Universidad de Alcalá

DATOS PERSONALES: REGULACIÓN Y TRATAMIENTO NORMATIVO

PERSONAL DATA SURVEILLANCE: REGULATION AND LEGAL CHALLENGES

Máster Universitario en Acceso a la Profesión de Abogado

Presentado por:
D. ADRIÁN HIGUERA DEL CAMPO

Dirigido por:
Dra. Dª MARÍA INMACULADA RODRÍGUEZ ROBLERO
Dra. Dª MONTSERRAT GUZMÁN PECES

Alcalá de Henares, a 3 de mayo de 2023

ÍNDICE

RESUMEN

El presente trabajo tiene como finalidad aquella de ofrecer un resumen de los principales hitos históricos y normativos en el ámbito de la protección de datos, realizar un análisis simple sobre los elementos principales de la estructura de la protección de datos, incluyendo los derechos en la materia, y estudiar su proyección práctica en relación al tratamiento automatizado de datos personales y la elaboración de perfiles.

CONCEPTOS CLAVE

Protección de datos; elaboración de perfiles; tratamiento automatizado; Reglamento General de Protección de Datos; consentimiento.

ABSTRACT

The following work seeks that purpose of trying to offer a *resumé* of the main historical-regulatory highlights on data protection law, whereas trying to deliver a simple analysis on the leading concepts from data protection legislative's structure, including derived rights from the field of study, while following a series of work lines on their practical projection in relation to automated data processing and profiling.

KEY CONCEPTS

Data protection; profiling; automated data processing; Data Protection Regulation; consent.

TABLA DE ABREVIATURAS

AEPD Agencia Española de Protección de Datos

CDFUE Carta de Derechos Fundamentales de la Unión Europea

CEPD Comité Europeo de Protección de Datos

GT29 Grupo de Trabajo del Artículo 29

LOPD Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales

LSSI Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico

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

TJUE Tribunal de Justicia de la Unión Europea

TFUE Tratado de Funcionamiento de la Unión Europea

TS Tribunal Supremo

UE Unión Europea

INTRODUCCIÓN

JUSTIFICACIÓN DE LA ELECCIÓN DEL TEMA

La normativa sobre protección de datos constituye uno de los bloques arquitectónicos normativos de mayor dimensión legislativa de nuestros tiempos. Esto es así porque pretende ser una legislación de gran calado y proyección, con ambición de alcance general e intenso, reduciendo al máximo las posibles filtraciones que puedan ocurrir en detrimento de las garantías de los ciudadanos. Sin embargo, a pesar de las dimensiones, implicaciones y espíritu que conforman la norma, esta no es indiferente a otras ramas del Derecho que son sometidas a una motorización legislativa en aras de las necesidades sociales por el desfase constante entre regulación y realidad. Es por ello que la norma se enfrenta a un horizonte lleno de retos políticos, sociales, económicos y, consecuentemente, jurídicos, a fin de alcanzar o al menos dotar del refuerzo necesario los derechos que pretende consagrar, estos son, las herramientas frente a las intromisiones indebidas de los ciudadanos mediante tecnologías invasivas de la privacidad, con la finalidad de tratar sus datos y así elaborar perfiles.

OBJETO DEL TRABAJO

Es objeto de este trabajo hacer un recorrido histórico en lo que al ámbito de la protección de datos concierne para ofrecer suficiente contexto al lector y, correlativamente, entender la justificación de la existencia de normativa de protección de datos y su conceptualización, reflexionando sobre esta última y concluyendo de qué formas puede ser completada, a modo de sucinta crítica. En esta línea, se hace un breve recorrido sobre las normas principales de protección de datos en la actualidad, para trasladarnos al contexto normativo, y así analizar con especial detenimiento la normativa esencial, esta es, el Reglamento General de Protección de Datos y normas sectoriales relevantes. Este trabajo persigue cinco objetivos: ilustrar de forma somera los cimientos de la protección de datos; estudiar sus elementos estructurales más básicos; y, a la luz de estos, criticar la conceptualización de la protección de datos; determinar si existen lugares oscuros sobre el análisis de dichos derechos; y dilucidar si es mejor transitar de un modelo de consentimiento tradicional, a uno en el que medie contraprestación económica como consecuencia de la deslocalización de los datos.

METODOLOGÍA

Se ofrecen una serie de reflexiones bibliográficas sobre los elementos más destacados del 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, conocido como Reglamento General de Protección de Datos, concretamente, sobre los derechos que asisten al interesado y las bases que justifican el tratamiento de datos personales, con especial atención a la institución jurídica del consentimiento, todo ello a la luz de la práctica de la elaboración de perfiles.

CAPÍTULO I: CONCEPTUALIZACIÓN HISTÓRICO-NORMATIVA DEL DERECHO A LA PROTECCIÓN DE DATOS

1. CONTEXTO Y ANTECEDENTES NORMATIVOS EN LA PROTECCIÓN DE DATOS

Históricamente, podemos ligar la aparición del origen de la conceptualización del derecho a la protección de datos en las primeras acepciones del derecho a la intimidad[1], con motivo de su incardinación en los cambios histórico-sociales y prácticas mercantilistas inherentes a la segunda revolución industrial, así como a las tendencias de consumo de la época. Situándonos en los comienzos del siglo XX, caracterizado por el hambriento avance de desarrollo industrial y tecnológico, irrumpen en la sociedad nuevas sensibilizaciones que materializan su calado mediante reivindicaciones en forma de antecedentes judiciales, como aquellas relativas a la intimidad frente a las injerencias de los poderes públicos y, en lo que a los agentes privados compete, de la prensa rosa[2].

Este escenario propicia el desgaje de la configuración autónoma del derecho a la intimidad respecto del derecho al honor, operando el punto comúnmente aceptado de configuración inicial de dicho desgaje en la obra señera que, con el título de *The Right to Privacy*[3], fue publicada bajo la autoría de dos insignes juristas norteamericanos: Samuel D. Warren y Louis Brandeis.

Ambos autores plasman en el trabajo su preocupación por el surgimiento y transformación de nuevos derechos, reivindicando, al mismo tiempo, la necesidad de adaptar parcialmente el contenido de otros derechos de formulación más clásica y situación más estable por su tradicionalidad, respectivamente, debido al devenir político, económico y social propio de finales del siglo XIX y comienzos del XX. A fin de ofrecer una ajustada ilustración de las modificaciones sufridas por derechos ya consolidados, los autores conceden el ejemplo del derecho a la vida, que inicialmente "servía, únicamente, para proteger a los súbditos frente a las variadas formas de agresión violenta […] Y, hoy en día, el derecho a la vida significa el derecho a disfrutar de la vida, el derecho a no ser molestado" (S. D. Warren y L. D. Brandeis, 1980)).

---

[1] España, Cortes Generales (1978). Constitución Española de 29 de diciembre de 1978, Boletín Oficial del Estado, 1978-31229, accesible en <https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229>, art. 10.

Ruíz Miguel, C. (1992), *La configuración constitucional del derecho a la intimidad* [tesis doctoral]. Universidad Complutense de Madrid, págs. 76 y ss.

[2] Consejo General de la Abogacía Española. *Derecho a la información versus derecho a la intimidad e imagen en la sociedad de la información*, recuperado en enero de 2023, accesible en <https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/derecho-a-la-informacion-versus-derecho-a-la-intimidad-e-imagen-en-la-sociedad-de-la-informacion/>

[3] S. D. Warren y L. Brandeis, *The Right to Privacy*, Harvard Law Review, núm. 5 (1980). Obra completa.

Afirmaciones como la ofrecida por los autores, denotan la naturaleza refrescante e innovadora que el espíritu de su ensayo es identificable en bases culturales como, por ejemplo, aquellas relativas a la construcción de los Derechos Humanos de tercera generación, vinculados a la cultura postmaterialista y relacionados con la autorrealización personal, con un carácter más expresivo que instrumental, tomando distancia -los derechos- de necesidades más básicas que motivaron su surgimiento, como la seguridad física y económica[4].

En lo que a la estela del nacimiento del derecho a la intimidad compete, y en congruencia con el nacimiento de nuevos derechos con el devenir social y tecnológico referido, se pronuncia en 1879 el juez estadounidense Thomas M. Coole, quien, reseñando la importancia de blindar la esfera privada del ciudadano y las proyecciones de esta frente a las injerencias del Estado y, con mayor frecuencia, aquellas atribuibles *a las consecuencias sociales derivadas de los recientes inventos y nuevos métodos de hacer negocios*, formula el derecho a no ser molestado[5]. Así, lo que se planteaba era la necesidad directa de la protección de la intimidad de la persona frente al ánimo inquisitorio de la prensa rosa que, con mayor frecuencia, empujaba la línea de lo considerado apropiado para obtener informaciones escandalosas y sensacionalistas de la vida privada de sus objetivos.

Concluye la reflexión de los autores en la necesidad de otorgar un tratamiento filosófico distinto a la conceptualización tradicional del derecho al honor respecto de aquella del derecho a la intimidad, con cobertura este primero en la Ley de Difamación[6] que, entre otros mecanismos, preveía el ejercicio de una acción de protección de los perjuicios causados en la reputación personal. En efecto, la protección jurídica respecto del mancillamiento de la nombradía de un individuo siempre se manifestaba, tanto a juicio de los juristas por antonomasia[7], como en las reflexiones contenidas en el trabajo de Cooley[8], en aquellas relaciones que implicaban alteridad: es decir, en la vulneración del derecho al honor encontramos a dos sujetos, aquel afrentado y quien conoce de la afrenta. No sucedía así con la protección de la intimidad pues, como arguyen en el trabajo de referencia, la transgresión gravosa de la misma genera, en única instancia y a efectos de determinar el momento de producción del daño y sus efectos, perjuicios en la psique del afectado.

---

[4] E. Suñé Llinás, *La sociedad civil en la cultura postcontemporánea*. Ed. Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense y CESSJ Ramón Carande, Madrid, 1998, págs. 75 y ss.

[5] Nieves Saldaña, M. (2011), *El Derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego*, UNED, Revista *Teoría y Realidad Constitucional*, págs. 279-312.

[6] *Comittee to Protect Journalists, Las leyes penales de difamación en Norteamérica,* recuperado en diciembre de 2022, accesible en <https://cpj.org/es/2016/03/norteamerica/>

[7] S. D. Warren y L. Brandeis, Ibid.

[8] Nieves Saldaña, M. (2011), Ibid.

En esta línea, desarrollan Warren y Brandeis[9] la estrecha relación entre intimidad y derecho moral -no patrimonial- que todo autor ostenta sobre la publicación de su obra, entendiendo que el derecho a decidir sobre la publicación de la propia obra es una proyección del derecho moral de autor, que no es otra cosa que la manifestación del derecho a la intimidad e inviolabilidad de la persona, entendiendo esta relación entre intimidad e inviolabilidad un presupuesto para concebir el respeto hacia la dignidad del individuo. Sancionan así "estas consideraciones nos llevan a la conclusión de que la protección otorgada a los pensamientos, sentimientos y emociones manifestados por escrito o en forma artística, en tanto en cuanto consista en impedir la publicación, no es más que un ejemplo de la aplicación del derecho más general del individuo a no ser molestado […] El principio que ampara los escritos personales, y toda otra obra personal, no ya contra el robo o la apropiación física, sino contra cualquier forma de publicación, no es en realidad el principio de la propiedad privada, sino el de la inviolabilidad de la persona. Si estamos en lo cierto, el derecho vigente proporciona un principio que puede ser invocado para amparar la intimidad del individuo frente a la invasión de una prensa demasiado pujante, del fotógrafo o del poseedor de cualquier otro moderno aparato de grabación o reproducción de imágenes o sonidos ".

Tras este breve intento de conceptualización, Warren y Brandeis recogen una serie de limitaciones inherentes a cualquier derecho, y unas particulares respecto del tratado aquí, a saber:

A. Aquellas derivadas de la libertad de información, el derecho a la intimidad "no implica limitación alguna para la publicación de aquello relevante para el interés público o general" (S. D. Warren y L. D. Brandeis, 1980).
B. Los asuntos relevantes para la Administración de Justicia en el seno de un procedimiento judicial.
C. Existen limitaciones respecto de la publicación de los hechos por el propio afectado por las informaciones contenidas en los mismos, con independencia de la existencia o no de su consentimiento.

La preocupación por las singularidades del derecho a la intimidad creció hasta el punto de convertirse en un tema en auge en los Parlamentos de diversas naciones, pues constataba la experiencia histórica que, a menudo, las intromisiones en la intimidad solo presuponían un medio para la vulneración de otros derechos fundamentales de la persona[10]. Podemos constatar esta afirmación localizando al final de la época preinformática las técnicas del régimen nacionalsocialista alemán, tanto en la misma Alemania como en aquellos países ocupados por las fuerzas nazis, destinadas a la minuciosa recolección de apellidos vinculados a la etnia judía en padrones municipales

[9] Arce Janariz, A. (1996), *El derecho a la intimidad, de Samuel D. Warren y Louis D. Brandeis*, Revista Española de Derecho Constitucional, núm. 47, págs. 367-371.

[10] E. Suñé Llinás, *La sociedad civil en la cultura postcontemporánea*. Op. Cit., págs. 75 y ss.

a fin de sancionar con sus atrocidades a las víctimas[11]. En situaciones tan críticas, podemos entrever la relación crucial que existe entre el derecho a la intimidad y las agresiones susceptibles que pueden afectar a otros derechos, pues el recurso a la instrumentalidad mediante la transgresión de este derecho no es sino una forma de atentado frente a otras esferas de la vida del individuo, como la integridad física.

Una digitalización de las herramientas prestacionales dirigidas a satisfacer las necesidades personales en los años 70 contribuye a la creciente caracterización de vulnerabilidad del hombre, siendo factible, desde este momento, la recogida sin antes precedentes de datos de la más diversa índole, ante la falta de limitación legislativa y la posibilidad de elaborar perfiles individuales y categóricos mediante este poder de recogida de datos. Es en este punto cuando la sensibilización pública y mediática y el propio proceso de autorreflexión de las empresas que llevan a cabo estos ejercicios acaparan la atención del poder legislativo, preocupado por la precaria situación de una esfera del ciudadano carente de atención y protección alguna[12].

Sin embargo, y como se ha expuesto, las primeras leyes de protección de datos de las personas físicas y jurídicas frente al tratamiento automatizado de sus datos son ubicables a la primera mitad de la década de los 70. A día de hoy, todos los Estados miembros de la Unión Europea disponen de ellas, y son varios los Estados norteamericanos que también han acogido normativa al respecto, así como existen países en Asia y Oceanía que anhelan o se encuentra directamente en el proyecto normativo que a este trabajo compete[13]. Es por ello por lo que, tratándose de un fenómeno normativo que progresivamente se extiende sobre el globo, y cuyo desarrollo se encuentra irremediablemente asociado a la hambrienta capacidad de almacenamiento y recuperación de información contenida en el equipamiento informático, así como al extensivo uso de la informática y de las telecomunicaciones, el tratamiento de datos personales para el perfilado, configuración y optimización de las predicciones conductuales de los destinatarios del metaverso es una realidad no libre de riesgos.

Antes de examinar la heterogeneidad de mecanismos de control previstos en el Derecho comparado y las modalidades asumidas por cada Estado miembro conforme a su propia y particular caracterización, es necesario introducir de forma sucinta los rasgos fundamentales de la normativa en que se contextualiza cada uno de ellos, oportunidad en que podremos apreciar la evolución experimentada por las leyes de protección de datos frente al tratamiento de datos personales y, particularmente, la cumulativa

---

[11] *El País, Protejamos nuestros datos. No olvidemos cómo los usaban los nazis*, publicado en septiembre de 2021, accesible en <https://elpais.com/ideas/2021-09-12/protejamos-nuestros-datos-no-olvidemos-como-los-usaban-los-nazis.html>

[12] Revista chilena de Derecho informático, núm. 3, diciembre, accesible en <http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_publicaciones/index.html>

[13] Blog *Protección Data*, entrada *Para estar al día en protección de datos y seguridad de la información*, recuperado en octubre de 2022, accesible en <https://protecciondata.es/historia-normativa-proteccion-datos/>

diversificación de los medios de que estas han empleado a efectos de asegurarse del debido cumplimiento de sus previsiones.

Así, durante una primera estación, cuando el número y coste asociado al funcionamiento de equipamiento electrónico y computacional suponía el empleo de grandes dotaciones de fondos públicos, tiene lugar la promulgación de la primera norma en el ámbito material que aquí compete. Es en 1970 cuando surge la *Datenschutz*[14], como ley sobre tratamiento de datos personales del Land de Hesse, en la República Federal de Alemania, mediante la cual se pretendía brindar protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de Derecho Público y agrupaciones sujetas a la tutela y control estatal, en términos de Derecho administrativo. Es por ello que, a efectos de asegurar el cumplimiento de sus previsiones, la Ley creaba la figura del Comisario de Protección de Datos, a quien reconocía independencia en el desempeño de sus funciones, entre las que destacamos velar por la observancia de los preceptos de la propia Ley y cuantos otros estimasen necesarios para asegurar, de forma indirecta, el trato adecuado de los datos de los afectados[15].

Con posterioridad, y una vez existían ciertas disposiciones federales y territoriales que regulaban la materia, es dictada la *Bundesdatenschutzgesetz*, como Ley Federal de Protección de Datos de la República Federal Alemana de 1977, en la cual se recoge una normativa general de principios susceptible de ser aplicados subsidiariamente a otros ámbitos o contextos, lo cual explica que acuda con frecuencia al empleo de conceptos jurídicos indeterminados, y trate de no entrometerse en competencias que excedan de aquellas bajo el control del gobierno federal.

