TRATAMIENTO FRENTE A DATO. EL PROBLEMA DE LAS CATEGORÍAS ESPECIALES

Autor: Daniel Jove Villares

Tesis doctoral UDC / 2021

Directores:

Prof. Dr. Santiago Antonio Roura Gómez

Prof. Dr. Miguel Jesús Agudo Zamora

Programa Oficial de Doctorado en Derecho
regulado por el RD 99/2011, de 28 de enero

UNIVERSIDADE DA CORUÑA

AGRADECIMIENTOS

Confío que, quien tenga la predisposición y presencia de ánimo necesarios para leer esta tesis, sabrá disculpar este breve ejercicio de introspección, con el que pretendo, sabiendo que es imposible, hacer justicia a aquellos que, de algún modo, han contribuido a la materialización de este trabajo. Si toda obra humana requiere de tiempo, esfuerzo y recursos para su culminación. Esta tesis es, en cierto sentido, un producto colectivo.

Sin un sistema educativo público, hoy estaría dedicado a otros quehaceres, ni mejores ni peores, distintos. La formación ofrece alternativas y oportunidades de desarrollo vital invaluables. En mi caso, me permitió ser consciente de aquello a lo que quería dedicar mi tiempo y esfuerzo, y a lo que no. Dejar inconclusos los estudios de ingeniería química para comenzar los de Derecho puede parecer una decisión extraña y, sin embargo, sin ese paso previo, hoy no estaría escribiendo estas líneas.

Confieso que, al comenzar el grado en Derecho, albergaba ciertas dudas acerca de lo atinado de mi decisión. Pronto comprendí que había encontrado un universo que valía la pena explorar y tratar de comprender. En esa fascinante tarea sigo, si bien es cierto que, he acotado mi ámbito de estudio a una parte de ese macrocosmos, el Derecho Constitucional.

En ese proceso de especialización, cursar el Máster de Derecho Constitucional del Centro de Estudios Políticos y Constitucionales resultó decisivo. Tanto por la ampliación de conocimientos y perspectivas, como por los buenos amigos que pasar por el Palacio de Godoy me ha reportado. Pero, sobre todo, porque me ratificó en la decisión de dedicarme a la vida académica y al Derecho Constitucional. A todos los docentes y a la dirección del CEPC, muchas gracias.

Realizar un doctorado en España no deja de ser un conjunto de apuestas con un alto grado de incertidumbre y riesgo. En mi caso, he tenido suerte y he podido disfrutar de diversos contratos y ayudas que me han proporcionado la tranquilidad y oportunidades necesarias para poder sacar el máximo partido posible a esa etapa.

Los contratos predoctorales, de la Xunta de Galicia primero y de Formación del Profesorado Universitario (FPU) después, no solo me han proporcionado estabilidad económica, sino que me han dado la

oportunidad de impartir docencia a la par que realizaba la tesis, enriqueciendo sobremanera el proceso. Además, he tenido ayudas que han financiado mis estancias en la Università della Calabria (Ayudas Inditex para estancias) y en el Max Planck de Derecho Público Comparado y Derecho Internacional de Heidelberg (Ayudas complementarias de movilidad destinadas a beneficiarios del programa de Formación del Profesorado Universitario (FPU)). Soy consciente de lo afortunado que he sido y confío que, el trabajo aquí presentado, esté a la altura de los recursos puestos mi disposición.

A las dos estancias mencionadas, debo añadir una tercera que, pese a no contar con financiación externa, valoro especialmente. El mes que tuve ocasión de estar en la Cátedra de Derecho y Genoma Humano de la Universidad del País Vasco me sentí muy bien acogido e integrado. Más allá de lo mucho que me ha aportado desde el punto de vista académico, me quedo con la relación personal con sus integrantes, con especial mención a Íñigo y Guillermo, cuya preocupación por el devenir de esta tesis y por mis avatares personales agradezco profundamente.

En este sentido, no quiero olvidarme de la Universidade da Coruña, de los medios materiales y técnicos con los que facilita el trabajo diario y, sobre todo, del personal que, con su esfuerzo, la hace funcionar. Desde conserjería a biblioteca, pasando por cafetería, el servicio de limpieza o de administración; sin ellos, la calidad de vida que he tenido durante estos años habría sido menor y los resultados peores.

Más allá de la tranquilidad que proporciona tener cierta estabilidad profesional, por más que sea temporal y de futuro incierto, lo cierto es que, el factor diferencial es el tiempo, aprecio y conocimientos que otros me han dedicado. En este sentido, me gustaría hacer mención a los profesores del área de Derecho Constitucional (Javier Ruipérez, Ana Aba y Sonia García) quienes me han acogido con amabilidad y constituyen una referencia de trabajo diario y buen hacer.

Con todo, son los directores de esta tesis quienes más me han ensañado y a quienes más debo. A este respecto, debo confesar que he hecho trampa, pues por más que formalmente solo consten Miguel Agudo Zamora y Santiago Roura, he tenido un tercer maestro, Francisco Caamaño. Cada uno de ellos ha jugado un papel crucial en esta tesis. A Miguel Agudo debo agradecer la valentía de tomar parte en este proyecto, dándole mayor solidez y ampliando mis posibilidades como investigador predoctoral. Su

presencia es la demostración de que la tecnología puede ser un instrumento útil, pues ha permitido que, a pesar de la distancia que separa Córdoba y A Coruña, haya estado siempre presente.

Como lo ha estado, desde su feliz llegada a la Universidade da Coruña, Francisco Caamaño. Esta tesis sería mucho peor sin su presencia. El tiempo, esfuerzo y aprecio que me ha brindado estos años, las lecciones, críticas y correcciones que me ha realizado me han hecho mejor jurista y me hacen apreciar más la oportunidad de dedicarme al Derecho Constitucional. Para mí es un director y un maestro. Por más que la normativa me impida hacerlo constar oficialmente, sirvan estas líneas como reconocimiento; aunque soy consciente de la impagable deuda que con él he adquirido.

Pero todo comenzó con Santiago Roura. Si he realizado la tesis en la Universidade da Coruña es porque tuve la convicción, desde mi etapa de "bolseiro" en el área durante el grado, que era una persona con la que podía trabajar y de la que podía aprender. El tiempo me lo ha confirmado. La confianza que siempre ha tenido en mi capacidad para sacar adelante esta tesis o las tareas que, a lo largo de la etapa predoctoral, he ido asumiendo, la libertad que siempre ha sabido darme para elegir los temas a los que dedicarme y, sobre todo, su preocupación constante por mi bienestar me ratifican en lo acertado de mi elección. En él he encontrado a un director y un amigo.

La realización del doctorado no solo me ha reportado conocimientos y experiencias, también un buen números de compañeras y amigos, tanto en el mundo del Derecho Constitucional, como fuera de él. Andrés y Lara son la representación más genuina de los primeros; como lo son Noelia, David, Silvia, Marián, Nerea, Marta o Jorge de los segundos. Con ellos he compartido experiencias, incertidumbres y alegrías. Entre las cosas buenas que esta etapa me ha dado, su amistad es una de las mejores.

Todos ellos se han venido a sumar a quienes ya estaban y siguen estando, a los amigos y amigas del grado y a los de toda la vida. A todos ellos debo una disculpa, pues no he sido una buena compañía durante estos años, los he visto poco y no les he dedicado tiempo de calidad. Confío compensarlo en el futuro.

Finalmente, mis últimas palabras son para mis padres y mi hermana. Por ser y estar. El tiempo y esfuerzo que yo haya podido dedicar palidece al lado del apoyo incondicional que me han prestado durante estos años.

RESUMEN

Esta tesis doctoral analiza la adecuación del modelo europeo de protección de datos para afrontar los desafíos de las era digital. De manera específica, se centra en dos elementos que condicionan el régimen de protección: el concepto de dato personal y las llamadas categorías especiales.

Mediante una aproximación holística y gradual, en la que se toman en consideración los orígenes del derecho a la protección de datos, la cultura jurídica que caracteriza al sistema europeo y la naturaleza del derecho fundamental, se ponen de manifiesto las razones que justifican la existencia de las categorías especiales y se plantea una propuesta alternativa, más acorde a la idiosincrasia del modelo europeo de protección de datos. En relación con el concepto de dato personal, se apunta la conveniencia de ampliarlo, adoptando un enfoque en el que la realidad del tratamiento y sus riesgos tengan una relevancia mayor.

***

ABSTRACT

This thesis analyses the adequacy of the European data protection model to face the challenges of the digital age. Specifically, it focuses on two elements that condition the protection regime: the concept of personal data and the so-called special categories.

Through a holistic and gradual approach, in which the origins of the right to data protection, the legal culture that characterises the European system and the nature of the fundamental right are taken into consideration, the reasons that justify the existence of the special categories are highlighted and an alternative proposal is put forward, more in line with the idiosyncrasy of the European data protection model. In relation to the concept of personal data, it points out the convenience of broadening it, adopting an approach in which the reality of the processing and its risks have a higher relevance.

***

RESUMO

Esta tese doutoral analiza a adecuación do modelo europeo de protección de datos para afrontar os desafíos das era dixital. De maneira específica, céntrase en dous elementos que condicionan o seu réxime de protección: o concepto de dato persoal e as chamadas categorías especiais.

Mediante unha aproximación holística e gradual, na que se toman en consideración as orixes do dereito á protección de datos, a cultura xurídica que caracteriza ao sistema europeo e a natureza do dereito fundamental, póñense de manifesto as razóns que xustifican a existencia das categorías especiais e realízase unha proposta alternativa, máis acorde á idiosincrasia do modelo europeo de protección de datos. En relación co concepto de dato persoal, apúntase a conveniencia de amplialo, adoptando un enfoque no que a realidade do tratamento e os seus riscos teñan unha relevancia maior.

ÍNDICE

ABREVIATURAS

a.C.	Antes de Cristo
AA.VV	Autores Varios
AEPD	Agencia Española de Protección de Datos
Apdo/Apdos	Apartado/apartados
ARPANET	Advanced Research Projects Agency Network
Art.	Artículo
CdE	Consejo de Europa
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CE	Constitución española
CEDH	Convenio Europeo de Derechos Humanos de 1950
CIDH	Corte Interamericana de Derechos Humanos
DUDH	Declaración Universal de Derechos Humanos de 1948
ECRI	Comisión Europea contra el Racismo y la Intolerancia
EDPB	Comité Europeo de Protección de Datos
Etc.	etcétera
FIPs	Fair Information Practices
FJ	Fundamento Jurídico
GRETA	Grupo de Expertos sobre la lucha contra la Trata de seres humanos
GT29	Grupo de Trabajo del artículo 29
IA	Inteligencia artificial

LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LORTAD	Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal
OCDE	Organización para la Cooperación y el Desarrollo Económico
p. / pp.	Página/ páginas
p. ej.	Por ejemplo
Párr./Párrs.	Párrafo/párrafos
PE	Parlamento Europeo
RDNP	Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
SEPD	Supervisor Europeo de Protección de Datos
STC	Sentencia del Tribunal Constitucional español

STEDH/SSTEDH	Sentencia/Sentencias del Tribunal Europeo de Derechos Humanos
STJCE	Sentencia del Tribunal de Justicia de las Comunidades Europeas
STJUE/SSTJUE	Sentencia/Sentencias del Tribunal de Justicia de la Unión Europea
TC	Tribunal Constitucional español
TCE	Tratado Constitutivo de la Comunidad Europea
TCFA	Tribunal Constitucional Federal Alemán
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TJCE	Tribunal de Justicia de las Comunidades Europeas
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tratado de la Unión Europea
UCLA	Universidad de California en Los Ángeles
UE	Unión Europea
v. gr.	Verbi gratia
Vid.	véase
VV.AA	Varios Autores
WWW	World Wide Web

PREFACIO

Los petroglifos, las pinturas rupestres, la escritura, la imprenta, la fotografía, el vídeo… son el elemento físico, el soporte, que permite gestionar, almacenar y trasladar la información en el tiempo y el espacio, haciéndola llegar a otros. El uso de información como medio para la consecución de determinados fines es consustancial al ser humano. El proceso civilizatorio, los avances que a lo largo de milenios han desembocado en sociedades más tecnificadas, interconectadas e industrializadas[1] no se comprende sin la capacidad humana para producir y transmitir conocimiento. Su acopio integra el saber colectivo de la Humanidad[2], y es el entorno en el que nos socializamos[3]. Nuestras decisiones, comportamiento y modo de vivir son el producto de la información de la que disponemos.

Así, en la esfera privada, la gestión atinada de la información puede suponer la diferencia entre el éxito o el fracaso para una empresa, no solo para aquellas que tienen en el tratamiento de datos (personales o no) su modelo de negocio (ya sea para ofertar mecanismos y modelos de publicidad personalizada, para almacenar información en la nube o proveer servicios de comunicación); también para las que no. Para estas últimas, resulta crucial, por ejemplo, contar con información precisa y fiable acerca de las preferencias de los clientes. Del mismo modo, la información es fundamental para la gestión de las necesidades públicas. Sin ella, los estados no podrían establecer sistemas impositivos adecuados a su realidad económica, mantener la seguridad, dimensionar sus servicios públicos y mejorar su eficiencia.

A poco que uno se asome al balcón de la realidad, puede corroborar que el aforismo "el conocimiento es poder" cobra una nueva dimensión en la era digital. Los datos son la partitura de la banda sonora que rige el día a día. Su métrica pauta los procesos productivos y económicos[4]. En esta «era

---

[1] Más allá del progreso técnico, la transmisión de valores, cultura y costumbres son, en igual o mayor medida, la demostración palmaria de la importancia de la transmisión y conservación de la información en las sociedades humanas.

[2] Para un recorrido completo sobre la evolución y desarrollo de la humanidad, incluido el incremento de las capacidades de generar y transmitir información, desde los neandertales hasta la actualidad, vid. (Harari, 2016b).

[3] (Aristóteles).

[4] Sobre el valor de la información para las empresas y la importancia de un uso eficiente de la misma, vid. (Tallon, 2013).

de la información» (Castells, 2006), la cantidad de datos que pueden recabarse, tratarse e interrelacionarse es abrumadora. La agregación y el cruce de datos facilitado por el *big data* y la lógica algorítmica, genera nuevas informaciones, distintas de las originarias, propiciando nuevos usos y posibilidades. «Por si no fuera suficiente, las inferencias y predicciones resultantes pueden alcanzar un elevado nivel de fiabilidad y certeza, hasta el punto de hacernos olvidar su naturaleza conjetural y probabilística[5]» (Jove Villares, 2021, p. 305).

Esta tesis nace de la preocupación por el uso y control de la información personal que, en el marco jurídico de la Unión Europea, se ha pretendido garantizar a través de un derecho que, por su transcendencia, se ha incorporado a la selecta familia de los derechos fundamentales. Pero ¿es el actual sistema legal de la UE el más apropiado para hacer frente a los retos que la era digital plantea con relación al tratamiento de la información personal?

No se pretende ofrecer una respuesta general a esa cuestión. Tan solo persigo aproximarme a ella a través del examen de dos elementos estrechamente interrelacionados: el concepto de dato y las llamadas categorías especiales.

Esta elección obedece a su carácter condicionante del modelo. El dato personal es el centro de imputación del derecho, al punto de nombrarlo. Qué se entienda por dato personal determina el ámbito de aplicación del derecho. Por tanto, es preciso valorar si, el concepto de dato personal[6] establecido, es el más adecuado para responder a los desafíos que las inferencias y correlaciones que posibilita el tratamiento automatizado de la información. De ser necesario, ¿sería posible establecer un concepto de dato personal diferente y más amplio que el actualmente previsto?

---

[5] El nivel de precisión viene determinado por la cantidad y la calidad de los datos, como variables más destacadas. No obstante, debe tomarse en consideración que habrá informaciones que bien no se conozcan, bien sean imposibles de incorporar a los sistemas algorítmicos y cuya transcendencia puede afectar a la fiabilidad del resultado final. Un ejemplo del carácter predictivo, no siempre acertado, de estos sistemas puede verse en, (Lazer *et al.*, 2014).

[6] Art. 4.1. RGPD: «"datos personales": toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

Si el concepto de dato delimita el radio de acción del derecho a la protección de datos, las categorías especiales establecen un régimen jurídico más agravado para su tratamiento. Pero, ¿cuáles son las razones justifican y subyacen a su existencia? Esto es, ¿por qué, del conjunto de los datos personales, solo los reconocidos en el art. 9.1 del RGPD[7] tienen esa consideración singularizada? ¿Por qué los que figuran allí y no otros? ¿Acaso no existen otras informaciones, como pudieran ser las financieras, igual de delicadas? Es más, entre las tipologías definidas como especiales, ¿no debería haber una graduación? ¿Acaso son todas las informaciones que las integran igual de sensibles? Así, ¿tiene el mismo nivel de impacto para la persona que se conozca su afiliación a un sindicato mayoritario, el que sea heterosexual o el que padezca una enfermedad degenerativa? Por otra último, ¿sería posible una reforma legal que prescindiese de ellas, o las categorías especiales son un elemento inherente y consustancial al derecho fundamental a la protección de datos?

A las cuestiones jurídicas planteadas, se adiciona un problema técnico: el perfilado algorítmico. Su capacidad para establecer correlaciones y elaborar perfiles con un alto grado de fiabilidad y acierto, posibilita que, a partir de datos no considerados especiales, se puedan llegar a conocer informaciones sensibles. A partir de la ubicación (dato no especial) es posible conocer la orientación sexual de una persona (dato especial)[8].

Para hacer frente a estos y otros interrogantes se ha optado por una aproximación, holística y gradual (de lo general a lo particular) al sistema europeo de protección de datos.

En primer lugar, se contextualiza el espacio, el tiempo y el marco jurídico-normativo en el que el derecho a la protección de datos nace y se despliega. El **Capítulo I** se dedica, precisamente, a la descripción del contexto tecnológico actual y los retos jurídicos que plantea. La era digital, con sus constantes transformaciones y capacidad evolutiva (Shepherd, 2004), no es un simple decorado exterior. Si el contexto es esencial en la

[7] Pertenecen a las categorías especiales de datos, los «datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física» (art. 9.1 RGPD).

[8] Como las aplicaciones de rastreo de la Covid-19 han puesto de manifiesto en Corea del Sur. https://www.pri.org/stories/2020-05-22/south-korea-s-coronavirus-contact-tracing-puts-lgbtq-community-under-surveillance. (Última consulta: 20/10/2021).

interpretación de los derechos[9], en el caso del derecho a la protección de datos, en particular, constituye un imperativo del principio de realidad.

La quiebra de lo reservado, el reconocimiento de nuevos derechos adaptados a la era digital y la necesidad de articular de respuestas jurídicas eficaces frente a la ubicuidad de la Red, conforman el marco fáctico en el que el derecho a la protección de datos ha de desplegar sus efectos.

Para comprender su morfología, finalidades y naturaleza, es especialmente útil la cognición de los diferentes hitos tecnológicos, legislativos y jurisprudenciales que le han ido dando forma. En el **Capítulo II** se examina el largo camino recorrido desde la construcción doctrinal de la *privacy* por Warren y Brandeis hasta la consolidación del derecho a la protección de datos como derecho fundamental autónomo.

Una vez establecidas las condiciones fácticas e históricas que han dado vida y forma al derecho a la protección de datos, se procede a analizar, en el **Capítulo III**, su regulación jurídica. En nuestro caso, el objeto de estudio será el ecosistema jurídico de la Unión Europea (UE), esto es, el conjunto de normas que inciden en el tratamiento de la información personal. La elección de este enfoque obedece a diversas razones: la europeización del derecho a la protección de datos, la transcendencia del RGPD y la mejor posición de la UE para establecer un marco normativo omnicomprensivo, capaz de someter a las grandes empresas transnacionales que dominan el espacio digital.

Las características definitorias del modelo europeo de protección de datos permiten evaluar su capacidad para hacer frente a los desafíos que plantea el desarrollo tecnológico. Además, la comprensión de la idiosincrasia del modelo europeo resulta crucial para el planteamiento de cualquier propuesta reforma que afecte al concepto de dato o al régimen jurídico de las categorías especiales. No sería realista ni prudente proponer un sistema alternativo cuando caben soluciones menos incisivas y más acordes con la cultura jurídica europea.

Ahora bien, siendo importante que cualquier eventual modificación del marco jurídico se adecúe a la idiosincrasia del modelo europeo, lo

[9] «El contexto social forma parte de la teoría de la Constitución (y de los derechos fundamentales) que se encierra en el texto constitucional. Labor del intérprete es aprehender esa teoría para así poder hacer una interpretación constitucionalmente adecuada no sólo de los enunciados *iusfundamentales*, sino también de la realidad (contexto) que abstractamente está regulada en ellos» (Bastida Freijedo et al., 2004, p. 48).

realmente decisivo es que, además, sea respetuosa con los contenidos del derecho a la protección de datos. Por esta razón, en el **Capítulo IV**, se indaga acerca de la naturaleza del derecho fundamental del artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE).

A partir de estos presupuestos, se identifica el contenido y finalidades que dan forma al citado derecho fundamental, teniendo presente que, para su caracterización, son tan importantes las aportaciones jurisprudenciales, como las diferentes construcciones doctrinales existentes, incluidas aquellas que niegan su condición de derecho fundamental.

Finalmente, en el **Capítulo V**, se abordan en profundidad las cuestiones que inspiran este trabajo. Se ahonda en la razón de ser de las categorías especiales, así como en los problemas y ventajas que comporta la existencia de un conjunto tasado de informaciones a las que, en atención a su naturaleza, se dota, por imperativo legal, de una protección reforzada.

