la decisión.

De esta forma se salvaguarda el derecho a la tutela judicial efectiva del interesado, facilitándole la impugnación de las decisiones que lo perjudiquen ya que, de acuerdo con lo prescrito por el artículo 78.3 del Reglamento, los recursos judiciales contra las decisiones o la inactividad de las autoridades de control se deberán interponer ante los tribunales del Estado de designación de dicha autoridad. A su vez, en aplicación de las normas europeas de competencia jurisdiccional para dirimir cuestiones que involucren a consumidores, se equiparan éstos con los interesados afectados por un tratamiento de

[278] Art. 77.1 RGPD.

datos y, como consecuencia, se declara competente para entender en la reclamación de un interesado contra el responsable o el encargado a los tribunales del Estado donde el responsable o el encargado tenga un establecimiento o los del domicilio del interesado, a elección de éste[279], excepto en los casos en que el responsable o encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos[280], en cuyo caso sólo se podrá interponer la queja o reclamación ante la autoridad de dicho estado.

Los tribunales nacionales son competentes para elevar cuestiones prejudiciales sobre la interpretación del Reglamento ante el Tribunal de Justicia y son asimismo competentes para elevar ante dicho órgano las cuestiones de invalidez de las decisiones del Comité, ya que carecen de la competencia suficiente para declararla cuando ésta es invocada ante ellos[281].

En la misma línea de pensamiento, también se establecen mecanismos de declaración de incompetencia e inhibición para las cuestiones que se presenten ante autoridades judiciales que no se consideren competentes para resolver la cuestión planteada, y especialmente la declaración de litispendencia, que procederá cuando una autoridad judicial ante la que se plantea un determinado caso tiene conocimiento de que otro u otros procedimientos relativos al mismo asunto y en relación con el mismo tratamiento por el mismo responsable o encargado tramitan ante tribunales de otras jurisdicciones europeas[282]. En estos casos, el tribunal ante el que se haya planteado el segundo o

[279] Considerando 145.

[280] Art. 79.2

[281] Considerando 143.

[282] Considerando 144 y art. 81.

sucesivos asuntos se pondrá en contacto con los otros tribunales para confirmar la existencia de los otros procedimientos, pudiendo suspender el procedimiento e inhibirse si considera que el otro tribunal, ante el cual se ha planteado la acción en primer lugar, es competente para su resolución y corresponde la acumulación de acciones.

El considerando 146, en consonancia con el artículo 82.1, declara que los responsables y los encargados del tratamiento serán responsables por los daños y perjuicios que se hayan causado al interesado como consecuencia de un tratamiento realizado en infracción del Reglamento.

2.5. Procedimiento especial en caso de concurrencia de autoridades de control.

De acuerdo al artículo 60 RGPD, cuando en un caso, además de la autoridad principal, existan otras autoridades interesadas, la autoridad principal comunicará "*sin dilación*"[283] el proyecto de decisión a éstas, que tendrán un plazo de cuatro semanas para presentar objeciones pertinentes y motivadas. Al recibir las objeciones, la autoridad principal tiene dos opciones:

a) Admitir las objeciones, en cuyo caso elaborará un nuevo proyecto de decisión y lo enviará nuevamente, *sin dilación*, a las autoridades interesadas, que en este caso tendrán sólo dos semanas para presentar nuevas objeciones.
b) Rechazarlas, en cuyo caso se pondrá en marcha el mecanismo de coherencia del artículo 63.

[283] Destacamos la expresión *sin dilación* para llamar la atención sobre la indeterminación del término jurídico, que deberá ser precisado estimamos por la legislación de los Estados miembros.

Si ninguna de las autoridades presenta objeciones, la autoridad principal adoptará la decisión contenida en el proyecto (que será vinculante para todas las autoridades intervinientes) y la notificará al establecimiento único o principal del responsable o del encargado; asimismo las autoridades interesadas ante las que se haya presentado una reclamación deberán notificarla a los reclamantes.

Cuando la decisión implique la desestimación o rechazo de reclamaciones presentadas ante autoridades interesadas, la autoridad principal debe remitirla a éstas para que adopten la decisión de rechazo, la notifiquen al reclamante e informen de ello al responsable del tratamiento[284]. Para comprender esta disposición así como la del art. 60.9 que expondremos a continuación, hay que tener en cuenta que la regla de competencia para la revisión judicial de las decisiones de las APD es la del Estado miembro de designación; y que las referidas decisiones pueden ser impugnadas por el perjudicado por ellas, por lo que es necesario que la autoridad que adopte la decisión (o parte de ella como veremos más adelante) contraria a una de las partes debe ser la autoridad que más facilite su acceso a la justicia. Así, una decisión estimatoria de la reclamación de un interesado puede implicar la imposición de medidas sancionadoras y la exigencia de responsabilidad al responsable o encargado, por lo que debe poder facilitar para éstos la vía judicial; por el contrario, cuando se rechaza una reclamación, se debe abrir la vía judicial para el interesado. Por ello cuando las autoridades principal e interesadas hayan acordado admitir parcialmente la reclamación y rechazar el resto, la decisión se adoptará por partes: La de admisión parcial será asumida por la autoridad principal (que es la competente para aplicar medidas al responsable o encargado) y la de rechazo parcial, por la autoridad

[284] Art. 60.8.

interesada ante la cual se presentó la reclamación[285], a los efectos de poder habilitar la vía judicial al interesado y poder entender con éste las cuestiones que se planteen.

2.6. Actuación conjunta de varias autoridades de control.

Las disposiciones de los distintos apartados del artículo 62 tienen como finalidad permitir ciertas actuaciones a las autoridades de control que también implican la superación de los límites territoriales estatales, bajo la denominación *operaciones conjuntas*, en las que intervendrán autoridades de control de distintos estados miembros, en el territorio de uno o más estados de designación y cuyos mecanismos exponemos a continuación.

Cuando el responsable o el encargado de un tratamiento tiene establecimientos en varios Estados miembros o cuando sea posible que por las operaciones de un tratamiento se vean sustancialmente afectados un número significativo de interesados en más de un Estado miembro, las autoridades de control implicadas tendrán derecho a participar en operaciones conjuntas. Para ello, la autoridad de control principal o la que resulte competente por haberse presentado ante ella una reclamación cuyo tratamiento declinó la autoridad principal, deberá invitar a las autoridades de control de cada uno de los estados implicados a participar en operaciones conjuntas y, si recibe una solicitud de participación por parte de otra autoridad, deberá responder sin dilación[286].

Dichas operaciones conjuntas se llevarán a cabo siempre de acuerdo al derecho del Estado miembro en cuyo territorio se deba realizar (que se denominará *estado de acogida*), cuya autoridad de control, siempre que el derecho de dicho Estado lo permita, podrá conferir

[285] Art. 60.9.

[286] Art. 62.2.

o delegar poderes en los miembros o el personal de la autoridad de control de otro Estado miembro (la *autoridad de origen*) o, siempre que el derecho del Estado en cuyo territorio se desarrolle la operación lo autorice, aceptar que la autoridad de control de otro Estado miembro ejerza sus poderes y funciones en el Estado de acogida[287]. La operación deberá realizarse siempre bajo la orientación y en presencia de miembros o personal de la autoridad de control de acogida y todos los participantes (incluidos los miembros o el personal de la autoridad de origen) estarán sujetos al derecho de dicho Estado.

Cuando durante la realización de estas operaciones los miembros o el personal de una autoridad de control de origen provoquen daños y perjuicios en el territorio del Estado de acogida, éste deberá asumir la responsabilidad por los mismos como si su propio personal los hubiera causado, y sólo podrá reclamar al estado de origen el reintegro de las indemnizaciones que por dichos daños y perjuicios haya abonado a terceros, pero no podrá reclamar los daños que se hayan causado al propio Estado[288].

Todos los mecanismos de cooperación y de designación de la autoridad con competencia en un determinado caso ceden ante la necesidad de una actuación urgente, según el artículo 66 del Reglamento.

2.7. Caracteres añadidos por la modificación del Convenio 108

El artículo 15 del Convenio 108 prevé la creación, por cada Parte, de una o más autoridades de aplicación, estableciendo algunas de las prerrogativas, facultades y

[287] Art. 63.3.

[288] Art. 62, apartados 4. 5 y 6.

funciones de las que como mínimo deben estar revestidas dichas autoridades, de entre las cuales cabe destacar la facultad de instigación de acciones judiciales, el deber de actuar con independencia e imparcialidad, el deber de confidencialidad y el sometimiento de sus decisiones al control judicial[289], rasgos que ya se recogen en el derecho de la Unión. Otra de las funciones de estas autoridades serán las de cooperación y asistencia con las otras Partes de la Convención, para lo cual se notificarán las designaciones y datos de contacto al Secretario General del Consejo de Europa[290]. La cooperación consistirá, en particular, en el intercambio de información[291] y documentación en cuanto al derecho vigente y la práctica administrativa en su jurisdicción[292], en la coordinación de sus investigaciones e intervenciones así como en la realización de acciones conjuntas[293].

A las acciones de cooperación entre las autoridades designadas por distintas Partes le será de aplicación la prohibición de comunicación de datos personales, a menos que dichos datos sean esenciales para la cooperación o que el interesado haya dado su consentimiento explícito, específico, libre e informado[294] y el principio de limitación de la finalidad, en el sentido de que la información que una autoridad de aplicación reciba proveniente de otra autoridad y relacionada con una petición, sólo será utilizada para la finalidad establecida en dicha petición[295]. Las autoridades están obligadas a acceder a la petición de otra autoridad, siempre que ello esté dentro de sus funciones y poderes, que respete la

[289] Art. 15.2.

[290] Art. 16.2.a Convenio 108.

[291] Art. 17.1.a Convenio 108.

[292] Art. 17.1.c Convenio 108.

[293] Art. 17.1.b Convenio 108.

[294] Art. 17.2 Convenio 108.

[295] Art. 19.1 Convenio 108.

Convención y que no atente contra la soberanía, la seguridad nacional o el orden público de la Parte receptora de la petición, o los derechos y libertades fundamentales de los individuos sometidos a la jurisdicción de ésta[296].

3. El caso español: La Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos[297] fue creada por la primera ley sobre esta materia que se dictó en este país, es decir la LORTAD, y su Estatuto aprobado por Decreto 428/1993, de 26 de marzo.

Hasta el momento de aplicación del RGPD sus funciones eran las de crear, mantener y supervisar los registros de tratamientos de datos, atender las peticiones de los interesados, dictar documentos de información y divulgación sobre protección de datos en España, resolver los asuntos que se le presentan y, en virtud de dichas resoluciones y en su caso, imponer las sanciones que considere procedentes, las que se dividen en leves, graves y muy graves y tienen un importe mínimo, para las primeras, de 900 € y uno máximo, para las muy graves, de 600.000 €[298].

[296] Art. 20 Convenio 108.

[297] En adelante, AEPD

[298] Si bien no es relevante a los efectos de esta investigación, el panorama de las sanciones cambiará radicalmente desde la entrada en vigor del Reglamento, ya que en éste las sanciones administrativas no se dividen en función de su gravedad sino específicamente por la conducta infractora, estableciendo sanciones de hasta 10.000.000 € o del 2% del volumen de negocio total global anual del ejercicio anterior para las conductas enumeradas en el art. 83.4 RGPD y de hasta 20.000.000 € o el 4% del volumen de negocio total global anual del ejercicio anterior para las conductas descritas en el art. 83.5. Los mencionados son los importes máximos que pueden imponerse, graduándose de acuerdo a las pautas establecidas en el mismo Reglamento, no pudiendo ser modificadas por las normas nacionales. Por ello el Proyecto LOPD contiene una calificación de las sanciones en base a su gravedad, que regirá exclusivamente con respecto a la prescripción.

Como hemos visto, el RGPD desarrolla y amplía las funciones de las autoridades nacionales de aplicación, por lo que en línea con ello la LOPD 3/18 dedica a estos órganos su Titulo VII (arts. 44 a 62), dividido en dos capítulos, el primero de los cuales regula la autoridad nacional (AEPD) y el segundo, las autoridades autonómicas.

En consonancia con el RGPD, se otorga a la AEPD el estatus de autoridad administrativa independiente, de ámbito estatal, que se relaciona con el Gobierno a través del Ministerio de Justicia y para la cual se deberá dictar un nuevo Estatuto que la adapte a las nuevas funciones otorgadas por la norma europea.

En el Título VII de la LOPD 3/18 se otorga a la AEPD funciones de investigación y de auditoría preventivas. Las primeras pueden no desarrollarse en solitario sino con la colaboración de las autoridades de protección de datos de otros Estados miembros, en virtud de lo dispuesto por el artículo 62 del RGPD y las segundas se refieren a los tratamientos realizados por un sector concreto de actividad y podrán finalizar con el dictado de directrices generales o específicas, por parte del Presidente de la Agencia, para asegurar la plena adaptación del sector o del responsable al RGPD o a la Ley Orgánica que regula esta materia.

El artículo 55 regula las circulares de la AEPD, que ya hemos mencionado anteriormente como una fuente del derecho que consisten en disposiciones generales dictadas por su Presidencia, de desarrollo y ejecución del RGPD y de la LOPD 3/18, que se sujetarán al procedimiento establecido en el Estatuto de la AEPD y serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Cabe traer a colación en este punto que se trata de resoluciones de una autoridad administrativa y, por lo tanto, sujetas a recursos y revisiones judiciales como cualquier

otro acto de esta naturaleza. Es decir, que si bien la Agencia tendrá la primera palabra en cuanto a la interpretación y aplicación del Reglamento y de la Ley Orgánica, sus actos podrán ser declarados nulos o revocados por decisión judicial, no sólo en virtud de los recursos a los que están sujetos todos los actos administrativos sino también en base al derecho a la tutela judicial efectiva contra los actos de una autoridad de control, establecido en el art. 78 del RGPD y el art. 106 CE.

En virtud de lo dispuesto por el art. 68.4 del RGPD, en el sentido de que cuando en un Estado miembro convivan más de una autoridad de control de datos, el derecho de dicho estado debe designar a una de ellas para que lo represente como miembro del Comité Europeo de Protección de datos, el art. 56.2 LO 3/18 designa en tal carácter a la AEPD.

Entre sus funciones estará también toda la relativa a la de acción exterior y representación de España en el ámbito internacional en todo lo que esté relacionado con la protección de datos. En esa calidad, le corresponde la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos[299], es decir que participará como autoridad competente en la aplicación de todos los convenios internacionales en los que España sea parte sobre protección de las personas físicas con respecto al tratamiento de datos personales y también en cualquier otro tipo de foros, reuniones u organizaciones internacionales sobre esta materia, así como colaborar con autoridades, instituciones, organismos y administraciones de otros Estados en el ámbito de sus competencias, facultades que incluyen la suscripción de acuerdos internacionales administrativos y no normativos[300].

[299] Art. 56.1 LO 3/18

[300] Art. 56.3 LO 3/18.

Junto a la AEPD existen autoridades autonómicas en esta materia[301], que deberán coordinarse y cooperar para la aplicación homogénea del derecho europeo y nacional en todo el territorio español[302]. Sin perjuicio de ello, la LO 3/18 prevé que la AEPD pueda instar a las autoridades autonómicas a adoptar las medidas que considere necesarias para la correcta aplicación del Reglamento[303], pero no prevé lo contrario, es decir que las autoridades autonómicas puedan hacer lo propio con respecto a la autoridad nacional. Como única representante española ante el Comité, la AEPD será la vía de comunicación entre éste y las agencias autonómicas, teniendo la obligación de compartir toda la información y comunicaciones obtenidas en virtud de esa representación con las agencias autonómicas[304].

No obstante la competencia a nivel internacional y europeo que se confiere a la AEPD, cuando en un tratamiento transfronterizo el responsable o encargado sólo desarrolle actividades de tratamiento de impacto significativo en el ámbito territorial de una de las agencias autonómicas y no lo haga de forma significativa en el resto del territorio español, la autoridad de control principal o interesada, según corresponda de acuerdo a las disposiciones del RGPD, será la autoridad autonómica[305]. Pero las competencias de las autoridades autonómicas en los tratamientos transfronterizos se limitarán a las relaciones y cooperación con las demás autoridades del resto de Estados miembros, puesto que las relaciones con el Comité se llevarán a cabo siempre a través de la Agencia[306].

[301] Art. 57 LO 3/18.

[302] Art. 58 LO 3/18.

[303] Art. 59 LO 3/18.

[304] Arts. 60 y 62 LO 3/18,

[305] Art. 61 LO 3/18.

[306] Arts. 60 y 62 LO 3/18,

Al momento de redacción del presente trabajo existen dos organismos de este nivel: La Autoridad Catalana de Protección de Datos (Autoritat Catalana de Protecció de Dades[307]) y la Agencia Vasca de Protección de Datos (Datuak Babesteko Euskal Bulegoa[308]).

4. Consideraciones finales

Por un lado, las peculiaridades que hemos ido mencionando a través de este trabajo con respecto al ciberespacio, o la dificultad para asociar una actividad relacionada con medios y recursos informáticos o digitales con una localización geográfica determinada, se manifiesta no sólo en el plano exterior de la Unión sino también en su interior, tal como se evidencia en este capítulo relativo a las autoridades de control. Aquí se evidencia una vez más el carácter transnacional del ciberespacio, en el cual es inevitable que una autoridad que en principio es estrictamente nacional, principalmente en cuanto a sus competencias, funciones y poderes, puede disponer la adopción de medidas que, aunque dirigidas a causar efecto en su ámbito territorial de competencia, estén dirigidas a entidades, actividades o elementos que se encuentren fuera de su territorio y cuya ejecutividad sea imposible de lograr sin la intervención de autoridades con capacidad de ejercer sus competencias en ámbitos territoriales diferentes.

Y, en segundo término, no es casualidad que las últimas normas aprobadas tanto a nivel europeo como a nivel interno contengan una regulación más completa y profunda sobre

[307] http://apdcat.gencat.cat/ca/inici

[308] http://www.avpd.euskadi.eus/s04-5213/es/

las autoridades de protección de datos, ya que la eficacia de dichas normas y de la protección de los derechos de las personas físicas depende en gran medida de estos órganos. Por otra parte, la actividad de todas estas autoridades y su actuación coordinada y conjunta permite alimentar la evolución del derecho de protección de datos, actualizarlo y adaptarlo a las nuevas necesidades que la realidad va marcando. A todo ello contribuyes las funciones técnicas, especializadas y ágiles de que están investidas, que les permite emitir documentos de gran valor interpretativo con una mayor agilidad que si esta actividad estuviera reservada a la labor legislativa. Por otra parte, la existencia de autoridades nacionales y europeas independientes y con competencias específicas en materia de protección de datos personales permite apreciar la enorme importancia que esta materia tiene para la Unión y para los Estados miembros.

Con respecto al órgano de la Unión Europea, el CEPD, el RGPD no ha hecho más que reconocer un estatus y un cúmulo de funciones y facultades que el Grupo de Trabajo del Art. 29 (al que, como hemos expresado anteriormente, la Directiva 95/46 no otorgaba ni siquiera un nombre) se había otorgado a sí mismo por medio de su prolífica actividad. Aparentemente el CEPD, como continuador del Grupo de Trabajo, mantiene la misma tónica tal como se puede observar de las seis directrices (y muchos otros documentos) publicadas en apenas un año de existencia.

Algo similar cabe mencionar de la regulación de las autoridades de protección de datos, muchas de cuyas funciones, facultades y poderes que ya estaban reconocidos en la legislación interna han sido elevados a la categoría de derecho europeo positivo por el RGPD.

Con respecto a las normas de competencia territorial de las autoridades de protección de datos, en primer lugar rechazamos el nombre de "ventanilla única" que se le ha otorgado[309], nombre que evidencia una perspectiva exclusivamente empresarial ya que, por un lado, desde el punto de vista de los interesados existen diversas autoridades a las que puede recurrir y, en lo que a las propias autoridades respecta, a pesar de que el legislador europeo se ha esforzado en sentar reglas claras (siendo aún muy pronto para evaluar si con éxito o no) no ha hecho más que enmarañar sus interacciones, fijando un cúmulo de mecanismos y relaciones, a veces evidentemente forzadas,[310] que será muy difícil de desentrañar para que las APD puedan ejercer sus funciones de manera correcta. Al respecto, consideramos que la complejidad de los tratamientos de datos personales y las múltiples actividades en que éstos pueden llegar a subdividirse, así como la cantidad de agentes (responsables, co-responsables, encargados y subencargados) que pueden participar en ellos, sumado al complicado entramado de algunas personas jurídicas (que hará muy dificultosa la determinación de su administración principal a los efectos del tratamiento), seguramente generarán conflictos que deberán ser resueltos con la intermediación del CEPD.

Ya hemos expresado que este mecanismo de "ventanilla única" se estableció para evitar carga administrativa a los responsables y encargados. Opinamos que al sentarse las reglas de competencias y el mecanismo de coherencia se debería haber tenido en cuenta, si no

[309] Al menos, el otorgado en castellano, pero creemos que vale igualmente para el original en inglés del cual es una traducción literal: "one stop shop".

[310] Nos referimos especialmente al sistema de "desdoblamiento" de las decisiones mixtas, en las que la parte de rechazo parcial de las pretensiones del responsable o encargado debe ser adoptada por la autoridad principal y la de rechazo parcial de las pretensiones del interesado, por la autoridad interesada. En caso de que la decisión sea más compleja e involucre a uno o más encargados o a más de un interesado, situados en distintos Estados miembros, la decisión será aún más compleja, lo que puede llevar a su injusticia y declaración de nulidad debido a ese desmembramiento que denunciamos.

en mayor medida al menos en situación de igualdad, a las autoridades públicas de protección de datos tanto como a las empresas privadas.

A pesar de ello, confiamos en que tanto las mencionadas autoridades como el CEPD, a medida que la práctica lo vaya requiriendo, sentarán normas ágiles y cristalinas de actuación para resolver las dificultades que surjan en la aplicación de las normas de competencia geográfica.

CAPÍTULO VI. TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

1. Introducción

No sólo los flujos transfronterizos de datos por el interior de la Unión son beneficiosos para la expansión y el comercio internacional, también lo son los flujos entre los estados miembros de la Unión y terceros países, que son necesarios asimismo para la cooperación y las relaciones internacionales, tal como lo expresa el considerando 101 del RGPD[311].

Sin embargo, los flujos internacionales de datos presentan un problema que hemos mencionado en otras partes de esta investigación. Partimos aquí de la premisa de que, al ser datos cuyo tratamiento se está realizando en el contexto de las actividades de un establecimiento en un Estado miembro, entra dentro del ámbito de aplicación del RGPD, que otorga a los datos una protección especial que pueden llegar a perder si son comunicados a un responsable o a un encargado que no tenga ningún establecimiento en la Unión y el tratamiento no se encuadra en las previsiones del art. 3.2. RGPD.

[311] Siguiendo la denominación que les da el Reglamento, en este trabajo llamaremos *flujos transfronterizos de datos* a las comunicaciones de datos entre distintos países miembros de la Unión; y *flujos internacionales de datos* a las comunicaciones o transferencias de datos desde un Estado miembro hacia un estado tercero o hacia una organización internacional.