La Ley Federal de Protección de Datos de 1977 recoge una serie de disposiciones generales, cuyo objeto es evitar la lesión sobre intereses dignos de protección de las personas naturales afectas por el tratamiento automatizado de datos que le conciernen, cuando el tratamiento sea efectuado por el sector público y privado. Entre las disposiciones, se observan diversas innovaciones con motivo de la prontitud de tratamiento de la materia objeto de normativización, posteriormente acogidas por otras legislaciones, tales como el comisario de protección de datos, la concesión a los titulares de datos del derecho de bloqueo, y la tipificación de ilícitos penales e infracciones asociadas al tratamiento de datos. De otro lado, impone a aquellas entidades pertenecientes a la Administración Pública que procesen datos, la adopción de las medidas técnicas necesarias -esto es, la contratación y dotación de suministro de

[14] *Intersoft consulting, Datenschutz-Grundverordnung*, recuperado en julio de 2022, accesible desde <https://protecciondata.es/historia-normativa-proteccion-datos/>

[15] Suñé Llinás, E. (2021), *Derecho informático: informática jurídica y Derecho de la informática*, working papers, accesible en <https://dialnet.unirioja.es/servlet/autor?codigo=59108>

medios tecnológicos y personales suficientes y adecuados- para garantizar la observancia de la citada Ley[16].

Es atractivo que el texto legal hace una distinción entre las particularidades jurídicas aplicables al sector privado y al público, y fija, a su vez, un sistema de control congruente con dicha diferenciación, a saber, respecto de los organismos públicos, impone a las diversas entidades de la Administración Federal la obligación de cumplir con aquello dispuesto por la legislación, y dictar disposiciones administrativas que regulen la aplicación de la ley en su respectivo ámbito de competencias y, a su vez, configura una autoridad de control, el Comisario Federal de Protección de Datos, encargada de supervisar la observancia de la misma, así como otras disposiciones aplicables a la protección de datos, inclúyanse aquí disposiciones generales y actos administrativos incluso.

De otro lado, en cuanto al tratamiento de datos por entes privados, la Ley encomienda, de nuevo, la competencia para su vigilia al Comisario Federal de Protección de Datos y a las autoridades estatales. Respecto de la figura del Comisario, ha de ser nombrado, prevé la norma, por cada entidad que recoja, trate y elabore perfiles a través de datos personales, como responsable de las instrucciones propias del empeño de su cometido; y, en lo que a las autoridades estatales compete, éstas son fijadas por los Estados, a través de los Gobiernos, y, de nuevo, les es obligada la observancia de lo sancionado en la Ley, aunque solo a requerimiento del afectado cuando el mismo, vía instancia de parte, así lo requiera.

Ubicamos también en este periodo la *Data Lag 1973/289*, de Suecia, mediante la que se imponía un sistema de registro abierto para publicitar los bancos de almacenamiento de datos personales de personas físicas, cuando estos hubiesen sido cosechados mediante sistemas de automatización, cuyos sistemas, debían contar con autorización administrativa para proceder a la automatización y recolecta, asociados -dichos bancos- a una autoridad de control, denominada *Datainspektionen*, expresión del *Obusman* proyectado al tratamiento de datos que vela por el respeto a la ley, con facultades inspectoras, normativas y procedimentales para, incluso, aplicar sanciones, pero éstas de naturaleza judicial y no administrativa[17].

Como su análoga alemana, la *Data Lag 1973/289* contemplaba un extenso catálogo de ilícitos sancionados penalmente con penas alternativas de multa y, en algunos casos, privación de libertad[18]. Este intenso control que encontramos en la norma sueca ha sido reproducido de forma análoga en las experiencias del Derecho comparado. Conviene destacar algunas particularidades de su sistema como, por ejemplo, la presencia de autorización previa al funcionamiento de bases de datos, las cuales han sido

[16] Revista chilena de Derecho informático, Op. Cit., pág. 10.

[17] Suñé Llinás, E. (2021), *Derecho informático: informática jurídica y Derecho de la informática*, working papers, accesible en <https://dialnet.unirioja.es/servlet/autor?codigo=59108>

[18] Data Lag 1973/289, acceso disponible en <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>

transformadas en la práctica, y desde el punto de vista del Derecho administrativo, en sistemas de notificación y, según los casos, de inscripción registral, con transferencia de responsabilidad a la autoridad de control nacional[19].

Esta primera normativización se caracterizó por concentrar la protección mediante la técnica de reglamentación en bases de datos, imponiendo restricciones a la constitución de estas al férreo control de la Administración mediante sistemas de autorización y previa inscripción.[20] Así, se contemplan entidades y organismos de naturaleza administrativa con la obligación de velar por el cumplimiento de las prerrogativas contenidas en la norma, capaces de fiscalizar cualquier dato relativo a la fase de preparación, constitución o ejecución de la base o sistema.

En esta línea, las constantes y enérgicas transformaciones informáticas forzaron el nacimiento de una segunda generación de leyes que, aleccionadas de la práctica anterior, tenían como objetivo reducir el número de menoscabos administrativos a fin de prescindir de un control farragoso e inútil respecto de los objetivos de la norma, librar de competencias *ex ante* a las Administraciones competentes y, así, trasladar todas las garantías sobre el tratamiento de datos al particular mediante la consagración de derechos subjetivos plasmados en un procedimiento concreto[21]. Esta segunda generación normativa se yergue sobre una preocupación que en la doctrina aún no había cristalizado, cuál era la distinción entre datos sensibles y aquellos ajenos a esta categoría -pero no por ello menos merecedores de garantía y protección-, por dejar entrever algún que otro precedente judicial que el tratamiento de esta categoría de datos era, efectivamente, lesivo para la intimidad de las personas y cuando no, dicha lesión era instrumentar para profanar otros bienes jurídicos anejos a los derechos fundamentales del afectado. Este fue el caso de la *Privacy Act* de 1974 y la *Loi n. 78/17 de janvier, relative a la Informatique, aux Fichiers et aux Libertés*, de 1978[22] (Ley de Informática y Libertades de Francia en adelante).

---

[19] Data Lag 1973/289, ibid., art. 25.

[20]Entendemos un sometimiento del ejercicio a la creación de bases de datos a los controles administrativos del momento cumplía con las exigencias legales de la norma de aquel momento que, ambiciosa como era, se mostraba un poco parca en cuanto a las dotaciones técnicas que pudiesen lograr efectivo el control en términos materiales, pues la Administración del momento y su personal destacaban, como la práctica puso de manifiesto, por la ignorancia y desactualización tras las complejidades técnicas relativas al empleo de técnicas informáticas y tratamiento de datos. La irrupción normativa como novedad en el ordenamiento jurídico iba acompasada, proporcionalmente y cómo se ha tratado de exponer en la justificación que sirve a su aparición, con la novación de las técnicas y materiales informáticos inherentes al procesamiento de datos que no destacaban precisamente por su falta de complejidades a la hora de abordar su estudio y trabajo, tarea complicada aún más por la exponencial novación que motorizaba un cambio de dificultosa adaptación humana.

[21]*El Derecho, Historia de la Protección de Datos,* publicado el 8 de octubre de 2020, disponible en <https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido>

[22] *Légifrance, République Française,* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, disponible en <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460>

Respecto de la *Privacy Act* de 1974[23], la exposición de motivos de la norma prioriza su objetivo como proteger la intimidad de los individuos cuyos datos quedan recopilados en sistemas de tratamiento, información e identificación efectuados por entes y órganos federales, con exención de aquellos entes privados que, por encargo de un ente u organismo de Derecho público, proceda a la recolección de dichos datos para servir a los fines de aquellos.

De nuevo es relevante el control otorgado a la autoridad administrativa competente: la *Privacy Act* habilita, a los efectos de realizar una cosecha de datos, al otorgamiento y consentimiento del individuo cuyos datos son afectos por el tratamiento, salvando aquellos tratamientos que respondieran a necesidades de orden público.[24] Esta norma reconoce al titular el derecho de acceso, y el órgano concedente a la vista del expediente que contenga los datos objeto de vista, en el que debe figurar aquellos registros en los que obren sus datos, con posibilidad de solicitar una copia del expediente y, en caso de así considerarlo, instar la modificación de los datos que obren en él. Además, confería al afectado por el tratamiento la posibilidad de solicitar al órgano encargado del tratamiento el asesoramiento sobre la posible impugnación judicial de cualquier controversia cuyo origen se situara en el tratamiento de sus datos.

A diferencia de la *Privacy Act* de 1974, y como sucede con la legislación sueca y alemana, la ley francesa prevé la creación de un órgano nacional de control (*Comission Nationale de L'Informatique et des Libertés*), encargada de velar por la aplicación de la norma, recibir y atender las reclamaciones relativas al contenido de esta, y con potestades de supervisión[25].

El valor de este desenfreno normativo no agota su relevancia en el intento de reglamentar las bases de datos en sí, sino cómo tras un primer esfuerzo normativo por regular las mismas, proceden a centrar la atención normativa en la clasificación atendiendo a los datos en sí, estableciendo categorías y tipologías en virtud de su naturaleza, amén de conferir mejores derechos a los afectados por el tratamiento.

---

[23] *US Departament of Justice, Overview of the Privacy Act of 1974 (2020 edition)*, recuperado en junio de 2022, accessible en <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>

[24] La realidad es que la recogida por instituciones federales adscritas al Gobierno Estadounidense resultó en una práctica que, a ojos de cualquier jurista, fue fraudulenta bajo el amparo de la ley, pues la misma cláusula que concedía la exención de consentimiento del afectado para el tratamiento de datos por razón de orden público, fue empleada como paraguas para obrar prácticas abusivas determinantes en la realización de perfiles identitarios en la época de una paranoia política nutrida por la idiosincrasia propia del momento histórico-geográfico. Concretamente en Unated States, Department of Justice, *The Freedom of Information Act, 5 U.S.C.*, accessible en <https://www.justice.gov/oip/freedom-information-act-5-usc-552>

[25] Bibent, M. (1993), *Informática, personas y libertades. El proyecto de Ley español y la experiencia francesa*, publicado en *Encuentros sobre informática y Derecho*, Instituto de informática jurídica, págs. 53-62.

En 1978 tiene lugar el mayor esfuerzo legislativo en la materia[26], en el seno de una nueva Europa libre, con motivo de la promulgación de las Leyes de Francia, Noruega, Dinamarca y Austria -acompañando este último país las medidas legislativas de una modificación constitucional-, al mismo tiempo que la Constitución Española aportaba visibilidad sin intención alguna a la misma cuestión en su art. 18.4[27]. Conviene resaltar la especial sensibilidad de Portugal hacia la protección al derecho de datos personales que, en vista de las relaciones entre sus ciudadanos y las controvertidas actuaciones de la Administración en lo que a funciones de policía compete, condujo a la prohibición constitucional de un número nacional único e identificador de cada ciudadano.

Finalmente, queda por resaltar el papel de la *Data Protection Act* 1984[28], conformada por disposiciones generales y normas relativas a la inscripción y vigilancia de los usuarios de los datos y de las oficinas de servicios informáticos, denominación emplead para referirse a los responsables de base o de registro de datos; derechos de las personas concernidas, un saturado sistema de excepciones y un régimen de recursos, todo ello anejado de una serie de anexos con principios aplicables al tratamiento de los datos y su interpretación. Esta norma inglesa de tratamiento de datos personales es aplicable a sector público y privado, aun cuando se limita a los datos procesados de forma automatizada. En lo que concierne a los mecanismos de control, si bien contempla la adopción de códigos de conducta y el empleo de reglamentación especial, los mismos se relacionan con las funciones de una autoridad de control (denominada *Registrer*), a quien confía el registro de los bancos de tratamiento de datos de afectados, la asistencia jurídica y técnica a interesados y la disposición de una serie de medidas cautelar. Además, esta norma crea un órgano administrativo (*Data Protection Tribunal*) que, sin funciones jurisdiccionales, actúa como segunda instancia administrativa respecto de las decisiones tomadas por el *Registrer*, cuyas decisiones, a su vez, podrán ser impugnadas ante los órganos judiciales.

Desde la perspectiva nacional, encontramos en España la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (en adelante, LORTAD), adoptada en 1992, piedra angular en la posterior juridificación de otros aspectos relacionados con el Derecho de la informática y de la protección de datos[29]. Si bien como se ha indicado con anterioridad el art. 18 de la Constitución Española asegura que "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*",

[26] Suñé Llinás, E. (2021), *Derecho informático: informática jurídica y Derecho de la informática*, Op. Cit. Pág. 12.

[27] España, Cortes Generales (1978). Constitución Española de 29 de diciembre de 1978, Boletín Oficial del Estado, 1978-31229, accesible en <https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229>, art. 18.4

[28] *Legislation.gov.uk, Data Protection Act 1984 (whole act)*, recuperado en junio de 2022, accessible en <https://www.legislation.gov.uk/ukpga/1984/35/enacted>

[29] España, Cortes Generales (1992), Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento de datos automatizado de carácter personal, en BOE núm. 262-37037, accesible en <https://www.boe.es/boe/dias/1992/10/31/pdfs/A37037-37045.pdf>

esta declaración constitucional no se materializó en la adopción de una temprana legislación circunscrita a la protección de datos personales, pese a que diversos intentos normativos se sucedieron desde 1984 para satisfacer dicha necesidad.

Con anterioridad a la promulgación de esta norma, España ya había tenido ocasión de ratificar el Convenio 108 del Consejo de Europa para la Protección de las personas con respeto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981[30] (en adelante, Convenio 108) al que, por razones de singular importancia como su naturaleza y origen, nos referiremos en el epígrafe siguiente. La LORTAD extendió su ámbito de aplicación a los ficheros automatizados de los sectores público y privado, con una serie de excepciones detalladamente descritas y una serie de prerrogativas en lo que a la protección de los datos de las personas físicas concernía. Asimismo, enunciaba una serie de principios informadores del Derecho de la protección de datos, y enumeraba una serie de derechos subjetivos a disposición de los afectados por el tratamiento.

A fin de cumplir con las expectativas de su propio cuerpo legal, la LORTAD encomienda el control de su aplicación a un ente de Derecho público independiente, la Agencia de Protección de Datos, compuesta por un director y un órgano colegiado, el Consejo consultivo, compuesto por diversos representantes institucionales de diversos ámbitos (p. ej., de empresas grandes del sector privado; organizaciones de consumidores y usuarios; de determinados sectores económicos; etc.). La ley prevé la creación de entidades de control análogas y supeditadas a aquella de la Agencia de Protección de Datos a nivel autonómico. Contenía previsiones relativas a la transmisión internacional de los datos, punto en el cual trasponía el Convenio 108, optando por exigir que el Estado de destino de los datos proporcionara un nivel de protección análogo al español, garantía un tanto mermada en la práctica al reconocer la norma, a su vez, la potestad de la Agencia de Protección de Datos de otorgar autorización a dicha traslación de datos a pesar de las diferencias de protección entre la legislación de origen y la de llegada, a cambio de la satisfacción de unos niveles mínimos de garantía de protección[31].

La sucesión de novedades jurídico-formales tendentes a la protección de datos de carácter personal es tan relevante en cuanto a su novedad como abstracta en su formulación e imprecisión, con motivo de la falta de precedentes en lo que a la práctica de su vulneración y restitución -del derecho- sucede. Este auge normativo es identificable en el ámbito del Derecho internacional público que, en el ámbito regional

[30] España, Jefatura del Estado (1981), Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, en BOE núm. 274-36000, accesible en <https://www.boe.es/boe/dias/1985/11/15/pdfs/A36000-36004.pdf>

[31] La LORTAD, en este ámbito, era muy pobre y poco garantista respecto a las traslaciones de datos de carácter internacional: el volumen en la época era relativamente alto, y la supeditación de eximir de la garantía de asegurar un nivel análogo de protección al de la norma española mediante el sistema de autorización, ofrecía un alto nivel de discrecionalidad a la Agencia de Protección de Datos en lo que a la concesión de dicha autorización se refiere, que resultó en la merma de derechos de los ciudadanos y en la desvirtuación de la finalidad perseguida por la propia norma.

europeo, produce relevantes disposiciones con su raíz en el Convenio núm. 108 del Consejo de Europa, de 28 de enero de 1981 (en adelante el Convenio núm. 108), de protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal, que establece por primera vez un modelo que permitirá una relativa homogeneidad legislativa en Europa Occidental y más allá, pues el Convenio 108 no fue aprobado con carácter y naturaleza de Convenio Europeo, sancionando así la hipotética entrada de Estados ajenos al Consejo de Europa al referido. El texto fue ratificado por España en 1984, y no sería hasta 1987 que se produjera su entrada en vigor, momento en que era requerida la preceptiva ostentación de medidas legislativas y organizativas en funcionamiento por parte de los Estados parte, a fin de garantizar la efectiva sanción sobre los derechos de protección de datos.

2. EVOLUCIÓN NORMATIVA HACIA UN DERECHO AUTÓNOMO E INDEPENDIENTE

Los últimos ejercicios legislativos hasta la actualidad se suceden hasta comenzar de regular, de forma directa y estricta, la protección de datos personales configurándolo como un derecho autónomo e independiente.

Así, en cuanto a los primeros, encontramos la Declaración Universal de Derechos Humanos, en la que se afirma que nadie será objeto de injerencias arbitrarias en su vida privada, en su familia, en su domicilio o en su correspondencia, así como tampoco de ataques frente a su honra o reputación, pues toda persona tiene derecho a la protección de la ley ante dichas agresiones[32]. Igualmente, el Pacto Internacional de Derechos Civiles y Políticos proclama que nadie podrá ser objeto de injerencias arbitrarias o ilegales en su vida privada, familia, domicilio o correspondencia, ni agresiones frente a su honra o reputación[33].