A continuación, se formulan una serie de propuestas destinadas a mejorar la respuesta jurídica frente al tratamiento de la información personal. Las apreciaciones realizadas con relación al concepto de dato personal siguen idéntico proceso argumental y persiguen los mismos objetivos.

CAPÍTULO I. LA SOCIEDAD DIGITAL Y SUS INCERTIDUMBRES

«*Un instrumento barato, no más grande que un reloj, permitirá a su portador escuchar en cualquier lado, en el mar o en tierra, música o un discurso de un líder político, dictado en otro sitio distante. Del mismo modo, cualquier dibujo o impresión podrá ser transferida de un lugar a otro*»
Nikola Tesla. 1926

1. La era digital: ventajas

La socialización de usos en la era digital se apoya en la suma de externalidades positivas y comodidades suministradas por las nuevas tecnologías de la información. Las innovaciones digitales se presentan como herramientas para hacernos la vida más fácil, y gratis, o a un costo muy reducido.

Esta "casa de chocolate" se ha hecho realidad merced al crecimiento exponencial y constante de la capacidad de computación y de almacenamiento de información (big data); al desarrollo de dispositivos que incorporan nuevas formas de interconexión personal (v.gr. el internet de las cosas[1]); y a los diseños algorítmicos, cada vez más precisos, al punto de "pensar" por sí mismos. A ellos que nos referiremos, en un ejercicio de reducción consciente, como inteligencia artificial (IA)[2]. Naturalmente,

[1] Como apunta Barrio Andrés, «el Internet de las cosas es, desde hace unos años, una realidad ya presente en las sociedades tecnológicamente más acanzadas, puesto que hoy en día Internet intercomunica no sólo ordenadores, incluyendo en los primeros dispositivos como los teléfonos inteligentes (*smartphones*) o las tabletas (*tablets*), sino también otros muchos tipos de "objetos" (o cosas): desde ropas tecnológicas o *wearables* (tales como relojes, pulseras inteligentes o gafas de realidad aumentada), electrodomésticos (frigoríficos, aspiradoras …) televisores, videoconsolas, automóviles, elementos de edificios (p. ej. cerraduras, termostatos, bombillas, cámaras de seguridad, controles de acceso, sensores de temperatura…), hasta grandes infraestructuras públicas como puentes, autopistas o ciudades, etc., abriendo así la puerta a la interacción "máquina-máquina" (*Machine-to-Machine*, M2M). También conexiona a personas con esos objetos; puede incluso conectar animales, como sucede ya en algunas explotaciones ganaderas o en ciertos programas protectores de la biodiversidad» (Barrio Andrés, 2020, p. 20).

[2] Pese a que se viene utilizando el término inteligencia artificial desde hace décadas, concretamente desde su formulación por John McCarthy en 1956 (Haenlein y Kaplan, 2019), lo cierto es que, como han señalado Walters y Novak, «*there is no single definition of AI that has been accepted by all technology practitioners, or legal practitioners*» (Walters y Novak, 2021, p. 41). Con todo, a los efectos que aquí proceden, tomaremos como referencia la definición proporcionada por la Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión,

todos ellos son, en última instancia, herramientas puestas al servicio de objetivos concretos.

Para las autoridades gubernativas, las herramientas digitales son una vía para una gestión más eficiente de los recursos públicos y un poderoso aliado en el ejercicio del poder (Chopra, 2014)[3]. La tecnología es un recurso muy útil para el gobernante, (Todoruţ y Tselentis, 2018). La gobernanza por medio de algoritmos hasta puede crear una conveniente apariencia de neutralidad política o ideológica. ¿Qué argumentos podría tener la oposición política ante una decisión basada en la lógica matemática? ¿Quién podría acusarla de partidista cuando, en teoría, se funda en datos y no en posiciones de parte?

La tecnología facilita la comunicación de la ciudadanía con las instituciones públicas, agiliza trámites, asegura la trazabilidad de las decisiones y favorece la transparencia y la fiscalización[4]. También abre un escenario de cambio, en el modo y en la forma de entender la participación ciudadana en la vida política: acceso a candidatos, programas, propuestas de gobierno, diálogos en tiempo real, voto telemático…el ágora griega restaurada, ampliada y digitalizada, todo al alcance de un clic (Rodotà, 1997, pp. 62 a 70 y 164 a 168)[5].

Los avances de la era digital anuncian cuotas de seguridad y gobernanza antes tan solo soñadas: potentes sistemas de videovigilancia y

---

conforme a lo dispuesto en su artículo 3.1, se entiende por Sistema de inteligencia artificial al «software que se desarrolla empleando una o varias […] técnicas y estrategias […] y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa».
Puede consultarse el texto de la propuesta en:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206. (Última consulta: 20/10/2021).

[3] El uso de la tecnología incluso ha dado lugar a un modo específico de administrar y gobernar, el *e-government* se consolida día a día como el método de gestión de la vida pública por parte de las Administraciones y los gobiernos. Sobre el impacto de las tecnologías en las Administraciones Públicas y sus posibles usos, vid. (Valero Torrijos, 2013).

[4] Digitalizar las prácticas administrativas no implica, necesariamente, una mayor transparencia, dependerá, en última instancia del nivel de exigencia que se imponga y de cómo se articulen las medidas, en todo caso, no cabe duda que son nuevos medios que abren nuevas posibilidades de acceso. Vid. la completa obra colectiva *Administración electrónica, transparencia y contratación pública*, en ella se apuntan tanto las posibilidades de mejora técnica, como las necesidades y carencias de las regulaciones europea y española sobre la materia (AA. VV., 2020a).

[5] Si bien la participación política a través de sistemas digitales siempre genera ciertas suspicacias, especialmente en relación con su seguridad, su fiscalización o su accesibilidad por todos, vid. entre otros, (Hindman, 2008), (Gil de Zúñiga, Veenstra, Vraga, y Shah, 2010), (Al-Ameen y Talab, 2013) o (Teague, 2021).

localización para combatir la delincuencia; la inteligencia artificial se nos ha mostrado como un instrumento valiosísimo en la detección y seguimiento de enfermedades (Maddox, Rumsfeld, y Payne, 2019), en la política sanitaria (Schwalbe y Wahl, 2020) o en la personalización de los tratamientos (Shaban-Nejad, Michalowski, y Buckeridge, 2018). En plena pandemia por la Covid-19, han surgido aplicaciones capaces de rastrear los contactos con gran detalle (Borra, 2020), a fin de cuentas, al teléfono móvil no se le olvida ningún "contacto". ¿Cómo renunciar a semejantes oportunidades? ¿Cómo justificar ante la opinión pública que no se han utilizado todos los medios a disposición para asegurar la seguridad, la tranquilidad y el bienestar de la ciudadanía?

¿Qué decir de las personas y empresas privadas? La «telépolis» (Echevarría Ezponda, 1994) es un mundo repleto de oportunidades. Por primera vez, es posible anticiparse a lo que el consumidor demandará, sin excesivo temor a errar. El «*Big Data allows us to finally see what people really want and really do, not what they say they want and say they do. Providing honest data is the second power of Big Data*» (Stephens-Davidowitz, 2017, p. 54).

Los consumidores-usuarios tienen a su disposición nuevas e inimaginables formas de satisfacer sus deseos. Todo está a su alcance. La pantalla de su dispositivo es la puerta al mercado global. Pero también es la administradora de afectos. Allí se encuentran redes para charlar con amigos o buscar pareja, espacios para la diversión con videojuegos, vídeos, series, películas, libros, podcast o cualquier otro tipo de producto para el entretenimiento. Se acabaron las horas muertas. Siempre habrá un *Candy Crush* dispuesto a sacarnos de la apatía y el tedio.

Pero el encanto de lo virtual no se queda en la pantalla. Si se desea salir a cenar o a un concierto, se cuenta con un buscador dispuesto a ofrecerle las mejores opciones (de calidad, de precio o ambiente) todo ello avalado por una legión de consumidores-usuarios. El buscador le dará al consumidor-usuario la información deseada o le indicará dónde encontrarla. Muy extravagante ha de ser la pregunta para que Google, Bing o DuckDuckGo no tengan la respuesta.

Los dispositivos electrónicos no solo nos comunican. Nos proporcionan entretenimiento y ofrecen la posibilidad de comprar de todo, en todas partes; también nos cuidan, vigilan nuestra salud, mejoran nuestra audición, limpian nuestros pisos, nos avisan si la nevera está vacía,

cierran las persianas de nuestras casas cuando no estamos y, más pronto que tarde, conducirán nuestros automóviles, ofreciendo una seguridad nunca antes vista.

Se ha generado un macrocosmos en el que el consumidor-usuario puede desplegarse. Un universo virtual lleno de oportunidades en el que la realización del ser está a la vuelta de un clic, o de una pulsación de pantalla.

2. Las sombras del progreso digital

Toda "casa de chocolate" tiene su bruja. Mucho se ha escrito sobre los peligros del desarrollo digital, de su impacto en la sociedad, de las posibilidades de control de la población y de los riesgos que puede suponer para la democracia y los derechos[6].

Algunos de los males achacados a la era digital no son fruto de acciones individuales o la consecuencia de un plan predeterminado. Son el precipitado del modelo de sociedad que la vertiginosa evolución tecnológica ha ido conformando. Es fácil culpar, pero, a veces, los resultados perjudiciales no tienen su causa en el *big data*, los algoritmos, los robots o la conducta contraria a derecho de alguna entidad (pública o privada). Antes bien, son el resultado del ecosistema que el conjunto propicia.

Se puede establecer una distinción entre las consecuencias fruto del (mal)uso consciente de las tecnologías –afectación directa– y los efectos secundarios, inicialmente no previstos ni queridos –afectaciones indirectas–. En ambos casos es previsible la conculcación de derechos fundamentales, pero, al obedecer a causas distintas, los remedios también han de diferir.

[6] Una parte importante de la obra de Byun-Chul Han gira en torno a estas cuestiones ((Han, 2018a), (Han, 2018b) y (Han, 2019)), pero también otros como Baricco (Baricco, 2019) o Harari ((Harari, 2016a, pp. 311-431) y (Harari, 2018, pp. 21-104)) han incidido en los efectos que el desarrollo tecnológico puede tener sobre la vida en sociedad. Especialmente crítica es Shosana Zuboff, quien alerta de los riesgos de un «capitalismo de la vigilancia» incompatible con sistemas democráticos (Zuboff, 2015) y (Zuboff, 2020).

2.1. Las amenazas y los daños previsibles

Los supuestos de afectación directa se caracterizan por producir un impacto identificable, ya sea sobre los derechos de uno o más individuos, o sobre el sistema democrático en su conjunto. En esta tipología, el acto causante del riesgo o del daño, será siempre previsible. La vulneración del derecho a la vida privada, a la protección de datos, a la salud, a la libertad religiosa, a la libertad ideológica o cualesquiera otros, proviene de la actuación de un tercero (sea una persona física o jurídica, pública o privada) canalizada a través de un medio digital, lo que hace que hace que la lesión del derecho adopte ciertas particularidades.

De una parte, en el microcosmos virtual, ciertas violaciones de derechos pueden resultar menos evidentes o relevantes para su titular, ya sea por considerar que lo que pasa en la Red se queda en la Red, o porque, en la esfera digital, no todos los actos tienen una causa-efecto inmediata. Así, una lesión inadvertida del derecho a la protección de datos, puede ser, tiempo después, motivo de discriminación (impidiendo el acceso al trabajo o la contratación de un seguro) (Favaretto, De Clercq y Elger, 2019); y lo que parecía una inocente encuesta sobre gustos cinematográficos puede derivar en un condicionamiento selectivo en unas elecciones, segmentando mensajes y condicionando decisiones a partir de perfiles cuidadosamente elaborados (González, 2017; Missika y Verdier, 2021).

Merced a su ubicuidad, y a la erosión de las barreras y defensas que representaban el tiempo, el esfuerzo y los costes, la tecnología permite realizar tanto actuaciones muy especializadas sobre individuos concretos, como vulneraciones masivas que afecten a una pluralidad de sujetos e, incluso, a la sociedad en su conjunto. Conviene no olvidar que, por muy digitales que sean los medios para llevar a cabo las actuaciones, las consecuencias para la ciudadanía son muy reales.

Algunas de las prácticas y supuestos de afectación directa, por su gravedad o por el número de personas afectadas, pueden proyectar sus efectos más allá de las personas directamente concernidas y del acto concreto, generando una especie de *chilling effect* que condicione el comportamiento futuro de la ciudadanía. Las técnicas de condicionamiento conductual forman parte de las estrategias que la IA permite implementar, recompensando ciertos modos de actuación/o rasgos y penalizando otros (Seaver, 2019). Esta derivada les aproxima a los supuestos de afectación

social no querida, si bien, difieren de ella en la intencionalidad de sus promotores.

2.2. Los efectos en segundo plano

Todo proceso profundo de transformación agita las estructuras sociales y altera el modo de organizarse y vivir en comunidad. En esto, la era digital no difiere de otros momentos de inflexión en la evolución de la humanidad. Sin embargo, diverge en la velocidad con que los cambios se producen. La rápida modificación de comportamientos, la sucesión de innovaciones no asimiladas ni maduradas, la disolución del anterior sistema de valores, sin margen para construir unos nuevos, produce una transición sin brújula, un vagar por el desierto, para la que no estamos convenientemente pertrechados (Foer, 2017).

La caída acelerada en la cascada de lo urgente y lo inmediato no da tiempo a respirar. Se actúa de manera reactiva, minimizando daños o aceptándolos como parte de una nueva normalidad, en un conformismo adaptativo que dista mucho de ser revolucionario.

2.2.1. Las personas como generadoras de datos: de ciudadanos a consumidores-productores

A pesar de la muy extendida idea de que los datos son el nuevo petróleo, esta afirmación no es del todo exacta. Tal vez sí se corresponda con la realidad en cuanto a su condición de materia prima en muchos negocios, a su potencial económico o a su condición de agente peligroso para la ciudadanía (contaminación ambiental-afectación vida privada[7]) pero, en global, existen importantes diferencias. Desde la finitud del petróleo frente al carácter infinitamente renovable de los datos, su facilidad de producción, autogeneración y disponibilidad y, sobre todo, su "inmaterialidad", entendida como dificultad para percibir su uso,

[7] Hirsch realiza un interesante análisis comparativo de la efectividad de las medidas desarrollados para reducir los efectos contaminantes derivados del uso de combustibles fósiles y las utilizadas para prevenir la afectación de la *privacy* a raíz del uso de información personal, vid. (Hirsch, 2014).

consecuencias y efectos, especialmente cuando son tratados por medios digitales[8].

La revolución digital ha introducido parte de nuestra alma en el mercado, cosificándola como una *res intra comercium*. Toda información, sea o no personal, es susceptible de ser utilizada, de generar valor. No hay dato que no se pueda aprovechar[9]. La posibilidad de analizar grandes cantidades de información, combinada con el perfilado algorítmico, permiten obtener, incluso de datos aparentemente residuales, informaciones susceptibles de ser explotadas económicamente. Los datos (personales o no) son «el activo más importante en la economía y la única cosa que se intercambie en numerosas transacciones» (Harari, 2018, pp. 24-25).

El elemento determinante de este modelo es que los seres humanos somos productores conscientes e inconscientes de información. El contexto digital nos ha convertido en un cultivo de datos. Los generamos, incluso, sin querer: la pasividad, el no hacer, la decisión de no interactuar o no participar de un determinado proceso, también es un dato de interés.

La condición intrínseca del ser humano como generador de información ha cobrado una nueva magnitud en nuestro tiempo. Si la era digital es la era de la información, no es porque se haya producido una mutación en las personas que nos haya convertido en máquinas de producir datos en cantidades industriales, sino porque el proceso de digitalización ha ido de la mano de la mejora constante en la capacidad para captar, tratar y explotar la información que generamos.

---

[8] (Hoffman-Riem, 2018, pp. 54-57), (Mayer-Schönberger y Ramge, 2021) o (Foer, 2017, p. 183) explican por qué no son el nuevo petróleo

[9] Cuestión diferente al valor de la información es la de la calidad de los datos. Estos es, la adecuación (exactitud, pertinencia y modo de tratamiento) de las informaciones utilizadas para la consecución de los fines perseguidos. De hecho, la calidad de los datos es, sobre todo, un problema en el uso del *big data*, donde la cantidad de información gestionada opera como una espada de doble filo, proporcionado tendencias generales, pero también introduciendo muchas variables que, en lugar de clarificar, aportan ruido que impide obtener resultados claros y precisos, (Cai y Zhu, 2015), (Becker, King, y McMullen, 2015).
Del mismo modo, tampoco debe confundirse el valor de los datos con el reconocimiento jurídico de categorías específicas para las que se establece una protección reforzada. Que jurídicamente existan datos más sensibles por tener una conexión más directa con la persona y entrañar su uso un mayor riesgo de afectación de los derechos, no implica, necesariamente, que sean más valiosos en un sentido económico. Dependerá, en todo caso de la finalidad que se persiga con el tratamiento. Por ejemplo, para un fabricante de coches será más valioso saber el grado de preocupación de la ciudadanía por el medioambiente que la afiliación sindical de sus potenciales compradores.

Una vez consolidados los medios técnicos (dispositivos electrónicos, Internet, servicios de almacenamiento y procesado de información) el siguiente escalón evolutivo ha sido psicosocial. Ya no se trata de crear una tecnología mejor, cuanto de diseñar sistemas que capten la atención del usuario, manteniéndolo conectado, entretenido, mientras produce la información. Procesar datos del modo más eficiente sigue siendo la base del sistema, pero la batalla está en lograr la adhesión de unos consumidores-usuarios que son, a la vez, los generadores de un subproducto que constituye un valor en sí mismo: la información.

Tal es la magnitud del nivel de refinamiento alcanzado que hoy los ingenios tecnológicos, además de eficientes en el procesado de la información, están configurados para "motivar e incentivar" a las personas a interactuar e incrementar el suministro de datos. Generar datos se ha convertido en una acción inconsciente revestida de necesidad, o de placer voluntario[10].

La conformación de la sociedad, los modelos productivos y la organización de la vida colectiva se han construido sobre el presupuesto de la satisfacción del consumidor-usuario quién, a su vez, es productor-proveedor de la materia (los datos) con la que se construye la casa común digital. El consumidor-usuario desplaza al ciudadano de su antigua centralidad[11]. La revolución digital ha supuesto la emergencia de un mundo diverso –el virtual– dotado de sus propias particularidades[12].

El espacio digital es transfronterizo y, en él, los poderes públicos de los estados democráticos ya no son una potencial amenaza para los derechos y libertades de las personas[13]. En el mundo online, las grandes

[10] Como Llaneza expone, las empresas de *software* dedican grandes esfuerzos al diseño de sistemas que generen adicción «*adiction by design*», capaces de motivar a los usuarios a interactuar para seguir generando más información con la que operar, vid. (Llaneza González, 2019, pp. 141-161).

[11] Han pone el acento en la conmixtión que se produce «en el ágora digital, donde coinciden el local electoral y el mercado, la polis y la economía, [haciendo que] los electores se comporten como consumidores. […] Aquí ya no somos agentes activos, no somos ciudadanos, sino consumidores pasivos» (Han, 2018ª, pp. 97-98).

[12] Sobre las diferencias en la consideración de la intimidad entre mundo real y online, vid. (Passaglia, 2018, pp. 225-226).

[13] En China el gobierno sigue constituyendo la principal amenaza para la libertad personal y los derechos, también en el espacio virtual. El gobierno chino ha sido capaz de someter a sus condiciones a los proveedores de servicios online (cuando no los controlan directamente), lo que les permite seguir manteniendo un dominio sobre lo que ocurre en el basto mundo de la Red (Henochowicz, Creemers, Gallagher, Miller, y Ruan, 2017). Ese modelo de control de Internet no se circunscribe a China, otros países han utilizado fórmula de control y censura

corporaciones de naturaleza privada son los nuevos señores. Un pequeño grupo[14] de grandes empresas transnacionales[15] se han convertido en los «nuovi signori dell'informazione»[16] (Rodotà, 2019, p. 61).

2.2.2. El riesgo de colapso de los sistemas democráticos

La capacidad disruptiva y transformadora de la tecnología (Echevarría Ezponda, 2000), unida a su velocidad de expansión y constante innovación, es la principal fuerza de transformación social de las últimas décadas[17].

Los fundamentos tradicionales de la democracia comienzan a resentirse y ya han aparecido algunas pequeñas grietas que cumple observar y corregir[18].

En la era digital, las distancias y el tiempo se han reducido a la mínima expresión. Y, sin embargo, cada vez nos sentimos más aislados, encerrados y sumidos en el microcosmos que hemos ido generando (Spohr, 2017). Los vínculos que, hasta hace poco, eran el fundamento de la vida en sociedad, se están debilitando para abrir paso a una comunidad global, en la que coexisten e interaccionan una multitud de universos personales en constante configuración. Ha comenzado una nueva etapa en el proceso

similares, así, por ejemplo, Turquía mantuvo bloqueada la Wikipedia desde 2017 a enero de 2020 (Ruhdan, 2020).

[14] Alphabet (Google), Amazon, Facebook, Iphone, Twitter, Microsoft, Huawei o Xiaomi

[15] Entendidas estas como aquellos «operadores económicos privados cuya constitución y extinción, así como sus actividades, se encuentran sometidas a una pluralidad de jurisdicciones estatales» (Guamán Hernández y Moreno González, 2018, p. 20).

[16] Rodotà identificaba a algunos de ellos «Amazon o Apple, Google o Microsoft, Facebook o Yahoo!», a los que habría que añadir otros como Alibaba Group o Huawei, este último con entidad suficiente para ser el centro de una guerra comercial –y de posición estratégica global– entre China y EEUU.