Antes de continuar con este tema, haremos una pequeña aclaración: Siguiendo con el vocabulario propio del derecho basado en espacios territoriales, el RGPD denomina *transferencias*[312] a las operaciones de datos en las que intervienen ciertos elementos relacionados con el derecho de un estado tercero o de una organización internacional[313]; terminología que no es del todo precisa según lo explicamos a continuación.

El diccionario de la lengua de la Real Academia Española, en sus definiciones 1 y 3 del verbo *transferir* (únicas que consideramos pertinentes para el derecho de la Unión) le da el siguiente significado:

1. tr. Pasar o llevar algo desde un lugar a otro.

3. tr. Ceder a otra persona el derecho, dominio o atribución que se tiene sobre algo.

Es decir que el término *transferencia*, como sustantivo del verbo *transferir*, según la definición primera o en su sentido común, comunica la idea de movimiento; y en la definición tercera o en su aplicación al ámbito financiero, transmite la idea de que el objeto transferido deja de estar bajo la voluntad de quien *transfiere*. No obstante, en derecho de protección de datos personales este término no es del todo preciso pues éstos pueden ser *transferidos* o comunicados sin que haya movimiento (cuando se da acceso a una persona a un recurso donde se encuentran almacenados los datos sin que haya movimiento de éstos) o sin que la persona que los comunica pierda el poder sobre ellos,

[312] Es el caso del considerando 101, que se refiere a que "los datos personales se transfieren…" "…ni siquiera en las transferencias ulteriores de datos personales desde el tercer país…" "… las transferencias a terceros países y organizaciones internacionales sólo pueden llevarse a cabo... Una transferencia sólo podría tener lugar si…" Asimismo del Capítulo V, sobre "*Transferencias de datos personales a terceros países u organizaciones internacionales*".

[313] De aquí en más, en mérito a la simplificación y a la mejor comprensión, daremos por sobreentendido el derecho a que está sometido a una organización internacional cuando nos refiramos a la transferencia de datos personales a un país tercero.

cuando se transfiere una copia ya que los datos en formato digital se pueden reproducir ilimitadamente. Estos dos casos entran dentro del significado de *transferencia de datos personales* pero no de *transferencia* en su sentido común.

En los casos que hemos puesto como ejemplo, los datos no abandonan el territorio de la Unión ni dejan de estar sometidos al derecho del estado miembro sino que se permite el acceso y tratamiento por parte de (o se comparten con) personas no relacionadas con las actividades de un establecimiento ubicado en la Unión[314], a quienes puede serle aplicable el derecho de un país que no ofrezca un nivel de protección equivalente al de la Unión Europea.

Con frecuencia se presenta asimismo el caso contrario: Que los datos personales realmente se *transfieran* según el significado común de este término pero no exista una transferencia internacional de datos personales en el sentido del derecho europeo, sino que éstos continúen sometidos a un tratamiento que se realice en el contexto de las actividades de un establecimiento situado en la Unión. Entre muchos otros ejemplos, es lo que ocurre cuando un responsable titular de uno o más establecimientos en la Unión contrata un encargado que no tenga establecimientos en la Unión. Es asimismo lo que, interpretado *a sensu contrario*, ha decidido el TJUE en la sentencia Google Spain, pues considera acreditado que tanto Google Search (www.google.com) como su versión española (www.google.es) están gestionados por Google Inc., empresa establecida en Estados Unidos, desde servidores cuyo Estado de ubicación se desconoce por razones

[314] Existe un reconocimiento de esta problemática conceptual en el Anexo II *Principios del Marco del Escudo de la Privacidad UE-EE. UU publicados por el Departamento de Comercio Estadounidense,* de la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. En el Capítulo III, apartado 9 establece la pertinencia de los Principios cuando se transfieran registros que estén identificados o sean identificables, *"o se acceda a ellos"* (SIC).

competitivas[315]; a pesar de lo cual los tratamientos de datos personales realizados por los mencionados motores de búsqueda no son considerados transferencias de datos personales sino tratamientos realizados en el contexto de las actividades de Google Spain, que es un establecimiento en territorio europeo de Google Inc.[316]

Por esos motivos consideramos que término *transferencias*, en el sentido técnico que se le otorga en su aplicación a la protección de datos personales, adquiere un significado distinto cuyo contenido no están del todo determinados sino que tiene esa característica de ser lo suficientemente abierto para incorporar el alcance que le otorgue la jurisprudencia y la interpretación de las APD.

Debido a esa necesidad de mantener la protección y evitar el fraude a la ley a la que nos hemos referido en los párrafos anteriores, el RGPD dedica el Capítulo V a las transferencias de datos personales a terceros países o a organizaciones internacionales, estableciendo en el artículo 44 que los datos personales sólo podrán ser sometidos al derecho de un país tercero si al responsable o encargado les son aplicables las condiciones establecidas en este Capítulo del RGPD, que en resumen garantiza a las personas físicas que el nivel de protección al que los datos estarán sometidos será equivalente al del RGPD.

En relación con el último punto citado, algunas disposiciones del RGPD que están dedicadas a las (mal llamadas) transferencias internacionales de datos personales, veremos que no son normas de reenvío sino que establecen otro tipo de relaciones entre ordenamientos jurídicos independientes: Estas normas no eligen otro ordenamiento del

[315] STJUE Google Spain, apartado 43.

[316] STJUE Google Spain, apartado 57.

que extraer la solución del caso; tampoco deciden que los tratamientos relacionados con otro ordenamiento o los datos que se conecten con el territorio de un estado tercero continúen rigiéndose por el derecho de la Unión. Lo que hace es "aprobar" el derecho sobre protección de datos de un estado tercero como requisito previo para permitir la transferencia de los datos. En el esquema de Bobbio[317], se trataría de una relación de coordinación entre ordenamientos jurídicos distintos; en los cuales el derecho de la Unión actúa en un plano de superioridad dado que se arroga la prerrogativa de examinar, evaluar y en su caso aprobar el nivel de protección que otro ordenamiento otorga a los datos personales.

En lo que consiste una originalidad del derecho europeo, en estos casos no se trata de que las normas sobre protección de datos personales que forman parte de éste extiendan su vigencia más allá del territorio de la Unión, sino de que las autoridades de la Unión verifiquen que a los datos que han estado bajo la protección del derecho europeo y luego penetran el ámbito de vigencia de otro ordenamiento, continúen sometidas a un nivel de protección similar al de la Unión, estableciendo para ello distintos mecanismos. En otros términos, los datos no pueden colocarse bajo la vigencia de otro ordenamiento sin que las autoridades de la Unión hayan estudiado la protección otorgada y hayan *aprobado* su nivel de protección o hayan evaluado y aprobado el derecho al que estarán sometidos los datos, ya sea el derecho general o sectorial del Estado de recepción, las normas particulares a que están sometidas las partes (previsiones contractuales o similares), el *soft law* (códigos de conducta, certificaciones o normas corporativas vinculates) o las

[317] Ver página 11 de este trabajo.

particulares obligaciones que asumen las partes respecto a la transferencia o transferencias que llevarán a cabo.

Hemos visto que la protección de datos personales es hoy en día un derecho fundamental en el ordenamiento de la Unión y de los Estados miembros al que se le da una alta protección; sin embargo, ello no es así en el resto de países terceros.

Consecuentemente con lo expresado en los párrafos precedentes, la finalidad de este capítulo no es la protección de los datos personales ante el abandono del territorio de la Unión porque los datos pueden no haber estado nunca en este territorio, sino del abandono del campo de aplicación del Reglamento o, lo que puede considerarse equivalente, el abandono del marco de las actividades de un establecimiento en la Unión, para incorporarse al marco de las actividades, ya sea de una entidad establecida en el territorio de un país tercero y sin ningún establecimiento en la Unión, o de una organización internacional. Al respecto el Tribunal de Justicia ha declarado, en la sentencia "*Schrems*"[318], que en virtud del mandato que contiene la Carta de Derechos Fundamentales de la Unión en su artículo 8 apartado 1, es obligatorio asegurar la continuidad del elevado nivel de protección que otorga la Unión, en caso de transferencia de datos personales a un tercer país. Continúa manifestando en el apartado siguiente de la sentencia, que si no fuera así sería fácil eludir el elevado nivel de protección con transferencias de datos personales hacia terceros países.

En los artículos siguientes, el Reglamento prevé distintos mecanismos para garantizar que los datos no pierdan su especial protección, que hemos adelantado someramente y analizaremos a continuación.

[318] Sent. Schrems, apartado 72.

2. Decisión de adecuación adoptada por la Comisión

El artículo 45, complementado por los considerandos 103 y 104 del RGPD, faculta a la Comisión para decidir que un determinado país tercero, un territorio, un sector específico de un país tercero o una organización internacional garantizan un nivel de protección de los datos personales adecuado al de la Unión. Dicha decisión se debe adoptar luego de realizar una evaluación de distintos aspectos relacionados con el derecho vigente en el país, territorio, sector o sectores, a través de la cual la Comisión puede analizar, además de las normas, organización administrativa y recursos procesales específicos sobre protección de datos personales, factores tales como el respeto al Estado de derecho, la situación de protección de los derechos humanos, la legislación y organización administrativa y jurisdiccional en distintas materias como la penal, de seguridad pública, defensa y seguridad nacional, el acceso de las autoridades públicas a los datos personales, el acceso a la justicia y compromisos internacionales, para finalmente decidir si ese país, territorio o sector ofrece un nivel de protección de datos adecuado según los estándares de la Unión Europea, en cuyo caso se podrán comunicar datos personales hacia ese país, territorio, sector u organización internacional, sin necesidad de cumplir ningún otro requisito.

Para interpretar qué se debe entender por *nivel adecuado* de protección, podemos basarnos en la sentencia Schrems en la cual el Tribunal de Justicia aclara que *adecuado* no quiere decir un nivel de protección *idéntico* al de la Unión, sino uno *equivalente* según

los estándares de la Carta, que esté efectivamente garantizado por su legislación interna o sus compromisos internacionales[319].

El mecanismo de adopción de decisiones de adecuación, si bien no consiste en la aplicación extraterritorial del Reglamento consiste en un método por medio del cual se fiscalizan distintos aspectos del ordenamiento jurídico de un país u organización internacional, con el objetivo de otorgar una ventaja al Estado cuyo nivel de protección se declara adecuado o se aprueba: La de permitir la libre circulación de datos con la Unión Europea. Por el contrario, los Estados cuyo nivel de protección de los datos personales no es considerado adecuado por parte de la Comisión, tendrán la desventaja de que con ellos la circulación de datos personales no será libre sino condicionada: para realizar transferencias se deberá, en cada caso concreto, contar con garantías adicionales.

Entre los aspectos a evaluar por la Comisión para tomar la Decisión se incluyen materias tales como la seguridad pública y nacional y el acceso de las autoridades a los datos personales, advirtiéndose aquí la influencia de la Sentencia Schrems, en la cual el alto órgano judicial declaró la nulidad del Acuerdo Safe Harbour, entre la Unión Europea y los Estados Unidos, entre otras razones debido a la legislación norteamericana sobre seguridad y defensa, que permite a las fuerzas y cuerpos nacionales el acceso indiscriminado y masivo a las comunicaciones y datos personales de los individuos con fines de investigación. La fiscalización puede ser realizada por la Comisión o por el Tribunal de Justicia, que lo hace de forma indirecta al ejercer el control de validez sobre los actos de la Comisión, como sucedió en el fallo Schrems, en el cual constató la falta de adecuación del nivel de protección otorgado por el derecho de los Estados Unidos y

[319] Sent. Schrems, apartado 73.

que, por consiguiente, los principios de "*Puerto Seguro*" no eran suficientes para otorgar una protección adecuada, por lo que declaró la nulidad de la Decisión 2000/520 de la Comisión[320].

Cabe resaltar la exigencia que fija el considerando 104 para la Comisión, de asegurarse que en el tercer país se realice un control verdaderamente independiente de la protección de datos, así como que se reconozcan a los interesados la efectividad de los recursos administrativos y judiciales, antes de emitir la decisión de adecuación.

Al adoptarse la decisión mencionada en el párrafo anterior, las transferencias de datos personales hacia el tercer país u organización internacional se pueden realizar sin la exigencia de ningún otro requisito adicional.

Ahora bien, una vez adoptada la decisión por parte de la Comisión, ésta debe realizar una labor periódica de seguimiento de los parámetros analizados para su adopción, al menos cada cuatro años, a efectos de revocar, modificar o suspender la decisión en caso de que éstos hayan variado de tal manera que el nivel de protección de los datos personales del país, territorio, sector u organización de que se trate haya dejado de ser adecuado en comparación con el nivel de la Unión[321].

En caso de revocación de la decisión, así como en todos los casos en que la Comisión no haya adoptado ninguna decisión, el responsable o el encargado pueden sustituir la falta de protección del ordenamiento jurídico del país de destino por unas garantías adecuadas que protejan los datos que son objeto de una o una serie de transferencias, siempre que los interesados cuenten con derechos exigibles y acciones legales efectivas.

[320] Que examinamos más adelante en este capítulo.

[321] Apartado 5, artículo 45 RGPD.

Según lo autorizan el artículo 46 y el considerando 108, las garantías adecuadas pueden consistir en cláusulas de protección de datos, adoptadas por la Comisión o por las autoridades nacionales de control y aprobadas con la Comisión; normas corporativas vinculantes; un código de conducta o un mecanismo de certificación, en estos últimos dos casos unidos al compromiso de aplicar garantías adecuadas, adoptados por el responsable y el encargado, que sean para ellos vinculantes y exigibles en el tercer país. Pero además de estos mecanismos, los interesados deben contar con un conjunto de derechos efectivos y exigibles y de acciones legales, incluyendo entre ellos el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, ya sea en la Unión o en un tercer país. El nivel de protección de los datos personales otorgado por estas garantías debe ser similar al de la Unión Europea, lo que en palabras del considerando 108 implica que deben contener principios similares a los del Reglamento.

Las normas corporativas vinculantes son códigos de conducta que puede adoptar todo grupo empresarial o unión de empresas que pretenda realizar transferencias de datos personales a otras empresas del grupo o unión, que para ser válidas a estos efectos deben estar aprobadas por la autoridad de supervisión competente al efecto.

Fuera de los casos contemplados en los párrafos anteriores, también se podrán efectuar transferencias legítimas de datos personales hacia países terceros cuando medie consentimiento explícito del o los interesados, cuando la transferencia se realice en el marco de un contrato o una reclamación y cuando lo requieran razones de interés público.

3. Garantías consideradas adecuadas.

El artículo 46.2 del RGPD enumera distintos tipos de garantías a las que el responsable o el encargado pueden acudir para realizar transferencias internacionales de datos personales a países terceros que no estén cubiertos por ninguna decisión de la Comisión.

En relación con responsables y encargados pertenecientes a entidades privadas, dichas garantías pueden consistir en:

- Normas corporativas vinculantes
- Cláusulas tipo de protección de datos personales adoptadas por la Comisión o por una autoridad de control y aprobadas por la Comisión
- La adhesión a un código de conducta o a un mecanismo de certificación, siempre que estén acompañados por compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país, de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3.1. Normas corporativas vinculantes.

Las normas corporativas vinculantes[322] son las políticas de protección de datos personales adoptadas por escrito por un grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, a los efectos de realizar transferencias internacionales de datos en calidad de responsable o encargado, desde un establecimiento en un estado miembro a otro establecimiento del mismo grupo o unión en un país tercero[323]. Consisten en un conjunto de normas escritas aprobadas por el órgano competente para adoptar decisiones de un grupo empresarial o unión de empresas que, en tal carácter, vinculan a

[322] En adelante "BCR" por sus siglas en inglés: *binding corporate rules*.

[323] Art. 4 apartado 20 RGPD.

todos los miembros de dicho grupo así como a todo el personal, especialmente el que realice los tratamientos de datos personales o que tenga acceso a ellos.

Para tener eficacia a los efectos de las transferencias internacionales de datos personales, deben estar aprobadas por la autoridad de control competente (que deberá ser la autoridad de control principal para el grupo empresarial o unión de empresas) de conformidad con el mecanismo de coherencia del art. 63 del RGPD.

De conformidad con el artículo 47 del RGPD, para poder ser aprobadas, las normas corporativas vinculantes deben contar con los siguientes requisitos:

- Ser jurídicamente vinculantes y aplicarse y ser cumplidas por todos los miembros del grupo o unión de empresas, incluidos sus empleados (art. 47.1.a);
- Deben conferir expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales (art. 47.1.b);
- Contener, como mínimo, los elementos enumerados en el art. 47.2, de entre los cuales destacamos los siguientes:
    - Principios de protección de datos vigentes en el sistema europeo, en particular los de limitación de la finalidad, de minimización de datos, de limitación del plazo de conservación, de calidad, de protección de datos desde el diseño y por defecto, de legalidad del tratamiento, de protección especial a ciertas categorías de datos sensibles, de obligatoriedad de medidas de seguridad de los datos (art. 47.2.d);
    - La información detallada con respecto a las transferencias que estarán cubiertas por las BCR (art. 47.2.b);

- Aceptación, por parte del responsable o del encargado del tratamiento que estén establecidos en el territorio de un Estado miembro, de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de otro miembro del grupo o unión de empresas que no esté establecido en la Unión y, en relación con ello, los derechos del interesado a presentar una reclamación ante una autoridad de control y ante tribunales de los Estados miembros y a obtener, si procede, dos tipos de indemnizaciones: una por violación del derecho a la protección de datos personales y otra por violación de las normas corporativas vinculantes (art. 47.2.e). Podrá exonerarse total o parcialmente el responsable o encargado si se demuestra que el incumplimiento no es imputable a los miembros por los que se ha hecho responsable (art. 47.2.f);
- Los derechos de los interesados en relación con el tratamiento y medios para ejercerlos (en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado) y los procedimientos de reclamación internos (art. 47.2.i);
- El medio por el cual se facilitará a los interesados la información de los artículos 13 y 14 del Reglamento, a la que se sumará la información sobre las normas corporativas vinculantes del grupo empresarial o de la Unión de empresas (art. 47.2.g);
- Los mecanismos establecidos dentro del grupo empresarial o unión de empresas para garantizar la verificación del cumplimiento de las normas corporativas vinculantes, para comunicar y registrar sus modificaciones y

para cooperar con la autoridad de control respecto a este y otros asuntos (Art. 47.2.j)

De estos requisitos consideramos que tiene gran relevancia el relativo a la responsabilidad del responsable o encargado establecido en el territorio de la Unión, ya que con ello se logra conceder cierto poder de control sobre sus datos personales a los interesados, aunque es posible que ese poder se reduzca a la compensación económica consiguiente a la vulneración del derecho a la protección de los datos personales, es decir que no será suficiente para evitar dicha vulneración. Por otra parte, al habilitar la competencia de la autoridad principal mediante este mecanismo, el RGPD en cierto sentido extiende la competencia territorial de las autoridades de control y de los tribunales de los Estados miembros por medio del establecimiento de una base jurídica para que puedan intervenir en la resolución de casos relacionados con el derecho y la jurisdicción de un país tercero. La competencia de la autoridad principal y la jurisdicción de los tribunales del Estado miembro de designación se fundamentan en la asunción de responsabilidad por parte del responsable o del encargado.

Por otra parte, el art. 48 del RGPD dispone que las transferencias que no estén amparadas por este capítulo y que sean requeridas por una sentencia de un órgano jurisdiccional o una decisión de una autoridad administrativa de un país tercero sólo serán reconocibles o ejecutables si existe un tratado internacional (como puede serlo un tratado de asistencia jurídica mutua) entre ese país y la Unión o un Estado miembro.

El G29, interpretando el artículo 26 (2) de la Directiva 95/46, relativo a transferencias internacionales, ha elaborado el Documento de Trabajo: "*Transferencias de datos personales a países terceros: Aplicación del Artículo 26 (2) de la Directiva de Protección*

de Datos de la Unión Europea a las normas corporativas vinculantes para transferencias internacionales de datos"[324], en el cual confecciona algunas pautas para que sirvan de guía a los grupos de empresas multinacionales para elaborar normas corporativas vinculantes.

El mencionado Documento reconoce que las normas corporativas vinculantes no tienen la misma validez en todos los Estados miembros ya que en el ordenamiento jurídico de algunos de ellos no está claro si las declaraciones unilaterales confieren a los terceros derechos judicialmente exigibles, casos en los cuales se necesitarán adaptaciones contractuales para asegurarse la exigibilidad de los derechos[325]. Pensamos que, con la regulación en el RGPD de estas normas se ha superado este escollo, principalmente debido a su calidad de derecho directamente aplicable en todos los Estados miembros.

Algunos aspectos de las pautas contenidas en dicho Documento se han vaciado de contenido con la aprobación del RGPD, de los restantes podemos destacar:

- Las normas deben ser aplicadas en general por los distintos miembros del grupo, independientemente de su lugar de establecimiento, de la nacionalidad de los sujetos o de cualquier otro criterio similar.
- Cada grupo, al elaborar un cuerpo de BCR, debe hacerlo teniendo especialmente en cuenta cómo está constituido, ya que existen diferentes categorías de grupos corporativos que pueden ser de muy distinta naturaleza.

---

[324] Título original en inglés Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. 11639/02/EN (WP 74) (en Adelante, "Documento de trabajo sobre BCR"), adoptado el 03/06/2003. Disponible en inglés en la dirección: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf (último acceso el 03/08/2018).

[325] Apartado 3.3.2 del documento de trabajo sobre BCR.

- Estas Normas sólo cubrirían las transferencias de datos efectuadas entre los miembros del grupo corporativo. Las transferencias de datos personales hacia destinatarios no miembros del grupo que estén establecidos fuera del territorio del EEE deberían estar garantizadas por las cláusulas tipo aprobadas por la Comisión o por cualquier otro mecanismo de garantía.
- El carácter vinculante de estas normas tiene dos aspectos: El interno y el externo. El interno consiste en la fuerza vinculante en la práctica (es decir, que las normas sean realmente aceptadas como vinculantes por los trabajadores de la empresa) y el externo, en la vinculación jurídica de las normas para las empresas del grupo (su valor obligacional). Ambas deben ser efectivas para que la adopción de las BCR pueda ser considerada garantía suficiente por las autoridades nacionales a los efectos de las autorizaciones de transferencias.
- Los sujetos que comuniquen sus datos personales a los miembros del grupo deben poder ser considerados terceros beneficiarios ya sea por la fuerza obligatoria de la declaración unilateral (en los Estados donde ello sea jurídicamente posible) o mediante la adopción de estipulaciones contractuales entre los miembros del grupo para hacerlo posible. Esta consideración de tercero beneficiario debe permitirles plantear reclamaciones, tanto ante las autoridades administrativas como ante las autoridades judiciales. Asimismo, el miembro del grupo responsable de la transferencia debe ofrecer garantías de la asunción de su responsabilidad así como de las compensaciones o indemnizaciones que corresponderán al interesado por cualquier incumplimiento de las BCR.
- Como lo expresa el apartado 5.4 del Documento, uno de los elementos más importantes para valorar la efectividad de un sistema de autorregulación es el nivel

de apoyo y colaboración puesto a disposición de los interesados. En este sentido, las BCR deben expresar claramente el deber de colaboración de las empresas del grupo con las autoridades nacionales, de tal modo que los particulares puedan beneficiarse de este doble apoyo institucional.