En el Convenio Europeo para la Protección de los Derechos Humanos se explicita que toda persona tiene derecho al respeto de su vida privada y familiar, así como de su domicilio y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto dicha injerencia está prevista por la ley, y constituya una medida que, en una sociedad democrática, resulte necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás[34].

[32]España, Cortes Generales (1977), Instrumento de Ratificación de España del Pacto Internacional de Derechos Civiles y Políticos, hecho en Nueva York el 19 de diciembre de 1966, BOE núm. 103-9337, de 30 de abril de 1977, accesible en <https://www.boe.es/buscar/doc.php?id=BOE-A-1977-10733>, art. 12.

[33] España, Cortes Generales (1977), Ibid.

[34] España, Jefatura del Estado (1973), Instrumento de Ratificación del Convenio para la Protección de los derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente, en BOE núm. 243, de 10 de octubre de 1979, BOE-A-1979-24010, <https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010>, art. 8.

La perspectiva que justificaba los orígenes del derecho a la protección de datos era clara, pues apuntaba hacia la conciliación entre la tensión existente por el uso intensivo de las técnicas que ofrecía la informática frente a la vida privada. Esta es la lógica que se trató de perseguir, a nivel nacional, mediante el forzado encaje al amparo del art. 18.4 CE, desarrollado mediante la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, aprobada con premura por la proximidad de la entrada en vigor del Convenio de Schengen, justificada por la flexibilidad económica resultado de aquella predicada de la nueva situación político-jurídica en la que las limitaciones entre los Estados signatarios de este Tratado trasladaban el control entre intercambios a las fronteras de los países terceros, miembros del mismo. Igualmente, a pesar de que la Ley de Regulación del Tratamiento automatizado entró en vigor con anterioridad a las disposiciones de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Paralelamente a este proceso de juridificación, los intereses económicos participativos de los procesos legislativos que intervienen en la creación de estas normas promueven una liberalización de la circulación de los datos, no prescindiendo de la regulación en sentido estricto, sino a través de fórmulas legislativas que, sin perder el horizonte de protección de datos, favorezcan la creación de un protomercado de circulación de datos personales. Es a razón de estas pretensiones cuando las instituciones de la Unión trabajan hasta resultar en la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En el año 2000, con el advenimiento de un nuevo siglo marcado por la cristalización de los avances tecnológicos anteriormente expuestos, el panorama en protección de datos sufre un cambio radical: doctrinalmente comienza una nueva etapa reflexiva sobre la consideración como derecho autónomo e independiente de la protección de datos respecto de aquellos tradicionales como el honor o la intimidad que, a efectos ilustrativos, son materializados mediante el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea[35], además de la deductiva separación respecto del tradicional engarce que se hace sobre el derecho aquí tratado frente a aquel del respeto a la vida privada y familiar, consagrado, respectiva y separadamente, en el art. 7 del mismo texto normativo.

Existe ya en términos normativos y con un alcance jurídico institucionalizado y de aplicación directa una proyección bien diferenciada del derecho a la protección de datos frente a otros de los que, en las ocasiones más afortunadas, era en todo caso deducido de los tradicionales, pero nunca invocable de modo autónomo por cuanto su juridificación se encontraba implícita y, a menudo, bajo la responsabilidad de la

[35] Unión Europea (2010), Carta de Derechos Fundamentales de la Unión Europea, DOUE núm. 83, de 30 de marzo de 2010, págs. 389 a 403, accesible en <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>, art. 8.

discrecionalidad y perspectiva del juez que estudiara el caso controvertido sobre según qué derecho -intimidad o vida privada- se tratase.

De forma análoga a la visibilización de este derecho como consecuencia de su proceso de independencia conceptual y material, es consecuente que los particulares pudiesen reputar determinadas violaciones de este derecho a la invocación del mismo pues, como es lógico, la ausencia de consagración de un derecho en una norma invocable por el particular hacía difícil, cuando no imposible, la invocación del mismo, dado que pendía en todo caso de la valoración del juez a quien correspondiese el conocimiento del caso de estimar (o no) dicha violación de un derecho que, o bien se infería de la interpretación de aquellos tradicionales, o bien se ocultaba bajo una absorción de las violaciones del derecho a la protección de datos por los derechos a la intimidad o al honor.

Así sucedía con anterioridad a la conceptualización de este derecho, como podemos observar mediante la seleccionada jurisprudencia del Tribunal Europeo de derechos Humanos que, de forma cautelosa y aproximada, hace concesiones hacia el derecho a la protección de datos, pero siempre desde la cómoda y conocida perspectiva del derecho a la vida privada y familiar[36]. Hay que añadir a estos precedentes los pronunciamientos del Tribunal de Justicia de la Unión Europea en materia de protección de datos, que coadyuvan a la configuración de la protección de datos como derecho autónomo[37].

Por su parte, y en lo que a la óptica nacional compete, el Tribunal Constitucional consagra la naturaleza de derecho autónomo e independiente del derecho a la protección de datos mediante dos sentencias de intensa trascendencia, no solo por la novedad material tratada en el pronunciamiento, sino por el comprometido esfuerzo que realiza para desprender, del art. 18.1 CE[38], el derecho a la protección de datos.

Como conclusión, entiende el que suscribe que, si bien las preocupaciones por el derecho a la protección de datos son loables por cuanto persiguen limitar las intromisiones indebidas, la configuración de este derecho, desde su evolución histórica, está pensada para actuar frente a las barreras de regímenes políticos autocráticos e injerencias de la prensa sensacionalista. Sin embargo, una mejor conceptualización de este derecho, más actualizada, requiere de una regulación orientada a frenar las intromisiones ilegítimas de las nuevas tecnologías en lo que al tratamiento de datos privados se refiere.

---

[36] España, Jefatura del Estado (1979), instrumento de ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente, accesible en <https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010>, art. 7.

[37] Unión Europea, Tribunal de Justicia de la Unión (2003), Asunto C-101/01, de 6 de noviembre de 2003, accesible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN>, fundamento jurídico 99.

[38]España, Tribunal Constitucional (2000), Sentencia del Tribunal Constitucional 290/2000, 30 de noviembre de 2000, núm. de recurso 201/1993 <https://vlex.es/vid/ri-56-29-106371>, fundamento jurídico 9.

CAPÍTULO II: EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

1. EL REGLAMENTO DE PROTECCIÓN DE DATOS: INTRODUCCIÓN

El Reglamento UE 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, es la norma principal y general en materia de protección y tratamiento de datos personales a nivel comunitario y, junto con la Directiva UE 2016/680, sobre protección de datos personales para las autoridades policiales y de justicia, del paquete de normas sobre protección de datos en la Unión.

Tres son los objetivos del Reglamento, cuales son (i) garantizar el derecho fundamental a la protección de datos personales; (ii) proteger los derechos y libertades fundamentales de las personas físicas; y (iii) lograr la libre circulación de los datos personales en la Unión. La Ley Orgánica 3/2018, de protección de datos personales y garantías de los derechos digitales emula, a su vez, estos tres objetivos del Reglamento con su propia terminología[39]: (i) adaptar el ordenamiento jurídico español al RGPD; (ii) completar las disposiciones del RGPD, pues los Estados miembros tienen la capacidad de precisar aún más la aplicación de las normas de protección de datos en sectores específicos -sector público acceso a documentos oficiales, p. ej.,-; y (iii) garantizar los derechos digitales de la ciudadanía, a la luz del art. 18.4 de la Constitución, así como garantizar el pleno ejercicio de estos derechos.

Respecto del primer objetivo del Reglamento, la garantía del derecho fundamental a la protección de datos personales[40], este es consagrado en la norma con una serie de peculiaridades en relación al tratamiento de sus datos cuando se trate de personas físicas, articulando así el derecho de toda persona a la protección de datos personales que a esta le conciernan. En cuanto a las peculiaridades del tratamiento, están orientadas a dotar de un espíritu garantista al procedimiento de tratamiento en sí, en tanto que este debe ser llevado a cabo de forma lícita, leal y transparente.

En concreto, establece las normas para aquellos que realizan tratamientos de datos de personas físicas, con independencia de que sean responsables o encargados del tratamiento, y han de cumplir con estas exigencias -de licitud, lealtad y transparencia- para ver colmado el mandato en la norma sobre protección de datos personales. Estas tres exigencias están íntimamente relacionadas con los principios que marcan la línea de cumplimiento del tratamiento de datos personales; las bases o condiciones jurídicas de legitimación del tratamiento que operan entre la persona física cuyos datos están

[39] España, Cortes Generales (2018), Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en BOE núm. 294, de 6 de diciembre de 2018, accesible en <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>, art. 1.

[40] España, Cortes Generales (2010), Tratado de Funcionamiento de la Unión Europea, DOUE núm. 83, de 30 de marzo de 2010, accesible en <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002>, art. 16.1.

siendo tratados y el responsable o encargado del tratamiento; los derechos de los afectados por el tratamiento y de los interesados por el tratamiento; y la existencia de una autoridad de control independiente. Redunda que de una lectura de estas exigencias en relación con los fines para os que están previstas se deduzca que la finalidad del Reglamento es aquella de garantizar el control sobre sus datos personales a la persona física a la que se refieren los datos personales, quien puede ser el interesado, la persona concernida por el tratamiento o el titular de los datos.

Respecto del segundo objetivo, cual es la protección de los derechos y libertades fundamentales de la persona, el Reglamento tiene por finalidad proteger a la persona física en lo que respecta al tratamiento de sus datos de carácter personal, con independencia de su nacionalidad o residencia, pues la norma protege las libertades y derechos fundamentales de la persona física en cuanto a protección de datos. Esta indiferencia frente a la nacionalidad o residencia de la persona cuyos datos están siendo tratados a efectos de otorgarle -o no- protección a dicho tratamiento, se desprende de la lógica que acompaña a la circulación de datos personales y, por ende, al tratamiento de los mismos: son flujos de informaciones que cuentan con toda clase de facilidades para lograr su inmediación por las características del entorno en el que se desplazan -la red- sin consecuencia alguna por la fijación de estos a las particularidades del flujo de los bienes tradicionales (no han de pasar por aduanas, adolecen de cualquier tipo de permiso o sistema de vigilancia y control que examine todo lo relativo a su fluctuación en la red). Esta práctica no solo puede resultar patológica y perjudicial para los datos de la persona tratada, evidentemente, cual es en parte el ánimo del Reglamento evitarla, sino que este también, y como se desarrollará respecto al régimen sancionador, pretende disuadir al responsable o encargado del tratamiento -así como personas ajenas a estas figuras con la lascivia suficiente como para querer sacar provecho del tratamiento- de hacer un uso indebido -ilegítimo, desleal e ilícito- de los datos de la persona, cualquiera que sea su nacionalidad o residencia. Estas precisiones, por lógica, atienden más a la circunstancia de residencia que a aquella de nacionalidad pues, como se ha expuesto, la naturaleza de los flujos transfronterizos de datos es de una fuerza tan agresiva que una reducción del ámbito de aplicación del Reglamento que atomizara su protección garantista en términos de estas características de la persona -localización física o fijación jurídica de la residencia- devendría, no solo en una ineficacia objetiva por la naturaleza de los mencionados flujos, sino en un autosabotaje por parte de la propia norma, que debería prever mecanismos de filtro y sesgo de búsqueda a la hora de determinar qué tratamientos han de regirse por lo dispuesto en la norma atendiendo a tales circunstancias.

En cuanto a la libre circulación de datos personales en la Unión Europea y su circulación, no puede ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que al tratamiento de datos personales incumbe. Pretende la norma conferir así la protección suficiente al derecho de las personas a los datos personales, reflejando la naturaleza de la protección de datos personales como derecho fundamental en la Unión Europea. Por tanto, la libre circulación de datos personales, entendiendo por esta el libre flujo transfronterizo de datos personales en territorio comunitario facilita la integración económica y social de la que se nutre el mercado interior, contribuyendo así el legislador europeo a la plena realización de un espacio de

libertad, seguridad y justifica y de una Unión económica, así como al progreso económico y social, con especial mención al refuerzo de las novaciones sobre las convergencias económicas y su materialización en nuevos tipos de bienes o productos y los mercados que dichos tipos puedan crear[41].

2. ÁMBITO DE APLICACIÓN MATERIAL

Como en el estudio de toda norma, debemos distinguir entre el ámbito de aplicación personal y territorial.

Partiendo del ámbito de aplicación material del Reglamento[42], la norma se aplica al tratamiento parcial o total automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. La protección de datos, como se desarrollará en cuanto a los sistemas competentes, está orientada a la protección de las facetas de la vida íntima de las personas frente a aquellas técnicas de alto riesgo que comprometan la respuesta conductual de alguien en base a los datos recabados de esta. Por tanto, no se aplicará a la protección de datos personales cuando estos sean contenidos en un fichero que no esté sistematizado conforme a los criterios específicos del Reglamento, no siéndole de aplicación esta norma. La práctica se ha mostrado atomizada y dispar en lo que a la aplicación del Reglamento compete y, por ello, los sujetos obligados -bien sean particulares como empresas o Administraciones Públicas- prefieren recurrir a los avisos de tratamiento de datos conforme a la normativa del Reglamento aun cuando los ficheros en los que se consignan los datos, o las características del tratamiento, en contadas ocasiones, no se ajusten al ámbito de aplicación del Reglamento, lo cual tampoco resulta contrario a la propia norma ni a la intención del legislador comunitario cuando introdujo las disposiciones al efecto con la abstracción de la que se nutren los conceptos del Reglamento, como así ha entendido la jurisprudencia del Tribunal de Justicia de la Unión. Así, el TJUE se ha pronunciado, p. ej., sobre la obligación de los Testigos de Jehová y sus predicadores en el sentido de que, tanto la comunidad [de Testigos de Jehová] como sus predicadores, es responsable del tratamiento de la información que recogen en sus visitas puerta a puerta, y dicha recogida y tratamiento sobre la información ha de ser respetuosa con la normativa de Protección de Datos[43].
Por tanto, de forma positiva, el ámbito de aplicación material del Reglamento sobre Protección de Datos Personales será el del tratamiento automatizado de datos, así como

[41] El mercado interior: principios generales, en Fichas temáticas sobre la Unión Europea, recuperado en diciembre de 2022, accesible en <https://www.europarl.europa.eu/factsheets/es/sheet/33/el-mercado-interior-principios-generales>.

[42] Unión Europea (2016), Op. Cit. Pág. 22.

[43] Unión Europea, Tribunal de Justicia (2018), Asunto C-25/17, accesible en <https://curia.europa.eu/juris/document/document.jsf;jsessionid=B4D45BD37420CB20CCDADD6A530A761C?text=&docid=198949&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=3738318>, fundamento jurídico 44.

aquellos tratamientos que, sin inferir automatización alguna, serán incluidos en un fichero.

Al efecto de establecer las excepciones y exclusiones del ámbito de aplicación, ha de recurrirse a un criterio de proporcionalidad, pues un resultado no deseado [por la norma] sería el de aplicar las normas de protección de datos en los que esta norma no resulta competente para su aplicación. En este sentido, no será de aplicación el Reglamento en los siguientes supuestos:

A. Actividades fuera del ámbito de aplicación del Derecho comunitario. En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, como algunos servicios que emplean tecnologías que sirven como, por ejemplo, sistemas de financiación alternativos a los de la Directiva 2018/843, sobre prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.

B. Actividades relativas a política exterior y seguridad común. Por parte de los Estados miembros, cuando lleven a cabo actividades relacionadas con la política exterior y la seguridad común, comprendidas en el Título V, Cap. 2º TUE[44].

C. Actividades exclusivamente personales o domésticas. Se excluye el tratamiento de datos efectuado por una persona física en el ejercicio de actividades circunscritas al ámbito personal o doméstico, entendiendo por aquellas las que se realicen en la esfera privada, como la correspondencia y la llevanza de un repertorio de direcciones o la actividad en redes sociales y la actividad en línea que se efectúe como consecuencia de las actividades citadas. Conviene distinguir que, sin perjuicio de lo anterior, la normativa sí se aplicará a los responsables y a los encargados del tratamiento de los datos generados como consecuencia de estas actividades, que por lógica excede ya la domesticidad del ámbito que trata de salvar el Reglamento por cuestiones de lógica práctica normativa[45].

[44] Unión Europea, Tribunal de Justicia (2020), Asunto C-311/18, accesible en <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=3742569>, y, en la misma línea, Unión Europea, Tribunal de Justicia (2020), Asunto C-623/17, accesible en <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=3744808>.

[45] Unión Europea (2016), Reglamento 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 esos datos, y por el que se deroga la Directiva 95/46/CE, considerando núm. 18, accesible en GDPR TEXT, <https://gdpr-text.com/es/read/recital-18/>

D. Tratamiento de datos por autoridades policiales o judiciales en el ámbito penal. El Reglamento no será de aplicación al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención, cuyo tratamiento se encuentra regulado en la Directiva 2016/680, transpuesta al Ordenamiento nacional mediante la Ley Orgánica 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[46].

Sin perjuicio de lo anterior, se encuentran excluidos por definición del ámbito de aplicación del Reglamento:

A. Los datos de personas jurídicas, pues la norma no regula el tratamiento de datos personales relativos a personas jurídicas y, concretamente, cuando estas se constituyan como personas jurídicas. Así, no serán de aplicación las disposiciones de la norma a datos como la firma, el nombre o los datos de contacto de la persona jurídica[47].

B. Las instituciones, órganos y organismos de la Unión. A los tratamientos de datos personales llevados a cabo por las instituciones comunitarias -Comisión Europea, Parlamento Europeo, Consejo de la Unión, Banco Central de la Unión y Supervisor Europeo de Protección de Datos- les será de aplicación una normativa específica, el Reglamento UE 2018/1725, 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.