[17] Sirvan como ejemplo: La disputa por la hegemonía mundial (v. gr. las disputas por el 5G y el 6G) y la lucha por la supremacía mundial entre EEUU y China, vid. (Quadri y Khan, 2020) y (Groves y Schulte, 2020); los procesos políticos revolucionarios (v. gr. la primera árabe en la que las redes sociales desempeñaron un papel crucial (Norris, 2015) y (Rihawi Pérez, 2019)) o la inmediatez de la comunicación a escala global. A los que habría que añadir otros cambios que, no por asumidos, dejan de ser relevantes, como las posibilidades de comunicación y transmisión de información, las vías de negocio que propician, las posibilidades de mejora de la calidad de vida que generan, merced a descubrimientos derivados del uso de tecnologías que posibilitan realizar en minutos tareas e investigaciones que tomarían años).

[18] Sartori, señaló hace más de veinte años un conjunto de riesgos para la democracia derivados de la formación de una sociedad teledirigida, forjada al calor del progreso tecnológico, vid. (Sartori, 1998, pp. 105-152).

evolutivo de los modos de vivir y relacionarnos (Harari, 2018, pp. 107-131).

Nadie duda de la capacidad del entorno digital para generar sensación de comunidad. Pero, interesa no olvidar, que no es posible vivir en el mundo online todo el tiempo.

Quienes sepan administrar el equilibrio entre realidades podrán beneficiarse de la pluralidad de opciones puestas a su disposición. Pero, a su lado, convivirá una multitud situada en el ostracismo, tras perder los anclajes en su comunidad presencial (no deben olvidarse las depresiones y la ansiedad derivadas de las dinámicas surgidas en las redes sociales (Keles, McCrae, y Grealish, 2020)).

Algunas tecnologías de la comunicación tienen un efecto –secundario– disolvente de la comunidad, dando lugar a lo que Bauman denominó «vida líquida»[19]. Una quiebra de lo común que, paradójicamente, proviene del uso de ingenios que buscan interconectar a las personas y que acaban provocando burbujas y desarraigos: «la psicopolítica digital […] se apodera de la conducta social de las masas» (Han, 2018a, p. 109)[20].

Las relaciones en la Red han traído otras consecuencias como las *fake news*, la pérdida de pluralidad y los riesgos para la formación de una opinión pública libre que constituye uno de los pilares de toda sociedad democrática[21]. En palabras de Stengel, «si la información es poder, la desinformación es abuso de poder» (Stengel, 2021, p. 14). Cada persona es un editor capaz de trasladar contenidos y darles visibilidad[22]. Con todo, los medios que el desarrollo tecnológico ha puesto a disposición de la difusión

[19] La vida líquida sería el rasgo definitorio de las sociedades contemporáneas. Estas vendrían marcadas por su inconsistencia, por no tener una contextura estable, por el ritmo desenfrenado destinado a mantenerse actualizado y al día, en una carrera sin un final claro, pues el horizonte de futuro muestra infinitos cambios a los que tratar de llegar, generando una incertidumbre y precariedad constantes, ante la imposibilidad de alcanzar un punto de estabilidad y consistencia (Bauman, 2006).

[20] Por psicopolítica Han entiende aquella capacidad para controlar la «conducta de las masas a partir de grandes datos» (Han, 2018a, p. 108).

[21] Existe abundante bibliografía al respecto, destacan, entre otros, (Mason, Krutka, y Stoddard, 2018), (Morgan, 2018) o (Farkas y Schou, 2019). Entre nosotros, son de gran interés los trabajos Serra Cristóbal (Serra Cristóbal, 2021), Balaguer Callejón (Balaguer Callejón, 2019) o Rubio Núñez (Rubio Núñez, 2018).

[22] Las libertades de expresión e información, esenciales en un sistema democrático, pudieran verse como un parapeto para la difusión de *fake news*, sin embargo, como apunta Aba Catoira, «la calidad democrática no pasa por prohibir los bulos sino por un refuerzo de la libertad. […] La mejor práctica para luchar contra las noticias falsas es la implementación de más y mejores medidas educativas que generen cultura democrática» (Aba Catoira, 2021, pp. 76-77).

de cualquier idea o información no son, *per se*, malos. Como apunta el citado Stengel, «la guerra de la información no es una batalla de tecnologías o plataformas, sino una lucha de ideas» (Stengel, 2021, p. 14).

Internet facilita el libre intercambio de información y conocimiento como nunca antes en la historia, «es un logro considerable de la libertad del individuo» (Frosini, 2018). Sin embargo, el medio no condiciona los fines y puede utilizarse para dar difusión a informaciones falsas, equívocas, tergiversadas o malintencionadas, a menudo con el propósito de satisfacer aviesos intereses y, otras veces, por puro divertimento o por tener la convicción de que son correctas.

La Red permite dotar de la misma apariencia a la mayor de las mentiras que a una verdad universal. Esta situación, que podría quedar una mera anécdota, deja de serlo cuando millones de personas pueden acceder a esas informaciones (preformadas y dirigidas) y terminan por confiar en ellas. Los riesgos para la vida democrática son evidentes. Una realidad en la que todo es susceptible de ser manipulado y falseado, carece de horizonte. Si todo es dubitable, si lo verdadero queda opacado por una sinfonía de falsedades ¿Cómo decidir? ¿Cómo distinguir qué parte del tsunami informativo de cada día es el que debemos elegir para articular nuestras ideas?

Acaso como reacción frente a ese aluvión informativo, las personas acaban agrupándose en esferas homogéneas, en las que las discrepancias se diluyen y lo distinto se castiga con la exclusión, de modo tal que cada uno solo interactúa con los afines (Arano Uría, 2020). Esa capacidad de silenciar, de apagar todo aquello que no guste, puede facilitar los tránsitos por la Red, al evitar perderse en el maremágnum de informaciones y tentaciones que acechan en ella, pero, cuando se aplica bajo el sesgo de lo ideológico, cuando se anula lo discordante, la pluralidad pasa a ser un enemigo.

A lo anterior ha de añadirse el efecto autoconstrictor que las redes infunden en sus operadores y usuarios. Como todo lo que se dice y hace es susceptible de ser multiplicado por la enorme caja de resonancia que son las redes, se procura, casi inconscientemente, evitar un efecto boomerang, de suerte que lo manifestado no opere en contra, trucando cualquier expectativa vital o comercial. La prudencia del *self restraint* se amplifica hasta traducirse en una especie de autocensura destinada a evitar el patíbulo público de las redes y el contenido viral.

La otra cara de esa misma moneda es la conversión de los prestadores de servicios en guardianes de las esencias y en los jueces de lo correcto y admisible (v. gr. en última instancia son los responsables de Facebook, Twitter o de cualquier otra empresa del sector, los que deciden a quien silenciar en un determinado momento o qué contenidos son aceptables en sus plataformas, y cuáles no).

Se cavan trincheras virtuales. Se levantan muros de corrección política y aparecen guetos morales o ideológicos. Todo ello contradice al espíritu de libertad e intercambio con el que Internet nació. Sin embargo, ahora, forman parte de su ser.

2.2.2.1. La comodidad como problema

No cabe duda acerca de las ventajas y comodidades que las tecnologías reportan. Pero semejantes beneficios tienen ciertas contrapartidas, no siempre explicitadas. La información que se nos proporciona está tamizada. Es el producto de una serie de filtraciones y procesos de depuración y purga, basados en preferencias previas: quien paga más por posicionarse y toda una miríada de variables que el algoritmo considera, y que no tienen por qué ser, necesariamente, neutrales, aunque aparezca revestida con los ropajes de la lógica matemática.

El *big data* y los algoritmos son lo que sus usuarios y programadores quieran que sean. Depende de su uso. Más aún: «los algoritmos nunca buscan causalidades, sino solo correlaciones», no explican, anticipan (De Miguel Beriain y Diéguez Lucena, 2021) por lo que el error forma parte de su naturaleza. Nada impide que puedan ofrecer respuestas sesgadas, ya sea por diseño o por omisión, al no incluir alguna variable de cálculo[23]. Ahora bien, el margen de error queda ocluido por la ventaja que supone diferir a una fórmula matemática la responsabilidad por las decisiones adoptadas. Cuando la inteligencia artificial puede ofrecer respuestas mayoritariamente válidas a decisiones complicadas y revestirlas, además,

[23] Las razones por las que puede producirse una decisión algorítmica sesgada son variadas (desde un diseño que reproduce las dinámicas sociales hasta una información incompleta). Los resultados más preocupantes en este sentido son aquellos que dan lugar a algún tipo de discriminación (racial, género o económica). Sobre las causas y consecuencias de la discriminación derivada de decisiones algorítmicas se ha escrito mucho, a efectos puramente ilustrativos y por su carácter descriptivo de las diferentes variables a considerar, vid. (Ferrer, Nuenen, Such, Coté, y Criado, 2021), (Criado y Such, 2019), (Kleinberg, Ludwig, Mullainathan, y Sunstein, 2018), (Chander, 2017) o (Hajian, Bonchi, y Castillo, 2016).

de la certeza y objetividad de un proceso automatizado ¿quién asumirá los costes de rebatirlas? En un contexto semejante, no es de extrañar que «la capacidad humana para decidir libremente […] [esté] colapsando» (Lassalle: 2019: 30) o, al menos, se encuentre severamente amenazada.

2.2.2.2. Sociedad digital y ejercicio del poder

En las sombras del esplendor digital se va gestando un nuevo ser, un «Leviatán tecnológico […] desde el que se reorganizará la arquitectura artificial de un poder concebido como un panóptico perfecto» (Lassalle, 2019: 48). Un Leviatán, en efecto, con múltiples cabezas. Unas veces serán las grandes empresas transnacionales, más ricas y poderosas que muchos estados, las que determinen el modo de vida de los ciudadanos, gobernando sin gobernar y dirigiendo sin dirigir. Otras, serán los gobiernos los que, aprovechando posiciones de fortaleza preexistentes, se valgan de los medios que la técnica ofrece para reforzar su control sobre su ciudadanía. El Ciberleviatán operará con una u otra cabeza según lo demanden las circunstancias. Con todo, quizá, en algún lugar logren resistir la implacable fuerza atractiva de ese nuevo poder[24].

Mis palabras no se deben a un «terror cósmico» a la innovación y el progreso (Ortega y Gasset, 1965), sino una preocupación nacida del impacto de la «tecnodemocracia y la soberanía electrónica» (Bastida Freijedo, 1998)[25] en los derechos fundamentales y la democracia. La respuesta jurídica a este desafío resulta crucial. No se trata de frenar los avances tecnológicos, sino de guiar su avance, orillando, en lo posible, sus consecuencias más dañinas.

[24] Tal vez, en un futuro lejano, ¿acaso de ciencia ficción?, no sean ni los entes privados, ni los gobiernos sino una inteligencia artificial diseñada expresamente para gobernarnos y hacernos la vida más fácil, quien actúe como leviatán único y todopoderoso, pero esto, por el momento, se adentra demasiado en los terrenos fangosos de las hipótesis fantasiosas. Con todo, y aunque sea como eventualidad, es un escenario a plantear.

[25] En este trabajo de 1998, Bastida Freijedo enuncia, con gran acierto y anticipación, tanto las posibilidades como los riesgos de la tecnodemocracia. En especial, advierte sobre la posibilidad de diluir los actuales sistemas democráticos y que acaben transformados en «un régimen de opinión pública, en […] [una] democracia "en directo"» que cortocircuite el sistema, deslegitimando sus instituciones y «operando como un metasistema y, además, sin las garantías del sistema democrático» (Bastida Freijedo, 1998, p. 422-423).

2.2.3. La quiebra de lo reservado

La disputa por la atención de los consumidores-usuarios está en la base de muchos de los servicios de la era digital. Las redes sociales, los motores de búsqueda, muchas de las aplicaciones que miden nuestro estado de salud o nos facilitan la vida proporcionándonos métodos más cómodos de realización de actividades cotidianas (desde comprar a viajar, pasando por entretenimiento, alojamiento u organización de tareas) justifican la gratuidad de su modelo de negocio en su capacidad para detraer información útil para otros productos y servicios.

El éxito de ese modelo requiere generar entornos amigables en los que los consumidores-usuarios estén dispuestos a facilitar información, pues cuanto más se les conozca, más fácil resultará determinar qué producto es el adecuado para cada uno de ellos. Así, poco a poco, seguramente sin quererlo, o sin ser el objetivo principal, se va generando un sistema de interrelación que incita, prácticamente aboca, al exhibicionismo (Han, 2018b).

La prodigalidad con que se comparte información no es, exclusivamente, el fruto de una decisión neutra y consciente. Más que un acto voluntario, es una exigencia del mercado. La economía capitalista ha encontrado en el desarrollo tecnológico a su más poderoso aliado, pues ha transformado a cada sujeto en «su propio objeto de publicidad. Todo se mide en su valor de exposición. La sociedad expuesta es una sociedad pornográfica. Todo está vuelto hacia fuera, descubierto, despojado, desvestido y expuesto. […]. [Pues] solo la escenificación expositiva engendra valor» (Han, 2018b, p. 29).

La información personal deja de ser un bien del sujeto para convertirse en un producto. Los efectos que a medio y largo plazo puede tener para la ciudadanía quedan opacados por la inmediatez de la satisfacción que proporciona. El valor intrínseco de mantener una esfera reservada al conocimiento ajeno quiebra y, por esa brecha, fluye la información que alimenta el mundo digital. A ese efecto directo, se suman los ya apuntados efectos secundarios: la sensación de saberse vigilado; la impresión de que sus actos terminarán siendo conocidos; la inquietud ante el escrutinio constante de una pluralidad de jueces anónimos e implacables. Todo ello, termina condicionando el modo de relacionarse y vivir en sociedad. La transparencia se presenta como la condena inevitable de nuestro tiempo (Han, 2018b).

Ante un panorama así, ¿cómo mantener una esfera reservada?, ¿cómo escapar de la voracidad de las redes? Sorprende comprobar como el mercado ha encontrado una nueva vía de negocio: la preservación de la vida privada cómo producto; la seguridad de ver protegida tu esfera íntima a cambio de un precio. No solo los misántropos desconectados podrán preservar su vida del conocimiento ajeno. Ahora –y más en el futuro– la cuestión será averiguar qué nivel de reserva nos podemos permitir, cuánto estamos dispuestos a pagar para tener los servicios y ventajas que la tecnología ofrece, pero con la tranquilidad de que tu información personal permanecerá a salvo del conocimiento ajeno

La transformación producida es sorprendente. Lo que antes era un derecho, se fue desvalorizando en aras del progreso y la comodidad. Ahora, las mismas entidades que lo hicieron posible, comienzan a ofrecer espacios de inviolabilidad a cambio de un precio o de fidelizar a los consumidores-usuarios[26]. La era digital ha apurado al límite la noción de vida privada, recordando su valor a la sociedad mediante su conversión en un servicio con valor añadido.

3. Dos desafíos de la era digital: los derechos digitales y la globalidad de la Red

3.1. Derechos digitales y derechos en la era digital

El mundo digital no es un lugar sin ley, no es un salvaje oeste 2.0. La vida en la Red no es ajena al Derecho. Las amenazas antes descritas hacen imprescindible un marco normativo sólido, que aporte la previsibilidad y seguridad jurídica sobre la que se asientan las sociedades democráticas.

La realidad *online* y la *offline* tienen notables divergencias. Cada una de ellas presenta sus particularidades y retos. La realidad online se encuentra en constante expansión: la Red de redes, las mejoras exponenciales en las capacidades de almacenamiento y procesamiento de información, la robótica o la inteligencia artificial, generan escenarios nuevos, que exigen soluciones innovadoras y originales (v. gr. el acceso a Internet es una demanda que difícilmente puede encontrar anclaje en los

[26] Algunas marcas de tecnología móvil, v. gr. Apple, ya realizan anuncios publicitarios cuyo único mensaje es: «Tú decides quién rastrea tu información. Y quién no. Privacidad. Esto es el iPhone». Puede verse en: https://www.youtube.com/watch?v=J4qXRkecnco. (Última consulta: 20/10/2021).

derechos preexistentes a la emergencia de la Red, se trata de una aspiración nueva, necesitada de un reconocimiento y protección específicos[27]).

En ocasiones, esta evolución técnica solo requiere ajustes en los sistemas de protección y garantía de los derechos. Pero, otras veces, se hace necesario diseñar nuevos derechos y fórmulas para su defensa.

Si se analizan los bienes jurídicos afectados, y se toma en consideración aquello que se pretende proteger, se puede comprobar como hay circunstancias en las que, más que proclamar nuevos derechos digitales, basta con aplicar los ya existentes en la esfera virtual. No toda necesidad de respuesta normativa se ha de remitir, necesariamente, al reconocimiento de nuevos derechos, a veces, bastará con actualizar los mecanismos de protección con los que ya se cuenta.

Desconozco cuál pueda ser el mejor modo de afrontar desde lo jurídico la ordenación de ese mundo paralelo que es la Red (Rodotà, 2019). Se trata de un camino apenas explorado, con diversas opciones abiertas, y en el que no puede descartarse que su ordenación básica deba asignarse «a una constitución que fije sus principios rectores para garantizar la plena realización de los ciudadanos en el nuevo entorno sobre los valores de libertad, igualdad, justicia y pluralismo» (Teruel Lozano, 2016, p. 240). Sin especular tanto, las cartas de derechos digitales son una realidad jurídica destinada a consolidarse, al menos, en el espacio europeo.

Nuestro objetivo aquí es mucho menos ambicioso. Tan solo se quiere advertir que antes de incrementar la nómina de los derechos digitales[28],

---

[27] Como apunta Rodotà, el derecho de acceso a Internet «se presenta como síntesis entre una situación instrumental y la indicación de una serie abierta de poderes que la persona puede ejercer en la red» (Rodotà, 2014, 349). Sobre el reconocimiento de un derecho de acceso a Internet, resultan de gran interés los trabajos Álvarez Robles (Álvarez Robles, 2021) y (Álvarez Robles, 2018). En este último trabajo, además del derecho de acceso a Internet, apunta la necesidad de reconocer la ciberseguridad como derecho.

[28] En el caso de España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales (LOPDGDD) reconoce, en su Título X un listado de derechos digitales, entre otros el derecho de acceso universal a Internet (art. 81), el derecho a la seguridad digital (art. 82), a la educación digital (art. 83), el derecho a la desconexión digital (art. 88) o el derecho al testamento digital (art. 96).

Además, se ha elaborado una Carta de Derechos Digitales (2021), cuyo objetivo es «no es el de elaborar un proyecto de norma jurídica (algo que ha decepcionado a no pocos estudiosos de los derechos digitales) sino el de redactar un documento que pueda servir de referencia para una futura norma que regule los derechos digitales, partiendo de la base de que en principio sería muy conveniente una reforma de la Constitución de 1978 […] [Además,] puede servir para el fomento activo por los poderes públicos de códigos de conducta inspirados en los principios del texto, podría ser un útil instrumento interpretativo de

conviene analizar con detenimiento si no existen remedios jurídicos suficientes para afrontar la nueva situación[29].

Como recuerda Hoffman-Riem, «la protección de la dignidad humana, del principio de igualdad, la libertad de comunicación, la protección de la personalidad, la libertad del ejercicio profesional, la libertad religiosa o la garantía de la propiedad se aplican universalmente y no están limitados al empleo de tecnologías tradicionales. [Por tanto, es innecesario] […] complementar todas la regulaciones de la protección de los derechos humanos y las libertades con fórmulas de ampliación que incluyan la comunicación digital, el uso de infraestructuras digitales y el análisis de *big data* o […] el empleo de instrumentos de dirección digital del comportamiento» (Hoffman-Riem, 2018, p. 77).

En caso contrario, podría llegar a producirse una situación en la que una persona tuviese, para proteger un mismo interés jurídico, dos derechos cuya única diferenciación sustantiva fuese el medio en que se aplican. Cualquier derecho podría desdoblarse, desde la vida[30] hasta el derecho de

algunos conceptos difusos en la legislación vigente, y asimismo constituye el inicio de un debate sobre nuevos derechos digitales no positivizados hasta la fecha y la forma en que deberían modularse» (Barrio Andrés, 2021, p. 219-220). El texto de la Carta de Derechos Digitales puede consultarse en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf. (Última consulta: 20/10/2021).
En el ámbito europeo, el Parlamento Europeo emitió una resolución el 21 de enero de 2021 en la que insta a la Comisión a elaborar una propuesta regulatoria que se regule el derecho a la desconexión digital, puede consultarse en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0021_EN.html#title1. (Última consulta: 20/10/2021).
Además, de esta propuesta específica, la UE cuenta con la Estrategia digital, además de haber fijado los objetivos digitales de la Década Digital de Europa, lo que da cuenta de la importancia de la regulación digital en el proceso de integración europeo. Ambos documentos, están disponibles en el siguiente enlace: https://www.consilium.europa.eu/es/policies/a-digital-future-for-europe/. (Última consulta: 20/10/2021).

[29] V. gr. el derecho a la desconexión digital ¿es un derecho nuevo o es una manifestación del derecho a la educación? Personalmente considero que se trata de una concreción enriquecedora y actualizadora del derecho fundamental, pero que carece de entidad para ser considerado como un derecho nuevo y distinto. Sobre este particular, y referido al reconocimiento de este derecho en la LOPDGDD, he tenido ocasión de pronunciarme en (Jove Villares, 2020).

[30] La muerte digital es posible, si bien conectaría más con la libertad de expresión u otros derechos, pero ¿cómo se encauzará cuando la muerte digital sea una amenaza al modo de vivir de una entidad equiparable a una amenaza a su vida física? ¿Qué se hará cuando, en un futuro ¿lejano? se produzca una hibridación humano-tecnología que haga indiferenciable la afectación digital y la "analógica"?

manifestación, pasando por la educación, la salud o el descanso, todo es, o lo será en el futuro, susceptible de afectación desde lo digital.