Las BCR forman parte del *soft law* y, como tal, un elemento que puede ser muy valioso en disciplinas tales como el derecho de protección de datos personales, especialmente en los casos en que uno de los agentes (el responsable o encargado) es una compañía multinacional cuyo ámbito territorial de actuación supera no sólo el de las autoridades nacionales sino también el de la propia Unión Europea, motivo por el cual resultaría muy sencillo eludir normas imperativas por el simple método de delegar la realización de ciertas actividades en alguno de los miembros del grupo que no esté ubicado en el ámbito de aplicación de un determinado ordenamiento jurídico, situación posibilitada por las comunicaciones y los medios tecnológicos. De la propia naturaleza de multinacional de las empresas o grupos de empresas surge también una de las características de este tipo de regulaciones, que deben adaptarse a más de un ordenamiento jurídico, por lo que en caso de involucrar el de un país tercero deberán adaptarse a su normativa además del RGPD. Pero ni la multinacionalidad de estas empresas ni la posibilidad de dictar su autorregulación implican que están por encima de las normas jurídicas tradicionales ni que queden fuera del control o supervisión de los órganos destinados para ello. Por ello en estos casos compete a las autoridades estudiadas en el capítulo anterior la aprobación de las BCR y disponer los mecanismos necesarios para el control de su aplicación, que deberá adaptarse a la naturaleza y características de la empresa o grupo de empresas.

3.2. Cláusulas contractuales tipo.

Para que un responsable o encargado puedan exportar legítimamente datos personales desde la Unión hacia un país tercero respecto del cual no exista decisión de adecuación de la Comisión, podrán suscribir cláusulas contractuales tipo o normalizadas, que deberán ser aprobadas previamente por la Comisión[326].

En uso de las facultades conferidas por el art. 26 apartado 4) de la Directiva 95/46, la Comisión ha dictado con anterioridad a la entrada en vigor del RGPD cuatro decisiones a efectos de adoptar un conjunto de cláusulas contractuales tipo que garantizan un nivel adecuado de protección en las transferencias internacionales de datos personales, en los casos en que el país del destinatario de la transferencia no lo ofrezca. Estas decisiones, que exponemos a continuación, continuarán siendo válidas hasta que sean revocadas, anuladas o modificadas por una decisión posterior de la Comisión o por sentencia del Tribunal de Justicia de la Unión pero deben adaptarse en su aplicación al nuevo derecho europeo.

a) *Transferencias internacionales efectuadas por un* responsable *desde un Estado miembro, hacia un* responsable *establecido en un país tercero.*

Dos de esas decisiones tienen por objeto la protección de los interesados en los casos de transferencias efectuadas por el responsable del tratamiento, desde un Estado miembro, hacia un responsable establecido en un país tercero: La decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE (en adelante "Decisión 2001/497") y la Decisión 2004/915/CE de 27 de diciembre de 2004 por la que se modifica

[326] Arts. 46.2.c y 46.2.d RGPD

la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países (en adelante, "Decisión 2004/915").

En la primera de dichas decisiones, adoptada teniendo en cuenta los dictámenes del G29[327], la Comisión expresa con meridiana claridad que las cláusulas adoptadas mediante la decisión lo son al solo efecto de que los remitentes y receptores de datos cuenten con una herramienta para lograr que los Estados miembros autoricen sus transferencias de datos y no afectan a las restantes cláusulas contractuales pactadas con motivo de las transferencias[328].

Las cláusulas contractuales tipo no reemplazan el derecho nacional del remitente que se haya adoptado para transponer la Directiva 95/46, el que por el contrario es plenamente aplicable a la transferencia[329]. Por lo tanto la adopción de las cláusulas por sí sola no subsana otro tipo de vicios que impidan que la transferencia sea autorizada (arts. 2 y 4 de la Decisión).

A nuestro juicio es importante destacar que la decisión, en su artículo 4 habilita a los Estados miembros a no autorizar una transferencia o una serie de ellas, si la legislación a la que está sujeto el importador contiene normas de derecho público que impongan comunicación de determinados datos a las autoridades y que ello atente contra el derecho

[327] Considerando 10 de la Decisión 2001/497.

[328] Considerando 6 de la Decisión 2004/915.

[329] Así lo aceptan las partes firmantes de las Cláusulas en la Cláusula 4 a) de la Decisión 2001/497/CE y la Cláusula I a) del Conjunto II aprobado por la Decisión 2004/915/CE. En las transferencias de un responsable establecido en un Estado miembro a otro responsable establecido en un país tercero, el derecho del primero de ellos, o parte remitente, es aplicable a todos los tratamientos previos y a la transferencia en sí, en su calidad de tratamiento. Si bien las Cláusulas no lo especifican y ello dependerá de las legislaciones que resulten aplicables, consideramos que la transferencia se completa y por lo tanto, el derecho del remitente deja de ser aplicable, en el momento en que el receptor toma conocimiento de que los datos están a su disposición.

a la intimidad del interesado o que vayan más allá de las restricciones necesarias en una sociedad democrática. En este mismo orden de ideas, el considerando 3 de la Decisión bajo estudio reafirma la facultad con que cuentan las autoridades de aplicación de los estados miembros, de adoptar una decisión en cada caso particular, teniendo en cuenta todas las circunstancias relacionadas con la transferencia.

Los estados miembros podrán no autorizar las transferencias que se realicen mediante la adopción de las cláusulas tipo aprobadas por la Decisión, si tienen fundados motivos para considerar que las cláusulas no están siendo respetadas o no lo serán en el futuro. La adopción de este tipo de decisiones será informada a la Comisión, quien a su vez lo informará a los restantes Estados miembros.

La segunda Decisión mencionada (Decisión 2001/497/CE), adoptada por la Comisión tomando en consideración tanto el dictamen del Grupo de Trabajo del Artículo 29[330] como un grupo de cláusulas contractuales tipo propuestas por las asociaciones empresariales[331], amplía el catálogo de cláusulas aprobadas por su antecesora mediante la aprobación de otro conjunto de cláusulas contractuales tipo, para dar a los agentes intervinientes en las transferencias la opción de suscribir cualquiera de ellos, pero se prohíbe que las cláusulas adoptadas se modifiquen o que se combinen elementos de ambos conjuntos de cláusulas. Esta segunda decisión denomina Conjunto I el clausulado aprobado por la decisión

[330] Dictamen 8/2003 del Grupo de Trabajo del Art. 29.

[331] Sancho Villa, D: *Transferencia internacional de datos personales*. Agencia de protección de datos, Madrid, 2003. Según esta autora, las características principales del modelo de la decisión de 2004 son "*la supresión del principio de responsabilidad solidaria de los empresarios, un mayor desarrollo de lo que son las obligaciones entre los empresarios que busca el reequilibrio de las posiciones de éstos, y un matiz de laxitud en la formulación de los derechos de garantía que el importador se compromete a cumplir con los afectados"* (pág. 136).

anterior y Conjunto II el aprobado por ésta, como denominaremos en adelante a ambos conjuntos de cláusulas.

Igualmente, se amplían los casos en que las autoridades de protección de datos del país remitente están habilitadas para impedir o suspender las transferencias.

Los dos conjuntos de cláusulas tipo aprobadas por la Decisión 2001/497/CE, en general, establecen las obligaciones y responsabilidades del exportador y del importador, entre las cuales se encuentran el respeto a los principios de protección de datos personales según el derecho comunitario o el de transposición de éste en el país de establecimiento del exportador y, especialmente para el importador, las garantías de seguridad técnica y organizativa en la transferencia. También especifican la responsabilidad de cada parte en los tratamientos, tanto frente a la otra parte como frente a terceros, y garantizan el acceso de los interesados al ejercicio de sus derechos.

Entre las obligaciones de las partes, es de destacar además de la de respeto a los principios, la de colaboración con las autoridades de control de datos y con los interesados en orden a permitir o facilitar el ejercicio de sus derechos y la solución de controversias en que estén involucradas en relación con la protección de datos[332].

b) Transferencias internacionales realizadas por un responsable *desde un Estado miembro, a un* encargado *establecido en un país tercero.*

La Decisión 2002/16/CE, de 27 de diciembre de 2001 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del

[332] Para la resolución de los conflictos, mediante las Cláusulas las partes aceptan el sometimiento a procedimientos de mediación o arbitraje, a elección de los interesados o de la autoridad, además del método jurisdiccional de solución de controversias (Cláusula 7 del Conjunto I y Cláusula V del Conjunto II).

tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE; y la Decisión 2010/87/UE de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, tienen por objeto la protección del interesado en los casos en que el receptor de la transferencia es un encargado establecido en un país tercero cuyo ordenamiento jurídico no ofrece garantías suficientes de protección de los datos personales.

A diferencia de las decisiones analizadas en el parágrafo anterior, en que la última decisión adoptada complementa a la anterior, la Decisión 2010/87/UE deroga a la Decisión 2002/15/CE[333]. Por este motivo restringiremos nuestro análisis a las disposiciones de esta última[334].

En primer término cabe mencionar que de acuerdo a la finalidad para la que fue concebida, esta Decisión hace hincapié en las medidas de seguridad técnicas y organizativas que deben aplicar los importadores, encargados del tratamiento establecidos en un país tercero, teniendo en cuenta especialmente que se tratará de países que ofrezcan un nivel de protección de los datos personales que no ha sido declarado adecuado por la Comisión.

[333] Una de las principales deficiencias de la Decisión derogada es que no preveía la intervención de sucesivos subencargados de los tratamientos, figura que desde hace algunos años aparece con mucha frecuencia en los negocios internacionales de tratamiento de datos. Ver Dictamen 3/2009 del Grupo de Trabajo del Artículo 29, sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (WP 161), emitido el 5 de marzo de 2009

[334] El art. 7 de esta Decisión, que deroga la Decisión anterior, asegura la vigencia de los contratos suscritos bajo las disposiciones de ésta, mientras permanezcan sin cambios las transferencias y operaciones de tratamiento de datos que conforman su objeto ni las circunstancias de las transferencias de datos personales. En el momento en que las partes decidan modificar alguno de estos aspectos, o subcontratar operaciones de tratamiento de datos, deberán suscribir un nuevo contrato que cumpla las cláusulas tipo aprobadas por la Decisión 2010/87/UE.

Debemos recordar que, según las disposiciones de la Directiva 95/46 el responsable del tratamiento asume la responsabilidad de garantizar el respeto a todos los principios de protección de datos establecidos en la misma pero, en el caso del principio de seguridad en el tratamiento, la responsabilidad es compartida con el encargado. Esta regla no pierde vigencia cuando el encargado está establecido en un país tercero, tal como emana del contenido de la Cláusula 6 2., que establece que el responsable principal de todo daño que puedan sufrir los interesados será el exportador, a quien tendrán el derecho de exigir una indemnización[335], independientemente de cuál haya sido la parte incumplidora, incluso si lo han sido los subencargados de los tratamientos.

Una de las características de este tipo de cláusulas es que, al igual que las anteriores, otorgan derechos a los interesados (terceros en la relación contractual entre exportador, importador y subencargado del tratamiento de datos), que podrán ser exigidos por éstos y de forma directa al exportador, al importador o al subencargado según corresponda (Cláusula 3ª). Entre las obligaciones de las partes figura la de poner a disposición de los interesados una copia de las cláusulas (Cláusulas 4 h) y 5 g). Asimismo, el exportador asume la obligación de depositar una copia de las Cláusulas ante la autoridad de control cuando ésta así lo requiera o cuando el depósito venga exigido por la legislación de protección de datos aplicable (Cláusula 6.1.). Todo ello a efectos de permitir a los interesados el ejercicio de sus derechos.

[335] Cuando el autor del incumplimiento de alguna de sus obligaciones haya sido el importador de datos o su subencargado, los interesados podrán dirigirse contra el importador, especialmente en los casos en que sea imposible lograr una indemnización del exportador, ya sea porque haya desaparecido de iure o de facto, o en caso de insolvencia. En estos casos, también podrán dirigirse contra la entidad que haya asumido las obligaciones del exportador, si la hay.

Si la parte incumplidora es el subencargado y los interesados no puedan exigir la indemnización a ninguna de las otras partes por los motivos expresados en el párrafo anterior, el subencargado acepta que se dirijan contra él las reclamaciones

Estas Cláusulas incluyen también una ampliación de la competencia territorial de las APD al permitir realizar auditorías al importador a efectos de analizar el nivel de protección de datos personales que puede brindar a los interesados[336] y, en caso de considerarlo inadecuado, prohibir o suspender la transferencia o serie de transferencias.

En cuanto al importador de datos, de las obligaciones a su cargo destacamos principalmente la de adoptar todas las medidas de seguridad técnicas y organizativas que se indican en el apéndice 2 de las Cláusulas y la de efectuar el tratamiento de los datos personales exclusivamente en nombre del exportador y de conformidad con sus instrucciones y lo pactado en las cláusulas. También deberá notificar inmediatamente al exportador de cualquier incidencia que surja en el tratamiento de datos y que pueda poner en peligro la confidencialidad de los mismos (Cláusula 5). Por medio de la Cláusula 11 se obliga asimismo a subcontratar el tratamiento sólo con la autorización escrita previa del exportador y mediante un contrato por escrito de contenido obligacional para el subencargado similar al establecido en las Cláusulas.

La Cláusula 9 impone a las partes la elección, como derecho aplicable a la protección de los datos personales a tratar, de la legislación del Estado miembro del establecimiento del exportador.

Finalmente, las partes son libres de pactar las cláusulas que regulen las responsabilidades que corresponderán a cada una de ellas en sus relaciones internas.

En nuestra opinión las cláusulas contractuales tipo aparentan ser los instrumentos más débiles para que los datos personales que abandonen el ordenamiento jurídico europeo

[336] En virtud de lo pactado en la Cláusula 8, las autoridades de control del Estado miembro de establecimiento del exportador no sólo tendrán facultades para efectuar auditorías a las entidades importadoras sino también a cualquier entidad subcontratada por éstas.

mantengan un nivel de protección equivalente al brindado por éste debido, principalmente, a que no son fuentes de *soft law* sino estipulaciones entre partes contratantes y por lo tanto carecen de las medidas de control de su aplicación que están presentes en los códigos y las BCR.

No obstante esa carencia se ven parcialmente compensada en la medida en que esas cláusulas resulten efectivas al responsabilizar a una entidad establecida en la Unión por las vulneraciones a la protección de datos personales que se puedan cometer bajo la vigencia del orden jurídico del país tercero, se convierten en un instrumento que, a pesar de su debilidad para prevenir o evitar tratamientos ilegítimos bajo la vigencia de ordenamientos jurídicos terceros, al menos tienen la capacidad necesaria para que el interesado sea reparado al igual que la tienen (a nuestro juicio parcialmente ya que lo hacen sólo en determinadas circunstancias y sólo con respecto a sujetos privados) para extender las competencias territoriales de las APD, y así permitirles seguir protegiendo los datos en el país tercero de destino de la transferencia.

3.3. Códigos de conducta.

De los considerandos 98 y 99 se puede inferir que Códigos de Conducta son los conjuntos de normas de conducta o deontológicas adoptados por las asociaciones u otro tipo de organismos que aglutinen a categorías de responsables o encargados, previa consulta a sus miembros y aprobados posteriormente por la autoridad de protección de datos competente.

Estos códigos no están pensados específicamente para las transferencias internacionales de datos personales sino para facilitar y guiar a los responsables y encargados miembros

de la asociación u organismo de que se trate, en la aplicación de la totalidad del RGPD[337], ya que está formados por reglas de conducta por medio de las cuales, al aceptarlas los miembros del colectivo de que se trate, adoptan las conductas, responsabilidades y obligaciones impuestas por el RGPD. A ellos podrán adherirse incluso aquéllos a los que no se aplique el RGPD en virtud del art. 3[338]. La efectiva aplicación y respeto de estos Códigos por parte de sus miembros debe ser supervisada por un organismo especializado, fiscalizado y acreditado por la APD competente[339].

El art. 46 RGPD no añade más detalles a la regulación de estos Códigos; del apartado e) de dicho artículo sólo se puede inferir que los mismos podrán contener garantías adecuadas para asegurar la protección de los datos personales en las transferencias internacionales realizadas por los responsables o encargados que sean miembros de las asociaciones u organismos que hayan adoptado el Código.

Añadimos nosotros que las garantías deben incluir la responsabilidad de los responsables o encargados establecidos en la Unión, con respecto a las vulneraciones a la protección de datos personales que se cometan bajo la vigencia del ordenamiento jurídico de los países terceros.

[337] Art. 40.1 RGPD.

[338] Art. 40.3 RGPD.

[339] Art. 41 RGPD.

3.4. Valoración conjunta.

Sin perjuicio de que en el análisis de las garantías hayamos introducido nuestras opiniones sobre cada una de ellas en particular, estimamos oportuno realizar una valoración de ellas en su conjunto, que extendemos a continuación.

Las garantías diseñadas para permitir las transferencias internacionales de datos personales en caso de ausencia de Decisión de adecuación, tienen la finalidad de que los datos personales continúen manteniendo un nivel de protección similar al que gozan en la Unión, aunque queden sometidos a otro ordenamiento jurídico. Obsérvese que utilizamos el verbo *permitir* dado que, si analizáramos este tipo específico de tratamiento de datos (las comunicaciones internacionales) estrictamente desde el punto de vista de los derechos fundamentales de los interesados, no deberían estar permitidos por ausencia de garantías suficientes. Sin embargo, la regulación del derecho europeo de protección de datos tiene como uno de sus objetivos el equilibrio entre los derechos de los interesados y la libertad de empresa y, si lo analizamos desde esta óptica, se hace necesaria una solución alternativa debido a que es imposible que la Comisión estudie el derecho y emita una Decisión de aprobación para cada uno de los países terceros a la Unión.

Se advierte en las diferentes garantías que consisten en fuentes de derechos y obligaciones adoptados directamente por los agentes intervinientes en los tratamientos de datos personales o por entidades intermedias que los representan, pero no constituyen una manifestación de la libertad de contratación absoluta sino que está estrictamente reglada, tanto en su vertiente de *soft law* (BCR o códigos de conducta) como en su vertiente contractual (cláusulas tipo).

Ahora bien, la protección de los datos personales en un contexto virtual tiene una dificultad que se encuentra presente cuando el tratamiento que se les está dando está

sometido al ordenamiento jurídico comunitario, que se agrava al estar regulado por un ordenamiento distinto y más aún en ciertos casos en que podríamos comparar a los tratamientos con la posición de "*apátridas*" con respecto a cualquier ordenamiento jurídico ya que en este entorno existen actividades o elementos a los que es muy difícil que llegue la aplicación de las normas jurídicas tradicionales y pueden incluso ocultar su origen y los distintos elementos de tal forma que logren extraerse a toda regulación jurídica[340], ya sea porque las conexiones a internet estén codificadas de tal forma que no sea posible conocer su origen, porque en el tratamiento de los datos personales intervengan tantos elementos de origen distinto o desconocido que sea difícil determinar qué derecho es aplicable y cuál no lo es y, finalmente, porque en actividades tales como el control de la conducta o la elaboración de perfiles, en ocasiones si esas actividades no se trasladan a la "vida real"[341] por medio de un hecho concreto que, además, guarde una relación evidente con la actividad virtual, en ocasiones será imposible que incluso el interesado cuya conducta se está controlando o cuyo perfil se haya elaborado, sea consciente de cómo están siendo utilizados sus datos personales.

Otra observación que podemos extraer de estas garantías es que bajo determinadas circunstancias pueden extender transnacionalmente la competencia de las autoridades de protección de datos personales para evaluar las condiciones de protección en que se encontrarán los datos una vez recibidos, si bien esta extensión de su competencia no

[340] Es lo que ocurre en la "*dark web*" o internet oscura, en la que en muchas ocasiones resulta imposible vincular, ya sea subjetiva u objetivamente, las comunicaciones con un ordenamiento jurídico determinado. Crf. Chertoff, M: "A public policy perspective of the Dark Web". Journal of Cyber Policy, Volume 2, 2017, Issue 1.- Accesible en: https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643.

[341] Nos referimos a "vida real" por oposición a entorno virtual o ciberespacio.

alcanza el grado de general otorgado a la Comisión a través de sus Decisiones sino que se limita al caso concreto que se esté controlando.

4. Excepciones a la exigencia de garantías adicionales (art. 49 RGPD).

Las transferencias internacionales de datos personales son tratamientos, si bien tienen la particularidad de que su consecuencia principal en lo que a los efectos jurídicos se refiere es que los datos entrarán bajo la aplicación de un ordenamiento jurídico extra europeo, motivo por el cual el Reglamento exige que continúen manteniendo un nivel de protección similar, para lo cual exige determinadas propiedades al ordenamiento jurídico receptor, o garantías por parte del exportador y del importador.

Pero, a manera de excepción para la exigencia de un nivel de protección similar, el art. 49 RGPD admite para este tipo específico de tratamientos algunos de los fundamentos de licitud establecidos en el artículo 6 que harán que la transferencia internacional de datos personales sea lícita aún ante la ausencia de una decisión de adecuación o de garantías adecuadas, sin dejar de tener en cuenta que estas circunstancias constituyen excepciones al régimen general de las transferencias, por lo se deben aplicar sólo en ausencia del sistema de adecuación o de garantías[342].

Las excepciones a las reglas generales de la transferencia son:

a) La transferencia internacional podrá realizarse, excepcionalmente, si cuenta con el consentimiento informado, libre y explícito del interesado o si se realiza desde un registro público que, con arreglo al Derecho de la Unión o de los Estados

[342] Directrices 2/2018 del CEPD, pp. 3-4.

miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta. En estos casos, la transferencia no debe abarcar la totalidad de los datos personales ni categorías enteras de dichos datos y, si el registro es de consulta restringida a personas con un interés legítimo, la transferencia sólo podrá efectuarse a solicitud de dichas personas o si éstas han de ser las destinatarias.

b) En su defecto, se podrá realizar si es necesaria en las circunstancias que enumeraremos a continuación, para lo cual el exportador debe realizar un "test de necesidad"[343] que excluirá en primer lugar las transferencias que deban realizarse por una circunstancia casual, como por ejemplo que el exportador haya seleccionado una empresa ubicada en el exterior como encargado para realizar el tratamiento, cuya ubicación sea fortuita y no un requisito esencial para dicho tratamiento.

Las circunstancias para las cuales la transferencia debe ser necesaria son:

a) La celebración o ejecución de un contrato en el que el interesado sea parte o la aplicación, a petición de éste, de medidas precontractuales. Respecto a esta circunstancia el considerando 111 establece que, además de necesaria, la

[343] Ibidem, pp. 4 y 8-9.

transferencia debe ser ocasional, por lo que el CEPD[344] considera que el requisito de ocasional debe también estar presente.

b) Interés público que sea importante en el derecho de la Unión o de los Estados miembros, para lo cual pueden servir de indicador las condiciones de reciprocidad establecidas en instrumentos internacionales344
c) El ejercicio o la defensa de reclamaciones
d) Proteger intereses vitales del interesado o de un tercero, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

Las transferencias que no estén respaldadas por una decisión de adecuación de la Comisión, que no cuenten con las garantías específicas ofrecidas por el responsable o encargado y no estén justificadas por ninguno de los motivos ya expuestos no serán lícitas bajo la aplicación del Reglamento, a menos que:

a) No sea repetitiva, término que ha sido interpretado por el CEPD[345] como excluyendo las transferencias que sean sistemáticas y repetitivas dentro de una relación estable entre exportador e importador. Sin embargo, pueden realizarse más de una vez, siempre que no sea regularmente.
b) Afecte sólo a un número limitado de interesados;
c) Sea necesaria a los fines de protección de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado;

[344] Directrices 2/2018, pág. 10

[345] Ibidem, pp. 4-5.

d) El responsable del tratamiento haya evaluado todas las circunstancias concurrentes en ella y en base a este análisis haya ofrecido garantías apropiadas para la protección de los datos personales.