C. Los datos anonimizados. Cuando los datos personales son objeto de un tratamiento cuyo resultado no permita identificar de forma definitiva a la persona física a la que se refieren, tiene lugar la anonimización. Por tanto, si los datos personales son anonimizados, la consecuencia es que deja de ser aplicable la normativa sobre protección de datos personales, pues ya es imposible la identificación por los datos que hacen identificable a la persona, al quedar todo rastro de nexo con identidad en estos eliminado.

[46] España, Cortes Generales (2021), Ley Orgánica 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, en BOE núm. 126, accesible en <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=3744808>.

[47] Unión Europea (2016), Op. Cit. Pág. 23, considerando núm. 14.

D. Datos de personas fallecidas. El Reglamento se aplica a la protección de datos personales de personas fallecidas, sin perjuicio de que los Estados miembros puedan establecer normas relativas al tratamiento de datos personales de estas[48].

En línea con aquellos datos excluidos del ámbito de aplicación del Reglamento, también podemos encontrar una serie de categorías de datos a los que no les es directamente aplicable el Reglamento[49]. Así, se trata de aquellos datos cuyas actividades no se encuentran comprendidas de forma directa en el ámbito de aplicación del Derecho comunitario y, por ende, en caso de que exista una legislación específica aplicable al caso, será esta la prioritaria a la hora de determinar la regulación sobre el tratamiento concreto, siendo dichos datos excluidos aquellos relativos a los realizados al amparo de la legislación orgánica sobre régimen electoral; aquellos de instituciones penitenciarias; y, finalmente, todos aquellos de registros como el Registro Mercantil, Civil o cualesquiera de propiedad.

Finalmente, respecto de la información relativa a las personas jurídicas, dicha información no se encuentra, en términos generales, cubierta por la normativa de protección de datos, ya que estas se rigen por los principios de publicidad registral. Esta regla presenta una excepción, y es aquella en la que la denominación de la persona jurídica tiene su origen en el nombre de una persona física. Por ello, cuando los criterios de contenido, finalidad y resultado permitan considerar la información relativa a una persona jurídica o a actividades empresariales sobre información de una persona física, dicha información recibirá el tratamiento de datos personales y, por tanto, le será de aplicación la normativa de protección de datos.

3. ÁMBITO DE APLICACIÓN TERRITORIAL.

El ámbito de aplicación territorial del RGPD se encuentra recogido en el art. 3 del texto, y distingue tres supuestos de aplicación en función de la ubicación del sujeto cuya obligación es aquella desprendida del tratamiento de los datos. Así, encontramos una distinción entre responsable o encargado del tratamiento establecido en la Unión Europea, por motivos evidentes; responsable o encargado del tratamiento no establecido en la Unión Europea, por cuanto como se ha expuesto por las características de los propios datos y aquellos del ecosistema en el que se desenvuelven, así como los de los intereses y capacidades de los sujetos que los transmiten, la fluctuación de datos es la mayoría de las veces extracomunitaria; y responsable no establecido en la Unión Europea cuando le sea de aplicación el Derecho nacional.

[48] Unión Europea (2016), Op. Cit., pág. 23, considerando núm. 17.

[49] Unión Europea (2022), Reglamento (UE) 2022/868, del Parlamento Europeo y del Consejo de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724, en DOUE núm. 152, de 3 de junio de 2022, págs. 1 a 44, accesible en <https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80835>.

A efectos ilustrativos, cada supuesto de aplicación territorial del Reglamento es acompañado de las preceptivas indicaciones a la luz de las Directrices del Comité Europeo para la Protección de Datos, cuya configuración como *soft law* es especialmente relevante al objeto de estudio del presente trabajo.

A. Responsable o encargado del tratamiento establecido en la Unión. El primer supuesto en el que Reglamento es aplicable es aquel en el que el responsable o encargado tratan datos personales en actividades cuyo origen o situación de desarrollo de la actividad se encuentra en la Unión Europea, con independencia de que el tratamiento correlativo a la actividad tenga ya lugar o no en territorio comunitario[50]. Es decir, si la actividad que produce el tratamiento se encuentra en territorio comunitario, este supuesto configurará la procedencia de la aplicación de la norma, con independencia de que posteriormente el tratamiento tenga lugar en territorio comunitario o sea realice más allá de las fronteras de la Unión. Es relevante reflexionar entonces sobre el concepto de establecimiento, que a la luz de las de las Directrices 3/2018 del Comité Europeo de Protección de Datos, hace referencia no solo al establecimiento de un responsable o encargado del tratamiento, sino a la concreción de establecimiento en sentido estricto en la Unión Europea, de forma que para determinar si una entidad cuya base se encuentra fuera de la Unión ostenta un establecimiento en un Estado miembro, deberá realizarse una reflexión sobre dónde se realizan de forma efectiva las actividades económicas y el tipo de prestación que se lleve a cabo, así como el tipo de instalaciones en cuanto a las características -de rendimiento o infraestructuras, por ejemplo,- que presenten estas.

Las Directrices avalan la apreciación de establecimiento tras la comprobación de que las instalaciones al efecto son de una entidad eminentemente menor, pero lo suficiente como para garantizar la prestación de servicios en línea. Así, pretende el órgano supervisor que las empresas de internet prestadoras de servicios en línea, prescindiendo de maquinaria o medios de entidad suficiente o llamativa, recurran al empleo de tecnologías punteras y de una presencia mínima que, de un lado, presten servicios íntimamente relacionados o implicados en el tratamiento de datos personales y, de otro lado, eludan la aplicación de la normativa comunitaria por cuanto no cumplen los requisitos de establecimiento a la luz de la aplicación territorial de la norma.

Detallan las indicaciones que la mera presencia de un empleado de la entidad en la Unión Europea no es suficiente para colmar los requisitos de aplicación territorial del Reglamento, salvo que su

[50] Unión Europea (2016), Op. Cit., pág. 23, considerando núm. 22.

actividad se realice en el siguiente contexto, a saber, cuando la mera presencia de un solo empleado realice la actividad de forma suficiente y con un grado de autonomía y eficiencia suficiente que logre mantener, por sí solo, la estabilidad de las actividades. Por ende, y de forma negativa, cuando el empleado tenga su lugar principal de actividad en la Unión, pero el tratamiento no se lleve a cabo en el contexto de las actividades del empleado con base en la Unión, porque el mismo sea imputable a las actividades del responsable sito fuera de la Unión, la mera presencia del empleado no es suficiente para colmar las exigencias de la aplicación del ámbito territorial del Reglamento.

Por tanto, lo determinante para proceder a la aplicación del Reglamento en virtud del ámbito territorial no es tanto que el tratamiento en cuestión sea realizado por el propio establecimiento de la Unión, sino que el tratamiento sea consecuencia de las actividades realizadas en la Unión por el establecimiento sito, de forma que los dos elementos esenciales que han de observarse para la aplicación territorial de la norma son, de un lado, que el tratamiento sea correlativo a la actividad desarrollada en territorio comunitario y, de otro, que dicho contexto de actividad se desarrolle físicamente en territorio comunitario.

Para llegar a estas conclusiones ha de observarse, en primer lugar, la relación entre un responsable o encargado del tratamiento no perteneciente a la Unión y la existencia de establecimiento físico en dicho territorio, de forma que el análisis casuístico de los hechos demuestre la existencia de un vínculo indisociable entre las actividades de un establecimiento sito en la Unión, y el tratamiento de datos de un responsable o encargado del tratamiento no perteneciente a la Unión. De otro lado, otro criterio a tener en cuenta por parte del sujeto responsable a efectos del tratamiento o del órgano conocedor del litigio una vez tiene lugar la controversia concreta -como sucede a menudo en la práctica- es aquel relativo a la recaudación de ingresos pues, aquella llevada a cabo en la Unión por un establecimiento sito en territorio de esta, en la medida en que las actividades que realice puedan considerarse indisociablemente ligadas al tratamiento de datos personales cuando este tenga lugar fuera de la Unión, puede ser indicativo de un tratamiento de datos personales realizado por un responsable o encargado que derive en la suficiencia jurídica exigida a la hora de determinar la aplicación del Reglamento.

B. Responsable o encargado del tratamiento no establecido en la Unión Europea. El Reglamento será de aplicación a aquellos tratamientos de datos personales realizados por un responsable o encargado no

establecido en la Unión Europea, siempre que los afectados por el tratamiento de datos personales -es decir, aquellos cuyos datos se traten o sean legitimados en virtud del reconocimiento de interesados por la norma- se encuentren en la Unión y, además, su actividad se encuentre relacionada con: (i) la oferta de bienes o servicios a dichos interesados o afectados en la Unión, con independencia de que la relación prestacional de bienes o servicios esté afectada a la contraprestación económica a favor del prestador. Es por tanto preceptivo que se determine la evidencia sobre si el responsable o encargado, o bien un intermediario entre estos y el afectado o interesado, proyecta la oferta de dichos servicios a los interesados, pues no basta para determinar dicha intención el mero acceso al sitio web del responsable, encargado o intermediario en la Unión, mucho menos la disponibilidad y contacto mediante un medio de comunicación como, por ejemplo, un correo electrónico, o el uso de una lengua utilizada en el país de residencia del encargado, responsable o intermediario del tratamiento. Por tanto, lo relevante para el responsable o encargado, así como para el órgano enjuiciador *ex post* es determinar si mediante el empleo de una lengua de uno de los Estados miembros o de aquel en el que se prestan los servicios de acceso a la página web, así como el acceso a la propia página web, están orientados a la potencialidad de la prestación de servicios o bienes a personas en la Unión y, en caso de ser así, procederá la aplicación del Reglamento. Como se viene reiterando a lo largo de este trabajo, es intención de la norma evitar la desprotección y el fraude de la protección sobre la información de los usuarios comunitarios cuando estos accedan a páginas web o contacten con personas o entidades sitas fuera de la Unión y que ofrezcan a través de esta servicios o bienes. (ii) El control de su comportamiento, en cuanto que este se desarrolle en la Unión. Así, a fin de determinar si es considerable que una actividad de tratamiento control el comportamiento de los interesados, ha de evaluarse previamente si las personas físicas son objeto de un seguimiento en internet, lo cual incluye, lógicamente, la posibilidad potencial y no real de que posteriormente sea plausible el empleo de técnicas de tratamiento de datos personales, orientados a la elaboración de perfiles de una persona física con el fin de adoptar decisiones sobre él o de analizar o predecir sus preferencias, comportamientos y conductas.

En cuanto a las Directrices del Comité de Protección de Datos[51] sobre el tratamiento de datos personales efectuado por responsables o encargados no sitos en la Unión, las indicaciones sobre la aplicación del criterio de selección de destinatarios son:

[51] Comité Europeo de Protección de Datos (European Data Protection Board), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, accessible en <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en>.

A. Además de ser aplicables las Directrices al tratamiento por parte de un responsable o encargado del tratamiento no establecido en la Unión, el criterio de la selección de destinatarios se centra mayoritariamente en el objeto de relación cuyo nexo se relaciona con las actividades y, en base a un estudio o reflexión sobre dicho nexo, se dilucidará la aplicabilidad del Reglamento, caso por caso. Es por ello por lo que, por ejemplo, un responsable o encargado del tratamiento puede encontrarse sujeto al Reglamento en algunos supuestos de tratamiento de datos, pero no en otras, todo ello en base a una ponderación acerca del nexo respecto del objeto del tratamiento de datos.

B. Que el interesado se encuentre residiendo en territorio comunitario es un factor determinante para la determinación de la aplicación del criterio de selección de destinatarios, pero su nacionalidad o estatus jurídico no puede devenir en una limitación en contra de los fines perseguidos por la propia norma del ámbito de aplicación territorial del Reglamento. Así, el requisito de la situación de la residencia en territorio de la Unión ha de ser evaluado al mismo tiempo que se realice la actividad de tratamiento, a saber, la oferta de servicios o bienes o bien se realice el control del comportamiento conductual, con independencia de la duración de la oferta realizada o del seguimiento efectuado.

C. El tratamiento de datos personales de residentes o ciudadanos de la Unión que tiene lugar en un tercer país no conlleva la aplicación del Reglamento, salvo en aquellos casos en los que la oferta esté dirigida o relacionada con un seguimiento conductual de personas en territorio comunitario, de forma que sí será de aplicación el Reglamento.

D. Respecto de las actividades de tratamiento relacionadas con la oferta de servicios, la disposición apunta a actividades que, de forma intencionada, se dirigen a particulares sitos en la Unión.

Por supuesto, la oferta de servicios incluye igualmente la oferta de servicios de la sociedad de la información. Este criterio de selección de destinatarios de aplicación del Reglamento en función de las características objetivas del servicio y del tratamiento y subjetivas tanto de la intención del tratamiento como de la ubicuidad de los afectados por dicho servicio es aplicado con independencia de la obligación de contraprestación al interesado por el acceso al servicio. Conviene subrayar en este punto, respecto de las particularidades de la fiscalización conductual por parte del oferente de los servicios de la sociedad de la información, que para que sea de aplicación el Reglamento cuando el oferente se encuentre fuera de territorio comunitario, el servicio ha de estar dirigido a

un particular de la Unión que, además, se encuentre en territorio comunitario. De nuevo, existe una gran abstracción en la reflexión acerca de cómo determinar si determinadas prácticas indivisibles de la oferta de servicios en línea constituyen técnicas de fiscalización conductual: para ello, ha de evaluarse si las personas físicas son seguidas en internet, atendiendo a la naturaleza de las tecnologías empleadas para el tratamiento particular. Anejo a esto, el Comité Europeo de Protección de Datos entiende que la recogida en línea o el análisis de datos personales de las personas en la Unión se considere automáticamente control. Por ello, es necesario examinar la finalidad del tratamiento de los datos por parte del responsable e, igualmente, dilucidar cuáles son los fines o resultados consecuencia de cualquier análisis posterior del comportamiento de las técnicas de elaboración de perfiles con los datos recogidos. Es decir, el Reglamento, para determinar su aplicación, se mueve siempre en un momento de control *ex post* en la fase de prevención, de forma que su empleo se instrumentaliza a la luz de los datos recogidos y las características de la recolección de datos *per se*, y nunca al revés.

Finalmente, es imperativo examinar si las actividades de tratamiento realizadas por el encargado se encuentran relacionadas con las actividades de selección de destinatarios del responsable. Así, cuando las actividades de tratamiento realizadas por un responsable se refieran a la oferta de servicios y bienes, o a la fiscalización conductual de personas residentes en territorio comunitario y ubicadas en territorio comunitario, el encargado que proceda a efectuar el tratamiento de dicha actividad se encontrará bajo el paraguas de la aplicabilidad del Reglamento.

> **E.** Responsable establecido en un tercer país donde sea de aplicación el Derecho de los Estados de la Unión Europea. Será de aplicación del Reglamento al tratamiento de datos personales por parte de un responsable no establecido en la Unión, pero sí en un lugar en el que las disposiciones de Derecho de los Estados miembros se apliquen en virtud del Derecho internacional público. De ello se desprende que, cuando se aplique en base al Derecho internacional el Derecho de un Estado miembro de la Unión, los responsables de tratamientos fuera de la Unión tendrán sujeción al Reglamento. En la práctica es sencillo ofrecer un ejemplo de esta disposición: esto sucede, por ejemplo, en las oficinas consulares de un Estado miembro o en misiones diplomáticas.

CAPÍTULO III: BASES JURÍDICAS LEGITIMADORAS PARA EL TRATAMIENTO DE DATOS

Como se ha adelantado, la norma vertebra dos dimensiones configuradoras de la protección de datos: una subjetiva y otra objetiva. Así, la primera de ellas ampara las condiciones que hacen viable, a la luz del Reglamento y de las expectativas de cumplimiento de la Agencia Española de Protección de Datos, el tratamiento de datos en sentido estricto. En efecto, hablamos de lo que se denomina licitud del tratamiento[52] y, así, nos encontraremos ante un tratamiento de datos lícito cuando se cumplan las condiciones de legitimación del tratamiento. Es lógico que el tratamiento sea lícito en el sentido de que sea una de las cuestiones esenciales del derecho fundamental a la protección de datos, pues los datos solo pueden ser tratados conforme al consentimiento del interesado o bien sobre otra base legitimadora de tratamiento, como se adelantará en las siguientes líneas. Dicha licitud sobre el tratamiento de los datos ha de estar vigente durante todo el ciclo de vida del tratamiento, es decir, la extensión de sus efectos ha de prolongarse hasta la supresión o anonimización de los datos de la persona. En cualquier caso, cualquier base de legitimación prevista en la normativa es requisito *sine qua non* para que pueda efectuarse el tratamiento, siendo bases para la legitimación del tratamiento el consentimiento, la necesidad de ejecución de un contrato, la obligación legal, el interés vital o público, y el interés legítimo.

1. EL CONSENTIMIENTO

El Reglamento entiende por consentimiento toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, bien mediante una declaración o una acción afirmativa, del tratamiento de sus datos personales. Se exige también que este consentimiento que sea manifestado a través de un acto afirmativo claro, reflejo de una voluntad libre, específica, informada e inequívoca del interesado cuyo contenido sea, por supuesto, la aceptación del tratamiento de sus datos personales. Analizamos a continuación los elementos que conforman este consentimiento y, así, podemos decir que para que se trate de una manifestación de voluntad libre, es necesario que no se produzca posteriormente el desequilibrio de poder que ya existe entre el afectado por el tratamiento y aquel sujeto que tiene intención de llevar a cabo el tratamiento. Respecto de esta afirmación, es interesante reproducir[53] que la norma comunitaria es reacia a permitir el tratamiento de datos personales cuando quien lleva a cabo dicho tratamiento es una autoridad pública en base al consentimiento, por la evidente existencia de un desequilibrio entre las partes afectadas (Administración y particular); y lo mismo sucede respecto de las relaciones laborales. Así, en el escenario del empleo, la norma entiende que la negación del empleado a su empleador sobre el tratamiento de sus datos personales no es ajena a la

[52] Unión Europea (2010), Carta de los Derechos Fundamentales de la Unión Europea, en DOUE núm. 83, de 30 de marzo de 2010, págs. 389 a 403, accesible en <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>, art. 8.