En todo caso, lo que no cambiará, será que las consecuencias últimas las sufre una persona física y no su avatar. Por muy virtual que sea la esfera digital, las consecuencias son para las personas, para sus derechos y libertades. Los derechos deben adaptarse a los imperativos de la sociedad digital. Pero no debe confundirse flexibilidad y adaptabilidad con promiscuidad.

3.2. Respuestas locales a un desafío global

Tan globales son los servicios prestados como las amenazas para los derechos. Desde el momento en que entramos en contacto con la Red, las fronteras, la jurisdicción y el ordenamiento jurídico de cada estado comienzan a difuminarse. En su lugar emergen auténticos «continentes virtuales» (Lucena-Cid, 2014, p. 16) que quiebran la base territorial sobre la que se ha edificado la protección jurídica de los derechos.

Una protección que varía en función de las garantías jurídicas e institucionales[31]. Por este motivo, aunque existen valiosos instrumentos internacionales de reconocimiento y protección de derechos (v. gr. la Declaración Universal de los Derechos Humanos de 1948 o los Pactos Internacionales de Derechos Civiles y Políticos (1966) y de Derechos Económicos, Sociales y Culturales, también de 1966), al final, es en la esfera estatal y en los sistemas de protección de derechos regionales con algún tipo de capacidad vinculante (p. ej. el Convenio Europeo de Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH) merced al Tribunal Europeo de Derechos humanos (TEDH), la Convención Americana sobre Derechos Humanos y la Corte Interamericana de Derechos Humanos (CIDH) o el derecho de la Unión Europea y el Tribunal de Justicia de la

[31] La Declaración de Derechos del Hombre y del Ciudadano de 1789 ya establecía (art. 16) la necesidad de garantizar los Derechos como una condición *sine qua non* para la existencia de Constitución. Si bien, «un derecho no tiene la consideración de fundamental por contar con unas garantías específicas, pero lo cierto es que este refuerzo en su protección, si se compara con la que se dispensa a otras normas constitucionales, se convierte en uno de sus elementos más característicos» (Bastida Freijedo et al., 2004, p. 196). Aunque se han señalado la garantía jurisdiccional y la orgánica como referencia, lo cierto es que estas no son las únicas posibles, así, la exigencia de regulación legal para el establecimiento de limitaciones en el contenido de los derechos que la Carta de Derechos Fundamentales de la Unión Europea establece en el art. 52.1 también constituye un modo de garantizar los derechos de la ciudadanía.

Unión (TJUE)), donde se dan las condiciones reales y efectivas para hacer valer los derechos de la ciudadanía.

Esta realidad se torna aún más compleja si se toman en consideración las significativas diferencias culturales existentes sobre los derechos[32]. Las diferencias en cuanto a valoración social, cultura jurídica e, incluso, conformación histórica de un determinado derecho se reflejan en el modo en que termina siendo regulado, haciendo que su protección sea muy diferente a lo largo y ancho del globo. Sin embargo, esas divergencias resultan ciertamente problemáticas cuando se trata de regular la realidad de la Red. Es global y sus servicios tienen un alcance universal, pero sus prestadores, aun cuando operen en todo el mundo, se basan y actúan bajo una lógica determinada, marcada por un sistema jurídico y de valores concreto.

Uno de los desafíos jurídicos más notables de la era digital es asegurar, para todos los casos, que prácticas globales, regidas con diseños y lógicas locales, garanticen los derechos y libertades de la ciudadanía. El reto para los operadores jurídicos es inmenso, pues los sitúa en la tesitura de someter la globalidad y ubicuidad de la Red a los ordenamientos de cada lugar o, sino, tratar de forjar un sustrato común de alcance mundial.

Cualquiera de las dos opciones resulta complejas de ejecutar. La primera llevaría a transformar el mercado global en mercados locales, con sus usos y costumbres. La humanidad sigue siendo el potencial cliente, pero el acceso a ella se mediatiza por los ordenamientos jurídicos de cada país. Jurídica y políticamente parece la opción más viable, pero no deja de entrañar ciertas dificultades prácticas, derivadas de la ubicuidad de la Red, así como de las trabas económicas y técnicas que las divergencias jurídicas suponen para el flujo de la información, amén de los conflictos que pudieran derivarse de la competencia por ofrecer ventajas regulatorias que, acaso, pudieran ir en detrimento de los derechos de los usuarios de la Red (p. ej. adoptando regulaciones más laxas para la protección de los derechos a cambio de atraer a las compañías prestadoras de servicios).

[32] Pensemos, por ejemplo, la diferente consideración de la vida privada que puede existir entre España y Japón. Baste con señalar que el concepto de privacidad es considerado una noción importada, ajena a la realidad nipona (Orito y Murata, 2005). Con todo, en el caso de Japón se aprecia como el establecimiento de normativas de protección de datos ha ido generando una cierta conciencia acerca de la importancia de su salvaguarda (Fukuta et al., 2020). Sobre la protección de la privacidad en Japón, no puede dejar de referenciarse, el capítulo 6 de la monografía de Hildebrandt, *Smart technologies and the End(s) of Law*, (Hildebrandt, 2015, pp. 104-130).

La segunda de las opciones (una regulación global) eliminaría gran parte de los inconvenientes derivados de la existencia de una pluralidad de regulaciones. Sin embargo, su materialización tiene un obstáculo ¿insalvable? en la diversidad de concepciones, valores e intereses de los países[33]. Con todo, no ha de descartarse una paulatina aproximación normativa, precisamente para reducir las ineficiencias y sobrecostes derivados de la heterogeneidad regulatoria.

El reto no puede ser más complejo, pues se trata de organizar racionalmente un campo que fue creado y diseñado para que, por muchas puertas que se le pongan, siempre se pueda circular sin tener que atravesarlas.

4. El derecho a la protección de datos. Un camino por recorrer

Hoy existen los medios tecnológicos «*to monitor everyone all the time*» (Harari, 2020), sin embargo, el modo en que se utilicen, las finalidades y garantías que se implementen harán de esa práctica un acto más o menos invasivo, más o menos peligroso.

En la lucha por preservar la esfera personal frente a las injerencias y peligros de la era digital, la protección de datos es la punta de lanza del sistema de protección –aún en construcción– frente a los desafíos que el nuevo paradigma tecnológico plantea. Su dinamismo, carácter proteico y capacidad para dar respuesta a los desafíos que van surgiendo, le convierten en «una de las áreas del derecho, y de forma concreta de los derechos fundamentales, más evolucionada, mejor normada y con más medios de garantía y protección, tanto a nivel estatal como europeo» (Rebollo Delgado y Serrano Pérez, 2008, p. 102). Esas caracterísiticas hacen de él un derecho especialmente adecuado para operar en la esfera digital, sin que, por ello, deje de ser aplicable a los tratamientos no automatizados de datos.

[33] No niego con ello que, con el tiempo, la igualdad y la garantía de los derechos pudieran permitir «la formación de las identidades colectivas» más allá de la esfera nacional (Ferrajoli, 2006, p. 125), solo constato las dificultades de configurar ese sustrato común. Complejidades que, en todo caso, no dejan de ser una versión 2.0 de los desafíos de la globalización. Como, con precisión y acierto, advierte Ruipérez, la construcción de esa nueva Arcadia entraña un riesgo real para la libertad de la ciudadanía. Frente a ellos, los fundamentos del Estado constitucional y democrático se presentan como la respuesta más eficaz (Ruipérez, 2005, pp. 173-186 y 207-208), ¿acaso la única posible?.

Los datos son el sustrato que alimenta la vida en la red. Si bien no toda la información que mueve los complejos engranajes de la era digital tiene carácter personal, en el sentido de información relativa a personas físicas concretas –hay datos anonimizados, datos referidos a personas jurídicas o datos sobre consumos de materias primas cuyo valor e importancia es ciertamente relevante–, lo cierto es que la información personal es parte imprescindible del modelo de sociedad que el desarrollo tecnológico propicia.

La existencia de un derecho que posibilita gobernar lo personal, al asegurar un ámbito de actuación a los ciudadanos frente al tratamiento de sus informaciones personales es imprescindible. La transcendencia de su cometido y su valor referencial son las razones que me han llevado recorrerlo, aunque mi interés se haya centrado en las relaciones existentes entre el concepto de dato y las categorías especiales como test de evaluación de la adecuación del modelo europeo de protección de datos para afrontar los desafíos de las era digital.

CAPÍTULO II. LA PROTECCIÓN DE LA SUBJETIVIDAD: LO RESERVADO. LO CONTROLADO

«*Lo pasado no alumbra el porvenir, y el espíritu marcha en las tinieblas*»
Alexis de Tocqueville[1]

1. La importancia de los orígenes y el camino recorrido

En una materia presidida por la innovación y acuciada por un futuro lleno de desafíos, mirar al pasado puede parecer más una exigencia académica que una necesidad real. Sin embargo, cuando el camino no es claro y las decisiones se ocultan tras un velo de incertidumbre, volver la vista atrás y aprender de las experiencias que nos han traído hasta el presente puede ser una buena decisión.

Desconocemos las tecnologías que pueden llegar y los riesgos a que conducirán, pero podemos aprender de las respuestas que otros dieron ante innovaciones pretéritas. Ciertamente, los grandes ingenios tecnológicos del ayer –la fotografía, el telégrafo o el teléfono– palidecen frente a la ubicuidad de Internet o las potencialidades que alberga la inteligencia artificial. Pero, en su momento, esas invenciones fueron tan disruptivas como las que hoy nos desvelan, aunque, quizá, fuesen menos incisivas. Contamos con un amplio arsenal de respuestas y aprendizajes que conviene no olvidar.

Ante las injerencias que determinados usos de las tecnologías suponen para los derechos y libertades fundamentales e, incluso, para la democracia y el estado de derecho bueno es responder aprovechando el ayer y procurando nuevas funcionalidades para las soluciones jurídicas de contención que ya hemos construido.

En las próximas páginas, se realizará un somero recorrido por los más de 130 años transcurridos desde las primeras caracterizaciones y regulaciones de lo que hoy conocemos como derecho a la protección de datos personales. Podremos comprobar cómo, a través del Derecho, se han ido articulando una suma de remedios y garantías orientadas a asegurar, la

[1] En (de Tocqueville, s. f.).

subjetividad, seguridad e individualidad de las personas en ese cambiante contexto.

2. El dominio de la subjetividad y su huella

Los datos personales, al igual que el resto de tipologías de la información, se han utilizado desde hace siglos, incluso, milenios[2]. Siempre han sido un bien preciado y protegido (Casado Robledo, 2020). Su utilización (en la política, en la religión, en la medicina, en la abogacía o en cualquier otro ámbito) ha sido –es– necesaria para la consecución de determinados fines: desde la gestión de cuestiones de interés general (v. gr. información tributaria, seguridad pública) hasta para beneficio de la persona a la que están referidos (v. gr. salud), pasando por usos de dudosa virtuosidad y merecido reproche (v. gr. espionaje o chantaje) u otros aparentemente más prosaicos, aunque sean los más comunes, como es el caso de la publicidad comercial.

Hasta la irrupción del tratamiento automático de la información, la protección de los derechos afectados por la utilización de esos datos se canalizó a través de normativas específicas, sectoriales, destinadas a regular la confidencialidad en sus respectivos ámbitos[3]. El fundamento de esta reserva, desde un punto de vista jurídico[4], encuentra su engarce en la protección de los bienes de la personalidad: la dignidad, el honor, la salud

[2] Los tratados médicos que conforman el *Corpus Hippocraticum* se enmarcan en un período de unos 70 años, entre finales del siglo V y mediados del siglo IV a.C. (420 y el 350 a.C.). Entre las contribuciones que en ellos se realizan se cuenta el desarrollo de la historia clínica o la exigencia de guardar secreto de lo que se ve y escucha del paciente, durante el ejercicio de la medicina. Sobre esta cuestión vid. (Domínguez, 1996), (Martínez Saura, 1996). Sobre el secreto profesional de abogados, procuradores y escribanos, constan referencias en el *Corpus Iuris* Civilis, Digesto (Ley 25 de Test. XXII, V); sobre esta cuestión, así como la extensión de dicho secreto a los notarios, vid. (Vidal Domínguez, 2002).

[3] La confidencialidad médico-paciente (Suárez Rubio, 2015, pp. 151-169), el secreto profesional del abogado o el secreto de confesión, son ejemplo de la atención particularizada y el valor específico del deber de secreto en esos contextos.

[4] Desde una perspectiva extrajurídica, no puede obviarse la importancia que el asegurar un espacio de confidencialidad y confianza reviste para el éxito de las relaciones interpersonales en dichos sectores. De no tener la certeza de que lo revelado al médico permanecerá en secreto, una parte de las personas renunciarían a consultar ciertas enfermedades. Así lo ha apuntado el TEDH, en Z c. Finlandia, cuando señala «*It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general*», Z c. Finlandia, de 25 de febrero de 1997, apdo. 95. Del mismo modo, ¿quién se fiaría de un abogado que divulga los pormenores del caso que le ha llegado esa mañana? O, en la esfera religiosa, ¿cuánto se reduciría el número de personas dispuestas a confesarse si no tuviesen la garantía del secreto de confesión?

y en otros intereses generales, como la libertad de información[5] o la protección de la vida privada[6].

3. El origen remoto: La *privacy* estadounidense

La búsqueda de una salvaguarda frente a la intromisión en la esfera reservada de la persona tuvo como respuesta jurídica, en los Estados Unidos de América, la conceptualización de la *privacy*. Fue la réplica dogmática a los riesgos que representaban la generalización de las innovaciones técnicas para los bienes jurídicos de las personas.

Como Habermas ha puesto de manifiesto[7], la separación entre lo público y lo privado que se consolidó al calor de las modificaciones en las dinámicas sociales generadas por la revolución liberal y la aparición de las primeras formas de constitucionalismo de base popular, está variando. En las últimas décadas, el modelo de sociedad tiende hacia el «ensamblamiento de [la] esfera pública y [el] ámbito privado» (Habermas, 1981, p. 172).

El origen de la *privacy* es una referencia indispensable en el estudio del derecho a la protección de datos personales. Por ser su antecedente, pero también porque, en ocasiones, recaen sobre el mismo objeto. El nacimiento y consolidación del derecho a la protección de datos se explica, en buena medida, como la búsqueda de un status propio y diferenciado del que corresponde a los derechos a la vida privada y a la intimidad, que son el contenido primero de la *privacy*. Hoy, la *privacy*, en su conceptualización estadounidense, es un «*sweeping concept*» (Solove, 2002, p. 1088). Abarca una pléyade de realidades jurídico-normativas[8] –incluida la protección frente al tratamiento de datos personales– que, sin embargo, tienen como

[5] Como el deber de secreto del periodista, que tiene entre sus finalidades asegurar la libertad de información (Carrillo, 1993, pp. 175-181).

[6] Entendida la vida privada, en este contexto, en un sentido amplio, abarcando no solo la intimidad personal sino, también, la familiar o el secreto de las comunicaciones.

[7] La aproximación de Habermas a la conformación de la esfera privada parte del papel desempeñado por la conformación de la opinión pública –y la publicada–. No obstante, resulta plenamente aplicable a este ámbito, al describir, de manera muy atinada, las interrelaciones entre lo reservado, lo público y lo privado que es de interés o conocimiento público (Habermas, 1981).

[8] Abarca desde la libertad de pensamiento al control sobre el propio cuerpo, pasando por la inviolabilidad del domicilio, la reputación o la protección frente a registros e interceptación de comunicaciones. Es decir, hay en ella una profunda conexión con la realización y no condicionalidad del individuo.

nexo común, que son «*a form of protection against certain harmful or problematic activities* […] *caused not by technology alone, but primarily through activitities of people, businesses, and the government*» (Solove, 2006, pp. 559-560).

La fundamentación doctrinal que situó a la *privacy*[9] como un bien acreedor de una defensa jurídica singularizada, en tanto que proyección del ser, es obra Samuel D. Warren y Louis D. Brandeis[10]. Se hacía necesario «*to protect the privacy of private life*» (Warren y Brandeis, 1890, p. 215) ante la curiosidad ajena. Sin embargo, la *privacy* no encontraba, entre las instituciones y remedios que, en ese momento, ofrecía el *Common Law*[11] –vinculados, fundamentalmente, al derecho de propiedad– una protección jurídica mínimamente satisfactoria.

La solución propuesta por Warren y Brandeis pasaba por trasladar «la tutela del derecho a la intimidad desde el plano de la propiedad al ámbito del derecho a la personalidad […] [,] [definiendo a esta] como un derecho de contenido amplio, ajustado a las repercusiones que en la vida privada podía plantear un nuevo ingenio tecnológico, la fotografía» (Martínez Martínez, 2004, pp. 71-73). En efecto, fue la capacidad de las «*instantaneous photographs and [the] newspaper enterprise [to invade] […] the sacred precincts of private and domestic life*» (Warren y Brandeis, 1890, p. 195) lo que, en gran medida, impulsó a los autores[12] a cuestionarse las respuestas con las que contaba el ordenamiento jurídico estadounidense para afrontar ese nuevo desafío.

---

[9] Cuya traducción más ajustada a los conceptos europeos, al menos para representar el bien jurídico que, en ese momento, los dos abogados de Boston están formulando, sería el derecho a la intimidad. Así lo entendieron también PENDÁS y BASELGA, en la traducción que realizaron del ensayo de Warren y Brandeis, donde prescinden, «con gusto», del término privacidad, (Pendás y Baselga, 1995, p. 11).

[10] «*The Right to Privacy*» (Warren y Brandeis, 1890) es, «*perhaps* [,] *the most famous and certainly the most influential law review article ever written*» (Nimmer, 1954, p. 203). Al tratarse de una referencia obligada, son innumerables los trabajos que analizan este artículo, no obstante, por su grado de detalle, vid. (Richards, 2010, pp. 1296-1310).

[11] Descartan, por insuficiente e inadecuada, la ley de calumnias y difamación (Warren y Brandeis, 1890, pp. 197-198); tampoco el derecho a la propiedad intelectual y artística se adapta a la realidad que pretenden proteger (Warren y Brandeis, 1890, pp. 198-199).

[12] Prosser apunta a la intromisión de la prensa en la boda de hija de Samuel Warren, «*the face that launched a thousand lawsuits*» (Prosser, 1960, p. 423), como uno de los detonantes para la redacción del artículo. No parece que esta fuera la causa, pues, como apunta Gormley, en 1890 la hija de Warren tenía solamente seis años (Gormley, 1992, p.1349). Para un análisis más detallado del contexto y posibles motivaciones personales que pudieron impulsar a Warren y Brandeis a escribir su famosa obra, vid. (Glancy, 1979, pp. 5-7) y (Saldaña, 2012, pp. 209-211).

La ausencia de una cobertura jurídica apropiada, les llevó a configurar «*a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds*» (Warren y Brandeis, 1890, p. 206). No se agotó ahí la aportación de estos abogados de Boston. En su ensayo también apuntaron los límites y contornos del derecho a la *privacy*[13], así como los posibles remedios frente a eventuales afectaciones de la misma[14].

La relevante aportación doctrinal diseñada por Warren y Brandeis no tuvo una traslación fácil, ni rápida, a la práctica jurídica estadounidense, aun cuando, a principios del siglo XX (1903), el estado de Nueva York se dotó de una ley, la primera, sobre *privacy*[15]. A pesar de este y otros referentes[16], transcurrieron décadas hasta que el Tribunal Supremo de los Estados Unidos reconoció el engarce constitucional del derecho a la *privacy,* deslindándolo definitivamente[17] del derecho de propiedad[18].

---

[13] Este no permitiría prohibir la publicación de informaciones de interés público, ni impedir comunicaciones. La mera comunicación oral, sin daños relevantes, no supondría una vulneración del derecho a la *privacy*, su protección no operaría en los casos en que la persona hubiese consentido la publicación de la información o ella misma la hubiese hecho pública. Tampoco cabría prohibir una publicación si no hay «*malice*» por parte del editor, o la información revelada es una verdad que no ofrezca discusión (Warren y Brandeis, 1890, pp. 214-219).

[14] Una reparación por daños y perjuicios y, en determinados supuestos, actuaciones judiciales específicas. Por otra parte, descartan, en ese momento, la posibilidad de emprender actuaciones penales, por ser necesario desarrollo legal, aunque las consideran deseables (Warren y Brandeis, 1890, pp. 219-220).

[15] *New York Laws ch*. 132, §§ 1-2, 1903. En ella se prohibía el uso, sin su consentimiento, del nombre o la imagen de una persona para realizar anuncios. Sobre el contexto y decisiones judiciales que llevaron a elaborar el primer estatuto sobre *privacy*, vid. (Rosenthal y Werbin, 2018). En la actualidad, con las modificaciones lógicas derivadas de la evolución normativa, se corresponde con las secciones §§ 50-51 de la *New York Civil Rights Law*.

[16] Especialmente significativo, por pionero, es el pronunciamiento de la Corte Suprema de Georgia en el caso Pavesich v. New England Life Ins. Co. - 122 Ga. 190, 50 S.E. 68 (1905), en él se reconoce la «*privacy as a specific, remediable common-law right*» (Kent Jr., 2009, p. 3).