En estas circunstancias, el responsable del tratamiento informará sobre la transferencia a la autoridad de control y al interesado, a quien además de la información establecida en los artículos 13 y 14 informará sobre las distintas circunstancias de la transferencia y sobre los intereses legítimos imperiosos perseguidos.

Para finalizar este apartado, el CEPD recomienda que este artículo no sea utilizado para legitimar transferencias que se realizan en el curso de una relación estable (excepto si, aún dentro de ésta, se realizan de forma ocasional), en cuyo caso es conveniente otorgar las garantías adecuadas de acuerdo al art. 46 RGPD[346].

5. El Reglamento 18/1725.

El Reglamento 18/1725 regula en el Capítulo V, artículos 46 a 51, las transferencias internacionales de datos personales realizadas por las Instituciones, órganos y organismos de la Unión Europea hacia terceros países u organizaciones internacionales. Las disposiciones de estos artículos son similares a las del RGPD, aunque con las lógicas adaptaciones motivadas en su especial campo de aplicación.

Se admiten las mismas decisiones de la Comisión a efectos de declarar que un país tercero, su ordenamiento jurídico o un sector de éste ofrecen un nivel de protección

[346] Ibidem, pág. 11.

equivalente[347], así como las mismas excepciones a la necesidad de decisión de adecuación o de garantías adecuadas[348].

Con respecto a estas últimas, es decir las garantías adecuadas, se aceptan las siguientes:

- "*Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos*" (art. 48.2.a Reglamento 18/1725);
- Cláusulas tipo adoptadas por la Comisión (art. 48.2.b Reglamento 18/1725) o adoptadas por el SEPD y aprobadas por la Comisión (art. 48.2.c Reglamento 18/1725);
- Cuando el encargado del tratamiento no sea un organismo de la Unión, las garantías aceptadas por el art. 46 apartado 2, letras b), e) y f) RGPD.

Las garantías anteriormente mencionadas no necesitan de la aprobación del SEPD; pero, con la autorización de este órgano, también se podrán cláusulas contractuales o disposiciones que se incorporen a acuerdos administrativos y que incluyan derechos efectivos y exigibles para los interesados (art. 48.3 Reglamento 18/1725).

6. Actos adoptados en base a las facultades otorgadas por el artículo 25 de la Directiva 95/46 y el artículo 9 del Reglamento 2001/45[349].

[347] Art. 47 Reglamento 18/1725.

[348] Art. 50 Reglamento 18/1725.

[349] Cabe traer a colación que las decisiones de la Comisión basadas en estos artículos de la Directiva 95/46 permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con el artículo 45 del RGPDP y por el art. 47 Regl. 18/1725, que remite al artículo citado del RGPD.

6.1. Decisiones de la Comisión en las que se declara adecuada la protección otorgada por distintos ámbitos jurídicos, países o territorios terceros

Antes de comenzar a analizar las Decisiones que ha adoptado la Comisión en base a los arts. 25 y 31 de la Directiva 94/46, debemos aclarar que la primera de las mencionadas disposiciones establece, en su apartado 1, que el nivel adecuado de protección lo debe garantizar el país tercero. Sin perjuicio de ello, el apartado siguiente dispone que entre las variables que la Comisión debe tener en cuenta a efectos de evaluar el nivel de protección, se encuentran entre otras "… *las normas de derecho, generales o sectoriales, vigentes en el país de que se trate…*". Interpretando esta norma, la Comisión ha adoptado distintas decisiones en las que se declara adecuada la protección otorgada por un país tercero, pero también por determinados sectores o aspectos de ese país o por un territorio. Las analizaremos a continuación en base a esta clasificación.

A modo de cuestión preliminar para sentar las bases teóricas generales sobre las cuales han trabajado las Instituciones a efectos de adoptar las decisiones destinadas a regular las transferencias hacia países terceros, expondremos algunas pautas para la interpretación del concepto de "protección adecuada de datos personales" elaborada por el G29.

Este Grupo de Trabajo expresaba su voluntad por medio de dictámenes, recomendaciones y otro tipo de elementos tales como documentos de trabajo y de debate, entre los cuales se encuentran algunos que efectúan un análisis de los artículos 25 y 26 de la Directiva 95/46 que, si bien carecen de valor vinculante, arrojan pautas orientativas que la Comisión ha seguido para la adopción de las Decisiones que analizaremos en los apartados siguientes, motivo por el cual nos parece adecuado exponerlas como cuestión previa.

La opinión de este grupo sobre el nivel adecuado de protección a los fines de la autorización para las transferencias internacionales se recoge principalmente en dos documentos: El documento de debate sobre "Primeras orientaciones sobre la transferencia de datos personales a países terceros – Posibles formas de evaluar la adecuación", adoptado el 26 de junio de 1997[350] y el documento de trabajo titulado: "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", adoptado el 24 de julio de 1998[351] .

En el primero de los documentos y entre otras consideraciones, el G29, consciente de que será imposible analizar en profundidad y uno a uno todos los pedidos de autorizaciones de transferencias internacionales de datos, recomienda que se consideren prioritarios, a efectos de otorgar o denegar la autorización, los siguientes casos:

– Transferencias que afecten a las categorías sensibles de datos definidas en el artículo 8 de la Directiva;

– Transferencias que supongan un riesgo de pérdida financiera;

– Las que supongan un riesgo para la seguridad personal;

– Las que se realicen a efectos de tomar una decisión que afecte significativamente a un individuo, o que supongan un riesgo de perjudicar o manchar su reputación;

[350] Originalmente titulado en inglés: "Discussion document: First orientations on transfers of personal data to third countries – Possible ways forward in assessing adequacy". Traducción de la autora.

[351] Original en inglés: "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive". Traducción de la autora.

– Transferencias que pueden resultar en acciones concretas que constituyan una considerable invasión de la vida privada de los individuos, tales como llamadas telefónicas no deseadas.

– Transferencias que supongan la recogida de datos de forma especialmente cubierta o clandestina (por ejemplo, cookies).

En el segundo de los documentos mencionados, el Grupo de Trabajo se fija como finalidad la de establecer unas bases positivas y objetivas para determinar si un país tercero ofrece garantías adecuadas, según el artículo 25 apartado 2, para la protección de los datos personales y las circunstancias en que una transmisión de datos a un país tercero se permitirá o no.

Algunos de los requisitos mínimos que debería reunir la legislación o reglamentación, ya sea sectorial o general del país tercero son:

a) Principios: Algunos de los principios contenidos en la regulación de la Unión Europea en materia de protección de datos personales, como el de proporcionalidad y calidad de los datos, de transparencia, de seguridad, de limitación de objetivos, restricciones respecto a transferencias a otros países, derechos de acceso, rectificación y oposición, etc.

b) En cuanto a la implementación en la práctica del sistema legal de protección, ésta debe ser efectiva y satisfactoria, debe ofrecer apoyo y asistencia a los interesados y también vías de recurso adecuadas. La existencia de una autoridad independiente de supervisión de la protección de datos es un requisito deseable.

Con respecto a los países que han suscrito el Convenio 108 del Consejo de Europa y no forman parte del EEE, el Grupo decide que, bajo un par de condiciones, la firma de dicho Convenio puede indicar un nivel adecuado de protección. Las condiciones son:

a) Que el país disponga de mecanismos adecuados para garantizar su cumplimiento, para ayudar a las personas físicas a que lo consigan, para facilitar la reparación (por ejemplo, una autoridad independiente de aplicación y control) y, como elemento clave, que ofrezca vías adecuadas de recurso a quienes se consideren perjudicados por la violación de los principios.

b) Que el país en cuestión sea destino final de los datos o, en su caso, que sea país de tránsito hacia otro país de la Unión Europea u otro país tercero que ofrezca niveles adecuados de protección.

Uno de los problemas específicos que surgen en el caso de las transferencias hacia terceros países en el análisis del Grupo de Trabajo, radica en el imperativo legal de comunicar esos datos a las autoridades al que puede estar sometido el receptor, obligación que dada su fuerza legal, tendría preponderancia frente a las obligaciones contractuales.

Tanto en la Directiva como en el RGPD se contempla esa posibilidad[352] al establecer que las personas que estén bajo la autoridad del responsable o del encargado únicamente podrán procesar los datos bajo encargo de uno de estos sujetos o por imperativo legal. Pero en este caso, el derecho europeo lo permite ya que, tratándose de los estados miembros, existe la presunción de que su legislación ofrece una protección adecuada, lo que puede no suceder tratándose de un país tercero.

En utilización de las facultades mencionadas en el epígrafe, la Comisión ha adoptado diversas decisiones respecto a países terceros, dejando constancia fehaciente de que

[352] Art. 16 de la Directiva 95/46 y art. 28.3.a) en el RGPD.

garantizan un nivel adecuado de protección, que presentan un par de características comunes:

En primer lugar, su adopción fue posible gracias al interés de las autoridades locales del país o territorio en cuestión, que asesoraron a la Comisión y a los distintos órganos consultivos que colaboran con esta Institución en el procedimiento de adopción de estas decisiones, para acercarles la legislación sobre protección de datos vigente en su ordenamiento jurídico así como las pautas de interpretación y aplicación de la misma. Esta tarea de estudio previo de las condiciones jurídicas vigentes en el país o territorio, se efectuó en la mayoría de los casos a través de la intervención del Grupo de Trabajo del Artículo 29.

Por otro lado, en todas ellas se recuerda que la declaración de adecuado nivel de protección no impide a las autoridades de control de datos de los estados miembros el ejercicio de las facultades que la Directiva 95/46 les otorga, de prohibir o suspender los flujos de datos hacia cualquier país tercero, con justificación en las disposiciones de la Directiva 95/46, que deben ser expresamente invocadas por las autoridades.

Para su estudio las dividiremos en tres grupos distintos: a) Protección adecuada brindada por el orden jurídico de un país; b) Protección adecuada otorgada por el derecho aplicable en un determinado territorio; c) Protección adecuada brindada por un sector del derecho de un determinado país.

Dentro de cada grupo, se expondrán las decisiones por orden cronológico.

6.1.1. Protección adecuada brindada por el ordenamiento jurídico de un país.

Hungría y Suiza: Decisiones de 26 de julio de 2000. Para llegar a la declaración de adecuada protección a los datos personales en Hungría y Suiza, la Comisión considera que la Constitución de estos países brinda protección a la vida privada y, especialmente, a los datos personales; igualmente existen leyes generales de protección de los datos personales, también leyes sectoriales y decretos de desarrollo. Ambos países han ratificado el convenio 108 del Consejo de Europa. En el caso de Suiza se ha tenido en cuenta, además, la jurisprudencia sobre protección de datos personales desarrollada por los distintos órganos judiciales, especialmente debido a la organización política de este estado merced a la cual, si bien cada cantón dicta sus propias leyes en la materia, las disposiciones constitucionales son de aplicación en todos ellos.

Argentina: Decisión de 30 de junio de 2003. Este país también garantiza la protección de datos personales en su Constitución, en una ley general y en leyes sectoriales específicas. Como novedad destacada por la Comisión en su decisión, entre los recursos previstos en la Constitución para el ejercicio y protección de los derechos y garantías fundamentales, existe uno específico para el ejercicio de la garantía de protección de los datos personales que se denomina hábeas data . También existen autoridades de control y la legislación prevé sanciones de distinta naturaleza de aplicación ante las violaciones a la intimidad mediante los tratamientos ilícitos de datos personales.

Principado de Andorra: Decisión de 19 de octubre de 2010. Para su adopción la Comisión tiene en cuenta que Andorra es un país democrático y su constitución garantiza el derecho a la intimidad, que existe una Ley Cualificada de Protección de los Datos Personales en vigor cuyos principios están en gran medida basados en la Directiva 95/46, también cuenta con autoridades independientes de protección de datos así como diversas

legislaciones sectoriales de protección de datos y, por otra parte, ha ratificado el Convenio 108 del Consejo de Europa.

Israel: Decisión de la Comisión de 31 de enero de 2011. El Estado de Israel tiene la particularidad de adherir a los principios del Derecho Común y, en consecuencia, carece de constitución escrita. Sin embargo, se ha conferido validez constitucional a distintas Leyes Fundamentales, una de las cuales garantiza la protección a la intimidad. Esta protección se desarrolla en una ley general y otros instrumentos jurídicos que regulan la protección de datos personales en distintos sectores, así como en decisiones gubernamentales. También existe una autoridad de supervisión.

Pero la ley israelí de protección de datos se refiere solamente a aquellos datos que sean tratados en Israel por medios automatizados, lo que es aplicable tanto a la transferencia en sí como a todo tratamiento posterior que se realice en dicho estado. Por consiguiente, toda transferencia de datos personales cuyo destinatario esté establecido en Israel, así como todo tratamiento posterior que deba realizarse en dicho estado, si se efectúan por medios no automatizados, no contarán con la protección adecuada, y así lo declara la Comisión en su decisión.

Uruguay: Decisión de la Comisión de fecha 21 de agosto de 2012. Este país no contiene una disposición constitucional que proteja expresamente el derecho a la vida privada y a los datos personales, pero la normativa jurídica en la materia declara a estos derechos incluidos entre los derechos no expresamente mencionados en la constitución, pero cuya protección constitucional deriva de su naturaleza inherente a la condición humana o que derivan del sistema republicano de gobierno.

Al igual que la legislación argentina, en la uruguaya se regula el recurso constitucional de hábeas data, de similar contenido al del país vecino.

Como hemos visto, en todos los casos la Comisión ha tenido en cuenta la protección constitucional del derecho a la vida privada o a la intimidad, especialmente en su aspecto de protección a los datos personales, la existencia de leyes y decretos, generales y sectoriales, que desarrollan ese derecho fundamental y de autoridades de control y supervisión con respecto a la protección de datos personales. Pero además, para adoptar la decisión de adecuación de la protección la Comisión ha tenido especialmente en cuenta que el derecho vigente se apoye en principios de contenido similar a los que en la Unión Europea prevé la Directiva 95/46.

6.1.2. Protección adecuada otorgada por el derecho aplicable en un determinado territorio.

Bailía de Guernsey: (Decisión de 21 de noviembre de 2003), Isla de Man: (Decisión de la Comisión de 28 de abril de 2004) y Bailía de Jersey (Decisión del 8 de mayo de 2008). Estos tres territorios pertenecen a la Corona británica (aunque no forman parte del Reino Unido ni son colonias), y gozan de total independencia, excepto en cuanto a relaciones internacionales y defensa, ámbitos que son competencia del Gobierno del Reino Unido. Por tanto la Comisión los considera un tercer país con arreglo a la Directiva y, analizado el derecho vigente en estos territorios, declara que ofrecen un adecuado nivel de protección para los tratamientos de datos personales.

Islas Feroe: Decisión de 5 de marzo de 2010. Estas islas constituyen una comunidad autónoma del Reino de Dinamarca, que en virtud de las facultades que le confiere su

Estatuto de autonomía, no se adhirió a la Unión Europea cuando lo hizo Dinamarca, en 1973, por lo que deben ser consideradas un país tercero. Según analiza y declara la Comisión en su decisión, la Ley de Tratamiento de Datos Personales de las Islas Feroe concede a los tratamientos de datos personales una protección que la Comisión considera adecuada; mas no todos los tratamientos de datos cuyo destinatario se halle en las Islas Feroe están cubiertos por esta ley, por lo que la Decisión de la Comisión se limita a los tratamientos que sí lo están.

6.1.3. Protección adecuada brindada por un sector del derecho de un determinado país.

Canadá: Esta decisión tiene la particularidad de que no se refiere a la protección adecuada del derecho canadiense en general, sino a la protección otorgada por la ley canadiense "Personal Information and Electronic Documents Act" (Art. 2 de la Decisión). Según se explica en los considerandos previos número 5; 6 y 7, esta ley no se aplica a todas las entidades que efectúan tratamiento de datos, ni en todos los casos ya que las provincias pueden tener regulaciones propias. Es por todo ello que no se declara adecuada la protección que otorga el derecho canadiense, sino sólo la otorgada por la mencionada ley.

6.2. Decisión de la Comisión sobre transferencias de datos personales efectuadas por las Instituciones u órganos de la Unión hacia terceros países.

El 29 de marzo de 2011 la Comisión adoptó una decisión de adecuada protección sectorial de datos personales en Japón, de conformidad con el artículo 9, apartados 1. y 2. del Reglamento 45/2001.

En efecto, en virtud del artículo 21 del Acuerdo entre la Comunidad Europea y el Gobierno de Japón, sobre cooperación y asistencia administrativa mutua en materia aduanera, el Comité Mixto de Cooperación Aduanera con Japón adoptó la Decisión 1/2010, de 24 de junio de 2010, sobre el reconocimiento mutuo de los regímenes de operador económico autorizado en la Unión Europea y en Japón.

Para posibilitar la aplicación de la Sección IV, apartado 4, letras a) a f) de dicha Decisión, la Comisión adoptó la Decisión de 29 de marzo de 2011, de conformidad con el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, cuyo único objetivo es declarar el grado adecuado de protección que ofrece la regulación a las que están sometidas las autoridades administrativas de Japón respecto a los datos personales transferidos por la Comisión Europea, con vistas al reconocimiento mutuo de los regímenes de operación económico autorizados.

7. El flujo de datos personales desde la Unión Europea hacia los Estados Unidos: Características especiales.

Uno de los destinos más frecuentes de las transferencias internacionales de datos desde remitentes establecidos en los estados miembros de la Unión Europea es el territorio de Estados Unidos[353].

[353] De las 202 solicitudes de transferencias de datos personales presentadas ante la Agencia Española de Protección de Datos, 40 eran transferencias hacia Estados Unidos, destino sólo superado por el conjunto de los países latinoamericanos para los cuales es necesario solicitar autorización (79 solicitudes). Ver Memoria 2011 AEPD 2011, en línea: http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf, página 48. Asimismo, en el primer semestre de 2007, de un total de 148 transferencias fuera del EEE, 87 correspondían a Estados Unidos (vid Informe sobre las transferencias internacionales de

Pero la concepción jurídica estadounidense de la protección a la intimidad es evidentemente distinta de la europea y en la escala de valores del ordenamiento jurídico transatlántico, la protección de datos personales no es un derecho fundamental autónomo, sino que se engloba en el derecho a la intimidad (*right to privacy*), ubicándose en un escalón inferior frente a otros bienes jurídicos[354], tales como la seguridad, la libertad de expresión, la libre competencia, etc.[355]

Por todo ello y dada la enorme importancia que tiene los Estados Unidos para el movimiento de datos personales generados en la Unión Europea, ha sido necesario adoptar distintas normas para conciliar la regulación comunitaria sobre protección de datos personales con el ordenamiento jurídico norteamericano.

7.1. Los principios de puerto seguro y la sentencia "Schrems" (2014).

Unos años después de la adopción por parte de la Unión Europea de la Directiva 95/46, surgió entre algunas entidades privadas norteamericanas la preocupación por la diferencia entre la protección otorgada a los datos personales por el derecho de los Estados Unidos y el de la Unión Europea ya que, siendo Estados Unidos un país tercero a los efectos del artículo 25 apartado 6 de la Directiva, esa diferencia podía constituirse en un verdadero

datos, julio 2007, AEPD; citado en Sancho Villa, D: Negocios internacionales de tratamiento de datos personales. Ed. Aranzadi, Cizur Menor (Navarra), 2010; página 123, cita 32.

354 Cfr. Sancho Villa, D: Op. cit, página 121.

355 Esto no implica que en la Unión Europea se le haya otorgado a la protección de datos personales un valor superior a todos estos bienes, sino que, en tanto que derechos fundamentales, en principio existe un equilibrio entre todos ellos, como se infiere de toda la regulación general establecida por la Directiva y la cantidad de excepciones a dichas normas generales. En los casos concretos en que los mismos entren en conflicto se deberán valorar las circunstancias del caso para decidir en qué forma se armonizan.

obstáculo para un desarrollo fluido de los negocios entre entidades o personas de ambos territorios, si los mismos implicaban la transmisión entre ellas de datos personales.

Por ello el gobierno de Estados Unidos, dando respuesta a esa preocupación, publicó el 21 de julio de 2000 un grupo de principios llamado de "Puerto Seguro" (safe harbour -en adelante "los principios"-) y siete anexos, entre los cuales destaca el Anexo II, consistente en un conjunto de normas de interpretación de dichos principios, que llevan el nombre de Preguntas Más Frecuentes (FAQ, por sus siglas en inglés). La finalidad principal de los principios de Safe Harbour era la de otorgar un marco jurídico a la protección de datos que permita a la Comisión adoptar una decisión de adecuación del nivel de protección, para las transferencias para las que la entidad receptora haya adherido a los principios, facilitando así el comercio y las transacciones entre Estados Unidos de América y la Unión Europea.

Debemos mencionar que la adopción de ese cuerpo normativo no fue casual ni producto de una decisión unilateral, sino que fue el resultado de una larga negociación entre las autoridades norteamericanas y las de la Unión, incluyendo varios dictámenes del Grupo de Trabajo del Artículo 29, algunos de los cuales han sido tomados en cuenta por las distintas autoridades para la redacción final de los principios.

Los principios funcionaban, mutatis mutandi, en forma similar a las reglas corporativas vinculantes (que hemos mencionado en el capítulo anterior), aunque adoptadas en una declaración unificada por el gobierno y a la cual la adhesión por parte de las empresas es voluntaria.

Ahora bien, como hemos mencionado anteriormente, existe una profunda diferencia entre el concepto de intimidad o privacidad del derecho norteamericano y el de la Unión

Europea; que a los efectos de la protección de datos, se manifiesta principalmente en que la seguridad tiene un valor jurídico superior al de la privacidad, en cuyo mérito se permite a las autoridades públicas la monitorización de las comunicaciones privadas sin ningún tipo de conocimiento ni control por parte de los interesados, lo que constituía tratamiento ilegítimo en los términos del articulado de la Directiva 95/46 y así fue declarado por el Tribunal de Justicia en la sentencia conocida como "Schrems"[356], por medio de la cual se declaró nula la decisión de adecuación del nivel de protección de los datos personales otorgado por los principios de Safe Harbour.

En este fallo, el Tribunal de Justicia enumera los graves defectos de fondo de que adolecía la Decisión 2000/520 de la Comisión, todos ellos, que detallamos a continuación.