[53] Unión Europea (2016), Op. Cit., pág. 23, considerando núm. 43.

experimentación de determinado nivel de temor o miedo y, por ello, se excluyen automáticamente el cumplimiento de los elementos exigidos para que concurra el consentimiento.

Por tanto, podemos describir los elementos que imbrican la concurrencia de consentimiento como los siguientes[54]: (i) libre, el cual implica elección y control reales por parte del interesado, eliminando cualquier riesgo real de engaño, intimidación o coerción o, en fin, situación negativa y perjudicial que incida de tal forma en la determinación de la prestación del consentimiento que sin ella éste no se hubiese prestado. (ii) Específico, que implica que el afectado conozca con anterioridad al tratamiento la existencia del fin del tratamiento y las finalidades para las que este se produce[55], y, así, el consentimiento del interesado para el tratamiento de sus datos puede erguirse sobre distintos fines. (iii) Informado, entendiendo por consentimiento informado aquel que versa sobre la información proporcionada al interesado. Entre los elementos que culminan la exigencia del consentimiento informado encontramos la comunicación de la identidad del responsable del tratamiento, los fines de las operaciones del tratamiento, el tipo de datos que se recogerán y las técnicas empleadas para dicha recolección, la existencia y mecanismos del interesado para retirar el consentimiento, y la información relativa a los riesgos derivados del tratamiento de datos. Finalmente, (iv) el consentimiento ha de ser inequívoco, de tal forma que el mismo pueda ser recabado a través de una declaración escrita o verbal (grabación de voz), con independencia del soporte (electrónico).

Otros supuestos en los que impera el consentimiento como óbice para la determinación de la licitud del tratamiento son aquellos para fines de investigación médica, pues el criterio seguido por el Reglamento es que ha de permitirse a los interesados otorgar su consentimiento para determinados ámbitos de investigación científica, siempre que respeten normas éticas inherentes a la investigación[56] -que no a la actividad de investigación-. En esta línea, las resoluciones de la Administración reguladora explican que los requisitos de idoneidad, especificidad y carácter inequívoco para la prestación del consentimiento no pueden ser interpretados en estas situaciones de forma restrictiva[57]. Lo mismo puede predicarse de las comunicaciones comerciales por medios

[54] Comité Europeo de Protección de Datos (European Data Protection Board), Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, accesible en <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_>

[55] Agencia Española de Protección de Datos, Gabinete Jurídico, núm. de ref. 0026/2021, en 7 de mayo de 2021 (Madrid), informe sobre relación entre compatibilidad de cesión de datos y tratamiento ulterior de estos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales a la luz del Reglamento 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, accesible en <https://www.aepd.es/es/documento/2021-0026.pdf>

[56] Unión Europea (2016), Op. Cit., pág. 23, considerando núm. 33.

[57] Agencia Española de Protección de Datos, Reglamento General de Protección de Datos en *Consentimiento de los interesados*, accesible en <https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/4-consentimiento-de-los-interesados>

electrónicos y, de esta forma, rige el principio de especialidad[58], e implica la cesión al Reglamento General de Protección de Datos[59], salvo para los casos de existencia de una relación contractual previa y siempre que se trate de productos iguales a los contratados o similares, siendo esta la única excepción a la necesidad del consentimiento expreso para el envío de comunicaciones comerciales[60]. Y así sucede también en el caso de transferencias internacionales de datos a terceros países u organizaciones internacionales, mediando el consentimiento del interesado[61].

Para finalizar este epígrafe, conviene hacer referencia, una vez más, a qué entiende el Reglamento por consentimiento explícito: un análisis detallado hace concluir al lector que, a pesar de que el legislador no lo diferencie así, la práctica recoge dos clases de consentimientos, uno expreso y otro explícito, siendo este último el más adecuado cuando por el tratamiento de los datos o las condiciones del tratamiento existan graves riesgos y, por tanto, es necesaria la presidencia de un elevado nivel de control. Por ello, cuando la norma habla de consentimiento explícito, se refiere a la forma en la que el interesado exterioriza y se refleja su consentimiento, siendo preceptivo en el tratamiento de datos pertenecientes a categorías especiales[62]; decisiones individuales automatizadas y, concretamente, cuando se trate de elaboración de perfiles; y transferencia internacional de datos.

El elemento del consentimiento es el más controvertido en lo que al análisis de este trabajo compete, pues plantea serias dudas por cuanto se muestra como una institución un tanto desactualizada respecto de las capacidades efectivas y reales de disposición y control del interesado sobre el tratamiento de sus datos.

2. EJECUCIÓN DE CONTRATOS

El tratamiento de datos será lícito conforme al Reglamento cuando dicho tratamiento sea inherente al cumplimiento de un contrato en el que el interesado es parte. Por tanto,

---

[58] España, Cortes Generales (2022), Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en BOE núm. 166 de 12 de julio de 2022, referencia BOE-A-2002-13758, accesible en <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

[59] Agencia Española de Protección de Datos, Gabinete Jurídico, núm. de ref. 210070/2018, accesible en <https://www.aepd.es/es/documento/2018-0181.pdf>

[60] España, Cortes Generales (2022), Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en BOE núm. 166 de 12 de julio de 2022, referencia BOE-A-2002-13758, accesible en <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

[61] Comité Europeo de Protección de Datos (European Data Protection Board), Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679, de 25 de mayo de 2018, accesible en <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_es>

[62] Unión Europea (2022), Op. Cit. Pág. 25.

la licitud del tratamiento desde la perspectiva de ejecución de un contrato está compuesta por dos elementos: (i) que dicho tratamiento sea inherente a la finalidad de ejecución del contrato; y (ii) que el interesado sea parte. De esta forma, las resoluciones sobre el tratamiento de datos como término de ejecución de un contrato han sido muy insistentes en la determinación de la finalidad del tratamiento, de forma que el responsable o encargado del tratamiento descarte de forma estricta realizar tratamientos prescindibles para la finalidad del vínculo contractual, circunscribiéndose únicamente al tratamiento de los datos justamente necesarios, pues, de lo contrario, excedería el límite de legitimidad por la ejecución del contrato y, por ende, el tratamiento devendría ilícito[63].

Respecto al segundo de los elementos -que el interesado sea parte-, ha de hacerse, en coherencia con las líneas anteriores, una interpretación restrictiva sobre el tratamiento de datos cuando la base legitimadora es la participación del interesado en la ejecución de un contrato (así sucede, por ejemplo, en contratos de suministro de luz o agua, o en pagos realizados con tarjeta de crédito), de forma que el tratamiento solo se limita a los datos necesarios para la ejecución del contrato. Quedan excluidos de este ámbito de legitimación y, por tanto, de licitud del tratamiento, aquellos supuestos en los que el responsable del tratamiento imponga unilateralmente el tratamiento de datos personales, pues la existencia de un contrato, como es obvio, no implica la asunción obligatoria del tratamiento de datos personales. En suma, el objetivo nuclear que determina la legitimación para el tratamiento de datos y así su licitud consiste en determinar si los datos a tratar son esenciales para la ejecución del contrato[64]. Curioso es el caso de las medidas precontractuales a petición del interesado: en el ámbito de las relaciones precontractuales solicitadas a petición del interesado, será necesario considerar, caso por caso, si el tratamiento de datos personales se lleva a cabo por necesidad de las medidas precontractuales (como sucede, por ejemplo, en la recepción de un presupuesto), de forma que sí pueden regir aquí los principios de la protección de datos.

3. CUMPLIMIENTO DE UNA OBLIGACIÓN LEGAL

Como es lógico, el Reglamento prevé la compatibilidad del tratamiento y sus propias disposiciones prescindiendo del consentimiento del interesado cuando dicho tratamiento venga impuesto por una obligación de naturaleza legal[65]. Esta obligación ha de ser impuesta por el Derecho comunitario o por la legislación nacional y, por ende, una norma puede constituir base suficiente para distintos tratamientos[66]. Dado que una

[63] Unión Europea (2016), Op. Cit. Pág. 23, considerando núm. 44.

[64] Grupo de Trabajo del art. 29, Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, adoptado el 16 de septiembre de 2014, WP 223, accesible en <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf>, págs. 6 y ss.

[65] Unión Europea (2022), Op. Cit., pág. 25.

[66] Unión Europea (2016), Reglamento 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

de las preocupaciones de la norma que justifican la protección de datos es la democratización y, en definitiva, el empoderamiento del interesado, el Reglamento incluye, para el caso del Derecho nacional, la posibilidad de introducir disposiciones más específicas para acotar en mayor medida el tipo de tratamiento adecuado[67]. En efecto, cuando el Derecho de la Unión o el nacional aplicable al responsable del tratamiento determinen la base de legitimación sobre este, determinarán, igualmente, la finalidad del tratamiento pudiendo determinar condiciones concretas que incluyan, entre otros elementos -respetuosos con el Reglamento-, (i) las condiciones generales de licitud del tratamiento; (ii) los tipos de datos que serán tratados; (iii) los sujetos afectados o cuyos datos estarán sometidos al tratamiento; (iv) los sujetos y entidades habilitados al efecto para recibir los datos o tratarlos; (v) los límites del tratamiento en relación al fin que justificó su obtención; y (vi) los plazos, operaciones y procedimientos del tratamiento. Una infracción de los principios o disposiciones del Reglamento por medio de una norma con rango de ley implica el desplazamiento de la norma nacional, por aplicación del principio de supremacía del Derecho de la Unión y, correlativamente, en el caso de disposiciones de naturaleza reglamentaria, determinan su nulidad de pleno Derecho por ser contrarias al ordenamiento[68]. La norma comunitaria es clara respecto a la habilitación de la licitud de un tratamiento vía obligación legal: el Derecho encargado de regular este tipo de tratamiento deberá cumplir un objetivo de interés público y en su formulación ha de incluir un sistema de proporcionalidad congruente con el fin perseguido, pues, de lo contrario, la norma es contraria al Derecho de la Unión y, por ende, el tratamiento rebasará la licitud prevista para este tipo de tratamientos. Como no puede ser de otra forma, y en base a las diferencias dimensionales entre Administración y administrado, cuando el tratamiento sea realizado por la Administración o uno de sus empleados, ha de cumplir con una serie de requisitos, a saber, (i) minimización del tratamiento, que implica el tratamiento circunscrito a los datos necesarios; y (ii) que la finalidad del tratamiento sea únicamente la de mantener relaciones de cualquier índole con la Administración.

4. LA PROTECCIÓN DE INTERESES VITALES

El tratamiento de datos personales es lícito cuando sea necesario para proteger intereses vitales de la persona o de otros interesados. De esta forma, y como otros derechos fundamentales, la norma no otorga una protección absoluta, sino que la configuración de los límites a este derecho prevén su rebase cuando la vida o circunstancias similares de otra persona justifiquen el tratamiento de datos[69].

---

y a la libre circulación de esos datos, y por el que se deroga la Directiva 95/46/CE, considerando núm. 45, accesible en GDPR TEXT, <https://gdpr-text.com/es/read/recital-45/>

[67] Unión Europea (2022), Ibid., art. 6.

[68] España, Cortes Generales (2015), Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, BOE núm. 236, en BOE-A-2015-10565, accesible en https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565, art. 47.

[69] Unión Europea (2016), Reglamento 2016/679, Op. Cit. Pág. 23, considerando núm. 46.

5. INTERÉS PÚBLICO Y SU RELACIÓN CON EL EJERCICIO DE PODERES PUBLICOS

Cuando un sujeto realice una actuación de naturaleza pública persiguiendo un fin de interés público, el tratamiento de datos de un interesado estará justificado y, por ende, será lícito de conformidad con el Reglamento[70]. Así, una actividad realizada en pro del interés público puede conllevar el tratamiento de datos de forma lícita. No es conveniente confundir este ámbito de actuación y, por tanto, legitimador de la licitud, con aquel sobre obligación legal: si el tratamiento de datos viene justificado por un imperativo legal para, p. ej., fiscalizar la situación de determinados sujetos prestadores de servicios de comunicación en redes[71], nos encontraremos ante la base legitimadora citada anteriormente, la obligación legal, pero si nos encontramos ante una actuación, p. ej., administrativa característica, es altamente posible que la determinación de la licitud del tratamiento sea aquella de interés público. A estos efectos, especialmente relevante es que cuando el tratamiento no se lleve a cabo en base a una obligación legal -nacional o comunitaria- ni a través del consentimiento del interesado, se han de cumplir una serie de condiciones, a saber, (i) proporcionalidad en la relación entre los fines que motiven la recolecta de datos; (ii) el contexto que justifique la recolección de los datos personales, con especial atención sobre la relación que une al responsable y al interesado; (iii) la naturaleza de los datos recogidos, fiscalizando de forma más intensa en el caso de que pertenezcan a categorías especiales de datos; (iv) previsión de las posibles consecuencias para los interesados como consecuencia del tratamiento; y (v) la planificación y puesta a disposición de garantías adecuadas para el tratamiento de datos -p. ej., recurso a la seudonimización-. Si los datos, además de ser recogidos por la caracterización de interés público de la actuación pretenden ser incluidos en algún fichero o responden a una finalidad de tratamiento, las garantías y excepciones son reforzadas[72].

Cuando la finalidad del tratamiento sea consecuencia de la necesidad del cumplimiento de una actuación realizada por los poderes públicos, pueden determinarse, a su vez, condiciones específicas dirigidas al procedimiento del tratamiento; como son las condiciones que rijan al mismo; los tipos de datos que serán objeto del tratamiento; las características o la determinación directa de los interesados; la limitación de la finalidad y los plazos de conservación de los datos. De nuevo, la norma pretende evitar la discrecionalidad, interdicción y discriminación del actor público en la recogida y tratamiento de datos, cuando no otras conductas reprochables e intensamente antidemocráticas como puedan ser recortes a la libertad de expresión, pues de lo contrario, la actuación estaría viciada y podrían acontecer escenarios de reclamación patrimonial de la Administración y sanción a esta. Conviene cerrar estas líneas

[71] Así sucede, por ejemplo, con la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. España, Cortes Generales (2007), Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, en BOE núm. 251, de 19 de octubre de 2007, BOE-A-2007-18243, accesible en <https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>

[72] Unión Europea (2022), Op. Cit., pág. 25.

destacando que la licitud del tratamiento en base al interés público solo es posible a través de la colaboración de una norma con rango de ley que determine el interés en concreto.

6. EL INTERÉS LEGÍTIMO

El último supuesto legitimador de un tratamiento y, por tanto, evidente de licitud es el interés legítimo. Así, el tratamiento de datos personales será lícito cuando sea indispensable para la consecución de los intereses legítimos del interesado. Esta regla de legitimación tiene una serie de excepciones, pues cuando sobre el interés legítimo y el fin perseguido se encuentren subyugados a otros derechos fundamentales o fines igualmente legítimos para el interesado, la base legitimadora perderá su función y, por ende, el tratamiento devendrá ilícito. Conviene reflexionar aquí sobre la extensión de la abstracción acerca de qué se entiende por interés legítimo y, de esta forma, la práctica reguladora[73] adelanta que ha de ser lícito conforme al Derecho de la Unión, ha de estar formulado con suficiente precisión y claridad y, además, ha de representar un interés actual y real, en el sentido de que su articulación no sea farragosa o artificiosa a fin de perseguir otros fines distintos de aquellos que representan al tratamiento.

Previo a la actuación en base al interés legítimo es fundamental la realización de una evaluación detallada que haga una ponderación entre el interés legítimo y los intereses, datos y derechos del interesado[74]. Puede suceder que, en ocasiones, los derechos e intereses de la persona cuyos datos serán tratados coincidan con los de otras personas: en esos casos, esta evaluación deberá ser más nutrida. Dicha evaluación deberá tener en consideración la situación del interesado, haciendo hincapié en el impacto y repercusión que el tratamiento tendrá sobre sus libertades y derechos pues, en fin, la finalidad de la evaluación no es aquella de impedir el tratamiento por sus consecuencias negativas, sino que estas sean mitigadas.

Como conclusión a los puntos que anteceden, conviene resaltar que el consentimiento es, a juicio del que suscribe, la base legitimadora del tratamiento más controvertida. Más adelante se detallada a modo de conclusión por qué la institución del consentimiento es, de un lado, un paso del legislador por tratar de otorgar agencia al interesado o usuario de los datos personales sobre el tratamiento de sus propios datos, pero esto parece, en realidad, la elección de un sistema de legitimidad que prescinde de reflexiones ulteriores y basado en una institución tradicional que entiendo es un tanto arcaica para las circunstancias que operan en la actualidad en la protección de datos.

[73] Grupo de Trabajo del art. 29, Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, WP 217, adoptado el 9 de abril de 2014, accesible en <https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf>, págs. 16 y ss.

[74] Unión Europea (2016), Op. Cit. Pág. 23, considerando núm. 47.