[17] Debe consignarse que, en relación con determinados supuestos, elaboró construcciones que irían añadiendo matices y esferas de actuación a la *privacy*. Pero no la presenta «como algo nuevo que conduce a una categoría autónoma, sino como corolario de los contenidos recogidos en el texto fundamental» (Lucas Murillo de la Cueva, 1990, p. 62). No obstante, algunos pronunciamientos no dejan de tener cierto interés e importancia, como son los referidos a cuestiones relativas a normativas antirruidos (Kovacs v. Cooper, 336 US 77 (1949)) o la *privacy* en la esfera conyugal, configurada a partir de la prohibición de la venta, distribución y utilización de anticonceptivos (Griswold v. Connecticut, 381 US 479 (1965)). Para un estudio detallado sobre la jurisprudencia del Tribunal Supremo estadounidense en relación con estos temas y los matices que el derecho a la *privacy* fue adoptando, vid. (Martínez Martínez, 2004, pp. 105-111 y 129-133).

[18] Warden v. Hayden, 387 US 294 (1967) y Katz v. United States, 389 US 347 (1967). Esta última es especialmente relevante por dos razones. En primer lugar, por introducir el test

El pronunciamiento que provocó el anquilosamiento de la jurisprudencia sobre la *privacy* fue el caso Olmstead v. United States[19]. En él, la discusión giraba en torno a si la intervención de los cables de teléfono para realizar las escuchas, que llevaron al procesamiento de setenta y cinco personas por conspiración al violar la *National Prohition Act* (entre ellas al propio Olmstead), suponía una violación de la Cuarta Enmienda[20] (que asegura el derecho de los ciudadanos frente a violaciones de su persona, domicilio, papeles y efectos), así como, si resultaba de aplicación la Quinta Enmienda[21] (prohibición de obligar a alguien a declarar contra sí mismo).

La posición mayoritaria de los integrantes del Tribunal Supremo de la época, favorables a una interpretación literal y originalista de la Constitución estadounidense (VV.AA, 2005, pp. 199-220), resultaron un obstáculo insalvable para el reconocimiento constitucional del derecho a la *privacy*. La resolución del Tribunal Supremo[22], por un ajustado 5-4, abogó por una interpretación literal de la Cuarta Enmienda, conforme a la cual, las comunicaciones telefónicas no estaban incluidas en su esfera de protección. Se descartaba, así, cualquier tipo de analogía con otras formas de comunicación que sí disfrutaban de protección constitucional, como ocurría con el servicio postal. La única vía que el Tribunal Supremo dejó abierta para salvaguardar el secreto de las comunicaciones telefónicas fue

---

acerca de las expectativas razonables de privacidad; sobre la problemática derivada de este concepto, vid. (Kerr, 2007, p. 504-505) o (Mund, 2018). En segundo lugar, por confirmar, definitivamente, que se produce un *overruled* del caso Olmstead v. United States, 277 U.S. 438 (1928), «*We conclude that the underpinnings of Olmstead* [*and similar cases*] *have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy on which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment*», en Katz v. United States, 389 US 353.

[19] Olmstead v. United States, 277 U.S. 438 (1928).

[20] Cuarta Enmienda de la Constitución de los Estados Unidos: «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*».

[21] Quinta Enmienda de la Constitución de los Estados Unidos: «*No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation*».

[22] Para un análisis crítico de la sentencia, vid. (Black, 1930).

la legislativa[23]. La vía judicial quedaba vedada, pues sería atribuirle a la Cuarta Enmienda «*an enlarged and unusual meaning*»[24].

Frente al formalismo de la posición mayoritaria[25], Brandeis[26] apostaba por una interpretación flexible de la Cuarta Enmienda, que permitiese «*to protect Americans in their beliefs, their thoughts, their emotions, and their sensations* […] [and assure them] *the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth*»[27].

Brandeis configura la *privacy*, el *right to be let alone*, como un derecho de protección frente a la capacidad de intrusión del gobierno en la esfera más reservada de las personas, que identificaba con sus pensamientos y emociones. El derecho a la *privacy* se erige en una garantía de la libertad y autonomía de los individuos frente a las eventuales injerencias provenientes del poder público. La interpretación extensiva de la Cuarta Enmienda se presentaría como el mecanismo más adecuado para lograr la protección de ese ámbito reservado frente a los descubrimientos, los existentes entonces y los que pudiesen producirse en el futuro, que permitiesen al Gobierno «*to obtain disclosure in court of what is whispered in the closet*»[28]. Esta formulación de la privacy, entendida como «*"intellectual privacy"* […] *holds the potential to help us better understand and resolve some of the most important issues of the Information Age*» (Richards, 2010, p. 1343).

---

[23] «*Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials by direct legislation*», Olmstead v. United States, 277 U.S. 465.

[24] Olmstead v. United States, 277 U.S. 466.

[25] Sobre las líneas interpretativas seguidas por el Tribunal Supremo, vid. (B. Schwartz, 1993), especialmente útil para la comprensión del contexto histórico de la sentencia resulta el análisis del período de White y Taft (1910-1930), pp. 203 a 224. Entre los *dissent* formulados, además del de Brandeis, se cuentan los de los jueces Butler, Stone y Holmes. Este último, conocido por como "*The Great Dissenter*", en su voto discrepante y, a la vez, esencialmente coincidente con el del juez Brandeis, en la importancia de que el Gobierno no se valga del delito para la obtención de pruebas, pareciéndole preferible «que algunos criminales escapen a que el Gobierno juego un papel innoble» (Arjona Sebastià, 2006, p. 230).

[26] El co-autor de *The Right to Privacy* fue juez del Tribunal Supremo desde 1916 hasta 1939.

[27] Olmstead v. United States, 277 U.S. 478.

[28] *Ibidem*, 473.

El voto particular de Brandeis[29] es una muestra más del acierto del aforismo «la minoría de hoy puede convertirse en la mayoría del mañana» (Häberle, 2001, p. 180). Lo que en su día fue *dissent*, hoy es criterio interpretativo y argumento de autoridad del Tribunal Supremo: «*as Justice Brandeis explained in his famous dissent, the Court is obligated—as "*[*s*]*ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections*»[30].

4. La protección de la esfera privada en la Europa pre-informática

En Europa, la protección de la intimidad y la vida privada se canalizó a través del derecho privado y la doctrina de los derechos de la personalidad[31], teniendo una recepción constitucional muy tardía. Los textos constitucionales posteriores a la Segunda Guerra Mundial no reconocen, de manera expresa, un derecho a la intimidad o la vida privada. No lo hace la constitución italiana (1947), ni la alemana (1949), ni el preámbulo de la constitución francesa de 1946 (que mantendría la de 1958). No obstante, ello no fue óbice para que otorgasen protección a los individuos frente a las injerencias en su esfera íntima.

En Italia, se reconoció la protección de aspectos específicos del ámbito privado, como la inviolabilidad del domicilio (artículo 14) o el secreto de la correspondencia (artículo 15). Solo doctrinalmente se ha acogido una noción de *privacy*, hasta cierto punto, coincidente a la estadounidense, pero con ciertas particularidades derivadas del reconocimiento de un núcleo más reservado: la *riservatezza*[32].

Alemania comparte ciertas notas comunes con Italia, aunque difiere en otras. De una parte, incluye tanto el derecho al secreto de las comunicaciones (art. 10) como la inviolabilidad del domicilio (art. 13), aunque la falta de sistematicidad podría apuntar a «la inexistencia de la

[29] Su importancia no se reduce a la conceptualización de la *privacy*, sino que realiza otras aportaciones reseñables, singularmente, en lo relativo al rol que el Gobierno debe desempeñar como ejemplo y guía para la sociedad como «*the omnipresent teacher*», Olmstead v. United States, 277 U.S. 484. Un estudio detallado sobre esta cuestión es el realizado por (Steiker, 2009).

[30] Carpenter v. United States, 585 U.S. (2018).

[31] (Lucas Murillo de la Cueva, 1990, pp. 69-71) y (Pascual Huerta, 2016, pp. 118-127).

[32] Para un análisis amplio sobre la evolución de la *privacy* y la *riservatezza* en Italia, *vid*. (Niger, 2006).

conciencia en los constituyentes de una raíz común de esos derechos» (Ruiz Miguel, 1995, p. 61).

En Francia, la ausencia de reconocimiento constitucional no impidió su protección legal, especialmente mediante la legislación civil[33]. Las constituciones portuguesa[34] y española[35] (1976 y 1978) serían las primeras en consagrar la protección de la intimidad y la vida privada.

Ahora bien, los primeros textos legales en incluir estos derechos tuvieron un marcado acento internacional: la Declaración Universal de Derechos Humanos de 1948 (DUDH) (art.12), el Convenio Europeo de Derechos Humanos de 1950 (CEDH) (art. 8) o el Pacto Internacional de Derecho Civiles y Políticos de 1966 (art. 17). De los tratados internacionales mencionados, destaca el CEDH que, merced a la labor interpretativa –y el carácter vinculante– de la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) (Saiz Arnaiz, 2004), ha operado como fuerza «armonizadora de los derechos fundamentales en el ámbito europeo» (Queralt Jiménez, 2007, p. 436)[36].

El CEDH, en una línea similar a la del artículo 12 de la DUDH[37], establece, en su artículo 8, que:

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

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea

---

[33] En lo referente al caso francés, su evolución, consagración y desafíos en la era digital, vid. (H. Alcaraz, 2007).

[34] Artículo 26.1 de la constitución portuguesa de 1976. «*A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação*». Sobre la protección de la vida privada en la Constitución portuguesa, vid. (Mota Pinto y Reis, 2006).

[35] Artículo 18 de la constitución española de 1978. La bibliografía es amplísima, pueden mencionarse, sin ánimo exhaustivo, (Herrero-Tejedor Algar, 1990); (Martínez de Pisón Cavero, 1992); (Ruiz Miguel, 1995); (Romero Coloma, 2001) o (Rebollo Delgado, 2005).

[36] El propio TEDH lo apunta en la STEDH, Irlanda c. Reino Unido, de 18 de enero de 1978, apdo. 154. En dicho pronunciamiento, señala que sus resoluciones no se agotan en la solución del caso concreto, sino que sirven, también para «*clarifier, sauvegarder et développer les normes de la Convention et à contribuer de la sorte au respect, par les Etats, des engagements qu'ils ont assumés en leur qualité de Parties contractantes*».

[37] Art. 12 DUDH: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

El objeto de este precepto es, esencialmente, «proteger al individuo frente a las injerencias arbitrarias de los poderes públicos en su vida privada o familiar»[38], lo que le convierte en un derecho eminentemente defensivo. No obstante, cuenta con una vertiente positiva, materializada en el deber de los Estados de «*to take the action required of it to secure the individual's right to respect for his private sphere*» (Connelly, 1986, p. 572).

En la práctica, el TEDH «ha renunciado a realizar una definición exhaustiva y cerrada del concepto "vida privada" y ha incluido en su contenido garantías de la "autonomía personal" en sentido amplio»[39], permitiendo, de este modo, que el artículo 8 sea «susceptible de proteger al individuo frente a amenazas atípicas y novedosas […] siempre que las condiciones de la vida social lo hagan necesario» (Arzoz Santisteban, 2015, p. 344).

Como puede constatarse, el panorama de la protección de la esfera privada en Europa, con anterioridad a la emergencia de la informática, era heterogéneo, con diversos enfoques y modos de afrontar la salvaguarda de dichos bienes jurídicos. Siendo el CEDH, y la jurisprudencia del TEDH[40], interpretación extensiva incluida[41], el elemento homogeneizador y vertebrador.

Las bases dogmáticas y jurídicas de la *privacy* estadounidense y del derecho a la vida privada[42] constituyen el sustrato perfecto para la germinación del derecho a la protección de datos. Su génisis y

[38] STEDH, asunto relativo a ciertos aspectos del régimen lingüístico en Bélgica, de 23 de julio de 1968, Fundamento de Derecho I.B.7.

[39] (Santolaya, 2014, p. 430). Vid. con, SSTEDH, Peck c. Reino Unido, de 28 de enero de 2003, apdo. 57 o Sidabras y Džiautas c. Lituania, de 27 de julio de 2004, apdo. 43.

[40] Ruiz Miguel realiza un análisis de las primeras sentencias del TEDH respecto del artículo 8, y como fue conformando su contenido caso a caso en (Ruiz Miguel, 1994). A veces, esa apertura puede resultar excesiva pues el TEDH ha declarado que los malos olores próximos a un domicilio y la inactividad del gobierno local vulneraban la intimidad de sus residentes. Vid la STEDH, López Ostra c. España, de 9 de diciembre de1994.

[41] Interpretación extensiva que tiene como finalidad «*to encompass notions of personal integrity and the free development of the personality*». En la misma línea, STEDH, Karakó c. Hungría, de 28 de abril de 2009, apdo. 21.

[42] Se ha optado por el término vida privada por ser el que mejor aglutina la diversidad de conceptualizaciones existentes en el panorama europeo previo a la automatización de los tratamientos de información.

consolidación habrían sido mucho más tortuosas sin ese inmenso bagaje doctrinal y jurisprudencial.

5. La era digital y la multiplicación del riesgo en el tratamiento de la información

5.1. Nuevas tecnologías, nuevos desafíos. De las fichas perforadas a la computación cuántica

El mismo año que Warren y Brandeis publicaban *The right to privacy*, la máquina tabuladora de Herman Hollerith[43] era seleccionada por el Gobierno de Estados Unidos para elaborar el censo. Esta máquina realizó en menos de tres años el censo de 63 millones de ciudadanos estadounidenses, acortando en dos terceras partes el tiempo que había tomado realizar el censo anterior, de una población inferior en número, (50 millones de habitantes) (da Costa Carballo, 1998, p. 246). El tratamiento automatizado de la información (la informática) daba sus primeros pasos.

La siguiente fase en la evolución de la informática vendría marcada por las aportaciones de Alan Turing y su formulación teórica acerca de las características que ha de tener una máquina automática de computación[44]. La primera plasmación material de los postulados de Turing sería el Z3, de Konrad Zuse (1941), el primer ordenador programable[45]. Unos años después, en 1944, IBM desarrolló, para la Universidad de Harvard, el Mark I, un sistema que utilizaba tarjetas perforadas, pero con una notable capacidad de cálculo. También de 1944 es el sistema *Colossus* del ejército británico, diseñado, específicamente, para descifrar los patrones de los engranajes que empleaban las máquinas de cifrado nazis durante la Segunda Guerra Mundial[46].

La incorporación de la electrónica a los sistemas de computación daría un nuevo impulso a la informática. ENIAC (*Electronic Numerical Integrator and Computer*) es el nombre que recibiría el primer ordenador electrónico de la historia (1946), fabricado por John Presper Eckert y John

[43] Herman Hollerith es uno de los padres de la computación automatizada, creó el primer sistema de tabulación mediante tarjetas perforadas, así como la primera llave perforadora. Vid. (Kistermann, 1991).
[44] Para una ampliación, vid. (Turing, 1937).
[45] Sobre las aportaciones de Zuse, y el desarrollo del Z3 (y sus predecesores), vid. (Rojas, 1997).
[46] Sobre el *Colossus*, su papel y su destino, vid. (Copeland, 2006).

William Mauchly, su programación corrió a cargo de Betty Snyder Holberton, Jean Jennings Bartik, Kathleen McNulty Mauchly Antonelli, Marlyn Wescoff Meltzer, Ruth Lichterman Teitelbaum y Frances Bilas Spence[47]. ENIAC suponía la aplicación práctica, y completa, de la teoría de Turing. Podía realizar en horas cálculos que a la Mark I le tomarían semanas, además de era reprogramable (Goldstine y Goldstine, 1946).

El proceso evolutivo de la informática demandaba hacerla accesible y manejable. La creación del ordenador personal fue el camino hacia su popularización. La Programma 101, de Olivetti, fue el primer ordenador de escritorio[48]. A partir de este punto, la evolución ha sido meteórica. En 1976, Steve Wozniak y Steve Jobs fabricaban el Apple I, el primer producto de la compañía Apple. En 1981, llegaría al mercado el IBM-PC. La década de los ochenta sería escenario de mejoras constantes en los dispositivos, cada vez más pequeños y asequibles.

En los noventa se produce la innovación que lo cambia todo y sobre la que se asientan gran parte de los desarrollos, tecnologías y servicios actuales: la World Wide Web (WWW)[49]. En realidad, su elemento básico, la conexión en red de ordenadores, lo que generalmente se conoce como Internet, es muy anterior a los noventa. En 1969, ARPANET (*Advanced Research Projects Agency Network*)[50] estableció su primer nodo en la Universidad de California en Los Ángeles (UCLA) y operó como precedente y referente de la Red de redes, de la WWW.

El hecho diferencial, lo que convierte a la WWW en el punto de inflexión y detonante del siguiente paso evolutivo en el desarrollo tecnológico es, precisamente, su alcance global. Internet es la piedra angular de la era digital, conforma un mundo paralelo, virtual, un cosmos nuevo, distinto; una realidad alternativa, pero muy real –las consecuencias de lo que acontece en la esfera virtual se proyectan sobre la realidad *offline*-–. Un mundo digital al que las personas dan vida y alimentan con su

[47] Estas seis mujeres fueron cruciales en el éxito de ENIAC, vid. (Fritz, 1996).
[48] En la prácticas se asemejaba más a lo que hoy sería una calculadora, aunque era posible imprimir las operaciones y cálculos con ella realizados. Para conocer la historia de la Programma 101, quien mejor que su diseñador, vid. (Perotto, 1995).
[49] Sobre los orígenes de Internet, en general, y de la World Wide Web en particular, nadie más apropiado que el creador de esta última, Tim Berners-Lee, vid. (Berners-Lee, 2000).
[50] Sobre ARPANET, vid. (Hauben, 2017), sobre la historia de Internet, vid. (Trigo Aranda, 2004).

información e interacción constante, especialmente desde que, merced a los *smartphones*, la Red está al alcance de nuestra mano[51].

El desarrollo tecnológico de la informática no se ha detenido, sigue evolucionando. Además de la combinación de mejoras técnicas e internet (clave en tecnologías como el Internet de las cosas), también se ha seguido profundizando en la obtención de procesadores capaces de realizar cálculos más complejos, de solventar problemas no resueltos. La computación cuántica se muestra como la línea de trabajo más proteica y avanzada en la consecución de tales objetivos. Su evolución, y eventual generalización, será, seguramente, una de esas fronteras que la informática pronto superará[52]. Con ella vendrán nuevos retos, especialmente en materia de seguridad de la información, al ser capaz de descifrar en minutos, cuando no en segundos, códigos que hoy se tardaría siglos (o milenios) en quebrar. Los mecanismos que hoy garantizan la seguridad de la información penden de un hilo, pronto habrán de ser actualizados si se pretende que lo que hoy es seguro lo siga siendo en el futuro.

5.2. Los Warren y Brandeis de la década de los 60

La fotografía y la naciente telefonía sirvieron de acicate a Warren y Brandeis para sentar las bases doctrinales de la *privacy*. Quizás motivados por la emergente automatización del tratamiento de la información, un buen puñado de autores trataron, durante la década de los sesenta, de definir, redefinir y delimitar en qué consistía la *privacy*, y determinar cuál era su contenido. El reto era, y sigue siendo, mayúsculo, pues la *privacy* es «*difficult to define because it is exasperatingly vague and evanescent*»

[51] A Steve Jobs y su Iphone se debe la revolución que supuso la conversión de los teléfonos móviles en un multiusos inteligente. El correo electrónico, la agenda, el entretenimiento, las tiendas de productos online, con el tiempo, las capacidades de un ordenador, todo en un solo dispositivo de bolsillo. El consumo de datos móviles no se entendería sin él y, a partir de él, el flujo de información se convirtió en un torrente imparable. Se puede consultar una evolución histórica del consumo diario de Internet en España, desde el año 2000 hasta 2019, en:
https://es.statista.com/estadisticas/508058/tiempo-medio-diario-destinado-a-navegar-por-Internet-en-espana/. (Última consulta: 20/10/2021).

[52] La diferencia entre la computación binaria y la cuántica sería que, mientras «en n la computación clásica, el almacenamiento y procesamiento de información está basado en bits, conocidos por todos, que tienen un valor binario, discreto y determinista; sin embargo, la computación cuántica trata la información mediante *qubits*, capaces de mantener dos estados simultáneamente con una cierta probabilidad. En consecuencia, se pueden procesar ambos estados a la vez, reduciendo enormemente el tiempo de procesamiento» (García González, 2020, p. 635).

(Miller, 1971, p. 25). Las aportaciones de Prosser, Bloustein, Freid, Wetin o Miller han contribuido a dotar de cierta nitidez al concepto, amén de aportar elementos que ayudarían a conformar el derecho, incluidas ciertas aportaciones que, directamente, atañen a la protección frente al tratamiento automatizado de los datos personales.

A Prosser se debe la reapertura del debate. En su artículo, «*Privacy»,* plantea cuatro formas posibles de inmiscuirse en ella: «1. *Intrusion […] into his private affairs*. 2. *Public disclosure of embarrassing private facts* […]. 3. *Publicity which places the plaintiff in a false light in the public eye*. 4. *Appropriation, for the defendant's advantage, of the plaintiff's name or likeness*» (Prosser, 1960, pp. 389). Se estaría, por tanto, ante un derecho con, al menos, cuatro dimensiones o ámbitos necesitados de protección. Ahora bien, como advirtió Bloustein, Prosser, no realiza aportaciones significativas en lo referente al derecho a la protección de datos, ni tampoco respecto de los riesgos derivados del tratamiento automatizado de la información, pues no toma en consideración las «*new and frightening invasions of privacy*» (Bloustein, 1964, p. 963) derivadas de los avances tecnológicos.