En primer lugar, el TJUE halla la Decisión 2000/520 no adecuada a las exigencias del artículo 25 apartado 6 de la Directiva 95/46, por cuanto la Comisión hace constar en la Decisión 2000/520 que los principios de puerto seguro garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos de América, pero no constataba que los Estados Unidos como país, ni su legislación interna ni los compromisos internacionales contraídos (los principios de Puerto Seguro no constituían un tratado internacional) garanticen un nivel adecuado de protección de los datos personales[357]. Por el contrario, el Tribunal de Justicia en la sentencia que aquí analizamos concluye que la legislación estadounidense no otorga un nivel de protección equivalente al de la Unión. Agregamos nosotros que, de esta forma,

[356] Sentencia dictada por el TJUE el 6 de octubre de 2014.

[357] Sentencia Schrems, apartado 83.

sólo garantizarían un nivel adecuado de protección las entidades autocertificadas, pero de ninguna forma la legislación o los compromisos internacionales de Estados Unidos.

Por otra parte, destaca[358] que las autoridades norteamericanas pueden limitar la aplicabilidad de estos principios por distintos motivos, entre los cuales se encuentran las exigencias de seguridad nacional, el interés público, disposiciones legales o reglamentarias y jurisprudencia, sin ningún límite ni posibilidad de control por parte del interesado.

Declara[359] asimismo el Tribunal de Justicia que la misma Comisión había constatado, en los puntos 2 y 3.2 de la Comunicación COM(2013) 846 final y en los puntos 7.1, 7.2 y 8 de la Comunicación COM(2013) 847 final, que las autoridades estadounidenses tenían poderes para acceder a los datos que habían sido transferidos desde entidades ubicadas en la Unión y tratarlos de forma incompatible con la finalidad de las transferencias.

Declara también[360] que el título B del anexo IV de la Decisión 2000/520 admite que la legislación estadounidense puede poner límites a la aplicabilidad de los principios de Puerto Seguro, en particular con respecto al plazo de conservación de los datos, y reconoce explícitamente la primacía de las exigencias de seguridad nacional e interés público por encima de estos principios. Ello así pues la normativa estadounidense permite a la legislación y autoridades públicas que amplíen indefinidamente el plazo de conservación de los datos transferidos[361] y a las autoridades relacionadas con la defensa y seguridad nacional, que accedan de forma generalizada al contenido de las

[358] Apartado 84 de la sentencia Schrems.

[359] Apartado 90 de la sentencia Schrems.

[360] Apartados 86 y 87 de la sentencia Schrems.

[361] Apartado 93 del mismo fallo.

comunicaciones y que sometan los datos a tratamientos que no sean compatibles con la finalidad de la transferencia, sin prever ningún criterio objetivo de motivación para estas acciones[362].

El derecho estadounidense permite, así, la injerencia de autoridades públicas en los derechos fundamentales de los interesados, frente a las cuales no se prevén recursos a disposición del interesado para ejercer sus derechos de acceso a los datos, de rectificación o de supresión, desconociendo así el derecho a la tutela judicial efectiva reconocido en el artículo 47 de la Carta[363].

Por otra parte, en los apartados 96 a 98 el Tribunal destaca que el artículo 25, apartado 6 de la Directiva 95/46 requiere que la Decisión de la Comisión haga constar que un país tercero garantiza un nivel de protección equivalente al de la Unión, a la vista de su legislación interna o sus compromisos internacionales. Ahora bien, la Decisión 2000/520 no constata que Estados Unidos garantiza un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales, vulnerando así las exigencias del art. 25 apartado 6 de la Directiva 95/46.

[362] En el derecho europeo, concretamente en el Reglamento 679/2016 se admite que el derecho de los Estados Miembros establezca un límite a ciertas obligaciones de los responsables y encargados de los tratamientos y a ciertos derechos de los interesados siempre que dicha limitación se establezca a través de una medida legislativa que determine con claridad su alcance, así como también que identifique el o los responsables, las categorías de datos a tratar, el plazo de conservación, la finalidad del tratamiento, las garantías para los interesados y que "*respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar*" (art. 23) ciertos valores que se enumeran taxativamente en el mismo artículo, tales como la seguridad y defensa del Estado, la seguridad pública, la persecución de infracciones penales y de normas deontológicas de profesiones reguladas, intereses públicos importantes, la independencia y funciones del poder judicial, algunas funciones vinculadas con el ejercicio de la autoridad pública, la protección del interesado o de los derechos y libertades de otras personas y la ejecución de demandas civiles.

[363] Apartado 95.

Por ello y sin perjuicio de las anteriores afirmaciones, sin entrar a analizar la validez de los principios de Puerto Seguro, la parte dispositiva del fallo declara inválida la Decisión 2000/520.

En los párrafos que hemos examinado de la Sentencia Schrems el Tribunal de Justicia analiza algunos aspectos del ordenamiento jurídico estadounidenses, dejando entrever que el nivel de protección de datos personales que éste ofrece no es equiparable al de la Unión Europea, porque su normativa permite tanto a la legislación como a las autoridades públicas la injerencia en los derechos de los interesados o los principios de los tratamientos de datos personales, sin ningún tipo de restricción ni limitación legal y sin establecer recursos a disposición de los interesados para que ejerzan el control de esas injerencias.

No obstante, la declaración de invalidez de la Decisión 2000/520 no se motiva en esa falta de garantías del derecho norteamericano sino en una deficiencia formal de dicha decisión.

7.2. El Escudo de Privacidad.

En el momento en que el Tribunal de Justicia de la Unión dictó el fallo Schrems, la Comisión ya estaba negociando con el gobierno de los Estados Unidos un nuevo convenio para reemplazar los principios de Puerto Seguro, a efectos de subsanar los numerosos defectos de que éstos adolecían, que eran evidentes no sólo para el Tribunal.

Dichas negociaciones finalizaron en julio de 2016 con la conclusión del acuerdo de Escudo de Privacidad[364], que motivó la Decisión de Ejecución (UE) 16/1250 de la

[364] Acuerdo que es llamado comúnmente por su nombre en inglés, *Privacy Shield*.

Comisión, de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE.UU[365].

El Escudo de Privacidad se basa, al igual que los principios de Puerto Seguro, en un régimen de autocertificación mediante el cual las entidades norteamericanas al adherir al mismo se comprometen[366] a cumplir los Principios que figuran en el Anexo II de la Decisión 16/1250.

Los documentos anexos a la Decisión 16/1250 se publicarán en el Registro Federal de Estados Unidos[367] y serán aplicados y controlados por el Departamento de Comercio (Department of Commerce) de los Estados Unidos[368], a través de la FTC (Federal Trade Commission) y el Departamento de Transporte (Department of Transport).

Entre los anexos de esta Decisión, se incorporan cartas de la Secretaria de Comercio (Secretary of Commerce) norteamericana (Anexo I), del Subsecretario de Comercio Internacional en funciones (Acting Under Secretary for International Trade) (Anexo I.1), del Secretario de Estado (Secretary of State) estadounidense (Anexo III), de la Presidente de la Comisión Federal de Comercio (Federal Trade Commission Chairwoman) (Anexo IV), del Secretario de Transporte (Secretary of Transportation) (Anexo V), del Asesor General del Director de Inteligencia Nacional (General Counsel, Office of the Director of

[365] En adelante, "*Decisión 16/1250*". Con respecto a la misma juzgamos de importancia destacar que, tal como se resalta en la parte introductoria de sus considerandos, esta Decisión se adoptó sobre la base del artículo 25 de la Directiva 95/46, sin perjuicio de que se prevea que la misma cumple con las exigencias del artículo 45 del RGPD.

[366] Considerando 19 de la Decisión 16/1250.

[367] Considerando 12 de la Decisión 16/1250.

[368] Considerandos 14 y 18 y Anexo II de la Decisión 16/1250. En este último se destaca que este Departamento publica los principios "*en virtud de su competencia legal para impulsar, promocionar y desarrollar el comercio internacional (USC, título 15, artículo 1512)*".

National Intelligence) (Anexo VI), dirigidas a la entonces Comisaria de Justicia, Consumidores e Igualdad de Género, Dª Vèra Jourová, en las que se implican en la aplicación y control de los principios del Escudo de Privacidad, no sólo asumiendo el contenido de los mismos sino también enumerando distintas normas internas norteamericanas que rigen en el ámbito de la protección de la privacidad de las personas.

El Anexo II de la decisión, en el apartado I (Síntesis), párrafo 1, reconoce que el enfoque de la privacidad adoptado por los Estados Unidos es distinto del que impera en la Unión Europea, ya que el primero consiste en una mezcla de legislación, regulación y autorregulación, siendo en esta última (en la autorregulación) donde se inserta el mecanismo de autocertificación en que se basa el régimen del Escudo de la Privacidad. Ahora bien, en este mismo párrafo se deja constancia que estos principios están destinados para ser utilizados exclusivamente por las entidades de los Estados Unidos que sean destinatarias de transferencias de datos personales desde la Unión Europea, es decir que éstos no afectan a las autoridades públicas que, según se menciona en la decisión (apartados 3.1; 3.1.1. y siguientes) y sus anexos, tienen acceso a los datos personales transferidos.

Recordaremos aquí que la finalidad principal del reconocimiento de los derechos fundamentales es la protección de las personas físicas frente a las injerencias del Estado y en el derecho de la Unión y de sus Estados miembros, cuando se permite una excepción a este principio de la protección de los ciudadanos frente al poder del Estado por medio del reconocimiento de los derechos fundamentales, dicha excepción es de interpretación restrictiva y está sometida a estrictas limitaciones así como al control judicial.

Sin embargo en los Estados Unidos no es así. Tal como se establece en la Decisión 2016/1250 y sus anexos, las limitaciones a que está sometida la injerencia de las autoridades públicas en las comunicaciones de los ciudadanos son muy débiles y, en el caso de los datos personales que han estado sometidos al derecho comunitario antes de entrar al ámbito del derecho estadounidense, el mecanismo que se establece para su control es de una eficacia mínima: El Defensor del Pueblo en el ámbito del Escudo de la Privacidad, que analizaremos más adelante.

La interceptación de comunicaciones de señales entre particulares se denomina en el derecho norteamericano (por su traducción del inglés) "*inteligencia de señales*" y debe estar basada en un acto legislativo o en una autorización presidencial. Cabe recordar que en el derecho europeo las limitaciones a los derechos fundamentales deben estar establecidas por ley (art. 52 de la Carta), que a su vez debe respetar límites estrictos y está sometida a procedimientos y controles políticos y judiciales. Por lo tanto consideramos que el hecho de que en este caso, las injerencias de las autoridades públicas en las comunicaciones y el tratamiento de datos personales sin ningún tipo de control o limitaciones pueda ser realizado sólo con una autorización presidencial, no constituye un nivel de protección de los datos personales equiparable al de la Unión.

Esa "*inteligencia de señales*" está regulada por distintas normas estadounidenses, entre ellas la Constitución, la Ley de Vigilancia de la Inteligencia Exterior (o Foreign Intelligence Surveillance Act, en inglés), la Orden Ejecutiva 12333 y sus procedimientos de implantación y una Directiva Presidencial y está sometida al control de un órgano administrativo (el Tribunal de la FISA) y del Fiscal General, órganos que tienen facultades para limitar la recopilación, conservación, uso y divulgación de la información de la inteligencia exterior.

Los principios del Escudo de Privacidad se encuentran desarrollados en el Anexo II de la Decisión, y son[369]:

- El principio de notificación,
- El principio de integridad de los datos y de limitación de la finalidad,
- El principio de opción
- El principio de seguridad
- El principio de acceso
- Principio de recurso, aplicación y responsabilidad
- Responsabilidad de la transferencia ulterior

Según el considerando 65, todos los documentos enumerados y adjuntos a la Decisión se publicarán en el Registro Federal de los Estados Unidos.

8. Consideraciones finales.

Ya hemos mencionado que no consideramos exacto el término *transferencias* para describir las situaciones en que los datos son extraídos del ámbito espacial de competencia del Reglamento, considerando más apropiada la expresión *exportación del tratamiento* de los datos personales, a la cual damos el sentido de que el tratamiento al cual son sometidos los datos cuenta con un elemento, subjetivo u objetivo, que constituye un punto de conexión con el ordenamiento jurídico de un país tercero con respecto a la Unión Europea. Ahora bien, si según lo expuesto en el capítulo tercero de esta tesis, los tratamientos de datos personales que se consideran regulados por el derecho europeo de

[369] Apartado 2.1. de la Decisión.

protección de datos personales son aquéllos que se realizan en el contexto de las actividades de un establecimiento, del responsable o del encargado, establecido en el territorio de la Unión, la exportación estaría constituida por aquellos tratamientos que, sin necesidad de abandonar el contexto de las actividades de un establecimiento en la Unión, entran en contacto con un elemento que los pone bajo la vigencia de un ordenamiento jurídico distinto.

La autorización condicionada (o prohibición con excepciones) de la exportación del tratamiento de los datos personales es un ejemplo más de la dificultad de someter las operaciones que se realizan en el ciberespacio o espacio virtual a un derecho de base territorial. Por ello el legislador europeo, con la finalidad de que los datos personales que han estado protegidos por el derecho de la Unión no pierdan dicha protección intenta una extraterritorialización de la misma, más allá de los límites territoriales de los Estados miembros. Extraterritorialización que se articula tanto mediante normas vinculantes como mediante la actuación de las distintas autoridades que conforman la red de protección de datos en el territorio de la Unión y permiten, dentro de éste, su libertad de circulación.

La protección del Reglamento a los datos personales y la extraterritorialización en relación a la protección de un derecho humano se justifica por dos causas: En primer lugar, que los datos personales son susceptibles de ser digitalizados y, al hacerlo, abandonan toda ubicación geográfica para ser parte del ciberespacio; y es aquí donde entra en juego la segunda causa, que consiste en la pérdida de control de los interesados sobre sus datos personales y la utilización no consentida o no controlada de éstos por parte de terceros, que son susceptibles de causar una seria intromisión a la vida privada de su titular, así como también daños morales, a su honor, a su personalidad y perjuicios materiales. A este respecto, el derecho a la protección de los datos personales tiene una

particularidad con respecto al resto de derechos fundamentales, y es que el objeto protegido no sólo se puede desvincular del sujeto (lo que ocurre también en otros derechos, como el de propiedad) sino que puede también multiplicarse en dos sentidos: por un lado, cualitativamente (hemos visto a lo largo de esta tesis que existe un número casi ilimitado de datos personales: Los de identificación como el nombre, el número de identificación personal, el domicilio y números de teléfono, las preferencias personales que se marcan a través de la huella digital, los metadatos, que identifican nuestras localizaciones, los datos biométricos, los físicos y psicológicos y un largo etcétera) sino también cuantitativamente, ya que esos datos se pueden transmitir ilimitadamente sin que sus poseedores pierdan por ello su posesión. Por este motivo es fundamental que los interesados tengan control sobre los datos que generan.

Finalizaremos este apartado manifestando que el contenido que se ha otorgado en la Unión Europea a la protección de los datos personales tiene, en nuestra opinión, una particularidad única en tanto que derecho fundamental por cuanto los restantes derechos incluidos en el catálogo de la Carta de Niza tienen una dimensión marcadamente territorial y oficial: Sus beneficiarios o sujetos protegidos son, en general, los seres humanos mientras se encuentren en territorio europeo; y, en la mayoría de ellos, los sujetos destinatarios de las prohibiciones o, en algunos casos, de las políticas activas, son principalmente (aunque no únicamente) las autoridades, ya sean europeas, nacionales o locales.

En el caso de los datos personales, los sujetos pasivos o destinatarios de las prohibiciones son en igual medida las autoridades públicas como los sujetos privados; y el derecho de la Unión Europea aspira a que la protección continúe incluso cuando el tratamiento está sometido al derecho de un país tercero, lo que sucede en muy pocas ocasiones con el resto

de derechos y libertades fundamentales, ya que sólo excepcionalmente el derecho europeo continúa protegiendo la libertad, la vida, los derechos sociales, las libertades políticas, de los ciudadanos europeos una vez que han dejado el territorio de la Unión.

CONCLUSIONES

Siguiendo los objetivos que nos hemos fijado en la Introducción de este trabajo de investigación, expondremos a continuación las reflexiones que hemos podido extraer del análisis deductivo de las disposiciones que componen la parte general del derecho de protección de datos personales en Europa, así como de la doctrina y la documentación utilizados.

I. El derecho a la inviolabilidad del domicilio y de la correspondencia que aparecen desde hace siglos en textos jurídicos designan un espacio en el cual el individuo desarrolla su vida, sus pensamientos y sus comportamientos más íntimos que desea ocultar (entre muros o dentro de un sobre), a cubierto de los ojos del resto de la sociedad, ámbitos que se consideraban un valor jurídico merecedor de una protección especial. De esta idea nació a principios del siglo XX el derecho a la vida privada, tronco del cual surgiría posteriormente la rama del derecho a la protección de los datos personales, un derecho que constituye la reacción sociojurídica ante la amenaza contra distintos valores que conlleva la evolución de la informática, la conectividad y las tecnologías relacionadas con las comunicaciones.

   Por ello el derecho a la protección de datos personales está íntimamente ligado a la evolución de la informática y la tecnología porque, si bien la protección que otorga esta especialidad jurídica no se limita a los tratamientos realizados por estos medios,

los tratamientos llevados a cabo sólo por medios analógicos no tienen la misma capacidad de amenaza a los valores protegidos. En los últimos años se ha vinculado asimismo a la expansión de la conectividad. En cierta medida, el ataque o amenaza a los valores jurídicos por medio del tratamiento de los datos personales está posibilitado por la interacción entre espacio virtual y vida real, que permite que las operaciones que se realizan en el primero tengan efectos de distinta naturaleza en la segunda, efectos que constituyen una de las razones fundamentales de la necesidad de la protección de los datos personales.

Con esas premisas podemos concluir que, si los derechos y libertades fundamentales han surgido como una necesidad del individuo de poner un límite al poder del Estado, el derecho a la protección de los datos personales nace como la necesidad de las personas físicas de poner un límite al poder de la informática y de la capacidad y velocidad de las conexiones en red. El derecho a la protección de datos personales es un derecho de cuarta generación, de los calificados como derecho de las nuevas tecnologías o ciberderechos.

La realización de tratamientos de datos personales en el entorno virtual conlleva la pérdida o, al menos, el extremo debilitamiento del elemento territorial que está ínsito en el derecho tradicional, pues existen una gran cantidad de operaciones electrónicas, tecnológicas o virtuales que no es posible relacionar con una determinada ubicación, aunque puede haber elementos que tengan presencia en un determinado punto geográfico: Las personas, los medios, los interesados, los efectos de los tratamientos sobre la vida real, etc. Esta es la causa por la que muchas de las disposiciones de este derecho deban trascender el ámbito territorial de vigencia de un determinado ordenamiento jurídico para lograr que la protección sea

eficaz, ya que las normas que ignoren la desterritorialización del espacio virtual carecerían de efectividad al mismo momento de su aprobación. Entrando en una visión más profunda de este aspecto, pensamos que esta pérdida de importancia de la dimensión territorial en el ciberespacio conlleva también una pérdida de importancia del Estado y del ordenamiento jurídico estatal tradicional. El ciberespacio está dominado por distintas tendencias, como por ejemplo grandes multinacionales tecnológicas (Google, Microsoft, Amazon, etc.) que ejercen en él un verdadero monopolio e imponen sus principios e ideologías, pero también individuos, que se expresan y se comunican, creando movimientos, tendencias, corrientes de opinión y hasta creencias o convicciones. En este universo virtual, las viejas estructuras políticas han quedado desfasadas.

Con todo ello no queremos sostener que el sentido tradicional del territorio o espacio geográfico como elemento del Estado y como presupuesto de la vigencia de un determinado ordenamiento jurídico esté ausente en el ciberderecho sino que convive con la desterritorialización, por ello las normas que regulan las diversas disciplinas en este ámbito, de distinta naturaleza (nacional, comunitarias, internacionales, transnacionales y flexibles) contienen elementos que trascienden las fronteras del sistema del cual forman parte para no desproteger a los individuos.

Ya en la década de los ’70 del siglo pasado existía la preocupación por la trascendencia de los límites geográficos del derecho tradicional, motivo que inspiró el Convenio 108 del Consejo de Europa que, si bien surge como un intento de dar respuesta a esa preocupación, en nuestra opinión no logra ese objetivo debido su naturaleza de instrumento internacional, que presupone una aplicación eminentemente territorial de sus disposiciones. Por otra parte, las disposiciones de

este tipo de instrumentos son, necesariamente, de mínimos por las profundas diferencias que muchas veces existen entre los ordenamientos jurídicos de los Estados partes y que es necesario armonizar en un instrumento único.

Otra de las características del derecho a la protección de los datos personales y que inciden sobre su ámbito de vigencia (en este caso, material) viene dado por el hecho de que, como derecho fundamental que es y al igual que el resto de derechos y libertades, no es absoluto sino que tiene límites, los que deben ser especialmente ponderados al entrar en conflicto con otros derechos y libertades fundamentales.

II. A través de disposiciones específicas de los Tratados de la Unión Europea, los Estados miembros han delegado en las Instituciones la facultad de regular sobre la protección de los datos personales, que, además, está integrada con calidad de derecho fundamental en la Carta de Derechos y Libertades Fundamentales de la Unión, lo que otorga a las normas de protección de datos el estatus de derecho constitucional de la Unión Europea, con prevalencia sobre las normas internas de los Estados miembros. La mayor parte de estas disposiciones son de orden público europeo pues la protección que se otorga a los datos personales es indisponible para las partes en una relación de tratamiento, lo que no impide que se conceda a los interesados la facultad de dispensar esa protección, pero siempre en casos concretos y contando con una amplia información previa, a través de la figura del consentimiento.

A diferencia de otros derechos y libertades fundamentales que se atribuyen a la Unión Europea en virtud de la cláusula residual del art. 6 TUE, el derecho de

protección de datos personales es una competencia específica de las Instituciones atribuida en los arts. 39 TUE y 16 TFUE, en virtud de los cuales la Unión ha dictado normas generales sobre protección de datos personales y también normas específicas para determinados aspectos, todas ellas con primacía y aplicación directa en todos los Estados miembros. A través del análisis de esas distintas normas se evidencia que en ellas el legislador europeo se ha preocupado por dar a este derecho unos ámbitos de vigencia que no coinciden con los límites geográficos de la Unión; aunque es deseable que en el futuro desarrollo del derecho a la protección de datos personales, se trabaje para que esa vigencia se convierta en ámbito de influencia en el espacio virtual.

Las normas de protección de datos de la Unión Europea han tenido siempre dos objetivos principales, que son: Por un lado la protección de las personas físicas con respecto a los tratamientos de sus datos personales, como parte del espacio de libertad, seguridad y justicia que está entre los objetivos de la Unión; y por el otro, garantizar la libertad de circulación de esta categoría de datos, necesaria para la conformación del mercado interior.