Otras bases legitimadoras menos controvertidas desde el punto de vista normativo pero que teóricamente sí que pueden plantear mayores problemas son, por ejemplo, la del interés legítimo o aquella de ejecución de contratos, por cuanto son determinadas ambas por el prestador de los servicios y, en definitiva, otorgan a este la discrecionalidad suficiente para determinar qué datos serán finalmente tratados, a pesar de que dichos datos no sean realmente los necesarios. En otras palabras, se trata de unas instituciones que yo entiendo, libres de ser determinadas materialmente por el responsable o encargado, cuando no operador directamente, pueden ser contrapuestas a la finalidad de esta base legitimadora y, así, a toda la arquitectura de la protección de datos, pues pueden ser más datos los realmente tratados que aquellos que son realmente necesarios.

CAPÍTULO IV: DERECHOS DE LOS INTERESADOS EN EL REGLAMENTO Y EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

Hasta el momento hemos hecho sendas referencias al Reglamento por ser el óbice normativo que compete a nuestro trabajo como punto referencial para abordar la cuestión de la mercantilización de datos personales, pero, en este momento, debemos remitirnos igualmente a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Como su propio nombre indica, la Ley Orgánica de Protección de Datos articula sobre la configuración de una serie de derechos el principio de transparencia del Reglamento y, así, desarrolla una serie de derechos de los interesados sobre el tratamiento de datos personales. Estos derechos son los de acceso a la información, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad. Por su parte, y alejándonos de la perspectiva normativa, en la práctica los prestadores de servicios de la sociedad de la información están obligados al respeto de los derechos fundamentales de cualquier sujeto que haga uso de sus servicios y, por ende, están obligados a la aplicación efectiva de las medidas de garantía de estos derechos. Otros derechos relevantes al efecto son el derecho a la actualización de informaciones en medios de comunicación; derecho a la protección de datos de menores en internet; derecho al olvido en búsquedas de internet, redes sociales y equivalentes; derecho a la portabilidad en servicios de redes sociales; y derecho al testamento digital. Otras consideraciones a tener en cuenta sobre el detalle de estos derechos se encuentran recogidas en la Carta de Derechos Digitales, bajo el Plan de Recuperación, Transformación y Resiliencia del Gobierno que, aun prescindiendo de carácter normativo, su consecución práctica hace que, a juicio del que suscribe, pueda enmarcarse de naturaleza *soft law*.

1. DERECHO DE ACCESO A LA INFORMACIÓN

El derecho de acceso a la información, también denominado derecho de suministro de información[75], implica que el responsable del tratamiento tome en consideración todas las medidas pertinentes a fin de facilitar al interesado la información que trate sobre el mismo, y ponga a su disposición las comunicaciones que detallen los ejercicios de los derechos que le competen y las violaciones de seguridad que a él le afecten. Como es lógico, este derecho es fundamental ante la proliferación de sujetos prestadores de servicios que implican el tratamiento de datos personales. Este principio es imbricado sobre la obligación de transparencia[76], que como principio implica el acceso en condiciones de accesibilidad, igualdad y no discriminación a la información sobre el

[75]Unión Europea (2022), Op. Cit., pág. 37, y España, Cortes Generales (2018), Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en BOE núm. 294, de 6 de diciembre de 2018, accesible en <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>, art. 11.

[76] Unión Europea (2022), Op. Cit. Pág. 25, art. 12

interesado de forma clara y sencilla. Esta información ha de contener, de forma obligatoria, quién es el responsable del tratamiento, las finalidades de este, y como se viene indicando, los derechos que sobre el tratamiento prevé la norma.

Especialmente relevante es la facilitación al interesado del ejercicio de sus derechos, pues el responsable del tratamiento está obligado a trasladar al interesado los instrumentos y medios de disposición oportunos para el ejercicio de los derechos citados. Esta obligación es el núcleo de la facilitación de información y, sobre la misma, el responsable de datos ha de trasladar al interesado las actuaciones que se lleven o se vayan a llevar a cabo sobre los datos personales de este, con arreglo a los derechos enunciados. Dicha información ha de ser proporcionada en el plazo de un mes tras la recepción de la solicitud hecha por el interesado, que, motivadamente, podrá ser prorrogado durante un plazo de dos meses adicionales de forma justificada y motivada. En caso de extensión del plazo o de denegación de atención a los derechos ejercitados por el interesado, el responsable ha de justificar de forma suficiente los motivos que le llevan a tomar esta decisión y, a su vez, indicar al afectado los recursos ante las autoridades independientes oportunas y los controles judiciales al efecto. El incumplimiento de esta obligación conlleva, como es natural, la imposición de una multa administrativa de cuantía máxima de 20.000 euros o del 4% del volumen de negocio total en base al ejercicio global anual anterior al de la comisión del ilícito.

La forma en la que la información ha de ser puesta en disposición del interesado ha sido objeto de un arduo trabajo por parte de las instituciones comunitarias[77], quienes han elaborado un número de recomendaciones sobre prácticas dirigidas a diseñadores y usuarios de redes sociales, para evaluar y así eliminar las zonas oscuras del Reglamento, entendiendo por estas aquellas en las que la aplicación del Reglamento requiere una interpretación extensiva de los preceptos contenidos en este. Relevante para el estudio de este trabajo es que estas recomendaciones inciden especialmente sobre los patrones creados por titulares y diseñadores de dichas plataformas, orientados a la influencia de comportamientos de usuarios.

Los requisitos de la obligación de información son los siguientes:

A. Concisión, en el sentido de que la información sea concisa y la comunicación que transmita dicha información sea eficiente y sucinta. La finalidad de este requisito es evitar la fatiga informativa como herramienta dolosa para menoscabar las garantías del interesado y, en detrimento de la finalidad de la norma, lograr un menoscabo con consecuencias deseadas para el prestador de los servicios digitales.

B. Inteligibilidad, de forma que la información se presente de forma reconocible y comprensible a los interesados, que tengan, al menos, lo

[77] Comité Europeo de Protección de Datos (European Data Protection Board), *Guidelines 3/2022 on Dark Patterns in social media platform interfaces: How to recognise and avoide them, published on march 2022*, accessible en <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en>

que se denomina un nivel medio de comprensión dentro de una audiencia objetiva.

C. Accesibilidad, implicando que el interesado no tenga que recurrir a la farragosa tarea de búsqueda de información, sino que ha de reconocer cómo y dónde acceder a la misma de forma directa y sencilla.

D. Claridad y sencillez, que conlleva la obligación de emplear un lenguaje claro y sencillo en el sentido de que la información facilitada complete un registro lo más simple posible, de forma concreta y categórica, no recurriendo a sentidos abstractos o ambivalentes ni empuje al interesado a la incertidumbre de lugares contextuales vagos o imprecisos. Una labor importante del responsable bajo esta categoría es aquella de prescindir de tecnicismos legales o, cuando recurra a ellos, incluya sistemas de remisión explicativos que aclaren la terminología empleada, siempre que no se haga un uso excesivo de esta herramienta so pena de infringir paradójicamente este mismo precepto o cualquier otro de los recogidos anteriormente.

2. EL DERECHO DE ACCESO

El derecho de acceso, tras una lectura del Reglamento, puede definirse como el derecho del interesado a recibir del responsable información acerca de la cuestión de si sus datos están siendo tratados y, en caso afirmativo, en qué condiciones y al servicio de qué fines[78]. Especialmente relevante es la conceptualización de este derecho pues, entre otras cosas, confiere al interesado un instrumento de fiscalización sobre determinados sujetos para conocer si sus datos están siendo tratados o no. Así, los interesados tienen derecho a acceder a los datos personales recogidos que a estos les conciernen y, en base a este derecho, pueden conocer qué datos personales están siendo objeto de tratamiento, cómo acceder a los mismos y, consecuentemente, a su información en los términos expuestos en el epígrafe anterior.

La información que ha de obtener el interesado por parte del sujeto responsable del tratamiento es aquella de los arts. 13 y 14 del Reglamento, y ha de contener, obligatoriamente, los fines del tratamiento; las categorías de datos personales que se traten; los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales; el derecho a presentar reclamación; y los sistemas y destinatarios en el caso de transferencias de datos a terceros, así como los sistemas de tratamiento.

[78]Unión Europea (2022), Reglamento (UE) 2022/868, del Parlamento Europeo y del Consejo de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724, Op. Cit. Pág. 46, art. 85.

3. DERECHO DE RECTIFICACIÓN

El interesado ostenta el derecho a que, sin dilación indebida, el responsable del tratamiento proceda a la modificación de los datos personales que, de forma fehaciente, sean inexactos y se completen aquellos que, de conformidad con la finalidad del tratamiento, estén incompletos[79]. Este derecho de rectificación tiene naturaleza de derecho fundamental, y pretende lograr la protección de datos personales, pues si los datos tratados no son reales, veraces o están incompletos, esto supone una inherencia a otros derechos de la esfera de libertades fundamentales de la persona, como p. ej., intimidad u honor.

4. DERECHO DE SUPRESIÓN

El derecho de supresión es comúnmente conocido como derecho al olvido, y es configurado como el derecho que ostenta el interesado sobre el tratamiento del responsable, y dirigido a este último, de solicitar la supresión de sus datos personales cuando resulte procedente[80]. Por tanto, el ejercicio de este derecho, está supeditado al cumplimiento de una serie de requisitos y limitado a la existencia de un número de excepciones. Así, el interesado tiene derecho a obtener del responsable del tratamiento la supresión de sus datos personales cuando concurra alguna de las siguientes circunstancias:

A. Los datos personales del interesado ya no son necesarios de acuerdo con los fines que justificaron su recogida y tratamiento.

B. Que se produzca la retracción del consentimiento respecto al tratamiento.

C. Oposición del interesado al tratamiento y, consecuentemente, no concurran otras bases legítimas de licitud para proceder al tratamiento de los datos.

D. Cuando los datos hayan sido tratados de manera ilícita, es decir, prescindiendo de alguna de las bases de legitimación del tratamiento.

E. Los datos personales deban ser suprimidos para dar cumplimiento a alguna obligación legal establecida en el Derecho de la Unión.

F. Cuando los datos obtenidos hayan sido obtenidos a través de la oferta de servicios de la sociedad de la información.

---

[79] Unión Europea (2022), Reglamento (UE) 2022/868, del Parlamento Europeo y del Consejo de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724, Op. Cit., pág. 47, art. 16.

[80] España, Cortes Generales (2018), Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en BOE núm. 294, de 6 de diciembre de 2018, accesible en <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>, art. 3.

Por tanto, puede advertir el lector que el ejercicio del derecho de supresión conlleva la supresión del tratamiento porque desaparece la base legítima que posibilita el tratamiento pues, por lógica, los datos han dejado de ser necesarios para la finalidad que justificó su obtención o tratamiento. Este derecho se imbrica sobre un principio general para la supresión de datos en seis casos concretos que fundamentan la solicitud del interesado[81], de los cuales el que suscribe solo recoge uno por su relevancia para el trabajo como principal y a fin de no redundar por lo ya expuesto. Así sucede cuando los datos personales ya no sean necesarios en relación con el tratamiento, de forma que el interesado solicite al proveedor de servicios y responsable la retirada de los datos de los motores de búsqueda asociados a la identidad del interesado. La jurisprudencia[82] ha sido bastante explícita en este sentido a la hora de conciliar este derecho como garante de la protección de la intimidad y aquel relativo a los intereses de la libertad de información, dictaminando que hay que examinar, caso por caso, si el transcurso del tiempo, el contexto social y la pérdida de relevancia u otros factores son determinantes para retirar o no determinadas publicaciones con contenido personal.

Importante igualmente es el derecho al olvido en el caso de redes sociales y servicios de la sociedad de la información análogos[83], que podrán ser retirados por el interesado cuando la publicación verse sobre él; y por terceros, de forma que toda persona tiene derecho a que se supriman los datos personales cuando los suyos sean referidos a la publicación y facilitados por terceros para su publicación.

En cuanto a los límites específicos al derecho de supresión, podemos adelantar, en congruencia con lo expuesto sobre la claridad jurisprudencial entre la libertad de información y el derecho a la intimidad, que será límite al derecho a la intimidad el derecho a la libertad de expresión y de información; aquellos supuestos en los que la injerencia en el derecho a la protección de datos sea consecuencia de una obligación legal; por razones de interés público, especialmente relevantes en el ámbito de salud pública siempre y cuando su tratamiento o exposición no denigre a los interesados; con fines de archivo, científico o histórico; y para la formulación de reclamaciones. Conviene advertir en este punto que el Comité Europeo para la Protección de Datos entiende que la mayoría de las excepciones al ejercicio del derecho a la protección de datos, son insuficientes para obstaculizar su ejercicio, especialmente en el caso del tratamiento de motores de búsqueda, y, por tanto, el ejercicio del derecho en la mayoría de las ocasiones resultará pertinente y la aplicabilidad de las excepciones es solo invocable ante <<motivos imperiosos legítimos>>[84].

[81] Unión Europea (2022), Op. Cit. Pág. 37.

[82] Unión Europea (2014), Tribunal de Justicia de la Unión, *Google Spain S.L. y Google Inc. Contra Agencia Española de Protección de Datos y Mario Costeja González*, accesible en <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62012CJ0131>

[83] Unión Europea (2022), Op. Cit., pág. 25, art. 13.

[84] Comité Europeo de Protección de Datos (European Data Protection Board), Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD (1ª parte) – versión

5. DERECHO A LA PORTABILIDAD DE LOS DATOS

Posiblemente el derecho más relevante a los motivos de la exposición que antecede, este derecho es aquel que permite a los interesados disponer sobre sus propios datos de las facultades de copia, transmisión o traslado, tomando como referencia la movilidad entre un entorno informático y otro. Este derecho fue introducido previa maquinación de dotar de mayor control y democratización de la disposición de los derechos del interesado. Por tanto, podemos entender que este derecho es un instrumento que faculta al interesado a recibir del responsable del tratamiento sus datos personales y a transmitirlos a otro responsable[85].

Este derecho es especialmente relevante porque, como adelantaremos posteriormente, abre la puerta a la incógnita jurídica que justifica parte del interés de este trabajo: la posible mercantilización de datos personales, ya una realidad, cuando la misma es puesta a disposición mediante la voluntad y, por ende, agencia, del interesado, como autor directo de la acción -disposición de los datos- y del contenido de esta -los mismos datos personales-.

Este derecho resulta de gran utilidad a usuarios de redes sociales y de servicios de la sociedad de la información, de forma que el interesado puede solicitar su transferencia entre responsables del tratamiento cuando esto sea técnicamente posible. Conviene examinar los requisitos para la portabilidad, a saber:

A. El derecho a la portabilidad será aplicable cuando el tratamiento esté basado en el consentimiento del interesado o en un contrato con el mismo, de forma que los datos creados por el responsable en base al tratamiento de los datos personales del interesado no serán objeto de portabilidad, aunque la expresión <<datos facilitados por el interesado>> ha de entenderse de forma extensiva para prevenir que el responsable haga una limitante que restrinja o merme las garantías de este derecho y, en última instancia, de la disposición de los datos al interesado.

B. Los datos han de ser tratados por medios automatizados pues, de lo contrario, no se podrá proceder a la portabilidad de datos.

En cuanto a la transmisión entre responsables, como se ha indicado, el interesado ostenta la prerrogativa de transmitir sus datos personales entre responsables cuando la técnica lo permita, y se considera impedimento cualquier obstáculo legal, técnico o financiero aducido por el responsable cuando tenga por objeto la limitación de la portabilidad de los datos del interesado. Quedan incluidos en el concepto de

adopted after public consultation, de 7 de julio de 2020, accesible en https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_es>

[85] Unión Europea (2016), Op. Cit. Pág. 23, considerando núm. 68.

impedimento, por ejemplo, el pago de determinadas cuantías para proceder a la portabilidad.

6. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

El derecho a la limitación del tratamiento puede definirse como el derecho a obtener del responsable la limitación del tratamiento de datos cuando se cumplan alguna de las siguientes condiciones:

A. Suspensión del tratamiento de datos personales, en el sentido de que el interesado puede solicitar la suspensión del tratamiento de sus datos personales cuando se impugne la exactitud de los datos personales durante un tiempo que permita al responsable examinar dicha exactitud; y se haya opuesto al tratamiento sobre la base del interés legítimo o interés público, en lo que el responsable examina si los motivos aducidos por el interesado prevalecen o no.

B. Conservación de datos personales, de forma que el interesado puede dirigirse al responsable sobre la conservación de datos personales cuando el tratamiento sea ilícito y el interesado, en lugar de instar la supresión de sus datos, ha optado por su conservación; y cuando el responsable pueda prescindir de los datos para los fines del tratamiento, pero el interesado entienda pertinente su conservación.

7. DERECHO A LA OPOSICIÓN DEL TRATAMIENTO

El derecho de oposición es definible, simplemente, como el derecho del interesado a negarse al tratamiento de sus datos en los siguientes supuestos:

A. Misión realizada en interés público, interés legítimo o defensa de reclamaciones. Para aquellos casos en los que el tratamiento pueda erguirse sobre la licitud para el cumplimiento de una misión realizada en aras del interés público o en el ejercicio de poderes públicos, el interesado debe, no obstante, ostentar el derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. La consecuencia será que el responsable del tratamiento dejará de tratar los datos personales del interesado, salvo acreditación debidamente justificada de los motivos legítimos imperiosos para el tratamiento y que, consecuentemente, prevalezcan sobre la oposición del interesado. Así, la oposición en el Reglamento se yergue como una institución concisa y debidamente articulada que, sin embargo, puede ceder frente a la discrecionalidad de los motivos que se aduzcan que, por el contrario, son una institución dependiente del contexto en el que se desenvuelvan.

B. Mercadotecnia directa. Cuando el tratamiento de datos personales está orientado a fines de publicidad, el interesado ostentará el derecho de oponerse al tratamiento de sus datos. Este derecho cobra especial relevancia

en este supuesto por los riesgos de la elaboración de perfiles con fines comerciales.