Para Bloustein, la injerencia en la *privacy* tiene un único resultado (en lugar de los cuatro de Prosser), la ofensa de «*our concept of individualism and the liberty it entails, so too should we regard privacy as a dignitary tort*» (Bloustein, 1964, p. 1002). Para él, la *privacy* estaría conectada íntimamente con la dignidad, que sería el bien realmente afectado. Además, al considerar la facultad de aislarse como una manifestación de la libertad individual, deja expedita la vía que Fried y Westin transitarán.

Fried plantea, sin ambages, una naturaleza dual de la *privacy*. La entiende, de una parte, como «*the control we have over information about ourselves*» (Fried, 1968, p. 482) y, de otra, como un instituto de garantía de la libertad personal[53]. Westin[54], por su parte, desarrolla un concepto de *privacy* como autodeterminación, planteando «un enfoque claramente informacional de la vida privada» (Martínez Martínez, 2004, p. 81). Esta conceptualización aseguraría que, tanto los individuos, como los grupos e incluso las instituciones, pudieran «*to determine for themselves when, how, and to what extend information is communicated to others*» (Westin, 1967,

[53] «*Besides giving us control over the context in which we act, privacy has a more defensive role in protecting our liberty*» (Fried, 1968, p. 483).
[54] Vid. (Westin, 1967).

p. 7). Westin apunta, además, la necesidad de encontrar el modo de equilibrar los deseos de *privacy* y los de participar en la sociedad. En esa tarea, y después de un concienzudo estudio casuístico sobre los modos en que pueden producirse intromisiones en la vida privada, apuesta por desarrollar una normativa que limite las posibilidades de vigilancia por parte de los poderes públicos.

Miller, por su parte, se centra, exclusivamente, en los desafíos que para la *privacy* suponía el, por entonces incipiente, uso de los ordenadores y como «*its insatiable appetite for information, its image of infabillibility, and its inability to forget anything that become has been stored in it*» (Miller, 1969, p. 1092) afecta a la capacidad de los individuos para controlar los flujos de información a ellos referida. Después de analizar el marco normativo estadounidense, concluye su análisis invitando a los diferentes operadores jurídicos a «*to develop a legal framework that will secure personal privacy while permitting effective implementation of the new information technologies*» (Miller, 1969, p. 1246).

5.3. Desarrollo tecnológico y protección de los derechos y libertades

La entidad de las innovaciones tecnológicas desarrolladas a lo largo de la segunda mitad del siglo XX –y de lo que va de siglo XXI– supone un desafío cuyos extremos, aún hoy, permanecen, en muchos casos, sin resolver.

El rápido desarrollo de la informática y sus riesgos para los derechos fundamentales, especialmente para el derecho a la vida privada, están en el origen de las primeras regulaciones sobre el tratamiento de la información personal.

En las primeras fases del tratamiento automatizado de datos, el principal factor de cambio que la informatización presenta –y el principal riesgo en lo que a la protección de datos se refiere– es la ruptura de las barreras que «el tiempo y el espacio o el mismo volumen de datos disponible» (Lucas Murillo de la Cueva, 2009, p. 15) ofrecían. La posibilidad de gestionar grandes volúmenes de información, en poco tiempo y con poco esfuerzo, es la gran contribución de las tecnologías de la información y la comunicación y, también, su principal peligro.

El siguiente gran salto, seguramente el más importante, es la irrupción de Internet, de su fuerza disolvente de los espacios personales, de su capacidad para generar «la ilusión de que la comunicación […] que establecemos a través suyo […] [en] un proceso de comunicación […] libre, abierto y público» (Villaverde Menéndez, 2013, p. 59). Los múltiples estímulos, posibilidades y tentaciones que genera, provocan la reducción de las cautelas o la despreocupación por la información personal que vertemos en la Red.

Esta problemática parece estar modulándose. Existe una mayor conciencia de los peligros derivados del uso Internet, y de las diferentes aplicaciones y posibilidades que la interconexión ofrece. Así, su constante desarrollo e implantación han venido acompañados de una mayor demanda de regulación normativa capaz de hacer compatible la protección de la privacidad[55] y el aprovechamiento de las posibilidades y bondades de la Red de redes.

Consecuentemente, se ha ido produciendo una modificación en el modo de articular los sistemas de protección. Las primeras regulaciones se centraban en dar solución a un riesgo específico, en un contexto muy focalizado: los potenciales efectos perjudiciales de los tratamientos de datos por parte de los gobiernos y administraciones públicas. Esto resultaba coherente con la realidad de esos años, el precio, el consumo energético y el tamaño de los primeros ordenadores, acotaba su disponibilidad, precisamente, a los gobiernos, a grandes laboratorios y universidades y un puñado de compañías. En los últimos años, sin embargo, la protección frente al tratamiento de datos ha ganado en importancia, debido a la popularización de estos ingenios tecnológicos, merced a la reducción de costes y tamaños.

---

[55] En España, el término privacidad no cuenta con una definición legal en la actualidad. Sin embargo, no cabe duda que es el término que, en el imaginario colectivo, evoca la idea de protección de la vida privada y familiar. En este sentido, puede recurrirse, a efectos meramente descriptivos de lo que pudiera ser la privacidad, a la definición que la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal ofrecía en su exposición de motivos. Esta la concebía como «un conjunto más amplio, más global [que la intimidad] de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado».
Curiosamente, tanto la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales prescindieron de incorporar una definición de privacidad.

En efecto, la extensión de la protección jurídica a las relaciones *inter privatos* ha ido de la mano de la ruptura del "oligopolio" en el uso de estas tecnologías. La ampliación de posibilidades y oportunidades para la ciudadanía es evidente, pero suma otro factor de riesgo a los ya conocidos, pues los sujetos capaces de vulnerar derechos mediante el uso de la informática se incrementan día a día, y la información a gestionar, se multiplica exponencialmente.

Las amenazas para los derechos derivadas de la utilización de información personal no provienen, en exclusiva, de los poderes públicos. El deber de abstención y no injerencia del Estado en los derechos de los ciudadanos, que late en la base las declaraciones de derechos liberales, se amplía a otros sujetos.

El derecho a la protección de datos es un ejemplo paradigmático de «la eficacia de los derechos fundamentales frente a particulares» (Bilbao Ubillos, 1997). En efecto, al conceder un poder vinculado a una expresión material, los datos, hace que resulte indiferente quien lleve a cabo el tratamiento, pues las facultades se ejercerán allí donde se constate que se está operando con datos de carácter personal. Ello no obsta para que, en la regulación de los diferentes tratamientos, se modulen las posibilidades de actuación en atención a las circunstancias concretas de cada operación, entre las que se incluiría el sujeto responsable de la misma.

Con todo, los poderes públicos mantienen una notable capacidad de incidir en la esfera personal de los ciudadanos a partir del uso de su información personal, ya sea por motivos de seguridad, recaudación de impuestos o gestión del interés público. Las posibilidades de injerencia gubernamental, en caso de no asegurar un marco de protección adecuado, pueden desembocar en escenarios en los que la libertad y la democracia se vean severamente cercenadas (v. gr. mediante sistemas de videovigilancia con reconocimiento facial, acompañados de sistemas de puntación de buen ciudadano[56]).

[56] Un sistema de este tipo ha sido implementado en China, sobre este tema se han publicado algunas noticias en los medios. Aunque, curiosamente, no ha tenido una transcendencia excesiva en occidente, cuando es una realidad que, pese a las diferencias culturales, no resulta tan difícilmente trasladable como pudiera parecer.
https://www.eldiario.es/tecnologia/ingredientes-hipervigilancia-reconocimiento-videovigilancia-credito_1_1632716.html; https://www.lasexta.com/noticias/ciencia-tecnologia/china-implanta-un-carne-por-puntos-que-controla-todos-los-comportamientos-de-la-gente-e-instala-200-millones-de-camaras_201908045d46e0620cf2a6f6494b9243.html o

Sin embargo, no pueden obviarse las amenazas para libertad y los derechos, derivadas de la gestión de datos por parte del sector privado y de otros particulares. Articular un sistema que asegure la eficacia *erga omnes* de los derechos fundamentales en los procesos de tratamiento de la información es el objetivo esencial de las normativas de protección de datos (v. gr. art. 1.2 RGPD[57]). Estas, han de establecer las condiciones del tratamiento, así como el modo en que se han de solventar los conflictos de intereses concurrentes sobre una misma información personal.

La regulación del tratamiento de datos es poliédrica, y sumamente compleja, sin embargo, entre sus funciones se cuenta, en todo caso, la de disciplinar las obligaciones entre privados. El éxito y eficacia de estas normativas se pude medir, entre otros factores, por su capacidad para controlar el poder de los nuevos señores feudales de los que hablaba Rodotà (Rodotà, 2019, p. 61) y evitar los efectos derivados de su posición privilegiada en la sociedad de la información.

Curiosamente, frente a estos peligros, los Estados tienen una capacidad de actuación minorada, debido al volumen de las empresas y, sobre todo, al rol estratégico que sus servicios representan en el día a día de la ciudadanía, pues los productos que sitúan a las corporaciones en una posición de dominio se han convertido en piezas irremplazables en el modelo económico. Consecuentemente, los sistemas de protección han de implementar mecanismos de protección capaces de hacer compatibles los derechos de las personas con la continuidad de la actividad económica y social. La regulación del tratamiento de la información, incluida la de carácter personal, no impide operar a estas compañías, pero exige de ellas un comportamiento más respetuoso con los derechos, y proporciona a los ciudadanos mejores instrumentos para defender sus intereses.

Finalmente, debe asumirse que, inherente a todo tratamiento, como reflejo de su condición de proceso abierto e íntimamente conectado al constante desarrollo tecnológico, existe un riesgo, dinámico y en constante evolución, de vulneración de los derechos de la ciudadanía. El incremento de los peligros no tiene una única causa, sino que se debe a diversos factores, como el aumento exponencial de la capacidad de recabar y gestionar información personal o la utilización de tecnologías como el *big*

https://retina.elpais.com/retina/2018/04/25/tendencias/1524640135_207540.html. (Última consulta: 20/10/2021).

[57] Art. 1.2 RGPD: «El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales».

data o la inteligencia artificial, cada vez más precisas y capaces de inferir información personal sensible a partir de datos no sensibles, incluso de informaciones que no revisten la condición legal de dato personal (los datos anonimizados).

De esta última problemática derivan otras de igual, o mayor, transcendencia, como el peso e importancia que se concede a los resultados probabilísticos ofrecidos por esas tecnologías en la toma de decisiones (ya sea en seguros de vida, concesión de créditos o procedimientos de selección de personal), o la pérdida de transcendencia de la naturaleza de los datos tratados, merced a la posibilidad de inferir unas informaciones a partir de otras.

En los albores del derecho a la protección de datos, muchos de estos riesgos no podían preverse –la sobreexposición en la Red, la capacidad disruptiva de Internet o la transcendencia que alcanzaría el *big data* en la toma de decisiones personales–. Fueron otros peligros, como la ruptura de las barreras del tiempo y el espacio o los derivados de la recopilación, uso y procesamiento de datos por medios informáticos, los que impulsaron y motivaron las primeras normativas sobre la materia.

Proporcionar, desde lo jurídico, una respuesta eficaz a las amenazas y peligros derivados del desarrollo tecnológico, ofreciendo remedios a la preocupación social generada, es lo que está en la raíz de las demandas de un mayor control en el tratamiento y gestión de la información personal. Las bases para el surgimiento de un nuevo derecho estaban establecidas. Se hacía patente la necesidad de articular una garantía adicional, que complementase y diese mayor calado dogmático, a los sistemas de protección existentes frente a las nuevas capacidades de injerencia en la esfera personal.

6. La legislación y la jurisprudencia como factores configuradores del derecho a la protección de datos

6.1. Dos factores evolutivos: legislación y jurisprudencia

La configuración jurídica del derecho a la protección de datos personales viene marcada por una serie de fases e hitos, a veces

concurrentes[58]. Si bien resulta inviable, a los efectos de este trabajo[59], describir aquí todos y cada uno de ellos, conviene recordar aquellos que mejor reflejan su proceso evolutivo, atendiendo a su desarrollo legislativo[60] y a la jurisprudencia.

En el análisis de los precedentes legislativos que sirven de antesala al reconocimiento del derecho, sea considerado, también, el tipo de fuente normativa (leyes, constituciones o tratados internacionales), mientras que, en lo referente a la configuración jurisprudencial del derecho a la protección de datos, se toma como punto de inflexión la conocida sentencia de 1983, del Tribunal Constitucional Federal Alemán (BVG) sobre la Ley del Censo[61].

6.2. La legislación abre camino. La protección que dio fundamento al derecho

6.2.1. La Datenschutzgesetz y la Datalag

La preocupación europea por los efectos que la informatización de la vida social pudiera tener sobre los derechos de los ciudadanos se refleja,

---

[58] A la hora de establecer estas fases se ha atendido a la naturaleza de las fuentes normativas, así como al impacto en la consolidación del derecho fundamental. Tomar como referencia la conformación del derecho, y no el desarrollo legislativo, ha llevado a prescindir de otros sistemas de clasificación existentes, como las generaciones de leyes de protección de datos. Sobre las generaciones de leyes de protección de datos, HONDIUS apuntó una posible correlación entre estas y las generaciones de desarrollo de los ordenadores (Hondius, 1975, p. 18); en la misma línea apunta (Heredero Higueras, 1988a). PÉREZ LUÑO, si bien asume como coherente la existencia de una conexión entre la «evolución generacional de los avances tecnológicos […][y la] evolución también generacional de las libertades» (Pérez Luño, 2000, p. 64), no extrae de ella un correlato absoluto, sino, más bien, una relación de causa-efecto no siempre coincidente. Esta interpretación justificaría, por ejemplo, que la segunda generación de normas no tuviese como fundamento un avance tecnológico concreto, sino una concreción de los intereses en conflicto, al tratarse de leyes que tendrían como «principal objetivo […] la garantía de los datos "sensibles", por su inmediata incidencia en la privacidad o su riesgo para prácticas discriminatorias» (Pérez Luño, 2000, p. 65). En sentido parecido se pronuncia REBOLLO DELGADO, al señalar que, si bien no existe coincidencia entre «la evolución de los ordenadores […] [y] las comúnmente llamadas también generaciones en las leyes de protección de datos […] [, sí] hay en ellas una lógica dependencia, dado que hasta que no se constata la posibilidad técnica, y esta se generaliza, no surge la necesidad jurídica» (Rebollo Delgado, 2014, p. 89).

[59] Como pone de manifiesto la existencia de monografías tan buenas como la de (González Fuster, 2014); o tesis doctorales, no menos clarificadoras e ilustrativas, como la de (Pascual Huerta, 2016).

[60] En un sentido amplio, pues se incluirán desde leyes hasta previsiones constitucionales, pasando por tratados internacionales.

[61] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983- 1 BvR 209/83 -, Rn. 1-215. Puede consultarse la versión en español de la sentencia en, Boletín de Jurisprudencia Constitucional, (1984) Núm. 33, IV, Jurisprudencia Constitucional Extranjera, pp. 126-170.

de manera elocuente, en la Recomendación 509 de 31 de enero de 1968 de la Asamblea del Consejo de Europa, *Human rights and modern scientific and technological developments*[62]. En ella se adviertía acerca de «*the serious dangers for the rights of the individual inherent in certain aspects of modern scientific and technological development*»[63]. Sin embargo, la primera plasmación normativa sobre protección de datos tendrá un alcance mucho más regional: la *Datenschutzgesetz* (Ley de protección de datos) del *Land* de Hesse, de 12 de octubre de 1970[64], pionera, en muchos sentidos.

Es la primera norma que regula, de manera exclusiva[65], cuestiones que hoy son inherentes al derecho a la protección de datos, aunque tal derecho todavía no existiese como tal. Obviamente, no puede desconocerse que el ámbito de aplicación de esta ley estaba muy mediatizado por la realidad de la época, por lo que se circunscribía al tratamiento de datos por

[62] A pesar de su carácter no vinculante, constata la existencia de un caldo de cultivo previo que propiciaría la eclosión de las normativas de protección de datos que se produciría en la década de los setenta. Puede consultarse en: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en. (Última consulta: 20/10/2021).

[63] Considerando 2 de la Resolución 509/1968 de la Asamblea del Consejo de Europa relativa a Los derechos humanos y los nuevos logros científicos y técnicos.

[64] Ley de Protección de Datos del *Land* de Hesse de 1970, en vigor desde el 13 de octubre de 1970, *GVOBl*, HE I, 1970, Nr. 41 (12 de octubre de 1970), pp. 625 y ss. Puede consultarse el texto original en: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1. (Última consulta: 20/10/2021). Versión en castellano, vid. (*Informática. Leyes de Protección de Datos*, 1977, pp. 16-22).

[65] Es la primera norma en la que la protección frente al tratamiento de los datos personales se desvincula de las normativas que implementaban el proceso de automatización de la administración y los mecanismos de gestión de información, otorgándole, de este modo, un papel protagónico y no como mera cláusula general de protección de derechos frente a ese concreto proceso de informatización de las administraciones de los Lander (Hondius, 1975). Ese contexto de computarización de la gestión de la información de los Lander, sería el fundamento que, en última instancia, propiciaría la promulgación de la Ley de Renania-Palatinado de 24 de enero de 1974, *"Ley contra la utilización abusiva de los datos" Gesetz gegen mißbräuchliche Datennutzung* (Landesdatenschutzgesetz -LDatG-) *Vom* 24. *Januar* 1974, VOBl. RP, 4 de febrero de 1974, Nº. 3, pp. 31-33. Sobre el contexto en que se aprueba la Ley de Protección de Datos del *Land* de Hesse, vid. (Pascual Huerta, 2016, pp. 227-230).
Esta característica la distingue de la normativa americana sobre ficheros de solvencia. Se trata de una normativa sectorial, incorporada mediante la *Act to amend the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in United States currency be reported to the Department of the Treasury, and for other purposes*, aprobada de manera prácticamente coetánea (solo unos días después, el 26 de octubre). Además de estar circunscrita a un ámbito específico, esta previsión normativa no deja de ser una parte (Título VI) de un todo con un contenido más amplio y diverso. Puede consultarse su traducción al castellano en, (*Informática. Leyes de Protección de Datos*, 1977, pp. 105-125).

la administración pública, abarcando todas las tipologías de la información, sin distinción alguna[66].

Con todo, las aportaciones de esta norma son significativas y, muchas de ellas, perviven en la actualidad. Desde elementos definitorios de la regulación del derecho a la protección de datos, incluida su denominación, a la exigencia de implementar técnicas adecuadas para asegurar el secreto de las informaciones[67], pasando por el derecho de rectificación frente a informaciones inexactas[68] o el establecimiento de un órgano independiente encargado de velar por el cumplimiento de las previsiones de la ley[69].

Es una norma embrionaria, sí, pero en ella se encuentran las piezas esenciales que han inspirado a las futuras regulaciones sobre tratamiento de datos, fuesen o no personales. En coherencia con su naturaleza administrativa, y su función de protección de los derechos de los administrados frente a los tratamientos automatizados, la *Datenschutzgesetz* abarcaba tanto los datos de las personas físicas como los de las personas jurídicas. No anidaba en esta legislación la pretensión de desarrollar un derecho fundamental, pues se concibe como una garantía frente a la Administración.

La siguiente etapa del proceso evolutivo nos lleva a Suecia. El país nórdico promulgó, el 11 de mayo de 1973, la Ley de Datos, *Datalag*[70]. Fue la primera ley estatal sobre protección de datos[71], y la primera ley de

---

[66] Agotando, de este modo, las posibilidades legislativas que su marco competencial le permitía.

[67] Ley de Protección de Datos del *Land* de Hesse, § 3.

[68] Ibídem, § 4.1.

[69] A la configuración y funciones de este órgano dedica una parte significativa de sus previsiones, §§ 7-15 de la Ley de Protección de Datos del *Land* de Hesse.

[70] Ley de Datos, de 11 de mayo de 1973, *SFS*: 289. La versión original en sueco, así como las diferentes enmiendas que se fueron incorporando al texto hasta su derogación y reemplazo por la Ley de Datos Personales, de 29 de abril de 1998, *SFS*: 204, pueden consultarse en: https://lagen.nu/1973:289#L. (Última consulta: 20/10/2021). El texto en español de esta ley puede consultarse en, (*Informática. Leyes de Protección de Datos*, 1977, pp. 23-33). Como puede comprobarse, la ley de 1998 introduce variaciones hasta en el nombre, al adjetivarlo con la incorporación de ese "personales", que viene a remarcar la naturaleza de los datos en concurso –aunque ya la ley de 1973 estaba referida, exclusivamente, a datos de personas físicas–. Puede consultarse una traducción de la ley de 1998, en inglés, en el siguiente enlace: https://www.wipo.int/edocs/lexdocs/laws/en/se/se097en.pdf. (Última consulta: 20/10/2021). Un análisis de las modificaciones realizadas por la Ley de Datos Personales de 1998, puede consultarse en el trabajo de ÖMAN, vid. (Öman, 2004).

[71] Entre las razones que justifican que haya sido Suecia el primer país en promulgar una ley de este tenor, BURKERT, apunta el avanzado desarrollo del proceso de informatización del país, los riesgos derivados de la existencia de un número de identificación personal único al

alcance general, en el sentido de que su ámbito de aplicación no se circunscribía al sector público, sino que también abarcaba los procesos de información llevados a cabo por entidades privadas. Además, a diferencia de la *Datenschutzgesetz*, solo tenía por objeto los datos de las personas físicas (§1).

La *Datalag* configuró un sistema de protección eminentemente preventivo, en la medida en que todo tratamiento, al menos originalmente[72], requería de un registro previo ante la autoridad de datos competente (*Datainspektionen*). De manera novedosa, consideró que determinadas informaciones eran merecedoras de especial protección[73] (§4), además de reconocer un derecho de acceso (§10) e incluir un cuadro sancionador frente a eventuales incumplimientos (§20-24)[74].