La primera norma derivada que se dictó en el último lustro del siglo pasado para desarrollar el derecho a la protección de datos personales, la Directiva 95/46, era una norma limitada a la armonización del derecho de los Estados miembros y, como tal, sus contenidos (aunque completos según la jurisprudencia del TJUE) eran de mínimos. Esta norma, aunque avanzada y correcta para el momento en que fue aprobada, fue superada a los pocos años de su vigencia debido a la constante evolución de la tecnología. A pesar de ello, sus méritos se plasmaban, principalmente, en algunos de los aspectos regulados como su vigencia o ámbito de

aplicación, las autoridades nacionales y las transferencias internacionales, características que se mantuvieron en la normativa posterior, aunque con las adecuaciones que el progreso ha hecho necesarias. Pero ante todo destacamos de esta norma la creación del Grupo de Trabajo del Art. 29, que tuvo la capacidad de conducir la evolución de la interpretación y aplicación de la Directiva 95/46 de la forma más adaptada a la realidad social y tecnológica de cada momento de su vigencia.

La Directiva 95/46 era la disposición general sobre protección de datos personales en el territorio de la Unión y junto a ella han existido otras que, antes como ahora, rigen en aspectos específicos como son los tratamientos realizados por las Instituciones, órganos y organismos de la Unión y los realizados en el ámbito de las comunicaciones electrónicas, que continúan la línea de la norma general, con las adaptaciones que se hacen necesarias en razón del ámbito de aplicación.

Uno de los derechos subjetivos con los que la protección de datos presenta mayor conflictividad (y sin duda presentará aún más en el futuro) es el derecho a la confidencialidad de las comunicaciones, muestra de ello es que en derecho europeo la conciliación entre ambos derechos fundamentales se regula mediante una norma específica (que actualmente es la Directiva 2002/58 que será próximamente reemplazada por un Reglamento que se encuentra en etapa de aprobación parlamentaria), y no por artículos del RGPD como ocurre con otros derechos que hemos analizado en el apartado 6 del Capítulo III.

III. Para actualizar la normativa europea sobre protección de datos personales y adecuarla al progreso de la tecnología, la Comisión y el Parlamento europeos han aprobado en abril de 2016 el Reglamento General de Protección de Datos personales, que entró en vigor en mayo de 2018, así como otras normas (algunas de las cuales fueron aprobadas en el mismo acto y otras con posterioridad) que siguen sus líneas generales.

Pensamos que, aunque no se menciona explícitamente, la totalidad del RGPD constituye una ponderación y balance entre la libertad de empresa (entendida en su sentido más amplio) y la protección de datos personales ya que los tratamientos de este tipo de información se llevan a cabo en su práctica totalidad por empresas, que los necesitan para desarrollar y expandir su actividad económica. Pues la libertad de empresa, como toda libertad fundamental, es susceptible de ser restringida especialmente cuando entra en colisión con otro derecho. Dada la necesidad de que dichos límites sean explícitos y motivados, el RGPD se erige como un conjunto de límites a la libertad de empresa para la protección de los datos personales. Así, en nuestra interpretación el RGPD presupone que, con respecto a los datos que identifican a las personas físicas, las empresas tienen una libertad de actuación que, si no se limita, es susceptible de causarles diversos daños a través de la manipulación de los mencionados datos. Empresas que, además de adquirir preponderancia frente a la administración pública de protección de datos personales, son las beneficiarias de la libertad de circulación de éstos, libertad que se erige hoy en día en la quinta libertad básica de la Unión, junto a las de circulación de personas, mercancías, capitales y servicios.

Como consecuencia de las características de la protección de los datos personales, para definir la vigencia material y territorial de sus disposiciones, algunos de los elementos que forman parte del derecho positivo tal como lo conocemos tradicionalmente no pueden ser aplicados de forma directa sino que es necesario redefinirlos, lo que en el derecho tradicional se podría interpretar como pérdida de seguridad jurídica pero que en el ámbito tecnológico debe tener otra lectura: El derecho digital exige términos y definiciones abiertos, inciertos e incluso ambiguos, al menos en esta etapa de su evolución, pues es posible que en el futuro se creen nuevas formas de regulación o de intervención en las relaciones humanas que se desarrollan en el espacio virtual, que permitan definiciones más concretas o, por el contrario, que se llegue a una reformulación del concepto de seguridad jurídica. Esa necesidad que hemos apuntado de que las normas que regulan materias relacionadas con la tecnología contengan elementos abiertos o indeterminados se debe a la constante evolución en que se encuentra este ámbito, en virtud de la cual estas normas deben tener la capacidad de poder abarcar la futura aparición de nuevos medios, técnicas de tratamiento y formas de procesamiento de la información que se creen en el futuro, que en la actualidad son inimaginables. Podemos poner como un ejemplo de la referida amplitud el concepto de datos personales a los efectos de la protección, que abarca información que en apariencia no es identificativa de una persona o que, al menos, no lo es fuera del ámbito tecnológico y que sin embargo es considerada un dato personal, como la dirección IP variable.

En ese orden de ideas, uno de los desafíos más complicados a los que se enfrenta el legislador al momento de regular la protección de datos personales (al igual que ocurre en muchas otras materias del derecho digital) es la definición de su ámbito

de vigencia, especialmente en lo que atañe al ámbito geográfico pues en este aspecto no es posible ceñirse al derecho tradicional y a su aplicación dentro de los límites territoriales del órgano legislativo que lo dicta. En este aspecto el derecho de protección de datos personales se aproxima a una característica del derecho internacional privado: En ambos, las normas definen con precisión un ámbito material de vigencia pero no uno territorial sino que seleccionan uno o más elementos de las relaciones jurídicas que constituyen su ámbito de aplicación material, que serán el nexo de conexión que remitirá al derecho material aplicable. Al respecto, el RGPD contiene un ámbito material de vigencia y un "ámbito territorial" que, a pesar de la terminología utilizada por el art. 3 RGPD (y que continuaremos utilizando aunque disentimos con la misma), no es un verdadero ámbito territorial pues se limita a seleccionar dos elementos vinculados con el responsable o el encargado, de los cuales uno es la existencia de un establecimiento, elemento que sí le otorga una conexión territorial con la Unión; pero el verdadero elemento de conexión con el derecho de la UE es el otro elemento (el contexto de sus actividades), cuya abstracción e indeterminación lo sustraen a toda ubicación geográfica. Lo interesante de esta solución y lo que le da efectividad, es que el primero de estos elementos es el que relaciona el caso geográficamente con el derecho de la Unión y establece su aplicación, pero este elemento no está necesariamente relacionado con el segundo, en el sentido de que el "contexto" en el cual se realice el tratamiento puede ser sumamente débil, como lo ha declarado el TJUE en la sentencia Google Spain. Por ello para interpretar en cada caso esos dos elementos y concretar mejor su relación con los tratamientos a los efectos de la aplicación del derecho europeo es necesaria la actividad de las APD y de los

órganos judiciales, entre otros efectos para evitar ampliar o reducir en exceso su campo de vigencia. Pues puede ser necesario decidir sobre tratamientos de datos cuya única relación con el derecho de la Unión es que se realicen en el contexto de las actividades de una empresa que tenga uno o más establecimientos en su territorio, aunque sus efectos en la vida real deban producirse exclusivamente fuera del mismo. A su vez, en la teoría no se puede descartar lo contrario: Que existan tratamientos que tengan una relación importante con el derecho o el territorio de la Unión, o efectos reales sobre personas que se encuentren en la Unión y que sin embargo no se realicen en el contexto de las actividades de ningún establecimiento en la Unión ni se encuentren abarcados por las disposiciones del art. 3.2 RGPD. Esta es una muestra más de la característica del ciberderecho a que hemos hecho referencia precedentemente, de necesitar términos abstractos o indeterminados y también de la particularidad de que tiene como objeto relaciones "virtuales" y no siempre "reales".

Por el contrario, las excepciones o normas especiales de aplicación del RGPD (establecidas en el art. 3.2 RGPD) sí presentan una conexión territorial clara con la Unión: Debe ser el lugar donde se encuentren las personas a quienes se ofrezcan los productos o servicios o que desarrollen el comportamiento controlado.

En los términos en que el RGPD concibe su aplicación territorial, los artículos 3.2 y 27 RGPD extienden la vigencia de esta norma fuera de las fronteras de la Unión, es decir a responsables o encargados que no cuentan con establecimientos en el territorio de ésta, siendo normas cuya aplicación y, en particular, su ejecutividad depende de distintas variables, entre las cuales se encuentra en primer lugar el hecho de que hayan designado representante en la Unión o no. En el último caso, es decir

si no han designado representante, no existirá una APD principal y sólo podrá resultar competente para entender en el asunto la autoridad ante la cual se haya presentado una queja o reclamación y aquélla en cuyo estado de designación se encuentren afectados por el tratamiento. Sin embargo, en cualquiera de estos casos, no existe norma alguna que extienda la competencia de las APD hasta el país tercero donde se encuentre el encargado o responsable que realice tratamientos relacionados con la oferta de bienes y servicios a destinatarios en la Unión o el control del comportamiento de las personas que se hallen en su territorio.

En el primero de los casos, es decir cuando hayan designado representante, la exigencia de responsabilidad a través de éste dependerá en primer lugar de la naturaleza y de la fuente de esa relación pues si ésta es meramente representativa, puede no ser suficiente para la exigibilidad de responsabilidad.

Por todo ello, en ambos casos, en cuestiones tales como la obligación de obedecer las órdenes de las APD con respecto al tratamiento, la imposición de medidas sancionadoras, los incumplimientos o los daños y perjuicios (entre muchas otras) y, especialmente, si para exigir la responsabilidad es necesario acudir a la vía judicial, se plantean cuestiones relativas al derecho aplicable, el órgano judicial competente y la posible ejecución de una decisión judicial extranjera, en las cuales entran en juego un gran número de normas que pueden ser de derecho internacional o transnacional y cuyo resultado desde la óptica del ordenamiento jurídico del país tercero al que está sometido el tratamiento puede no concluir en la aplicación del RGPD. Para que actúen con mayor eficacia, sería necesario dotar a las autoridades de protección de datos de herramientas tecnológicas efectivas para poder adoptar decisiones con respecto al tratamiento y ejecutarlas en el espacio virtual, cuando

sus resoluciones no se puedan hacer cumplir por los agentes que en ellos intervienen, como por ejemplo programas informáticos específicos para detectar los tratamientos ilegítimos de datos personales.

Ahora bien, la vigencia del derecho europeo de protección de datos se refiere no sólo a su ámbito geográfico sino también al ámbito material, contexto en el cual se interrelaciona con otros derechos y bienes jurídicos a los que en ocasiones se opone, como es el caso de la libertad de expresión y de información, la transparencia de la administración pública, el interés de la sociedad por la investigación y por la estadística, la obligación de secreto que tienen determinadas profesiones, o la confidencialidad de las comunicaciones electrónicas. Situaciones para las cuales el RGPD contiene el principio general para su resolución, si bien las autoridades de aplicación de esta norma deberán valorar, en cada caso que se presente, los intereses en juego y, en base a ellos, cuál es la solución más equitativa aplicando el principio general establecido en el RGPD. Ello es así pues la persona física no se protege frente a cualquier tratamiento sino, preponderantemente, frente a aquéllos que no están motivados por un interés social de mayor valor. Podemos sostener que la protección, dentro de los límites fijados por el RGPD, es absoluta cuando la motivación del tratamiento es el interés del responsable o del encargado; pero cede en muchos casos en que existe un interés social en la realización del tratamiento, lo que ocurre en la mayoría de los casos en que el Capítulo IX RGPD establece limitaciones para los tratamientos que se realizan en los ámbitos materiales específicos que hemos enumerado.

IV. En cuanto al derecho español de protección de datos personales, el hecho de que la Constitución se haya dictado en la segunda mitad de la década de 1970, cuando la informática ya había comenzado su fase de expansión, ha posibilitado la inclusión entre su articulado de una disposición genérica de protección del ser humano frente al uso de la informática, que se inserta en el artículo 18 de la Constitución, junto a las garantías para el derecho al honor, a la intimidad personal y familiar, a la propia imagen, a la inviolabilidad del domicilio y al secreto de las comunicaciones, garantías todas para cuya protección es imprescindible regular el uso de la informática.

Con respecto a la inviolabilidad del domicilio queremos expresar nuestra opinión personal a favor de la aplicación analógica de esta garantía al entorno digital, pues así como dentro del ámbito del domicilio familiar las personas físicas guardan su vida más íntima, de la misma forma en los dispositivos informáticos (ordenadores, tablets, teléfonos móviles así como, recientemente, los altavoces y televisores inteligentes) el ser humano guarda toda sus datos, detalles y, en definitiva, su vida más íntima, aunque a diferencia del domicilio que guarda la privacidad familiar, algunos de los dispositivos son personalísimos (evidentemente, es lo que sucede con el teléfono móvil) y, por lo tanto, su inviolabilidad se debe proteger no sólo frente a terceros sino también frente los miembros de la familia.

Regresando a la ubicación de la protección de la persona frente al uso de la informática en la CE, la LOPD continúa en esa línea al establecer la protección de datos personales como medio para la tutela de la intimidad y del honor.

En lo relativo al ámbito de aplicación geográfico del derecho nacional de protección de datos personales, al formar parte de un ordenamiento jurídico estatal, este tipo de normas tiene vigencia, como todas las demás, en el territorio del Estado que las ha dictado. Partiendo de esa base, tanto la anterior LOPD como la actual LO 3/18 secundan al derecho europeo en lo relativo a las disposiciones sobre su vigencia, por lo que son aplicables todos los comentarios realizados en relación con éste.

La LOPD, al igual que la Directiva 95/46, era una norma correcta y de mínimos, que otorgaba una protección deficiente ante todo con la aceptación del consentimiento implícito y condicionado que significó en la práctica (en especial en relación con los sitios web y las aplicaciones informáticas) que se imponía en todos los ámbitos y no sólo para los datos necesarios para el servicio o producto contratado sino como una verdadera intromisión en esa esfera privada que hemos comparado con el domicilio, para acceder y tratar todos los datos, sin ningún tipo de límites.

Otra de las deficiencias con que contaba la LOPD (a causa del modelo instaurado por la Directiva 95/46) era la centralización de la actividad de la autoridad de protección de datos en el sistema de registro de bases de datos y las aprobaciones o autorizaciones, que imponía a éstas una gran carga administrativa para verificar que los responsables cumplieran con los requisitos necesarios para los tratamientos, es decir que se volcaba en los tratamientos que sí cumplían los requisitos y no, como es deseable, en prevenir e impedir los incumplimientos.

En cuanto a su vigencia material, tanto la LO 3/18 como el RGPD están diseñados como normas generales pues los tratamientos de datos personales se realizan en una

gran diversidad de campos y ámbitos específicos que en principio deberían estar regulados por una normativa específica, sin perjuicio de lo cual la LO 3/18 extiende su propia vigencia y la del RGPD a la mayoría de esos campos, al menos hasta la aprobación de las normas especiales, lo que consideramos que no es incorrecto si se convierte en una medida definitiva por lo que es necesario que en un tiempo prudencial se proceda a la aprobación de las normas especiales.

En un intento por corregir, aunque sea parcialmente, la deficiencia que el RGPD presenta con respecto a los responsables y encargados sin establecimiento en la Unión que realizan los tratamientos establecidos en el art. 3.2., la LO 3/18 en su art. 30 atribuye a la AEPD o a las autoridades autonómicas la facultad de imponer medidas sancionadoras al representante, disposición que, además de no dar una solución eficaz al problema dado que la posibilidad de hacer efectivas esas medidas dependerá de la naturaleza de la relación entre el responsable o encargado y su representante, por su rigurosidad para con éste dificultará que las empresas no establecidas en la Unión designen un representante en España para cumplir con el RGPD.

Para finalizar con el análisis de la normativa nacional, destacamos la solución que esta norma establece para otra consecuencia de las relaciones en el ámbito tecnológico: Que la "vida virtual" continúe incluso una vez que se haya extinguido la "vida real" de una persona, situación que aborda con acierto la LO 3/18 al regular las consecuencias póstumas de la actividad de las personas en el ciberespacio, aunque sus disposiciones sean ciertamente mejorables.

V. De las autoridades europeas con competencias en la protección de datos resaltamos nuevamente, como ya lo hemos hecho en el texto de esta tesis, la actividad del Grupo de Trabajo del Art. 29, hoy Comité Europeo de Protección de Datos, muchos de cuyos documentos hemos utilizado en esta investigación. Tal es la importancia de este órgano para la interpretación, homogeneización, aplicación y adaptación a la realidad del derecho europeo de protección de datos, que tenemos la certeza de que ni éste ni el RGPD tendrían su conformación actual sin la actividad del CEPD. Esta importancia no sólo le viene dada por su propia actuación sino también por la relación de retroalimentación que mantiene con las autoridades nacionales de protección de datos, que lo conforman y paralelamente se nutren de su trabajo.

Y, a pesar de que los documentos elaborados por el SEPD han sido utilizados en esta tesis en menor medida que los del CEPD (debido principalmente a que su ámbito de competencia es más específico), este órgano ha desarrollado asimismo una labor de interpretación y aplicación del derecho europeo de protección de datos con unos contenidos y calidades de igual valor que los del CEPD, que constituyen otra fuente secundaria pero fundamental para el derecho europeo de protección de datos personales.

Respecto de las autoridades nacionales de protección de datos, independientemente de que su ámbito de competencia de esté, en principio, reducido a los límites geográficos del Estado de designación, la libertad de circulación de bienes, personas, capitales, servicios y datos en el territorio de la Unión hace necesario que estas autoridades, órganos fundamentales para el apropiado resguardo de este derecho, estén en constante interacción entre ellas, interacción que el RGPD establece en un conjunto de normas sumamente complicadas que tienen como

objetivo superar los límites territoriales rígidos que emanan de su creación y establecimiento por cada Estado miembro pero, además, se presuponen en todas las normas sobre actuación coordinada.

Para hacer posible esa interacción se ha seleccionado un elemento de base territorial (el establecimiento del responsable que se erija como principal a los efectos del tratamiento) que permite determinar a la autoridad principal, que será la autoridad designada para ese responsable, con algunas excepciones (autoridades interesadas y autoridades interesadas competentes).

Las disposiciones correspondientes a la interacción entre las distintas APD son de una complejidad excesiva debido a que a través de ellas se intenta trascender la base estrictamente territorial de su creación y regulación, para dar respuesta a la libre circulación de datos personales en el territorio de la Unión y a la vez a la protección de las personas con respecto a los tratamientos ilegítimos de aquéllos. Complejidad que se evidencia aún más en la necesidad de establecer normas que permitan el ejercicio del derecho de acceso a la justicia (fundamentado asimismo en criterios territoriales que en ocasiones resultan distintos de los de designación de la autoridad competente), tanto en general como para la impugnación de sus decisiones.

Si bien apreciamos enormemente el esfuerzo demostrado por los distintos actores que han intervenido en la redacción de las normas europeas, estimamos necesario, para resolver las cuestiones territoriales de esta índole, un enfoque nuevo que supere definitivamente los límites nacionales y establezca reglas de actuación realmente flexibles y transnacionales. Por ello el RGPD debería haber abierto la puerta hacia la utilización de herramientas tecnológicas, para la conexión y actuación coordinada

de estas autoridades así como para su actuación individual dentro de los límites de su Estado de designación y para el ejercicio de los derechos de interesados, responsables y encargados, que les permitan ejercer su actividad en un entorno tecnológico y conectado, ya que los poderes, funciones y competencias que el RGPD pone a cargo de las APD están, a nuestro entender, excesivamente dirigidos hacia la actividad de responsables y encargados en el plano físico y se ignora su actividad virtual. Se las podría dotar, por ejemplo, de programas informáticos específicos para la detección de datos personales y de incumplimientos del RGPD, o incluso de poderes para detectar, investigar y actuar en páginas web o en la realización de tratamientos clandestinos de datos personales en el ciberespacio, siempre recabando el auxilio de las fuerzas y cuerpos de seguridad y la autorización judicial si fuera necesario. En este sentido, se podrían adaptar herramientas similares a las cookies o programas espías, que permiten el control de la actividad de los internautas para ofrecer la posibilidad de "vigilar" que los tratamientos a que son sometidos los datos de determinados registros sean legítimos.

Hemos manifestado en el Capítulo II, apartado 1) de esta tesis que la Unión Europea no tiene competencias para legislar en materia penal sino sólo para armonizar las legislaciones de los Estados miembros, tarea que por su naturaleza debe ejercitarse a través de Directivas y no de Reglamentos, por ello el RGPD no puede contar con disposiciones de contenido penal, lo que consideramos una carencia de esta norma ya que la protección de datos personales se vería reforzada y los valores correctamente protegidos con el refuerzo que implicaría la tipificación de algunas de las conductas declaradas ilícitas por el RGPD. Por otra parte, la

homogeneización pretendida por la Unión se vería más completa al contar con ese refuerzo cualitativo.

VI. La normativa general y especial sobre datos personales de la Unión ha tenido como uno de sus objetivos principales la regulación de las *transferencias de datos personales* hacia países terceros u organizaciones internacionales, con la finalidad de que los datos conserven el alto nivel de protección que adquieren al estar regulados por el derecho europeo, aún cuando entren bajo el ámbito de aplicación del derecho de un país tercero o de una organización internacional. operaciones por medio de las cuales los datos se conectan con un elemento que los pone bajo la vigencia de un ordenamiento jurídico distinto al de la Unión. El mantenimiento de la protección es imperativo para evitar el fraude de ley pues de otro modo, con la facilidad que otorga hoy en día la tecnología sería sumamente sencillo sustraerlos de la protección brindada por el derecho de la Unión a pesar de que, conforme a lo dispuesto por éste, el mencionado tratamiento esté más vinculado a él que al del país tercero.

En el derecho que hemos calificado de tradicional, la protección garantizada a los bienes jurídicos tiene un fundamento que, si no está directamente relacionado con el territorio (la ubicación del titular de esos bienes o las cosas u objetos que los representan), lo están de manera indirecta: La nacionalidad, residencia habitual, lugar de ejecución o donde se materializan sus consecuencias. En el derecho de protección de datos hemos visto que el fundamento que conecta a los bienes protegidos con el derecho de la Unión es difuso: El contexto de las actividades de

un establecimiento ubicado en su territorio. Pero una vez que los datos adquieren la protección en base a ese fundamento, ese mismo hecho de haber adquirido protección por el derecho europeo se vuelve el fundamento de que la protección no se pierda aunque se pierda esa conexión difusa. Podríamos decir entonces que el fundamento cambia ya que una vez que los datos adquieren la protección brindada por el derecho de la Unión ya no se desprenden de ella aunque desaparezca la conexión con éste, si bien la protección puede no ser la misma que otorgaba el derecho de la Unión sino distinta y, a su vez, diferente a la que el país tercero brinda a los datos regulados por su derecho, como sucede en el caso de los datos amparados por el Privacy Shield. Puede asimismo estar otorgada por la voluntad de una o todas las partes, como ocurre con las soluciones de soft law.

El término *transferencias* que el derecho de la Unión utiliza para denominar a este tipo de tratamientos u operaciones adquiere en la protección de datos personales un sentido propio, que se diferencia levemente de otros ámbitos a los que se aplica esta palabra ya que hay situaciones en las que no se aplicaría el término transferencia en su sentido común o financiero y, por el contrario, sí constituyen una transferencia en el sentido de la protección de datos y viceversa. Es un término que a estos efectos se vuelve flexible y abierto para abarcar nuevas realidades creadas por la tecnología, como lo son que no haya movimiento de datos o que éstos no dejen de estar sometidos a la voluntad del responsable o encargado que los *transfiere*.