C. Fines de investigación científica, histórica o estadística y su archivo. Finalmente, el interesado tendrá derecho a oponerse al tratamiento de datos personales concernientes a fines de investigación científica, histórica-estadística y a su archivo, salvo que, de conformidad con lo expuesto anteriormente para los fines de interés público, este tratamiento esté debidamente justificado y prevalezca sobre la posible oposición del interesado.

CAPÍTULO V: DECISIONES INDIVIDUALES AUTOMATIZADAS Y ELABORACIÓN DE PERFILES. LAS BASES DE LA COMERCIALIZACIÓN DE DATOS PERSONALES Y SU RELACIÓN CON EL CONSENTIMIENTO

Es evidencia de la tendencia actual de los tiempos que vivimos que la incidencia tecnológica en las vidas de las personas es de tamaña injerencia que el análisis de grandes cantidades de datos es una realidad que nunca prescinde de riesgos. La amplia disponibilidad de datos personales en internet y en los dispositivos de internet de las cosas permite la determinación y el análisis de modelos conductuales con los que se generan perfiles que permiten, de un lado, determinar algunos aspectos de la personalidad y, de otro, anticiparse a ciertos hábitos de la persona. Es lo que se denomina modelos conductuales.

En este sentido, la doctrina califica a estos análisis como herramientas al servicio de mercados conductuales[86]. Los mercados conductuales son aquellos intercambios comerciales en los que el producto es el perfil o elaboración de una serie de datos tratados y analizados meticulosamente con determinadas técnicas orientados a la anticipación de futuros conductuales que permiten, en definitiva, adelantarse a las opciones de las que hará uso un usuario determinado. En la práctica, esta actividad cobra especial relevancia cuando, por ejemplo, en lugar de recurrir los motores de búsqueda al farragoso sistema de empleo de palabras clave para realizar una determinada búsqueda en internet, optan por criterios de búsqueda que permiten enlazar la experiencia de un usuario, sobre el que ya existe un perfil concreto elaborado, a un determinado tipo de publicidad. Es decir, el operador del servicio prescinde de dirigir al usuario a la publicidad y, por el contrario, dirige la publicidad, quirúrgicamente seleccionada, al usuario en concreto.

Esta práctica, como se presenta al lector, conlleva una serie de riesgos para las libertades y los derechos de las personas afectadas. Así, el interesado tiene derecho a no ser objeto del mecanismo selectivo que plantee una decisión individual automatizada, basada de forma exclusiva en el tratamiento de sus datos personales, cual es el caso de la elaboración de perfiles.

En esta línea, el interesado debe tener derecho a no ser objeto de una decisión cuyo fundamento sea la evaluación de aspectos concretos de él, basada únicamente en el tratamiento automatizado y tenga efectos jurídicos sobre él o bien tenga una incidencia directa sobre otros aspectos de su vida, como p. ej., la denegación de una línea de

[86] Zuboff, S. (2019), *La era del Capitalismo de la Vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder*, Paidós, págs. 107 y ss. "La publicidad siempre había sido un juego adivinatorio […] La idea de poder trasladar un mensaje particular a una persona en concreto justo en el momento en que más probabilidades tendría de influir realmente en su comportamiento era -y siempre ha sido- el santo grial de la publicidad […] Dicho de otro modo, Google ya no practicaría la minería de datos conductuales con la finalidad exclusiva de mejorar el servicio para los usuarios, sino que se dedicaría a leer sus mentes con la finalidad de hacer que recibieran anuncios que se correspondieran con los intereses de esos usuarios, unos intereses que deduciría a partir de los rastros colaterales dejados por su comportamiento en línea".

crédito por ser una vez un antiguo deudor o denegación de un seguro de vida por padecer un cáncer durante la adolescencia. Por su parte, el Reglamento no limita la elaboración de perfiles únicamente cuando esta situación sea exigida como tal por el interesado: todo lo contrario, establece una prohibición general de las decisiones basadas únicamente en el tratamiento automatizado, aplicada tanto si el interesado adopta una acción relativa al tratamiento de sus datos personales como si no lo hace. Sin embargo, existen excepciones a esta restricción y, en el caso de encontrarnos ante una, han de reforzarse los mecanismos sobre el control que tiene el interesado sobre estos datos, en correlación a los principios del Reglamento. Sin embargo y como adelantaremos, que el Reglamento prevea el reforzamiento de las prerrogativas del interesado cuando sus datos sean tratados de forma automática para la elaboración de un perfil pone en duda todo el sistema de control en base al consentimiento como base jurídica para la disposición de los datos personales.

En cualquier caso, la elaboración de perfiles consiste en toda forma de tratamiento automatizado de datos personales que los emplea para evaluar determinados aspectos personales de una persona física, en particular, para el análisis y predicción de conductas como, p. ej., el rendimiento profesional, la situación económica, la salud, las preferencias sexuales o ideológicas, raza, ubicación o patrones de movimientos, entre otras muchas categorías que, en fin, buscan la categorización de la persona para extraer de ella el mayor rendimiento en función de los propósitos buscados. Si bien el imaginario colectivo suele amedrentarse ante esta realidad buscando antecedentes históricos pertenecientes a épocas autocráticas, en la actualidad, los principales propósitos son, como se ha reivindicado, comerciales y, más concretamente, publicitarios. La Carta de Derechos Digitales recoge de forma explícita el derecho de las personas a no ser localizadas y perfiladas[87].

La elaboración de perfiles se encuentra conformada por tres elementos:

A. El tratamiento implica una técnica del este que conlleva su automatización, sin excluir la colaboración humana. Por lo general, estas prácticas tienen un claro componente humano, en tanto que el prestador de servicios es quién define qué características y de qué forma serán relevantes a la hora de elaborar el perfil en concreto.

B. El tratamiento ha de versar sobre datos personales, de forma que implica, obligatoriamente, una serie de deducciones de naturaleza estadística.

C. La finalidad del tratamiento es aquella de evaluación de aspectos personales, como análisis o impacto, normalmente conductual o de pertenencia a un grupo y respuesta de patrón de dicho grupo.

[87] España, Gobierno en el marco del Plan de Recuperación, Transformación y Resiliencia (2022), Carta de los Derechos Digitales (2022), accesible en <https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf>

El sistema de trabajo aquí planteado consistente en el rendimiento del excedente conductual de una persona, entendiendo por este el análisis efectuado tras los movimientos de esta a través de los servicios en línea o bien mediante los servicios en línea, disloca intensamente las garantías que el Reglamento pretende poner a disposición del interesado en relación con los derechos que éste ostenta y los datos tratados, hasta el punto de inclinar a las instituciones comunitarias así como a la preocupación social a considerar que el Reglamento de Protección de Datos es, en la realidad práctica, una norma genérica cuyo alcance, a pesar de su intensa ambición, es insuficiente para conciliar las finalidades en él consagradas y la velocidad y deslocalización característica de los servicios en los que estas actividades tienen lugar[88].

De otro lado, es reflexión del que suscribe sumarse a la corriente que por pugna la necesaria ruptura con el mito del consentimiento como sistema de legitimación del control de datos del usuario sobre la cesión de estos a terceros en el marco de los servicios en línea, precisamente, por la insuficiencia de la tradicional institución del consentimiento como sistema que logre una efectiva y real disposición de los datos cedidos a terceros, por las razones que a continuación se ofrecen.

En efecto, la institución del consentimiento persigue que lo datos personales del interesado sea únicamente procesada en el momento en el que ésta determine, conforme a los medios que ésta autorice y, por supuesto, para los fines que consienta y, de esta forma, se asegura el mayor control posible. En otras palabras, consentimiento y autodeterminación informativa[89] son el presupuesto que habilita el contexto consagrado por la norma -este es, aquel en el que se produce la autodeterminación- y, así, cuando falte el primero, presumiblemente faltará el segundo. Al menos esto es lo que expone el plano teórico y la teleología de la arquitectura de la protección de datos personales. Sin embargo, es logro de este trabajo mostrarse crítico con este sistema porque, en realidad, el consentimiento actúa como sistema ambivalente o espejo, en el sentido de que fluye en ambas direcciones: así, una vez otorgado el consentimiento por el interesado, lo que se asegura en realidad es el flujo constante sobre los datos personales y, consecuentemente, el aprovechamiento de dicho flujo por terceros. Por ende, el margen decisorio con el que cuenta el interesado es irrestricto: de un lado, porque el consentimiento legitima casi cualquier tratamiento, y de otro, por la naturaleza de los flujos de datos, pues el consentimiento no se presta sobre un grupo determinado de datos, sino sobre el flujo de este.

---

[88] European Comission, *The Digital Services Act Package* on Shaping Europe's Digital Future, accessible en <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>, actualizado a febrero de 2023.

[89] Daniel Oliver-Lalalana, A., y Muñoz Soro, J. F., en La Protección de los Datos Personales en Internet ante la Innovación Tecnológica, coordinada por Valero Torrijos, J. (2015), Aranzadi, Cap. 6 *El mito del consentimiento y el fracaso del modelo individualista de protección de datos*, pág. 155, importante reflexión entiendo es extraíble de la obra referenciada cuando los autores disponen "consentimiento y autodeterminación informativa se coimplican: si el derecho de protección de datos sirve para guardar la libertad individual, es natural que cada cual decida qué se hace con sus datos y que la legislación amapre su margen decisorio".

Es decir, la posibilidad del rastreo en línea es en definitiva posible porque el consentimiento no se otorga únicamente sobre un grupo de datos personales a ser tratados -que, por cierto, a priori es imposible porque el tratamiento legitima el acceso a conocer qué datos serán tratados y cuáles no, y sin él, no es posible hacer una deducción a priori de los datos relevantes para el responsable o encargado-, sino sobre la posibilidad de tratar datos personales como conjunto y flujo de datos. En esta línea, se encuentra la falta de conocimiento sobre lo que se consiente: es ingenuo presumir que todos los tratamientos consentidos son conocidos por el interesado, principalmente, por la maquinaria detrás del procesamiento de datos personales y las finalidades a las que responde su empleo[90].

La conclusión es que el consentimiento termina operando de forma paradójica en detrimento del interesado o, al menos, en detrimento del poder de disposición del interesado, pues actúa como una puerta legitimadora para el acceso del responsable o encargado al tratamiento a sus datos -de forma pasiva- pero, de forma activa, no permite el control sobre el conjunto de datos tratados, pues estos son operados como flujos y no como categorías, lo que imposibilita el control efectivo sobre dichos flujos.

En efecto, el consentimiento, cuyo empleo se yergue sobre el interés de garantizar al interesado el control sobre sus datos, opera como una renuncia unilateral y limitante de los datos cuyo tratamiento consiente. En todo caso, entiende el que suscribe que esta operación del consentimiento se debe a que el legislador ha configurado, en realidad, un modelo de traslación de la responsabilidad del interesado al responsable y encargado que, desde un punto de vista teórico, está bien ideado, pero, en la práctica, no deja de plantear incógnitas que ponen en duda las garantías sobre el control de datos personales, por cuanto los mecanismos de protección de datos del Reglamento y de la Ley Orgánica son, de un lado, arquetípicos y, por ende, farragosos en lo que a la efectiva práctica de los derechos en ellos contenidos comprenden.

Esto se debe a que la forma de ejercitar dichos derechos sigue sometida, de un lado, a la voluntad del interesado; es decir, es el interesado, de parte, quien ha de vigilar por el correcto tratamiento de sus datos pues, en la práctica, parece poco probable que de *motu proprio* el responsable o encargado no vaya a tratar datos personales que, recogidos bajo el interés legítimo o necesidad de ejecución de un contrato, sean beneficiosos en términos de rendimiento económico la perfilación del usuario y, en última instancia, puedan resultar en un beneficio empresarial. De otro lado, el ejercicio de estos derechos, como la técnica permite, sigue sometido al sistema de presentación de formulario y solicitud. Es constante en el Derecho administrativo que la realidad, en determinadas ocasiones, quede obstaculizada por su sometimiento a las formalidades del acto, pero en lo que a la protección de datos y de la privacidad compete, a pesar de la buena fe del legislador comunitario, esta debilidad se muestra aún más patente: como apuntábamos al comienzo de esta recensión, debido a las características de invasión de la tecnología de los servicios en línea y a la inmediatez del tratamiento y al perfilado de datos personales, es deficitario que el sistema normativo configure como control una

[90] Leith, *Privacy as a Slogan*, Legal Privacy (Lefi Series), Ahti Saarenpää (2009), págs. 98 y ss.

serie de mecanismos en los que el interesado ha de ponerse en contacto con el responsable o encargado del tratamiento, pasando por un sistema de solicitud y plazos, frente a la mutabilidad de los tratamientos y las garantías genéricas que pesan sobre responsable y encargado[91].

Llegados a este punto de la reflexión en la que concluimos con la parquedad de la capacidad de disposición efectiva del interesado sobre los datos personales, debemos asumir, al menos desde la reflexión que contiene este trabajo, que el sistema de control y disposición sobre datos personales es inefectivo, ideal y poco pragmático. Entonces, cabe preguntarse si, al no tener un control efectivo sobre los datos personales por ser estos tratados en forma de flujos y perder su ubicación porque el tratamiento implica una deslocalización de estos y rápida traslación a terceros, si existen otras medidas más eficaces que, de un lado, beneficien al interesado y, de otro, sean conceptualmente más conciliadoras con la configuración conceptual de la protección de datos personales.
En esta línea se sitúa en la actualidad un debate que, de un lado, ha empujado a las instituciones comunitarias a regular de forma más intensa la protección de datos en el ámbito de los servicios en línea, pues es patente que la protección de datos otorgada por el Reglamento tiene cada vez un mayor alcance genérico que evidencia una cantidad de huecos normativos que, en la práctica, empujan a las Administraciones independientes[92] a una actividad de control y sancionadora más expansiva. Como se apuntaba sobre una mejor conceptualización del derecho a la protección de datos, tal vez si no podemos garantizar normativamente un control y disposición efectivo de los

[91] Al efecto, el Reglamento General de Protección de Datos configura una serie de principios en su artículo 5, concretamente, de licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos, exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva. Posiblemente el más incidente sobre las obligaciones que pesan sobre responsable y encargado sea el último citado, aquel de responsabilidad proactiva, pues actúa como "paraguas" genérico de responsabilidad a través del cual dilucidar el grado de cuidado puesto en funcionamiento por aquellos que llevan a cabo el tratamiento mediante técnicas, también contenidas en el Reglamento, como el registro de actividades del tratamiento, el análisis de riesgos, la evaluación de impacto en la protección de datos, la consulta previa u otros mecanismos como los códigos de conducta. Todo ello en Unión Europea (2022), Op. Cit. Pág. 25, art. 5.

[92] Así sucede, por ejemplo, con la Agencia Española de Protección de Datos. Numerosos son los pronunciamientos en los últimos tres años en los que la Agencia cada vez tiene mayor actividad y esta se ejerce desde competencias un tanto dilatadas respecto de la normativa que habilita dichas competencias. No es extraño en el caso de las Administraciones independientes: así sucede, por ejemplo, con la Comisión Nacional de los Mercados y la Competencia, de la que el Tribunal de Justicia de la Unión ya ha dicho, en también numerosas ocasiones, que tiene competencia para intervenir mercados no previstos en su Ley de creación por cuanto su competencia de defensa de la competencia es transversal y adaptativa, en el sentido de que ha de prevalecer la tarea que tiene encomendada -la defensa de la competencia- frente a los elementos que conformen un mercado en concreto. Lo mismo puede decirse de la Agencia Española de Protección de Datos respecto de la protección de datos de forma genérica y, en su caso, respecto de las vulneraciones en materia de protección de datos que se acometan, aun cuando el procedimiento o el sujeto por los que se acometió dicha vulneración sean relativamente independientes del control de la Agencia. Sin embargo, no por ello debemos dejar de lado el reproche al legislador, que parece cada vez más concienciado de esta situación y trata, de un lado, regular normativamente un elenco cada vez más nutrido de sujetos, situaciones, obligaciones y derechos para cada contexto y, de otro lado y como no puede ser de otra forma, dotar, a través de estas nuevas normas, a la Agencia de mayores y mejores competencias para que su actividad sea más garantista por cuanto es más clara y transparente.

datos personales, tal vez sí sea necesario configurar una mejor cultura de la protección de datos, en el sentido de que los interesados tengan una mejor noción de la finalidad del tratamiento de sus datos personales, este es, aquel del rendimiento económico para, como se apuntaba, la publicidad individual, y, así, entender que tal vez el derecho a la privacidad y a la protección de datos puede ser, por ejemplo, análogo en algunas de sus características al de la propiedad. De esta forma, equiparando algunas de sus características al derecho de la propiedad, el interesado se liberaría de la carga de tener el control total sobre sus datos y con ella de la farragosa tarea de poder disponer de ellos para, a cambio de un tipo de remuneración, consentir el tratamiento de flujos de datos personales.