6.2.2. FIPs, *Privacy Act* y la crisis de liderazgo estadounidense en materia de privacidad

En la primera mitad de la década de los setenta del pasado siglo cristalizó todo el bagaje doctrinal y jurisprudencial que se había ido generando en los Estados Unidos desde la publicación de *The right to privacy* (1890)[75].

---

que se pretendían vincular diferentes ficheros y, también, la influencia del contexto internacional y la necesidad de proteger sus informaciones de las injerencias de terceros estados (Burkert, 2000, p. 48). HONDIUS añade un argumento adicional, el valor que la sociedad sueca otorga a la transparencia (Hondius, 1975, pp. 44-47). Recordemos, como ejemplo ilustrativo de la cultura y valores arraigados en el país nórdico, que a ellos se debe la figura del ombudsman, reconocido por la Constitución sueca de 1809; sobre el origen de esta figura, vid. (Fairen Guillen, 1981).

[72] Esta exigencia fue reformada en el año 1982 (*SFS*: 446), reservando esa autorización previa solo para los tratamientos de datos previstos en la §4 (referida a determinadas categorías de datos "sensibles"). Sobre el trasfondo y debates en torno a esta medida, así como la evolución de la protección de datos en Suecia, vid. (Flaherty, 1989, pp. 93-164).

[73] Condenas e investigaciones penales, informaciones sobre la salud, la asistencia social, drogodependencia, raza, opiniones políticas y religiosas; a los que se irían añadiendo, hasta la modificación de 1998, especificaciones sobre cuidado de la juventud, atención psiquiátrica y datos sobre cuidado de personas con problemas mentales, vida sexual, ciertas informaciones exigidas por la normativa de extranjería.

[74] Sobre estas innovaciones, y alguna otra que la *Datalag* incorpora, vid. (Pascual Huerta, 2016, pp. 234-237).

[75] Si bien es cierto que ya a finales de los sesenta, en 1968, se promulgó la "*Wiretap Act*": *The Omnibus Crime Control and Safe Streets Act of 1968* (Pub.L. 90–351, 82 Stat. 197, enacted June 19, 1968, codified at 34 U.S.C. § 10101), que regulaba la vigilancia de las comunicaciones telefónicas.

La *Privacy Act* de 1974[76] marcó un salto evolutivo en las normativas de protección de datos. En ella se delineaban los principios y facultades de actuación que vendrán a caracterizar el derecho a la protección de datos (derecho acceso (Sec. 3.d).1; rectificación (Sec. 3.d).2) o un embrionario principio de minimización[77]). Es, como apunta Rebollo Delgado, la ley que contenía el texto «más completo y mejor estructurado jurídicamente hasta esa fecha, y que es el auténtico precursor de las posteriores normas sobre protección de datos de carácter personal en Europa» (Rebollo Delgado, 2014, p. 87).

La Privacy Act contaba con una excelente referencia, el *Report of Secretary's Advisory Committee on Automated Personal Data System*[78] de 1973. Este informe, intitulado, de manera elocuente, como *Records, Computers and the Rights of Citizens*, fue elaborado por el Departamento de Salud de Estados Unidos y tenía como objeto de análisis las bases de datos telemáticas del Gobierno. En él, se regulaba un código de buenas prácticas en el tratamiento de la información (*Fair Information Practices* (FIPs)).

La gran aportación de este código[79] fue el establecimiento de una serie de principios de básicos en materia de protección de datos. Así, prohíbe la existencia de bases de datos personales secretas; establece la necesidad de crear canales de comunicación que faciliten información a las personas respecto de los datos que están siendo tratados; limita los tratamientos a la finalidad para la que fueron recabados, requiriéndose el consentimiento del afectado, si se quieren realizar otras operaciones diferentes con sus datos; y reconoce los derechos de acceso y rectificación,

---

[76] *The Privacy Act of* 1974 (Pub.L. 93–579, 88 Stat. 1896, *enacted December* 31, 1974, 5 U.S.C. § 552ª). Una excelente traducción al español puede consultarse en, (*Informática. Leyes de Protección de Datos*, 1977, pp. 75-102).

[77] Sec. 3.e).1 de la Privacy Act de 1974, en su versión original, «*maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required*». Puede consultarse en: https://www.justice.gov/opcl/privacy-act-1974. (Última consulta: 20/10/2021).

[78] Puede consultarse en: https://www.justice.gov/opcl/docs/rec-com-rights.pdf. (Última consulta: 20/10/2021).

[79] Más allá de la existencia de precedentes que pudieran haberlo inspirado, lo cierto es que ha sido el código elaborado por el Departamento de Salud el que ha influenciado la producción normativa posterior. Sobre el impacto e influencia de este código en toda la normativa estadounidense posterior (no solo en la *Privacy Act*), vid. (Solove y Schwartz, 2018, pp.67-70). En lo referente a posibles influencias de trabajos previos, como puede ser el caso del *Privacy: Younger committee's report*, de 6 de junio de 1973.
Puede consultarse en: https://api.parliament.uk/historic-hansard/lords/1973/jun/06/privacy-younger-committees-report. (Última consulta: 20/10/2021). Vid., sobre el origen, influencias e impacto de estos instrumentos, los trabajos de (Hoofnagle, 2014) y (Gellman, 2019).

así como, la pertinencia de operar con datos fiables o la necesidad de que se prevean cauciones para evitar usos indebidos.

Esa combinación funcional de derechos y principios ha inspirado las normativas de protección de datos en todo el mundo. Sin embargo, y a pesar de ser el país donde todo nació (el concepto de *privacy* y el establecimiento de las FIPs[80]), y donde primero se activó una política de «*ongoing effort to bring technological design within the control of the public and to safeguard the right of privacy*» (Rotenberg, 2001, p. 34), lo cierto es que, desde hace un tiempo, los Estados Unidos han cedido el liderazgo a Europa.

La pérdida de influencia del modelo estadounidense, y la mayor relevancia de las regulaciones europeas, obedecen a diversas razones, entre las que destaca, su concepción liberal de los derechos y la ausencia de una ley federal general que establezca unas condiciones aplicables a todo tratamiento, pues solo se disponen condiciones generales para los datos en posesión de las agencias federales[81]. Todo ello ha redundado en una baja eficacia del derecho a la protección de datos, sobre todo en las relaciones *inter privatos* (Martínez Martínez, 2014, p. 56). Carencia, que resulta especialmente crítica, pues las relaciones entre particulares constituyen el grueso de las interacciones en la esfera digital.

La situación se agravó con la apuesta, a partir de los años 90 del pasado siglo, por la autorregulación como fórmula más apropiada para la protección de la *privacy*. Las consecuencias fueron inevitables, la «*privacy policy in the United States […] reflects what industry is prepared to do rather than what the public wants done*» (Rotenberg, 2001, p. 34).

Estos elementos son los que han propiciado que «*the United States abdicated the moral authority on privacy*» (Hartzog y Richards, 2020, p. 1703). *A contrario sensu*, el acierto y la utilidad de las medidas *omnibus*

[80] «*The FIPs model of privacy regulation has been adopted by virtually every country in the world that has decided to take data protection seriously*» (Hartzog y Richards, 2020, p. 1702).
[81] Ello no obsta para que algunos estados hayan desarrollado sus propias normativas sobre tratamiento de datos ampliando el margen de aplicación, en ese sentido destaca la regulación del estado de California, especialmente activo en este ámbito. Como demuestra la modificación de la Consumer Privacy Act of 2018 por la California Privacy Rights Act of 2020, que aproximan la regulación de este estado a la de la Unión Europea. Alguna normativa sectorial sí establece previsiones específicas aplicables a las relaciones entre particulares, tal es el caso de ámbitos como el asegurador y de los servicios de salud (v. gr. Health Insurance Portability and Accountability Act) o el financiero (donde operan, entre otras la Right to Financial Privacy Act of 1978, la Fair Credit Reporting Act 1970 y la Equal Credit Opportunity Act de 1974).

adoptadas por los países europeos, y la fuerza armonizadora de sus previsiones[82], le han llevado a la posición de referencia regulatoria global, «llenando un vacío antaño ocupado por el Gobierno estadounidense» (Foer, 2017, p. 197).

6.2.3. La expansión de la legislación de finales de los años setenta

El final de la década de los setenta fue testigo de la generalización de las regulaciones de sobre protección de datos. Alemania promulgó, en 1977, la Ley para la protección del mal uso de los datos personales a través de su tratamiento, *Bundesdatenschutzgesetz* (Ley federal de protección de datos[83]). De esta ley, aplicable tanto al sector público como al tratamiento de datos por parte de empresas privadas[84], destaca el enfoque adoptado en la conformación del sistema de protección. El legislador alemán perseguía contrarrestar el deterioro de la protección de los intereses de los ciudadanos causados por el mal uso de la información personal[85]. Para ello, apostó por una aproximación contextual, concibiendo a la realidad del tratamiento como un elemento determinante en la selección y configuración de los instrumentos normativos más apropiados para salvaguardar los derechos de las personas.

Por su parte, la Ley francesa relativa a la informática, archivos y libertades (1978)[86], incorporó, en su artículo 31, un listado de datos cuyo almacenamiento o conservación estaría prohibido, salvo en casos tasados y de carácter excepcional. A día de hoy, esos datos forman parte de las tipologías que integran las conocidas como categorías especiales de datos (en concreto el artículo se refiere al: origen racial, opiniones políticas, filosóficas o religiosas, afiliación sindical).

---

[82] Vid. (Schwartz, 2009, p. 912).
[83] Aprobada el 27 de enero de 1977, no entraría en vigor hasta el 1 de enero de 1978. BGBl. I Nr. 7 S. 201.
[84] A diferencia de las normativas de los *Lander*, solo aplicables al sector público, vid. (Lucas Murillo de la Cueva, 1990, pp. 131-132).
[85] § 1, en la que se apunta la protección contra el mal uso de los datos personales como finalidad de la ley.
[86] Ley n° 78-17 del 6 de enero de 1978. Puede consultarse en: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460). (Última consulta: 20/10/2021). Su versión traducida al castellano puede consultarse en, (*Informática. Leyes de Protección de Datos (II)*, 1983, pp. 87-106).

También en 1978 se aprobarían la ley austríaca de protección de datos; las dos leyes danesas[87] y la ley Noruega[88]. En 1979 sería el Gran Ducado de Luxemburgo quien promulgaría una ley sobre la utilización de datos en tratamientos informáticos[89]. La regulación de esta materia se extiende y asienta entre las democracias europeas.

6.2.4. La impronta internacional. Especial referencia a las Directrices de la OCDE y al Convenio 108 del Consejo de Europa

Como se apunta en el capítulo I de este trabajo, los efectos derivados de la irrupción y consolidación de la informática y las tecnologías de la información, singularmente la necesidad de hacer compatibles el respeto a los derechos fundamentales con las enormes potencialidades de la gestión y transmisión de datos, son un desafío y un problema global. No resulta extraño que, desde finales de los sesenta[90] y, sobre todo, a partir de los años setenta, proliferen instrumentos que, desde diversas organizaciones internacionales, traten de dar respuesta a los retos de la, por entonces, embrionaria era digital.

El análisis de todas las Recomendaciones, Resoluciones y Directrices que, a lo largo de las décadas, han fomentado y contribuido a dar forma al derecho a la protección de datos –aún con las divergencias existentes entre países– excede, con mucho, el objeto de este trabajo[91].

---

87 Dinamarca, inicialmente, apostó por elaborar dos textos normativos, uno para registros públicos y otro para privados. Leyes nº. 293 y 294, ambas del 8 de junio de 1978. Los textos de ambas leyes, traducidos al castellano, pueden consultarse en, (*Informática. Leyes de Protección de Datos (II)*, 1983, pp. 55-86).

88 Ley de 9 de junio de 1978, núm. 47. Puede consultarse su texto traducido, así como un brece comentario realizado por HEREDERO HIGUERAS en, («La Ley noruega de protección de datos personales (Ley de 9 de junio de 1978, núm. 47). Presentación y Traducción de Manuel Heredero Higueras», 1981).

89 Un estudio sobre la cronología del reconocimiento legislativo del derecho a la protección de datos puede verse en (Dresner, 1994).

90 V. gr. la Recomendación 509 de 31 de enero de 1968 de la Asamblea del Consejo de Europa, *Human rights and modern scientific and technological developments*.

91 Motivo por el que no se incluyen en este trabajo los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales, adoptados por la Asamblea de las Naciones Unidas por resolución 45/95, de 14 de diciembre de 1990; la *Privacy Framework* del Foro de Cooperación Económica Asia Pacífico, de noviembre de 2004 o la Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el tratamiento de datos de carácter personal (Resolución de Madrid, 5 de noviembre de 2005).

En consecuencia, me limitaré a apuntar únicamente aquellas previsiones internacionales[92] que más influencia han tenido en la conformación del derecho: las Directrices del Consejo de la Organización para la Cooperación y el Desarrollo Económico (en adelante OCDE), sobre protección de la privacidad y el flujo transfronterizo de datos personales, de 23 de septiembre de 1980[93] y el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[94] (en adelante, Convenio 108).

6.2.4.1. Las Directrices de la OCDE de 1980

Si bien es cierto que las Directrices del Consejo de la OCDE sobre protección de la privacidad y el flujo transfronterizo de datos personales no tienen carácter vinculante, no puede desconocerse la importancia de dos de sus aportaciones en materia de protección de datos: Establecer un listado sistematizado de principios básicos del derecho a la protección de datos[95] –inspirado, probablemente, en las *FIPs* estadounidenses– y poner sobre la mesa la problemática de los flujos transfronterizos de información. En puridad, la segunda de las aportaciones es la que impulsa la materialización de la primera.

La incorporación al diseño de los sistemas de protección de datos de los efectos de la circulación de información entre Estados, supuso un avance de gran transcendencia. En la actualidad, la libre circulación de datos es un referente obligado en la configuración del derecho a la protección de datos, al punto de erigirse en destacado motor de cambios normativos y operar como límite al ejercicio del propio derecho[96].

---

[92] Aunque la Unión Europea es, también, una organización internacional –*sui generis*, eso sí–, sus peculiares características, tanto respecto de sus competencias como en la aplicabilidad de sus normas, la hacen merecedora de una atención particularizada.

[93] Puede accederse al documento en el siguiente enlace: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf. (Última consulta: 20/10/2021).

[94] Entró en vigor en España el 1 de octubre de 1985, tras su ratificación en enero de 1984, «BOE» núm. 274, de 15 de noviembre de 1985.

[95] En la Parte Segunda de las Directrices, apdos. 7-14, se enuncian los principios de: limitación de recogida; calidad de los datos; especificación de los fines; limitación de uso; salvaguarda de la seguridad; transparencia; principio de participación individual (que está configurado como el actual derecho de acceso) y el principio de responsabilidad.

[96] Como acreditan los Considerandos 2 y 3 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo

Las dificultades para la libre circulación de información, propiciadas por la heterogeneidad regulatoria existente, impulsaron a la OCDE a elaborar las Directrices. En ellas se propone un sustrato normativo común, mediante el que lograr cierta homogenización y remover los «obstáculos injustificados para los flujos transfronterizos de datos personales»[97]. Los principios propuestos en la Parte Segunda de las Directrices son la piedra angular del sistema[98]. A ese esfuerzo de asimilación, hay que añadir la utilidad de contar con ciertos conceptos clave que sirven de referencia común (v. gr. dato personal, inspector de datos –equivalente al responsable en la terminología del RGPD– o flujos transfronterizos de datos personales).

En el resto de previsiones[99], esto es, en las relativas a sanciones y datos especiales, las Directrices se muestran menos innovadoras y más comedidas, probablemente por la dificultad para establecer criterios comunes para todos los países. En este sentido, resulta muy elocuente la afirmación contenida en la Memoria Explicativa de las Directrices, cuando se declara que «puede que no sea posible identificar un conjunto de datos que se vean universalmente como sensibles»[100].

---

que respecta al tratamiento de datos personales y a la libre circulación de estos datos; o los Considerandos 3, 6 y 9 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 (Reglamento general de protección de datos). Especialmente significativo es el Considerando 13 del Reglamento, al establecer como límite infranqueable del derecho a la protección de datos la libre circulación de datos personales en la Unión Europea: «El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales». Exigencia confirmada por el apartado tercero del artículo 1 del RGPD.

[97] Recomendación del Consejo relativa a las Directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales.

[98] Servirán de inspiración para «todas las normas nacionales e internacionales sobre la materia adoptadas con posterioridad» (Puente Escobar, 2006, pp. 50-51).

[99] Para un estudio detallado de las Directrices de la OCDE de 1980, vid. (Gacitúa Espósito, 2014, pp. 91-99).

[100] Apdo. 19 de la Memoria Explicativa de las Directrices. Puede consultarse en: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf. (Última consulta: 20/10/2021).

6.2.4.2. El Convenio 108

Tampoco el Consejo de Europa[101] (en adelante, CdE) permaneció ajeno a los temores, dudas y suspicacias generadas por la creciente implantación de sistemas de procesamiento automatizado de información personal y sus consecuencias para la protección de la vida privada. Prueba de ello son las dos Resoluciones del Comité de Ministros de 1973 y 1974, referidas, respectivamente, a la protección de las personas físicas en relación con los bancos electrónicos del sector privado y del sector público[102]. «A pesar de su relativa modestia, estas Resoluciones adquieren una significación histórica: son los primeros textos internacionales que presentan a los Estados pautas de conducta sobre la materia» (Garzón Clariana, 1981, p. 13).

Sin embargo, la gran aportación del CdE es el Convenio 108. Sus objetivos y finalidades son, en parte, coincidentes con las de las Directrices de la OCDE, en tanto, que tienen por finalidad «garantizar […] a cualquier persona física […] el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respeto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona»[103] y también le impulsa la necesidad de establecer un marco de garantías que asegure la libre circulación de datos entre los Estados[104].

---

[101] «La finalidad del CdE consiste en realizar una unión más estrecha entre sus miembros para salvaguardar y promover los ideales y los principios que constituyen su patrimonio común y favorecer su progreso económico y social». Artículo I a) del Estatuto del CdE, hecho en Londres el 5 de mayo de 1949, al que España se adhiere en 1978. El instrumento de Adhesión fue publicado en el BOE de 1 de marzo de 1978. Puede consultarse en: https://www.boe.es/buscar/doc.php?id=BOE-A-1978-5972. (Última consulta: 20/10/2021).

[102] Resoluciones del Comité de Ministros del CdE: 73(22), de 26 de septiembre de 1973, relativa a la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector privado y 74(29), de 20 de septiembre de 1974, relativa a la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector público. Pueden consultarse, respectivamente, en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680502830 y https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804d1c51. (Última consulta: 20/10/2021).

[103] Artículo 1 del Convenio 108. Así lo entiende PIÑAR MAÑAS, quien señala que el Convenio 108 «pretende resolver la tensión existente entre el uso cada vez más generalizado de la informática y el riesgo que el mismo puede suponer para la vida privada» (Piñar Mañas, 2009, p. 88).

[104] Vid. Preámbulo Convenio 108, donde se señala: «Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras; Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información».

De hecho, la libre circulación es el acicate para que los Estados adopten regulaciones que aseguren «la presencia de un nivel mínimo de protección equivalente entre las partes» (Lazpita Gurtubay, 1994, p. 416). Como puede constatarse, el valor estratégico, no solo para la gestión política interna, sino para el comercio, la economía o la geopolítica internacional ya eran, a principios de los años ochenta, un factor determinante a la hora de configurar el derecho a la protección de datos.

A diferencia de las Directrices de la OCDE, el Convenio 108 posee fuerza vinculante[105], lo que lo convierte en el primer instrumento internacional jurídicamente exigible. Ahora bien, al no estar sujeto al control del TEDH y conceder a los Estados un amplio margen para la aplicación de sus principios y el desarrollo de las excepciones en él previstas, el Convenio no logró proporcionar «la […] protección homogénea […] que se había esperado» (Arenas Ramiro, 2006, p. 156), a pesar de que incluía el compromiso de los Estados Parte de establecer un régimen de sanciones como medio de coerción ante la vulneración de sus principios. También difiere de las Directrices en que, en este caso, sí identifica qué tipologías de información considera que merecen la condición de categorías "particulares" de datos[106], lo que resulta coherente con su objetivo de evitar divergencias y establecer unos presupuestos comunes de protección.

El CdE realiza un esfuerzo encomiable para ofrecer soluciones y propuestas con las que hacer frente a «las múltiples formas de erosión y agresión de los derechos fundamentales surgidas a partir del avance de las […] tecnologías de la información y la comunicación» (Guerrero Picó, 2006, p. 247)[107]. Durante estos años, ha desplegado una ardua labor de concienciación y producción normativa (materializada, sobre todo, en Recomendaciones)[108], con la que ha complementado el contenido del

[105] Tendrá fuerza vinculante, para aquellos que lo ratifiquen, evidentemente. En este sentido, debe apuntarse que no es necesario ser un estado miembro del CdE para poder adherirse a él.

[106] Artículo 6 del Convenio 108. Integrarían esa categoría los «datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual […] [y los] referentes a condenas penales».

[107] La autora también realiza un análisis del trabajo realizado por el CdE con posterioridad al Convenio 108, (Guerrero Picó, 2006, pp. 42-47).

[108] Ya antes del Convenio 108 se venían promoviendo instrumentos jurídicos para sectores concretos, como la Recomendación 80/3, del Comité de Ministros del Consejo de Europa de 18 de septiembre de 1980, relativa al intercambio de informaciones jurídicas en materia de protección de datos. Sin embargo, sería después del Convenio cuando el CdE realizaría la mayor parte de sus contribuciones, a título ejemplificativo pueden mencionarse las

Convenio 108[109], incluido un Protocolo adicional relativo a las autoridades de control y a los flujos transfronterizos de datos personales, de 8 de noviembre de 2001[110].