Para continuar esa protección el derecho europeo confía, en primer lugar, en la evaluación del ordenamiento jurídico tercero que realiza la Comisión, por medio del cual certifica que el mismo ofrece un nivel de protección equivalente y, por lo tanto, los datos personales se pueden poner bajo su vigencia sin más exigencias.

Para las transferencias realizadas a los países cuyo ordenamiento jurídico no ha sido evaluado favorablemente por la Comisión se adoptan otras soluciones que en su mayor parte constituyen soft law o soluciones contractuales que conforman un entorno jurídico suficientemente protector para garantizar a los interesados.

A pesar de esa intención manifiesta que motiva la regulación de las transferencias internacionales de datos personales, en el caso de las realizadas hacia los Estados Unidos existen otros intereses que han motivado el diseño de una solución jurídica que justifique la legalidad de las transferencias a este país, aunque la protección que otorga su ordenamiento jurídico no tiene el nivel requerido por el derecho europeo, tal como lo ha constatado el TJUE en su sentencia *Schrems*, mediante la cual se declaró la nulidad del sistema de Puerto Seguro, que ha sido posteriormente reemplazado por los acuerdos del Escudo de Privacidad, sistema que no rectifica las carencias del derecho estadounidense que motivaron la declaración de nulidad del anterior, pese a lo cual el CEPD lo considera válido.

Los esfuerzos del legislador europeo para mantener la protección en las transferencias internacionales de datos personales no han sido suficientes para lograr una protección cabal ya que no podemos olvidar que la tecnología brinda recursos para evitar que las autoridades o los interesados ejerzan control sobre algunos tratamientos de datos personales, que pueden realizarse en la clandestinidad de las redes privadas u ocultas e incluso estar protegidos por la confidencialidad de las comunicaciones. Por ello nos hemos manifestado a favor de una norma europea que armonice la tipificación de los delitos y las penas relacionadas con los tratamientos ilegítimos de datos personales ya que el RGPD y la normativa específica sólo pueden regular los tratamientos que son evidentes, transparentes o

manifiestos, pero no los clandestinos, de los que podemos citar como el ejemplo más claro el de acceso ilícito a los datos, que puede realizarse por medio de un delito.

BIBLIOGRAFÍA

1. ABBOT, C: "Bridging the Gap – Non-state Actors and the Challenges of Regulating New Technology." Journal of Law and Society. Vol. 39, nº 3 (2012): Pp. 329-358. doi:10.1111/j.1467-6478.2012.00588.x.

2. AGUADO RENEDO, C: "La protección de los datos personales ante el Tribunal Constitucional español." Cuestiones constitucionales: revista mexicana de derecho constitucional. Nº 23 (2010).

3. ALDECOA LUZÁRRAGA, F.; GUINEA LLORENTE, M. y col: *La Europa que viene: el Tratado de Lisboa.* 2ª ed. Ed. Marcial Pons, Madrid: 2010.

4. ALLEN, J.; HALLENE, A: "Protecting your data in cyberspace." American Journal of Family Law. Vol. 27, nº 3 (2013): Pp. 198.

5. ÁLVAREZ RUBIO, J.J: "El Tratado de Lisboa y la plena comunitarización del espacio de libertad, seguridad y justicia." Revista electrónica de estudios internacionales. no. 15 (2008).

6. ANARTE BORRALLO, E.: "Sobre los límites de la protección penal de datos personales." Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento. Nº 2 (2002): Pp. 225-254.

7. ANDERSON, G.W.: "Beyond ‘Constitutionalism Beyond the State’." Journal of Law and Society. Vol. 39, nº 3 (2012): Pp. 359-383. doi:10.1111/j.1467-6478.2012.00589.x.

8. ANDORNO, R.: "Universalidad de los derechos humanos y derecho natural." Persona y Derecho. Vol. 38, nº 38 (1998): Pp. 35-50.

9. ANGULO SÁNCHEZ, N.: "El derecho al desarrollo en el 60 aniversario de la Declaración Universal de los Derechos Humanos: Estado de la cuestión." Nómadas. Nº 22 (2009).

10. APARICIO ALDANA, R.K.; MARTÍNEZ PUJALTE, A.L. and SEMPERE NAVARRO, A.V.: *Derecho a la intimidad y a la propia imagen en las relaciones jurídico laborales.* Vol. 822. Ed. Aranzadi, Pamplona: 2016.

11. ARANGO, R.; ALEXY, R.: *El concepto de derechos sociales fundamentales.* Ed. Legis Bogotá, 2005.

12. RENAS RAMIRO, M.; PIÑAR MAÑAS, J.L.: *El derecho fundamental a la protección de datos personales en Europa*. Ed. Tirant lo Blanch, Valencia: 2006.

13. AZPITARTE SÁNCHEZ, M. : "Del derecho constitucional común europeo a la Constitución europea." Teoría y realidad constitucional *(16).* (2005).

14. BAHR, A.; SCHLÜNDER, I.: "Code of practice on secondary use of medical data in European scientific research projects." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 279-291.

15. BALAGUER CALLEJÓN, M.L.: *Lecciones de Derecho Constitucional.* 1st ed. Ed. Servicio de Publicaciones y Divulgación Científica de la Universidad de Málaga, Málaga: 2015.

16. BARIATTI, S.: *Cases and materials on EU private international law.* Vol. 4. Ed. Hart, Oxford [etc.]: 2011.

17. BELANDRO, R.S.: "La regla de conflicto y la definición de los puntos de conexión." Revista de la Facultad de Derecho. Nº 32 (2013): Pp. 291-323.

18. BENEYTO PÉREZ, J.M.; MAILLO GONZÁLEZ-ORÚS, J. *et al.*: *Tratado de Derecho y Políticas de la Unión Europea.* Ed. Aranzadi, Cizur Menor: 2009.

19. BERGEL, S.D.: "Diez años de la Declaración Universal sobre Bioética y Derechos Humanos." Revista Bioética. Vol. 23, nº 3 (2015).

20. BEUCHOT, M.: "La ley natural como fundamentación filosófica de los derechos humanos: Hermenéutica analógica y ontología." Veritas. Nº 25 (09-01, 2011): Pp. 27-37.

21. BIRNSTILL, P.; BRETTHAUER, S. *et al.*: "Privacy-preserving surveillance: an interdisciplinary approach." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 298-308.

22. BLUME, P.: "An alternative model for data protection law: changing the roles of controller and processor." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 292-297.

23. BOBBIO, N.: *Teoría general del derecho.* Ed. Temis, Bogotá: 1997.

24. BOEHME-NEßLER, V.: "Privacy: a matter of democracy. Why democracy needs privacy and data protection." International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 222-229.

25. BOGGIANO, A.: *Derecho Internacional Privado.* 6th ed. Ed. Abeledo Perrot, Buenos Aires: 2011.

26. BRKAN, M.: "Data protection and European private international law: observing a bull in a China shop." *International Data Privacy Law.* Vol. 5, nº 4 (2015): Pp. 257-278. doi:10.1093/idpl/ipv022.

27. BROWNLIE, I.: *Principles of public international law.* 6th ed. Ed. Oxford University Press, Oxford: 2003.

28. BUSTAMANTE DONÁS, J.: "La cuarta generación de derechos humanos en las redes digitales." TELOS. Revista de pensamiento sobre Comunicación, Tecnología y Sociedad. Vol. 85, (Octubre - Diciembre 2010, 2010).

29. BUSTAMANTE DONÁS, J.: "Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica." *Revista Iberoamericana de Ciencia, Tecnología y Sociedad.* Vol. 1, (Septiembre - Diciembre, 2001).

30. BUSTAMANTE DONÁS, J.: "Los nuevos derechos humanos: gobierno electrónico e informática comunitaria." Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento. Vol. Año 4, Nº 2 (Mayo-Agosto 2007, 2007): Pp. 13-27.

31. CAFAGGI, F.: "New Foundations of Transnational Private Regulation." Journal of Law and Society. Vol. 38, nº 1 (2011): Pp. 20-49. doi:10.1111/j.1467-6478.2011.00533.x.

32. CARLÓN RUIZ, M.: *Competencia territorial y responsabilidad extracontractual: perspectivas constitucional y comunitaria.* Ed. CEDECS, Barcelona: 1995.

33. CARRASCOSA GONZÁLEZ, J.: *Conflicto de leyes y teoría económica.* Vol. 20. Ed. Colex, Madrid: 2011.

34. CARRILLO SALCEDO, J.A.: *Dignidad frente a barbarie: la Declaración Universal de Derechos Humanos cincuenta años después.* Ed. Trotta, Madrid: 1999.

35. CASTAÑO, A.: "La conducta como elemento configurador en el concepto de derecho. Su ámbito de aplicación como el primer analogado en la filosofía práctica." Díkaion: revista de actualidad jurídica. Vol. 20, nº 2 (2011): Pp. 327-346.

36. CASTELLANOS RUIZ, E.: "Las normas de Derecho Internacional Privado sobre consumidores en la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico." *Cuadernos de derecho transnacional.* Vol. 1, no. 2 (2009): Pp. 134-159.

37. CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL (España): *El ciberespacio: nuevo escenario de confrontación.* Vol. 126. Ed. Ministerio de Defensa. Secretaría General Técnica, Madrid: 2012.

38. CHERTOFF, M: “A public policy perspective of the Dark Web”. Journal of Cyber Policy, Volume 2, 2017, Issue 1.

39. CONDE ORTIZ, C.: *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad.* Ed. Dykinson, Madrid: 2005.

40. CONSEIL D'ÉTAT: "Le droit souple". *Les rapports du Conseil d'État*, 2013. En línea: http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Etude-annuelle-2013-Le-droit-souple (último acceso 18/11/2018).

41. CORNISH, P.: "Governing Cyberspace through Constructive Ambiguity." Survival. Vol. 57, nº 3 (2015): Pp. 153-176. doi:10.1080/00396338.2015.1046230.

42. CUEVA GONZÁLEZ-COTERA, J.d.l.: "Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido." IDP: revista de Internet, derecho y política = revista d'Internet, dret i política. Nº 13 (2012): Pp. 84-90.

43. CURTIN, D.M.; SENDEN, L.A.J.: "Public Accountability of Transnational Private Regulation: Chimera or Reality?" Journal of law and society. Vol. 38, no. 1 (2011): Pp. 163-188. doi:10.1111/j.1467-6478.2011.00539.x.

44. DAN JERKER B Svantesson: "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation." *International Data Privacy Law.* Vol. 5, no. 4 (Nov 2015, 2015): Pp. 226-234.

45. DE HERT, P.; CZERNIAWSKI, M.: "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context." International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 230-243.

46. DÍEZ HOCHLEITNER, J.: *Ultimas tendencias en la jurisprudencia del Tribunal de Justicia de la Unión Europea: Recent trends in the case law of the Court of Justice of the European Union (2008-2011).* 1ª ed. Ed. La Ley, Las Rozas, Madrid: 2012.

47. DOCKSEY, C.: "Four fundamental rights: finding the balance." International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 195-209.

48. ERDOS, D.: "European Union data protection law and media expression: Fundamentally off balance". International & Comparative law quarterly. Vol. 65, nº 1 (2016): Pp. 139-183. doi:10.1017/S0020589315000512.

49. ESPINAR VICENTE, J.M.: "Teoría general del derecho internacional privado" Monografías de Derecho Internacional Privado Volumen I. Universidad de Alcalá, 2001.

50. ESPLUGUES MOTA, C.A.; IGLESIAS, J.L. y PALAO MORENO, G.: *Application of foreign law.* Ed. Sellier, Munich: 2011.

51. FARMER, L.: "Territorial jurisdiction and criminalization." University of Toronto Law Journal. Vol. 63, nº 2 (2013): Pp. 225-246. doi:10.3138/utlj.1117-3.

52. FAYOS GARDÓ, A.; CONDE COLMENERO, P.: *Los derechos a la intimidad y a la privacidad en el siglo XXI.* Ed. Dykinson, S.L, Madrid: 2014.

53. FERNÁNDEZ ARRIBAS, G.: *Las capacidades de la Unión europea como sujeto de Derecho Internacional.* Ed. Educatori, Granada: 2010.

54. FERNÁNDEZ NAVARRETE, D.; FERNÁNDEZ EGEA, R.M. and BARÓN CRESPO, E.: *Historia de la Unión Europea: España como estado miembro.* Ed. Delta, Madrid: 2010.

55. FERNÁNDEZ OGALLAR, B.: *El derecho penal armonizado de la Unión Europea.* Ed. Dykinson, Madrid: 2014.

56. FLORIDI, L: *The ethics of information*. Oxford University Press, Oxford, 2013.

57. FLORIDI, L: *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press, Oxford, 2014.

58. GARCÍA GONZÁLEZ, A.: "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado." Boletín Mexicano de Derecho Comparado. Nº 120 (2007): Pp. 743-778.

59. GARCÍA GONZÁLEZ, A.: "Reflexiones en torno a la protección de los datos personales en Internet y las redes sociales: retos y perspectivas en un mundo hiperconectado." Derecho Comparado de la Información. Nº 21 (2013): Pp. 2-20.

60. GARCIA LOPEZ, J.: "Derechos naturales y derechos humanos." Persona y Derecho. Vol. 4, nº 4 (1977): Pp. 407-424.

61. GARCÍA ROCA, F.J.; SANTOLAYA MACHETTI, P. and AGUILERA VAQUÉS, M.: *La Europa de los Derechos: el Convenio Europeo de Derechos Humanos.* Ed. Centro de Estudios Políticos y Constitucionales, Madrid: 2005.

62. GARCÍA SANZ, R.M.: "Redes sociales online: fuentes de acceso público o ficheros de datos personales privados: aplicación de las directivas de protección de

datos y privacidad en las comunicaciones electrónicas." Revista de Derecho Político. Nº 81 (2011). doi:10.5944/rdp.81.2011.9151.

63. GARCIMARTÍN ALFÉREZ, F.J.: *Sobre la norma de conflicto y su aplicación judicial: cinco cuestiones clásicas.* Ed. Tecnos, Madrid: 1994.

64. GARRIDO LÓPEZ, M.I: *El soft law como fuente del derecho extranacional*. Dykinson, Madrid, 2017.

65. GERALDES DA CUNHA LOPES, T.M.: "El derecho a la intimidad y a la protección de datos en la era de la seguridad global. Principios constitucionales versus riesgos tecnológicos." Anuario Jurídico y Económico Escurialense. Vol. XLVIII, (2015): Pp. 159-180.

66. GÓMEZ ISA, F.: *La declaración universal de derechos humanos en su cincuenta aniversario: un estudio interdisciplinar.* Vol. 1. Ed. Universidad de Deusto, Bilbao: 1999.

67. GÓMEZ SÁNCHEZ, Y.: *Constitucionalismo multinivel: derechos fundamentales.* Ed. Sanz y Torres, Madrid: 2011.

68. GÓMEZ SÁNCHEZ, Y.: *Constitucionalismo multinivel: derechos fundamentales.* 3ª [rev. y aum.] ed. Ed. Sanz y Torres, Alcorcón (Madrid): 2015.

69. GÓMEZ SÁNCHEZ, Y.: *Derecho constitucional europeo.* Ed. Sanz y Torres, Alcorcón (Madrid): 2015.

70. GÓMEZ SÁNCHEZ, Y.: *Derecho constitucional europeo: derechos y libertades.* Reimp. correg. y ampl. ed. Ed. Sanz y Torres, Madrid: 2008.

71. GONZÁLEZ FUSTER, G.: "Equilibrio entre propiedad intelectual y protección de datos: el peso oscilante de un nuevo derecho." IDP: revista de Internet, derecho y política = revista d'Internet, dret i política. Nº 14 (2012): Pp. 34-34.

72. GONZÁLEZ R. ARNÁIZ, G.: *Derechos humanos: la condición humana en la sociedad tecnológica.* Ed. Tecnos, Madrid: 1999.

73. GROS ESPIELL, H.; GÓMEZ SÁNCHEZ, Y.: *La Declaración Universal sobre Bioética y Derechos Humanos de la UNESCO.* Ed. Comares, Granada: 2006.

74. GUTTENBERG, K.T.; DETERMANN, L.: "On War and Peace in Cyberspace: Security, Privacy, Jurisdiction." Hastings constitutional law quarterly. Vol. 41, nº 4 (2014): Pp. 875-902.

75. HABERMAS, J.: *The crisis of the European Union: a response.* Ed. Polity Press, Cambridge: 2012.

76. HEMANN DA ROSA, T; RIGO FERRARI, G.M: " Privacidade, intimidade e proteçâo de dados pessoais/Privacy, intimacy and protection of personal data/Privacidad, confidencialidad y protección de datos personales." *Revista Argumenta.* no. 21 (2014): Pp. 137-166.

77. HERRÁN ORTIZ, A.I.: *El derecho a la protección de datos personales en la sociedad de la información.* Vol. 26. Ed. Universidad de Deusto, Bilbao: 2003.

78. HERRÁN ORTIZ, A.I.: *La violación de la intimidad en la protección de datos personales.* Ed. Dykinson, Madrid: 1998.

79. HEYMANN, J.: *Le droit international privé à l'épreuve du fédéralisme européen.* Ed. Economica, Paris: 2010.

80. HICKMAN, J.: "The new territorial imperative." Comparative strategy. Vol. 29, nº 5 (2010): Pp. 405-411. doi:10.1080/01495933.2010.520978.

81. HILDEBRANDT, M.: "Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace." University of Toronto Law Journal. Vol. 63, nº 2 (2013): Pp. 196-224. doi:10.3138/utlj.1119.

82. HIX, S.: *The political system of the European Union.* 3rd ed. Ed. Palgrave, Basingstoke, Hampshire: 2011.

83. HOFMANN, H.: "Dealing with trans-territorial executive rule-making." Missouri Law Review. Vol. 78, nº 2 (2013): Pp. 423.

84. HON, W.K.; HÖRNLE, J.y MILLARD, C.: "Data protection jurisdiction and cloud computing - when are cloud users and providers subject to EU data protection law? The cloud of unknowing." International Review of Law, Computers & Technology. Vol. 26, nº 2-3 (2012): Pp. 129-164. doi:10.1080/13600869.2012.698843.

85. KAMARINOU, D.; MILLARD, C.and HON, W.K.: "Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies--Part II." International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 170.

86. KOKOTT, J.; SOBOTTA, C.: "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR." International Data Privacy Law. Vol. 3, nº 4 (2013): Pp. 222-228.

87. KOOPS, E.J.: "The trouble with European data protection law." International Data Privacy Law. Vol. 4, nº 4 (2014): Pp. 250-261.

88. KROPF, J.W.: "Personal data-protection of individual privacy-right to be forgotten-responsibility of internet search engine operators-European data protection directive 95/46/EC." American Journal of International Law. Vol. 108, nº 3 (2014): Pp. 502-509.

89. KULESZA, J.: "International law challenges to location privacy protection." International Data Privacy Law. Vol. 3, nº 3 (2013): Pp. 158-169.

90. KULESZA, J..: "Transboundary data protection and international business compliance." International Data Privacy Law. Vol. 4, no. 4 (2014): Pp. 298-306.

91. KUNER, C.; CATE, F.H. *et al.*: "The (data privacy) law hasn't even checked in when technology takes off." International Data Privacy Law. Vol. 4, nº 3 (2014): Pp. 175-176. doi:10.1093/idpl/ipu013.

92. KUNER, C.; CATE, F.H. *et al.*.: "The extraterritoriality of data privacy laws--an explosive issue yet to detonate." International Data Privacy Law. Vol. 3, nº 3 (2013): Pp. 147-148. doi:10.1093/idpl/ipt009.

93. KUNER, C.: "Extraterritoriality and regulation of international data transfers in EU data protection law." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 235-245.

94. KUNER, C.: "Extraterritoriality and regulation of international data transfers in EU data protection law." International Data Privacy Law. Vol. 5, nº 4 (2015): Pp. 235-245. doi:10.1093/idpl/ipv019.

95. KUNER, C.; CATE, F.H. *et al.*: "The data protection credibility crisis." International Data Privacy Law. Vol. 5, nº 3 (2015): Pp. 161-162.

96. KUNER, C.; SVANTESSON, D.J.B. *et al.*: "The language of data privacy law (and how it differs from reality)." International Data Privacy Law. Vol. 6, nº 4 (2016): Pp. 259-260.

97. LABRADA RUBIO, V.: *Introducción a la teoría de los derechos humanos: fundamento, historia, Declaración Universal de 10 de diciembre de 1948.* 1ª ed. Ed. Civitas, Madrid: 1998.

98. LESIEUR, F.: "Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy." International Data Privacy Law. Vol. 2, nº 2 (2012): Pp. 93-104.

99. LIMA TORRADO, J.: "Ciberespacio y protección de los derechos: ¿hacia una cibercultura de los derechos humanos?" Cuadernos electrónicos de filosofía del derecho. Nº 5 (2002).

100. LINDE PANIAGUA, E.: "El ámbito de aplicación: el talón de Aquiles de la Carta de los Derechos Fundamentales de la Unión Europea." Revista de derecho de la Unión Europea (15). (2008).

101. LOBO RODRIGO, Á.: *La ordenación territorial y urbanística de las redes de telecomunicación.* Ed. Montecorvo, Madrid: 2007.

102. LÓPEZ CASTILLO, A.; SAIZ ARNAIZ, A. *et al.*: *Constitución Española y Constitución Europea.* 1st ed. Ed. Centro de Estudios Politicos y Constitucionales, Madrid: 2015.

103. LOSANO, M.G.; PÉREZ LUÑO, A.E. and GUERRERO MATEUS, M.F.: *Libertad informática y leyes de protección de datos personales.* Vol. 21. Ed. Centro de Estudios Constitucionales, Madrid: 1989.

104. LUCAS MURILLO DE LA CUEVA, P.: *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática.* Ed. Tecnos, Madrid: 1990.

105. MAHER, I.: "Competition Law and Transnational Private Regulatory Regimes: Marking the Cartel Boundary." Journal of Law and Society. Vol. 38, nº 1 (2011): Pp. 119-137. doi:10.1111/j.1467-6478.2011.00537.x.

106. MANGAS MARTÍN, A.: *Tratado de la Unión Europea, tratado de funcionamiento y otros actos básicos de la Unión Europea.* 18ª ed.Vol. 149. Ed. Tecnos, Madrid: 2014.

107. MANGAS MARTÍN, A.; LIÑÁN NOGUERAS, D.J.: *Instituciones y Derecho de la Unión Europea.* 8ª ed. Ed. Tecnos, Madrid: 2014.

108. MANTELERO, A.: "Data protection, e-ticketing, and intelligent systems for public transport." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 309-320.

109. MARÍN CASTÁN, M.L.: "En torno a la dignidad humana como fundamento de la Declaración Universal sobre Bioética y Derechos Humanos de la UNESCO." Revista de bioética y derecho: publicación del Máster en bioética *y* derecho. Nº 31 (2014): Pp. 17-37.

110. MARTÍN Y PÉREZ DE NANCLARES, J.: *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea.* Ed. Iustel, Madrid: 2012.

111. MARTÍNEZ DE PISÓN, J.: "Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo". Derechos y Libertades. Nº 37 (2017): Pp. 51.