En esta línea, desde la perspectiva del responsable y del encargado, la responsabilidad sobre el tratamiento sería mayor: por una parte, se encontraría más circunscrita y limitada, de forma que solo se tratarían los datos relevantes a comercializar que, precisamente por pasar por un momento de comercialización y acuerdo previo, quedarían mejor delimitados que aquellos que pueda predefinir previamente el responsable o encargado como necesarios o legítimos para el tratamiento, y, además, el valor monetario de esta transacción -sobre el flujo de datos- quedaría reforzado por una intensa cultura del valor de la protección de datos[93] que pivotaría entorno a la importancia económica de dichos datos. Podría decirse, en ese escenario, que las entidades y sujetos interesados en la explotación de datos personales para obtener de ellos rendimientos conductuales llevarían mejores prácticas, mucho más cuidadosas, que podrían estar sujetas a mejores condiciones a través de la promulgación de imposiciones jurídicas propias como sujetos regulados del derecho económico administrativo[94], pues, recordemos, el metaverso, como lugar en el que se acometen todas estas prácticas es, en realidad, un escenario en el que pasamos una gran cantidad de nuestro tiempo inversos, en el que nuestras vidas desarrollan un papel fundamental en niveles económico, social, laboral y personal y, en la actualidad, están dominadas por operadores privados cuyo control es ilimitado. Todo esto, como se ha expuesto, refuerza la idea de una promulgación de normativa en protección de datos más estricta y pragmática, acompasada de la realidad en la que la protección de datos tiene lugar y, en última instancia, más garantista para el ciudadano común.

Lo que aquí se pone de manifiesto no es sino una divergencia entre los compromisos legales que el legislador está dispuesto a asumir y lo que realmente termina sucediendo en el mundo real: la legislación sobre protección de datos persigue el efectivo control de los datos personales, pero, como se ha apuntado, las características de dichos datos

[93] Hann I. H., Hui K. L., *Online Information Privacy: Measuring the Cost-benefit Trade-Off*, 23rd International Conference on Information Systems, Barcelona, 2002.

[94] Así sucede, por ejemplo, en el ámbito de las telecomunicaciones o en el sector de la energía y los recursos naturales. Como declara Montero Pascual, J. J., "el contenido de la actividad administrativa reguladora es el control de la actividad de las entidades reguladas, en concreto mediante la imposición de obligaciones jurídicas. En primer lugar, la actividad de regulación consiste en lo fundamental en la imposición de obligaciones jurídicas y no meramente de recomendaciones o de creación de marcos de asunción voluntaria de obligaciones del tipo que ha venido denominándose autorregulación y que entendemos es un fenómeno interesante pero esencialmente diferente al que nos ocupa", en Regulación Económica: la actividad administrativa de regulación de los mercados, 4ª edición, Tirant lo Blanch (2021).

y de las técnicas que los tratan hacen imposible, en la configuración actual de protección de datos, garantizar mínimamente una protección de datos en sentido real, y, por ello, ha sido cada vez menos optimista la regulación de la configuración de las prácticas que llevan a cabo las Tecnologías de la Información y la Comunicación desde el plano jurídico respecto de su proyección efectiva.

CONCLUSIONES

A modo de conclusiones, conviene reivindicar los puntos elementales que configuran la línea principal de este trabajo, a saber, la reformulación conceptual del derecho a la protección de datos; una visión global, práctica y crítica de los derechos que asisten, en la legislación comunitaria y nacional, al interesado; las bases del tratamiento y su interconexión con la efectiva capacidad de control que ostenta el interesado sobre el tratamiento de sus datos personales; y, finalmente, por qué todas estas herramientas son necesarias en el contexto de la elaboración de perfiles y cómo hasta el momento, en base a las reflexiones aducidas anteriormente, son innecesarias y de qué formas, al menos partiendo de un <<imaginario legislativo>>, el legislador puede superar los obstáculos a los que se encuentran en el escenario de la protección de datos:

1. Así, en un primer momento histórico, las loables preocupaciones del legislador nacional y comunitario, y la sensibilización nacional a los diferentes formas que ha tomado la injerencia frente a la protección de datos han sido, de un lado, de naturaleza política, a través de regímenes autárquicos y, de otro, con la aparición de las primeras intromisiones ilegítimas en la vida del particular con motivo del sensacionalismo ligado a las primeras fases de desarrollo de programas televisivos o de radiodifusión. Sin embargo, la protección de datos no puede seguir proyectándose sobre conceptualizaciones de un derecho que protege la intimidad o los límites de esta; todo lo contrario, ha de ser configurado como un derecho que se proyecta desde estas conceptualizaciones, para lograr otras más instrumentales y acordes con la realidad actual que doten, de forma efectiva y verdadera, de control pleno al usuario. En efecto, las bases normativo-conceptuales de lo que es y ha sido la protección de datos hasta el momento son necesarias, pero no suficientes. Por ello, debemos reformularlas teniendo presentes las críticas que aquí se exponen y siguen.

2. En cuanto a la configuración de las herramientas como derechos a disposición del particular a efectos de librar su control sobre los datos que a él conciernen, es imprescindible tener en cuenta que a pesar de los innumerables beneficios que pueden reportarse del ejercicio de estos, debemos reconsiderar las siguientes críticas sobre cada uno de ellos, y, así, del derecho de acceso como derecho del interesado a ser informado por el responsable o encargado sobre la posibilidad de que sus datos estén siendo tratados es conforme a la crítica a la falta de garantías que se hace de la norma de protección de datos. Esto se debe a que este derecho permite conocer, de primera mano, si sus datos están siendo tratados o, al menos, cedidos a terceros. Si bien es cierto que este derecho materialmente no permite instrumentalizar la reclamación de cese del tratamiento de datos que se esté llevando a cabo, sí que permite conocer a quién dirigirse para poner coto al tratamiento en concreto y, consecuentemente, conocer a quién y en qué situación se han cedido sus datos, o cedido aquellos tratados inicialmente. Sobre el segundo derecho, aquel de rectificación, conviene resaltar que tiene cierta incidencia sobre la crítica de garantías en relación al derecho a la protección de datos cuando se ejerce conjuntamente con

el derecho de acceso, pues permite conocer, en el caso de decisiones automatizadas y creación de perfiles, qué datos quedan incompletos y de qué forma completarlos, lo cual puede resultar un tanto controvertido frente a los datos tratados de forma autónoma en el ámbito de elaboración de perfiles, pues la elaboración de un perfil implica, tras el tratamiento, la novación de los datos recogidos y cabe plantearse, en ese caso, hasta qué extremo tiene capacidad el usuario para completar unos <<paquetes>> de datos ya tratados y novados, frente al ocasional desacuerdo que pueda plantear frente al usuario de los datos. En cuanto al derecho de supresión, puede tener grandes implicaciones prácticas en la elaboración de perfiles y publicidad configurada, pues permite la supresión, de un lado, del tratamiento de los datos, es decir, de los datos originalmente cedidos, y, de otro, la supresión de aquellos datos tratados que ahora se constituyen como nuevos datos en base al tratamiento realizado. Posiblemente se configuren como la opción más realista desde la perspectiva del diseño de la protección de datos en lo que a control y garantías se refiere; sin embargo, su práctica también puede devenir controvertida, pues que un interesado inste la supresión de sus datos ya tratados no implica que el responsable o encargado del tratamiento, de forma efectiva y plena, ponga en conocimiento de aquellos terceros a los que ha cedido los datos o los datos ya tratados que el interesado quiere suprimir los datos tratados. De nuevo, se pone en jaque el control efectivo del tercero mediante la institución del consentimiento como sistema de control del flujo de datos tratados. Del derecho a la limitación del tratamiento podemos decir que es suficientemente garantista en la arquitectura de la protección de datos, pues su sentido eminentemente instrumentista actúa como extremo hasta el que puede llegar un encargado o responsable en el tratamiento, marcado por el interesado. Por tanto, a priori sí que hace efectivo el control mediante la institución del consentimiento, pero, en la práctica, pone de relieve uno de los problemas más reiterados a lo largo de este trabajo: que el consentimiento es insuficiente una vez los datos son, no solo tratados y procesados, sino trasladados a terceros. Es decir, la imposición de una limitación frente a unos datos cuyo rastro se ha perdido, frustran las expectativas de este derecho, al menos en su ejercicio pleno. El derecho a la portabilidad es, como indicábamos, el más interesante desde la perspectiva del trabajo: de un lado, se yergue como el antagonista del consentimiento.

3. Así, si el consentimiento opera como una disyuntiva jurídica basada en la voluntad del interesado (elegir entre aceptar el tratamiento o no, y según qué limitaciones), la portabilidad da un paso más allá y permite al interesado configurar un sistema de traslación de datos, que puede ser condicionado. En la actualidad, el diseño de la normativa de protección de datos es manifiestamente contraria a la comercialización de datos del interesado: no hay ninguna norma en el Reglamento que se pronuncie sobre este extremo, y tampoco existen casos en el paradigma social. Sin embargo, sí es real, como se ha expuesto anteriormente, que las empresas sacan beneficios del rendimiento de las experiencias on line de los usuarios en base al rastreo y perfilado de sus datos. En efecto, conviene entonces reflexionar que tal vez la institución más adecuada, capaz de transgredir las limitaciones del consentimiento, sea aquella de permita

la comercialización de los datos personales. Desde la perspectiva del interesado, se generaría mayor sensibilización sobre la protección de datos, no tanto por el peso normativo y garantiste que tiene el papel del interesado en esta norma, sino por el hecho de que el interesado, al saber que sus datos y el tratamiento de estos puede tener un especial valor monetario, se acerque con mayor curiosidad a conocer exactamente qué servicios pueden tener lugar como consecuencia del tratamiento, quién lleva a cabo este tratamiento y, en definitiva, en qué consiste.

4. Desde la perspectiva del operador interesado en el tratamiento de datos y perfilado, así como del responsable y encargado -pues, recordemos, estas figuras no tienen por qué coincidir siempre en la práctica-, lograríamos un mayor cuidado en el diseño de las prácticas del tratamiento de datos: de un lado, se limitaría la preconfiguración de las características del tratamiento realizada por el responsable o encargado pues, ahora que el interesado tiene conocimiento de que sus datos son susceptibles de rendimiento económico negociable, participaría en un proceso de negociación con el encargado y responsable del tratamiento; de otro lado, la posibilidad de que el encargado o responsable del tratamiento tengan que contar preceptivamente con la participación del interesado a expensas de mediar las características y finalidades del tratamiento, hacen que estos primeros detallen de forma más explícita, regulada y, en definitiva, transparente, todo ello redundado en el efectivo y mayor control de disposición de los datos del interesado. Si el interesado cede, a cambio de una contraprestación económica, transparente e informada, sus datos a un tercero, podemos mitigar el impacto de la falta de control sobre el consentimiento pues la comercialización de los datos desvirtuaría completamente la necesidad y justificación de crear un sistema de garantías que permitiese al interesado, cuando así considerara, instar una supresión o modificación del tratamiento previamente aceptado, a excepción de la constitución regulada de una serie de prerrogativas de revocación del consentimiento como, p. ej., ante la presencia de fraude.

5. Finalmente, todas estas críticas y aportaciones serían desvirtuadas si no respondiesen a un objeto controvertido concreto, para que el que entiende el que suscribe el legislador no ha sabido proporcionar una respuesta, pues el reto es complejo: la deslocalización de los datos y la relación de dicha deslocalización en base al tratamiento de estos para su posterior elaboración de perfiles. Esta práctica, como se ha expuesto, responde al ánimo comercial que existe sobre los datos personales y, al mismo tiempo, subraya la necesidad de adquirir verdadera conciencia sobre la falta de control que puede proporcionarse al interesado, al menos con las herramientas estudiadas actuales. Todo lo contrario, merece la pena detenerse a reflexionar sobre si esta práctica, como se ha demostrado, puede ser conciliadora con los derechos del interesado y, en caso de que la lectura de esta sea negativa, reflexionar acerca de qué puede fallar, en este caso, la circunscripción de toda la arquitectura de protección de datos a la institución del consentimiento. En efecto, como se desarrollaba, el consentimiento plantea intensas dudas acerca de su efectividad como elemento legitimador para

permitir el tratamiento deditos personales y, en esta línea, incide el autor que, dadas las implicaciones de la tecnología empleada para tratar los datos, es insuficiente para garantizar control alguno sobre el flujo de estos. Tal vez, y como se repite a lo largo del trabajo, lo conveniente sería supeditarlo todo a una regulación más explícita que, a través de la dotación efectiva de un valor económico de los datos personales, sitúe al interesado al nivel de un productor de datos y, así, el intercambio de información, supeditado a una legislación más clara en los términos comentados, le empiedre y, al mismo tiempo, siga permitiendo las operaciones de aquellas empresas prestadoras de servicios en la red.

BIBLIOGRAFÍA

Farreres, G. F. (2018), *Sistema de Derecho administrativo*, Civitas, Thomson Reuters.

García, R. A. (2014), *Sistema jurídico de la Unión Europea*, Civitas, Thomson Reuters.

Lombarte, A. R., (2018), *Tratado de Protección de Datos*, Tirant lo Blanch.

López, J. M. H., y Constitucional, E.T. (2012), *El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*.

Memento Derecho de las Nuevas Tecnologías 2022-2023 (2022), Lefebvre.

Memento Protección de Datos 2023 (2023), Lefebvre.

Torrijos, J. V. (2014), *La protección de datos personales en Internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*, Thomson Reuters Aranzadi.

Zuboff, S. (2020), *La era del capitalismo de la vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder*, Paidós.

NORMATIVA CITADA

España, Cortes Generales (2022), Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en BOE núm. 166 de 12 de julio de 2022, referencia BOE-A-2002-13758, accesible en <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

España, Cortes Generales (2018), Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en BOE núm. 294, de 6 de diciembre de 2018, accesible en <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>

España, Cortes Generales (2010), Tratado de Funcionamiento de la Unión Europea, DOUE núm. 83, de 30 de marzo de 2010, accesible en <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002>

Unión Europea (2022), Reglamento (UE) 2022/868, del Parlamento Europeo y del Consejo de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724, en DOUE núm. 152, de 3 de junio de 2022, págs. 1 a 44, accesible en <https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80835>

Unión Europea (2010), Carta de los Derechos Fundamentales de la Unión Europea, en DOUE núm. 83, de 30 de marzo de 2010, págs. 389 a 403, accesible en <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>

JURISPRUDENCIA

Unión Europea (2014), Tribunal de Justicia de la Unión, *Google Spain S.L. y Google Inc. Contra Agencia Española de Protección de Datos y Mario Costeja González*, accesible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62012CJ0131

Unión Europea, Tribunal de Justicia (2018), Asunto C-25/17, accesible en <https://curia.europa.eu/juris/document/document.jsf;jsessionid=B4D45BD37420CB20CCDADD6A530A761C?text=&docid=198949&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=3738318>

Unión Europea, Tribunal de Justicia (2020), Asunto C-311/18, accesible en <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=3742569>

Unión Europea, Tribunal de Justicia (2020), Asunto C-623/17, accesible en <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=3744808>

REVISTAS Y PUBLICACIONES

Nieves Saldaña, M. (2011), *El Derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego*, UNED, Revista *Teoría y Realidad Constitucional*, págs. 279-312.

Ruíz Miguel, C. (1992), *La configuración constitucional del derecho a la intimidad* [tesis doctoral]. Universidad Complutense de Madrid, págs. 76 y ss.

S. D. Warren y L. Brandeis, *The Right to Privacy*, Harvard Law Review, núm. 5 (1980).

Suñé Llinás, E., *La sociedad civil en la cultura postcontemporánea*. Ed. Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense y CESSJ Ramón Carande, Madrid, 1998, págs. 75 y ss.

WEBGRAFÍA

Agencia Española de Protección de Datos, Gabinete Jurídico, núm. de ref. 210070/2018, accesible en <https://www.aepd.es/es/documento/2018-0181.pdf>

Blog *Protección Data*, entrada *Para estar al día en protección de datos y seguridad de la información*, recuperado en octubre de 2022, accesible en <https://protecciondata.es/historia-normativa-proteccion-datos/>

Comité Europeo de Protección de Datos (European Data Protection Board), Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, accesible en https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679

Comité Europeo de Protección de Datos (European Data Protection Board), Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679, de 25 de mayo de 2018, accesible en https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_es

Comité Europeo de Protección de Datos (European Data Protection Board), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, accessible en <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en>.

Comittee to Protect Journalists, Las leyes penales de difamación en Norteamérica, recuperado en diciembre de 2022, accesible en <https://cpj.org/es/2016/03/norteamerica/>

Consejo General de la Abogacía Española. *Derecho a la información versus derecho a la intimidad e imagen en la sociedad de la información*, recuperado en enero de 2023, accesible en <https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/derecho-a-la-informacion-versus-derecho-a-la-intimidad-e-imagen-en-la-sociedad-de-la-informacion/>

Data Lag 1973/289, acceso disponible en <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>

El Derecho, Historia de la Protección de Datos, publicado el 8 de octubre de 2020, disponible en <https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido>

El País, Protejamos nuestros datos. No olvidemos cómo los usaban los nazis, publicado en septiembre de 2021, accesible en <https://elpais.com/ideas/2021-09-12/protejamos-nuestros-datos-no-olvidemos-como-los-usaban-los-nazis.html>

El mercado interior: principios generales, en Fichas temáticas sobre la Unión Europea, recuperado en diciembre de 2022, accesible en <https://www.europarl.europa.eu/factsheets/es/sheet/33/el-mercado-interior-principios-generales>

España, Gobierno en el marco del Plan de Recuperación, Transformación y Resiliencia (2022), Carta de los Derechos Digitales (2022), accesible en <https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf>

European Comission, *The Digital Services Act Package* on Shaping Europe's Digital Future, accessible en <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

Intersoft consulting, Datenschutz-Grundverordnung, recuperado en julio de 2022, accesible desde <https://protecciondata.es/historia-normativa-proteccion-datos/>

Légifrance, République Française, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, disponible en <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460>

Legislation.gov.uk, Data Protection Act 1984 (whole act), recuperado en junio de 2022, accessible en <https://www.legislation.gov.uk/ukpga/1984/35/enacted>

Unión Europea (2016), Reglamento 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 esos datos, y por el que se deroga la Directiva 95/46/CE, considerandos, accesible en GDPR TEXT, <https://gdpr-text.com/es/read/recital-18/>