112. MARTÍNEZ HINCAPIÉ, H.D: "Incorporación internacional de los derechos económicos, sociales y culturales y la integralidad de los derechos humanos." Ratio Juris. Vol. 9, nº 19 (2014): Pp. 175-198.

113. MARTÍNEZ MORÁN, N.*: Utopía y realidad de los derechos humanos en el cincuenta aniversario de su declaración universal.* Ed. UNED, 1999.

114. MC CULLAGH, K.: "Cross-Border Data Protection: Applicable Law and Teritorial Powers of National Data Protection Supervisors." Scripted. Vol. 13, nº 1 (Mayo 2016, 2016): Pp. 95-100.

115. MEGÍAS, J.J.: "Privacidad en la sociedad de la información." Persona y Derecho. Vol. 59, (2008): Pp. 205-251.

116. MENÉNDEZ MATO, J.C.: *El contrato vía Internet.* Ed. J.M. BOSCH EDITOR, 2008.

117. MEUWESE, A.; BOMHOFF, J.A.: "The meta-regulation of transnational private regulation." Journal of Law and Society. Vol. 38, no. 1 (2011): Pp. 138-162. doi:10.1111/j.1467-6478.2011.00538.x.

118. MICHINEL ÁLVAREZ, M.Á.: *El derecho internacional privado en los tiempos hipermodernos.* Ed. Dykinson, 2011; 2013.

119. MIGUEL ASENSIO, P.A.: "Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea." Revista Española de Derecho Internacional. Vol. 69, nº 1 (2017): Pp. 75-108.

120. MINISTERIO DEL INTERIOR: *El espacio europeo de libertad, seguridad y justicia.* Ed. Ministerio del Interior, Madrid: 2000.

121. MÖLLER, K.: *Formwandel der Verfassung: Die postdemokratische Verfasstheit des Transnationalen.* 1. Aufl. ed.Vol. 23; 23. Ed. transcript Verlag, Bielefeld: 2015.

122. MONEREO ATIENZA, C.; MONEREO PÉREZ, J.L. y ÁLVAREZ GONZÁLEZ, E.M.: *La Europa de los derechos: Estudio sistemático de la carta de los derechos fundamentales de la Unión Europea.* Vol. 22. Ed. Comares, Granada: 2012.

123. MUÑOZ, J.R.: "Zur Verfassung Europas. Ein Essay." Azafea. Vol. 15, (2013): Pp. 250-252.

124. NOGUEIRA ALCALÁ, H. : "Pautas para Superar las Tensiones entre los Derechos a la Libertad de Opinión e Información y los Derechos a la Honra y la Vida Privada." Revista de derecho (Valdivia). Vol. 17, (2004): Pp. 139-160.

125. OLLERO, A.: ″Los nuevos derechos". Persona y Derecho *Nº 66.* (2012).

126. ORAÁ ORAÁ, J.; GÓMEZ ISA, F.: *La Declaración Universal de Derechos Humanos.* Vol. 10. Ed. Universidad de Deusto, Bilbao: 2002.

127. ORDÓÑEZ SOLÍS, D.: *Privacidad y protección judicial de los datos personales.* 1ª ed. Ed. Bosch, Barcelona: 2011.

128. ORTEGA GIMÉNEZ, A.: "España: el Derecho Fundamental a la Protección de Datos de Carácter Personal en España." AR: Revista de Derecho Informático. Nº 121 (2008).

129. PALLARES YABUR, P.d.J.: "La justificación racional de los derechos humanos en los redactores de la Declaración Universal de los Derechos Humanos." Persona y derecho: Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos. Nº 68 (2013): Pp. 139-158.

130. PAMPILLO-BALIÑO, J.P.: "Una teoría global del derecho para una nueva época histórica/A comprehensive theory of law for a new historical period". Dikaion. Vol. 19, nº 1 (2010): Pp. 11-45.

131. PECES-BARBA MARTÍNEZ, G.; FERNÁNDEZ GARCÍA, E.: *Historia de los Derechos Fundamentales. Tomo I: Tránsito a la modernidad. Siglos XVI y XVII.* Ed. Dykinson, Madrid: 1998.

132. PIÑAR MAÑAS, J.L (Dir.): *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. 1ª Ed., Editorial Reus, Madrid 2016.

133. PIÑAR MAÑAS, J.L: "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio". Laboratorio Fundación Alternativas, Documento de Trabajo 147/2009. Accesible en la dirección: https://www.fundacionalternativas.org/laboratorio/documentos/documentos-de-trabajo/seguridad-transparencia-y-proteccion-de-datos-el-futuro-de-un-necesario-e-incierto-equilibrio

134. POL AK, R.: "Getting European data protection off the ground." International Data Privacy Law. Vol. 4, nº 4 (2014): Pp. 282-289. doi:10.1093/idpl/ipu019.

135. PONCE MARTÍNEZ, C.F.: "La declaración universal de derechos humanos. Naturaleza jurídica y aplicación por los órganos jurisdiccionales internos." Anuario de la Facultad de Derecho. º 19-20 (2001): Pp. 253-279.

136. PRIETO SANCHÍS, L.: "Los derechos sociales y el principio de igualdad sustancial." Revista del centro de estudios constitucionales. Nº 22 (1995).

137. RAFECAS BARCELÓ, S.: "Los Conflictos de interés. Comentario del artículo 15.2 de la Declaración Universal sobre Bioética y Derechos Humanos." Revista de bioética y derecho: publicación del Máster en bioética y derecho. Nº 25 (2012): Pp. 73-84.

138. RAYÓN BALLESTEROS, M.C; GÓMEZ HERNÁNDEZ, J.A: "Cibercrimen: particularidades en su investigación y enjuiciamiento/ Cybercrime: particularities in investigation and prosecution." Anuario Jurídico y Económico Escurialense. Nº 47 (2014): Pp. 209.

139. REBOLLO DELGADO, L.: *Derecho constitucional I.* 3ª ed. Ed. Dykinson, Madrid: 2017.

140. REBOLLO DELGADO, L.: *El derecho fundamental a la intimidad.* 2ª act ed. Ed. Dykinson, Madrid: 2005.

141. REBOLLO DELGADO, L.: *Derechos fundamentales y protección de datos.* Ed. Dykinson, Madrid, 2004.

142. REBOLLO DELGADO, L.: *La institución del Ombudsman en España.* Ed. Dykinson, Madrid: 2013.

143. REBOLLO DELGADO, L.: *Límites a la libertad de comunicación pública.* Ed. Dykinson, Madrid, 2008.

144. REBOLLO DELGADO, L.: *Protección de datos en Europa. Origen, evolución y regulación actual.* Ed. Dykinson, Madrid: 2018.

145. REBOLLO DELGADO, L.: "Veinticinco años de relación entre la informática y los derechos al honor y a la intimidad personal y familiar." Revista de Derecho Político. Nº 58-59 (2003). doi:10.5944/rdp.58-59.2003.8895.

146. REBOLLO DELGADO, L.: *Vida privada y protección de datos en la Unión Europea.* Ed. Dykinson, Madrid: 2008.

147. REBOLLO DELGADO, L.; GÓMEZ, Y.: *Biomedicina y protección de datos.* Ed. Dykinson, Madrid: 2008.

148. REBOLLO DELGADO, L.; SERRANO PÉREZ, M.M.: *Manual de protección de datos.* 3ª ed. Ed. Dykinson, Madrid: 2019.

149. RICHARDS, R.: "Compulsory process in cyberspace: rethinking privacy in the social networking age" Harvard Journal of Law and Public Policy. Vol. 36, nº 2 (2013): Pp. 519-548.

150. RODRÍGUEZ DÍAZ, B.: *La Aportación de la Sociedad Civil a la Constitución Europea.* Ed. Académica Española, Hermosillo: 2012.

151. ROIG, A.: *Derechos fundamentales y tecnologías de la información y de las comunicaciones (TICs).* Vol. 2. Ed. J.M. Bosch, Barcelona: 2010; 2009.

152. ROLLA, G.*: El difícil equilibrio entre derecho a la información y la tutela de la dignidad y la vida privada. Breves consideraciones a la luz de la experiencia italiana.* Ed. Servicio de Publicaciones de la Universidad de Navarra, 2001.

153. RUBENS, J.; MORSE, E.: "Survey of the Law of Cyberspace: Introduction." Business lawyer. Vol. 69, nº 1 (2013): Pp. 183-187.

154. RUIZ MIGUEL, C.: *La configuración constitucional del derecho a la intimidad.* Ed. Tecnos, Madrid: 1995.

155. RUIZ MIGUEL, C.: *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos.* Ed. Civitas, Madrid: 1994.

156. RUIZ MIGUEL, C.: "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico." Revista de Derecho Comunitario Europeo. Vol. 7, nº 14 (2003): Pp. 7-43.

157. RUIZ SANZ, M.: *Sistemas jurídicos y conflictos normativos.* Ed. Dykinson, 2002.

158. RUSSO, A.M.: "Un nuevo "juego interactivo" en el tablero de ajedrez del derecho transnacional: la cooperación territorial transfronteriza en el marco jurídico europeo." Revista catalana de dret públic. Nº 47 (2013): Pp. 159-180.

159. RYNGAERT, C.: "Symposium issue on extraterritoriality and EU data protection." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 221-225.

160. SÁENZ ROYO, E.: *Manual de Derecho Constitucional I.* 1st ed. Ed. Prensas de la Universidad de Zaragoza, Zaragoza: 2017.

161. SÁNCHEZ, N.A.: "El derecho al desarrollo en el 60 aniversario de la declaración universal de los derechos humanos: Estado de la cuestión". Nómadas. Nº 22 (2009).

162. SANCHO VILLA, D.: *Transferencia internacional de datos personales.* Ed. Agencia española de protección de datos, Madrid: 2003.

163. SANCHO, V.M.: "Una revisión de la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre la intimidad sexual y la autonomía individual." Derechos y Libertades. Nº 38 (2018): Pp. 327.

164. SCHLAIN, N.B.: *Internet y el Derecho a la Intimidad.* Editorial Académica Española, Hermosillo: 2012.

165. SCOTT, C.; CAFAGGI, F. y SENDEN, L.: "The Conceptual and Constitutional Challenge of Transnational Private Regulation." Journal of Law and Society. Vol. 38, nº 1 (2011): Pp. 1-19. doi:10.1111/j.1467-6478.2011.00532.x.

166. SCOTT, J.: "Extraterritoriality and Territorial Extension in EU Law." American Journal of Comparative Law, Vol. 62, nº 1 (2014; 1901): Pp. 87-125. doi:10.5131/AJCL.2013.0009.

167. SEGURA SERRANO, A.; GORDO GARCÍA, F.: *Ciberseguridad global: oportunidades y compromisos en el uso del ciberespacio.* Ed. Editorial Universidad de Granada, Granada: 2013.

168. SERRANO PÉREZ, M.M.: “El derecho fundamental a la protección de datos. Su contenido esencial”. Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas, 2005, Issue 1, pp.245-265

169. SILVA, A.C.: “El ‘nivel adecuado de protecciíon’ para las transferencias internacionales de datos personales desde la Unión Europea" ["The "Adequate Level of Protection" for International Personal Data Transfer from the European Union"]." Revista de Derecho. Nº 36 (2011): Pp. 327.

170. STILZ, A.: "Why do states have territorial rights?" International Theory. Vol. 1, nº 2 (2009): Pp. 185-213. doi:10.1017/S1752971909000104.

171. SVANTESSON, D.J.: "A "layered approach" to the extraterritoriality of data privacy laws." International Data Privacy Law. Vol. 3, nº 4 (2013): Pp. 278-286.

172. SVANTESSON, D.J.: "Article 4(1)(a) ‘establishment of the controller’ in EU data privacy law—time to rein in this expanding concept?" International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 210-221.

173. SVANTESSON, D.J.B.; Institutet för rättsinformatik (IRI) *et al.*: "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation." International Data Privacy Law. Vol. 5, nº 4 (2015): Pp. 226-234. doi:10.1093/idpl/ipv024.

174. SVANTESSON, D.J.B.; Stockholms universitet *et al.*: "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation." International Data Privacy Law. Vol. 5, nº 4 (2015): Pp. 226-234.

175. TAYLOR, M.: "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 246-256.

176. TENE, O.: "Privacy: The new generations." International Data Privacy Law. Vol. 1, nº 1 (2011): Pp. 15-22.

177. TERWANGNE, C.d.: "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido = Internet privacy and the right to be forgotten/right to oblivion." IDP: revista de Internet, derecho y política = revista d'Internet, dret i política. Nº 13 (2012): Pp. 53-56.

178. TORCOL, S.; BONNET, B. *et al.*: "Définir le droit constitutionnel européen.." Revue de l'Union Européenne. Nº 590 (Jul/Aug 2015, 2015): Pp. 456-463.

179. TRONCOSO REIGADA, A.: "La Administración electrónica y la protección de datos personales." Revista jurídica de Castilla y León. Nº 16 (2008): Pp. 31-112.

180. TRONCOSO REIGADA, A.: "La declaración de los ficheros de datos personales: acerca de un modelo centralizado o descentralizado." Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid. Nº 38 (2009).

181. TRONCOSO REIGADA, A.: "La protección de datos personales: una reflexión crítica de la jurisprudencia constitucional." Cuadernos de derecho público. Nº 19-20 (2003): Pp. 231-334.

182. TRONCOSO REIGADA, A.: "Las redes sociales a la luz de la propuesta de Reglamento general de protección de datos personales: Parte uno." IDP: revista de

Internet, derecho y política = revista d'Internet, dret i política. Nº 15 (2012): Pp. 61-75.

183. TRONCOSO REIGADA, A.: "Las redes sociales a la luz de la propuesta del reglamento general de protección de datos personales: Parte dos." IDP: revista de Internet, derecho y política = revista d'Internet, dret i política. Nº 16 (2013).

184. TRONCOSO REIGADA, A.: "El derecho al olvido en Internet a la luz de la propuesta de reglamento general de protección de datos personales de la Unión Europea." Revista de Derecho, Comunicaciones y Nuevas Tecnologías. Nº 8 (2012): Pp. 1-38. doi:10.15425/redecom.8.2012.03.

185. TRUYOL Y SERRA, A.: *Los derechos humanos: declaraciones y convenios internacionales.* 3ª ed. act., Ed. Tecnos, Madrid: 1982.

186. UGARTEMENDIA ECEIZABARRENA, J.I.: "¿Quién es el juez de los derechos fundamentales frente a la ley en el ámbito interno de aplicación del derecho comunitario?" Teoría y realidad constitucional. Vol. 20, (2007-07-01, 2007): Pp. 401-433.

187. UGARTEMENDIA ECEIZABARRENA, J.I.: "La tutela judicial de los derechos fundamentales en el ámbito de aplicación nacional del derecho de la Unión Europea: recientes acotaciones del Tribunal de Justicia y del Tribunal Constitucional Español = The judicial protection of fundamental rights in the sphere of the national application of EU law: recent remarks by the Court of Justice and by the Spanish Constitutional Court." Teoría y realidad constitucional (32). (2013).

188. VAN ALSENOY, B.; KOEKKOEK, M.: "Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'." International Data Privacy Law. Vol. 5, no. 2 (2015): Pp. 105-120. doi:10.1093/idpl/ipv003.

189. VAN DER SLOOT, B.*: A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle.* Vol. 34. 2018. doi:https://doi.org/10.1016/j.clsr.2017.11.013.

190. VARGAS, R.J.: "Luces y sombras del origen de la ONU y la Declaración Universal de Derechos Humanos." El Cotidiano. Vol. 28, no. 180 (2013): Pp. 31-40.

191. VELÁSQUEZ MONSALVE, J.D.: "El derecho natural en la Declaración Universal de los Derechos Humanos." Revista Facultad de Derecho y Ciencias Políticas. Vol. 43, no. 119 (2013): Pp. 735-772.

192. VILLACORTA MANCEBO, L.; VILLACORTA CAÑO VEGA, A.: *Nuevas dimensiones de protección asumidas por los derechos fundamentales.* Ed. Dykinson, Madrid, 2013.

193. VILLALOBOS ANTUNEZ, J.V.; HERNANDEZ, J.P. y PALMAR, M.: "El estatuto bioético de los derechos humanos de cuarta generación." Revista Fronesis. Vol. 19, nº 3 (2012): Pp. 350.

194. VILLAVERDE MENÉNDEZ, A.I.: "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo: A propósito de la STC 254/93." Revista española de derecho constitucional. Nº 41 (1994): Pp. 187-224.

195. VIOLA, F.: "Los Derechos Humanos, son derechos naturales? / Human Rights, are the natural rights?" Revista quaestio iuris. Vol. 6, nº 2 (2013).

196. YPI, L.: "A Permissive Theory of Territorial Rights." European Journal of Philosophy. Vol. 22, nº 2 (2014): Pp. 288-312. doi:10.1111/j.1468-0378.2011.00506.x.

197. ZABALO ESCUDERO, M.E.: "Conflictos de leyes internos e internacionales: conexiones y divergencias." Bitácora Millennium DIPr Nº 3. Nº 3 (2016): Pp. 54-68.

198. ZABALO ESCUDERO, M.E.: "La aplicación de las normas de conflicto del Derecho Interregional: a propósito de la sentencia del TSJ de Aragón de 10 de marzo de 1999." Revista de derecho civil aragonés. Vol. 5, nº 2 (1999): Pp. 247-252.

199. ZUIDERVEEN BORGESIUS, F.J.: "Personal Data Processing for Behavioural Targeting: Which Legal Basis?" International Data Privacy Law. Vol. 5, no. 3 (2015): Pp. 163-176.

200. ZUMBANSEN, P.: "Defining the space of transnational law: Legal theory, global governance and legal pluralism." Research Paper Series. Vol. 7, nº 5 (2011): Pp. 1-37.

201. ZUMBANSEN, P.: "Neither 'Public' nor 'Private', 'National' nor 'International': Transnational Corporate Governance from a Legal Pluralist Perspective." Journal of Law and Society. Vol. 38, no. 1 (2011): Pp. 50-75. doi:10.1111/j.1467-6478.2011.00534.x.

INSTRUMENTOS OFICIALES

1. Additional EDPS comments on the data protection reform package. Bruselas, 15 de marzo de 2013.
2. Anteproyecto de Ley Orgánica de protección de datos de carácter personal. Ministerio de Justicia de España.
3. Avis 01/2012 sur les propositions de réforme de la protection des donées (00530/12/FR – WP 191). Grupo de trabajo del art. 29 sobre protección de datos. 23 de marzo de 2012.
4. Avis 5/2016 préliminaire du CEPD sur le réexamen de la directive "vie privée et communications électroniques" (directive 2002/58/CE). 22 de julio de 2016.
5. Avis du Contrôleur Européen de la protection des données sur le paquet de mesures pour une réforme de la protection des donées. Supervisor Europeo de Protección de Datos. Bruselas, 07/03/2012.
6. Carta de los derechos fundamentales de la Unión Europea.
7. Communication from the Comission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century. Bruselas, 25 de enero de 2012.
8. Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Estrasburgo, 28 de enero de 1981.

9. Convenio Europeo de Derechos Humanos. Roma, 4 de noviembre de 1950.

10. Data protection review: Impact on EU innovation and competitiveness. European Parliament, Directorate General for Internal Policies. Policy department A: Economic and Scientific Policy. Diciembre 2012.

11. Decisión de la Comisión 2000/520/CE, de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes publicadas por el Departamento de Comercio de Estados Unidos de América. DOCE L 215/7 de 25.08.2000.

12. Decisión de la Comisión 2001/497/CE de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.

13. Decisión de la Comisión 2004/915/CE de 27 de diciembre de 2004 por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.

14. Decisión 2010/87/UE de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

15. Decisión de Ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. DOUE L 207/1 de 01.08.2016.

16. Dictamen del Comité Económico y Social Europeo sobre la "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (Reglamento general de protección de datos)" COM(2012) 11 final – 2012/011 (COD).

17. Dictamen 3/2015 del Supervisor Europeo de Protección de Datos: La gran oportunidad de Europa. Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos. 28 de julio de 2015.

18. Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DOCE L 281/31 de 23.11.1995.

19. 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). DOCE L 178/1 de 17.07.2000.

20. Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la

intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). DOCE L 201/37 de 31.07.2002.

21. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. DOUE L 119/89 de 04.05.2016.

22. Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. DOUE L 119/132 de 04.05.2016.

23. Discussion document: First orientations on transfers of personal data to third countries – Possible ways forward in assessing adequacy. Grupo de Trabajo del Artículo 29, 26.06.1997.

24. European Commission Press release: Agreement on Commission's EU data protection reform will boost Digital Single Market. Bruselas, 15/12/2015.

25. First orientation on transfers of personal data to third countries. Possible ways forward in assessing adequacy (XV D/5020/97-EN final, WP4). Grupo de Trabajo del Art. 29, Bruselas, 26/06/1997.

26. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Comité Europeo de Protección de Datos, 26 de noviembre de 2018.

27. Handbook on European data protection law. Agencia de los derechos fundamentals de la Unión Europea (FRA) y Consejo de Europa, 2018.

28. Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones presentado de conformidad con el artículo 29, apartado 2, de la Decisión Marco del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. SEC(2012) 75 final. Bruselas, 25 de enero de 2012.

29. Letter on Progress on the data protection reform package (C2011-1104). Supervisor Europeo de Protección de Datos, Bruselas, 14/02/2014.

30. Manual de legislación europea en materia de la protección de datos. Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2014.

31. Modernised convention for the protection of individuals with regard to the processing of personal data. Consolidated text. Council of Europe, 128th Session of the Committee of Ministers, Elsinore (Denmark), 17-18 de mayo de 2018.

32. Opinion 8/2003 on the draft standard contractual clauses submitted by a group of business associations ("the alternative model contract") (11754/03/EN – WP 84). Grupo de trabajo del art. 29 sobre protección de datos, 17/12/2003.

33. Opinion 8/2010 on applicable law (0836-02/10/EN - WP 179). Grupo de trabajo del art. 29 sobre protección de datos, 16/12/2010.

34. Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 estos datos, y por el que se deroga el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE. COM(2017) 8 final. 2017/0002 (COD). Bruselas, 10.01.2017.

35. Protocolo adicional de convenio nº 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos. Estrasburgo, 8 de noviembre de 2001.

36. Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. DOCE L 8/1 de 12.01.2001.

37. Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 por el que se establecen medidas en relación con el acceso a una internet abierta y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) nº 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión. DOUE L 310/1 de 26.11.2015.

38. 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). DOUE L 119/1 de 04.05.2016.

39. Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo de 28 de febrero de 2018 sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) nº 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE. DOUE L 60 I/1 de 23.02.2018.

40. Resolución R/00259/2018 de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00219/2017 contra FACEBOOK INC. Y WHATSAPP INC.

41. Tratado de la Unión Europea.

42. Tratado de Funcionamiento de la Unión Europea.

43. Un mercado único digital en Europa. Comisión Europea, Bélgica, 2016.

44. Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. (11639/02/EN – WP 74). Grupo de Trabajo del Art. 29 sobre Protección de Datos, 03.06.2003.

45. Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. Grupo de Trabajo del Art. 29 sobre Protección de Datos, 12.07.1998.

46. Working document on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Parlamento Europeo, Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE). 06/07/2012.