Finalmente, cabe recordar que, el Convenio 108, ha sido actualizado[111]. El objetivo que inspira sus modificaciones no es otro que asegurar su «coherencia» y «compatibilidad»[112] con el RGPD de la UE[113].

---

siguientes Recomendaciones que, ni mucho menos, agotan o hacen justicia a todo el acervo jurídico generado por el CdE: Recomendación 83/10, del Comité de Ministros del Consejo de Europa de 23 de septiembre de 1983, en materia jurídica a los estados miembros relativa a la protección de los datos de carácter personal utilizados con fines de investigación científica y de estadísticas; Recomendación 85/20, del Comité de Ministros del Consejo de Europa de 25 de octubre de 1985, en materia jurídica a los estados miembros relativa a la protección de los datos de carácter personal utilizados con fines de marketing directo; Recomendación 89/2, del Comité de Ministros del Consejo de Europa, de 18 de enero de 1989, en materia jurídica a los estados miembros sobre la protección de los datos de carácter personal utilizados con fines de empleo; Recomendación 90/19, del Comité de Ministros del Consejo de Europa de 13 de septiembre de 1990, en materia jurídica a los estados miembros sobre la protección de los datos de carácter personal utilizados con fines de pago y otras operaciones conexas; Recomendación 95/4del Comité de Ministros del Consejo de Europa de 7 de febrero de 1995, en materia jurídica a los estados miembros sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación, en especial con relación a los servicios telefónicos; Recomendación 97/5, del Comité de Ministros del Consejo de Europa de 13 de febrero de 1997, relativa a protección de datos médicos; Convenio sobre los Derechos Humanos y la Biomedicina, Oviedo, 4 de abril de 1997 (Convenio de Oviedo).

[109] A las Recomendaciones apuntadas, debe adicionarse otros mecanismos e instituciones que «contribuyen igualmente a generar mayor sensibilización y cultura de respeto de la protección de datos con respecto a personas vulnerables» (Jimena Quesada, 2019, p. 600). En concreto, JIMENA QUESADA identifica cuatro: la Comisión Europea contra el Racismo y la Intolerancia (ECRI); el Grupo de Expertos sobre la lucha contra la Trata de seres humanos (GRETA); el Grupo de Lanzarote (Comité de las Partes en el Convenio del Consejo de Europa sobre la protección de los niños contra la explotación y los abusos sexuales, creado por el Convenio de Lanzarote de 25 de octubre de 2007) y el Comité de Bioética, que trae causa del Convenio de Oviedo de 1997. Sobre estos instrumentos y su efecto sobre la protección de la vida privada y los datos personales, vid. (Jimena Quesada, 2019, pp. 600-604).

[110] Este Protocolo ha sido ratificado por España. Su instrumento de ratificación fue publicado en el «BOE» núm. 228, de 20 de septiembre de 2010. Puede consultarse en: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-14380. (Última consulta: 20/10/2021).

PAVÓN PÉREZ realiza un análisis de las principales implicaciones del mismo en, (Pavón Pérez, 2001).

[111] Protocolo de modificación del Convenio 108 (Protocolo CETS nº 223), de 18 de abril de 2018. El texto modernizado puede consultarse en: https://rm.coe.int/convenio-para-la-proteccion-de-las-personas-con-respecto-al-tratamient/1680968478. Además, el CdE proporciona un resumen de las principales novedades, puede consultarse en: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8. (Última consulta: 20/10/2021).

[112] (Agencia de los Derechos Fundamentales de la Union Europea, 2018, p. 30).

[113] Sobre la modernización del Convenio 108 y su retroalimentación normativa con la Unión Europea, vid. (Tomás Mallén, 2019).

6.3. Primeros reconocimientos constitucionales

La década de los setenta resultó especialmente prolífica para la protección frente al tratamiento de datos. Su primera mitad se caracteriza por la promulgación de las primeras leyes sobre la materia, mientras que en la segunda se inicia el período de la inclusión y generalización en los textos constitucionales de preceptos que, con mayor o menor claridad, constituyen la primera plasmación positiva del derecho a la protección de datos como derecho fundamental. Esas previsiones constitucionales, no siempre reconocieron un derecho autónomo y diferenciado. Sin embargo, gracias a ellas se conformó progresivamente una esfera de protección resistente a la capacidad regulatoria del legislador ordinario.

6.3.1. Portugal

Si hay un texto constitucional paradigmático y pionero en el reconocimiento de la protección de los datos personales frente al uso indebido de la información, ese es el portugués. En 1976, Portugal se convirtió en el primer país en constitucionalizar un precepto específico dedicado a la utilización de la informática: el artículo 35[114]. Además, en el artículo 33.2, ordena al legislador el establecimiento de garantías adecuadas frente a la utilización de información relativa a personas y familias (confiriéndole una proyección colectiva), siempre y cuando fuese abusiva (lo que entronca con la idea del principio de minimización) o contraria a la dignidad (situándola como un límite a las posibilidades de tratamiento de información)[115].

De la lectura combinada de los artículos 35 y 33.2 se extraen varias conclusiones. En primer lugar, se regula, en un artículo específico, el tratamiento informático de la información personal, separado del precepto

---

[114] Art. 35 Constitución portuguesa de 1976:
«1. *Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização*.
2. *A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos*.
3. *É proibida a atribuição de um número nacional único aos cidadãos*».

[115] Puede consultarse el texto original de la Constitución portuguesa en: https://www.parlamento.pt/parlamento/documents/crp1976.pdf. (Última consulta: 20/10/2021).

relativo al derecho a la intimidad (33.1 y 35). De este modo, se comienza a apuntar que podrían tratarse de realidades no siempre coincidentes. En esos dos preceptos se plasman las dos facetas del derecho: la objetiva, representada por los deberes que impone, esencialmente, al legislador (v. gr., art. 33.2); y la subjetiva, concretada en las facultades de actuación de los ciudadanos (art. 35.1) y las prohibiciones (art. 35.3[116]) de actuación a los poderes públicos.

La protección frente a los riesgos que, para otros derechos, pudieran derivarse del procesamiento de datos personales es uno de los elementos definitorios del nuevo derecho. En esa línea debe entenderse la inclusión, en el texto constitucional, de una mención específica a determinados tipologías de datos (convicciones políticas, fe religiosa y vida privada[117]), cuyo tratamiento informático se prohíbe, salvo en situaciones concretas (como los fines estadísticos).

6.3.2. Austria

El 18 de octubre de 1978 Austria aprobaba la *Datenschutzgesetz*[118]. El artículo primero de dicha ley es una "disposición constitucional"[119], en la que se dota de rango constitucional al derecho a la protección de datos. En él se incluye el derecho de la persona a mantener en secreto los datos sobre las informaciones que le conciernen, salvo circunstancias expresamente previstas, como el interés legítimo de terceros o la concurrencia de las razones previstas en el art. 8.2 del CEDH[120]. Se

[116] El apartado tercero del artículo 35 de la Constitución portuguesa refleja una preocupación por las interconexiones que se pudieran derivar de vincular toda la información personal de una persona a un único número de identificación personal, vid. (Dias Venancio, 2007).
[117] Artículo 35.2 de la Constitución portuguesa de 1976.
[118] Publicada en la BGBl. O. Nr. 565/1978, de 28 de noviembre de 1978. Versión en español: (Heredero Higueras, 1988b, pp. 25-71).
[119] Conforme al art. 44.1 de la Constitución austríaca, «*Verfassungsgesetze oder in einfachen Gesetzen enthaltene Verfassungsbestimmungen können vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden; sie sind als solche ("Verfassungsgesetz", "Verfassungsbestimmung") ausdrücklich zu bezeichnen*». Esto es: «Las leyes constitucionales o las disposiciones constitucionales contenidas en leyes simples sólo pueden ser aprobadas por el Consejo Nacional en presencia de al menos la mitad de los miembros y por una mayoría de dos tercios de los votos emitidos; se especificarán explícitamente como tales ("ley constitucional", "disposición constitucional")». Traducción propia a partir de la versión oficial en inglés que puede consultarse en: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.pdf. (Última consulta: 20/10/2021).
[120] Art. 8.2 CEDH.

reconocen, como parte inescindible del mismo, los derechos de acceso y rectificación de los datos inexactos[121].

6.3.3. ¿España?

En 1978 también se aprobó la Constitución española (en adelante, CE), esta dispone que la «ley limitará el uso de la informática» (artículo 18.4[122]). Aunque este mandato al legislador (Pérez-Ugena, 2012, p. 1840) no es equiparable al reconocimiento de un derecho fundamental[123], se trata de un texto que, en su parquedad, ofrece «una respuesta constitucional ante una amenaza concreta» (Troncoso Reigada, 2010, p. 68).

Es una previsión hija de su tiempo[124], aunque menos ambiciosa que la portuguesa o la austríaca. Sin restar méritos a la labor del constituyente, lo cierto es que se trata de un precepto que, ni por ubicación sistemática –el artículo 18, destinado a la regulación de la protección de la esfera privada– ni por dicción literal, parece estar pensando en la protección de datos[125], ni en su vertiente objetivo-instrumental, como instituto de garantía de otros derechos fundamentales[126], ni mucho menos como derecho autónomo.

Fue el Tribunal Constitucional español (TC) quien acometió la tarea de deslindar interpretativamente el derecho a la protección de datos de otros derechos, confiriéndole una posición constitucional diferenciada. El presupuesto constitucional del 18.4 CE ha experimentado una progresiva evolución, que ha transformado el originario mandato al legislador para limitar el uso de la informática en un genuino derecho fundamental.

---

121 Una versión en español del artículo 1 de la *Datenschutzgesetz* puede consultarse en, (Pascual Huerta, 2016, p. 262).

122 Art. 18.4 CE: «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».

123 STC 15/1982, 23 de abril, FJ 8, sobre la aplicabilidad directa del contenido constitucional.

124 Rallo Lombarte califica como «meritoria [la] referencia a la informática en el texto constitucional» (Rallo Lombarte, 2018, p. 75). Este mismo autor realiza un excelente recorrido del proceso evolutivo de la «libertad informática» en (Rallo Lombarte, 2017a). Sobre las virtudes y problemas de la previsión constitucional del 18.4 CE, me remito a lo ya apuntado en (Jove, 2018, pp. 81-86).

125 Sobre la incardinación en el 18.4CE del derecho a la protección de datos, alternativas y consecuencias de esta opción, vid. (Martínez Martínez, 2004, pp. 324-348).

126 STC 254/1993, de 20 de julio, FJ 6.

6.4. El factor jurisprudencial y la consolidación del derecho a la protección de datos

6.4.1. El TCFA y la autodeterminación informativa

Existe cierto consenso acerca de que fue la sentencia del Tribunal Constitucional Federal Alemán (en adelante, TCFA), de 15 de septiembre de 1983, qué declaró inconstitucionales algunos preceptos de la Ley del Censo[127], la que dispuso las bases para la consideración autónoma del derecho a la protección de datos (Martínez Martínez, 2007, p. 48). Hasta este pronunciamiento, el elemento central era la limitación del uso de la informática y el establecimiento de unos principios que reguladores del tratamiento de la información personal, con la consiguiente atribución de ciertos poderes de actuación a los ciudadanos para la salvaguarda de sus intereses. Esto es, las regulaciones sobre protección de datos operaban como un mecanismo de garantía de otros derechos.

En esta sentencia, sin embargo, el TCFA, al identificar el derecho a la autodeterminación informativa como un derecho autónomo, delimitó un espacio *iusfundamental* específico. Un derecho que es proyección directa de la dignidad y el libre desarrollo de la personalidad del individuo, cuya manifestación más genuina es la capacidad para decidir «sobre las acciones que vaya a realizar o, en su caso, a omitir»[128] respecto de su persona. En concreto, la autodeterminación informativa[129] vendría caracterizada por conceder al individuo la facultad «de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales»[130].

El derecho a la autodeterminación informativa supone el reconocimiento jurídico de la necesidad de administrar la identidad

---

[127] («Jurisprudencia Constitucional Extranjera, Núm. 33, IV», 1984). Para un análisis de la sentencia, vid. (Heredero Higueras, 1983).

[128] En el original alemán, desarrollado un poco más en extenso, el TCFA señala: «*mende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten*» BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983- 1 BvR 209/83 -, Rn. 1-215, Grunde C, II-1a), apdo. 146. Puede consultarse en español en: («Jurisprudencia Constitucional Extranjera, Núm. 33, IV», 1984, p. 153).

[129] Sobre el derecho a la autodeterminación informativa y lo adecuado de su denominación en lugar de derecho a la protección de datos, son referencia inexcusable los trabajos de LUCAS MURILLO de la CUEVA, vid. (Lucas Murillo de la Cueva, 2003) o (Lucas Murillo de la Cueva, 1990). También (Pérez Luño, 1986).

[130] Original en alemán: «*grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*», en BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983- 1 BvR 209/83 -, Rn. 1-215, Grunde C, II-1a), apdo. 147. Puede consultarse en español en: («Jurisprudencia Constitucional Extranjera, Núm. 33, IV», 1984).

personal –sobre todo en su vertiente externa– y, con ello, tratar de controlar los efectos, no solo *ad intra*, que puedan derivarse del tratamiento de informaciones a uno referidas.

Tras la sentencia del TCFA[131], el desarrollo del derecho, hasta su dimensión actual, ha estado presidido por un proceso caracterizado por: la concreción de contenidos; la ampliación de las facultades atribuidas a la ciudadanía para hacer efectivo ese poder de control y disposición; la precisión y detalle de las exigencias requeridas para su protección; la extrapolación a procesos no automatizados y el aumento de su complejidad técnica.

6.4.2. El Tribunal Constitucional español

El pronunciamiento del TCFA sobre la Ley del Censo es el ejemplo paradigmático de construcción jurisdiccional de un derecho constitucional. Pero no es el único. De la mano del TC, el reconocimiento del derecho a la protección de datos, como derecho fundamental autónomo, y distinto, del derecho a la intimidad, ha seguido un camino similar en España. Este proceso creador[132] comenzó con la sentencia 254/1993, de 20 de julio[133] y culminó con las SSTC 290/2000 y 292/2000, ambas de 30 de noviembre[134].

---

131 Aunque los textos legislativos continuarían estando inspirados por la función instrumental del derecho a la protección de datos –si bien la plasmación positiva en el articulado ya se centra en la regulación del poder de control y disposición–. Quizá el mejor ejemplo de esta regulación "entre dos aguas" sea la Directiva 95/46/CE. Esta, en su considerando segundo, incide en la subordinación y necesidad de adecuación de los sistemas informáticos para asegurar el respeto a "las libertades y Derechos fundamentales de las personas físicas y, en singular la intimidad". Sin embargo, el articulado ya es fiel reflejo de lo que, en ese momento, representa el derecho a la protección de datos.

132 La doctrina, establecida en la STC 254/1993, se reitera en las SSTC 143/1994, de 9 de mayo, FJ 7; 11/1998, de 13 de enero, FJ 4; 94/1998, de 4 de mayo, FJ 6 y 202/1999, de 8 de noviembre, FJ 2.

133 De la STC 254/1993 realiza un estudio detallado (Villaverde Menédez, 1994).

134 La STC 290/2000 está referida a disposiciones de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, (en adelante, LORTAD). A causa de la derogación de la LORTAD, el grueso del recurso de inconstitucionalidad no fue objeto de análisis por parte del TC, al haberse producido una pérdida sobrevenida de objeto (los artículos afectados por la pérdida de objeto sobrevenida fueron: 6.2, 19.1, 20.3, 22.1 y 2, 39.1 y 2). No obstante, el TC sí analizó el reparto competencial en ella establecido y el papel que debía desempeñar al Agencia Española de Protección de Datos (AEPD), Fundamentos Jurídicos 8 y 9 de la STC 290/2000.
Por su parte, la STC 292/2000 se centra en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD). En ella se realizan las aportaciones más significativas a la conformación del derecho a la protección de datos.

En la STC 254/1993, el TC señaló que, en el apartado 4 del artículo 18, además de promoverse la protección de la intimidad, se reconocía la existencia de «un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos» (STC 254/1993, FJ 6). La STC 290/2000 y, sobre todo la STC 292/2000[135] establecieron, en el plano constitucional, aquello que, en el ámbito legal, ya era una realidad[136], e incorporan al acervo constitucional, de manera clara y fehaciente[137], el derecho a la protección de datos que, a partir de dichos pronunciamientos, dejó de ser enteramente disponible por el legislador.

En este sentido, la STC 292/2000 es referencia obligada, no solo por reconocer sin ambages del derecho a la protección de datos como derecho fundamental, sino por concretar su contenido, naturaleza y obligaciones, deslindándolo de otras figuras afines[138]. A partir de ese pronunciamiento[139], el derecho fundamental a la protección de datos va a estar definido por un contenido específico y por un objeto determinado. El contenido consiste en «un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso» (STC 292/2000, FJ 7). En cuanto al objeto, serán los datos personales, en general; «no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato […], sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales» (STC 292/2000, FJ 6).

---

135 Seoane realiza un análisis detallado de ambas sentencias en (Seoane, 2002a) y (Seoane, 2002b).

136 En ese momento, en España estaba en vigor la segunda ley de protección de datos, la LOPD, y desde la esfera comunitaria se había promulgado, unos años antes, la Directiva 95/46/CE relativa a la protección de personas físicas en lo respectivo al tratamiento de datos personales y a la libre circulación de estos datos.

137 A partir de la STC 292/2000 no existe duda de la consideración del derecho a la protección de datos como derecho con unas características propias y únicas, cuyo anclaje constitucional sería el art. 18.4 CE. Sobre los problemas derivados de residenciar en el 18.4 CE el derecho a la protección de datos, vid. (Martínez Martínez, 2004). Para una crítica general a la configuración dogmática de la autodeterminación informativa como un derecho distinto del derecho a la intimidad, vid. (Ruiz Miguel, 1995).

138 Sobre las aportaciones de la STC 292/2000 vid. (Suárez Rubio, 2015, pp. 96-112).

139 Sobre el desarrollo del derecho a la protección de datos por el TC, vid. (Aguado Renedo, 2010).

6.4.3. El TEDH

Como se ha apuntado, el CEDH no contiene una mención específica a la protección de datos. Sin embargo, el TEDH, en su interpretación del artículo 8 del CEDH, ha ido forjando una sólida jurisprudencia en torno a la protección de la vida privada frente a las injerencias de la tecnología[140]. El Tribunal de Estrasburgo ha abordado un amplio abanico de asuntos, desde el control de los empleados (tanto en el espacio de trabajo[141] como en la inspección de correos electrónicos[142] o la negativa a su contratación basada en datos personales[143]) hasta la vigilancia gubernamental de las comunicaciones de sus ciudadanos[144], pasando por cuestiones relacionadas con el acceso a datos personales por parte de los órganos judiciales[145]. Caso a caso, sentencia a sentencia, el TEDH ha ido incorporando el derecho a la protección de datos al acervo de bines jurídicos salvaguardados por el artículo 8 del CEDH.

El CEDH, y la jurisprudencia del TEDH, son un elemento dinamizador de la protección de los derechos en la esfera europea. En no pocas ocasiones, han estado a la vanguardia en cuanto a protección de derechos, descubriendo nuevas facetas y modos posibles de interpretación (v. gr. art. 8 CEDH y medioambiente[146]). Sin embargo, en lo referente al derecho a la protección de datos, el papel protagónico en Europa lo tendrá la regulación y la jurisprudencia emanadas de las instituciones europeas[147]. A las

---

[140] Para un análisis detallado, sentencia a sentencia, de la protección de datos en la jurisprudencia del TEDH, vid. (Pérez Miras, 2018, p. 269-276) y (Martínez López-Sáez, 2018, pp. 146-154).
[141] STEDH, Copland contra Reino Unido, de 3 de abril de 2007.
[142] STEDH, Bărbulescu contra Rumanía, de 12 de enero de 2016.
[143] STEDH, Leander contra Suecia, de 26 de marzo de 1987.
[144] STEDH, Liberty y otros contra Reino Unido, de 1 de julio de 2008.
[145] STEDH, K.U. contra Finlandia, de 2 de diciembre de 2008.
[146] STEDH, López Ostra contra España, de 9 de diciembre de 1994. Además de medioambiente, la interpretación del art. 8 del CEDH también ha posibilitado la ampliación de la protección en cuestiones relativas a la vivienda (STEDH, McCann contra Reino Unido, de 13 de mayo de 2008 o STEDH, Chapman contra Reino Unido, de 18 enero de 2011, entre otras). O para conectar el derecho a ser informado en la prestación de servicios sanitarios con el respeto a la vida privada (STEDH, Pretty contra Reino Unido, de 29 de julio de 2002, apdos. 64-78 o STEDH, V. C. contra Eslovaquia, de 8 de febrero de 2012, apdos. 143-150).
[147] Sin que, por ello, pretenda restarse valor a los pronunciamientos de un tribunal que, en la salvaguarda de la vida privada ha actuado como «a European Constitutional Court» (van der Sloot, 2020).

aportaciones de estas, por constituir el objeto de estudio de esta tesis, se les dedicará una atención particularizada en los Capítulos siguientes.

6.5. La necesaria diferenciación entre la legislación de datos y el derecho a la protección de datos

En este punto, interesa poner de manifiesto que, si bien la *privacy* o la vida privada, pueden servir como antecedente, no absorben ni se confunden con el derecho a la protección de datos. Este surge a partir de la creciente necesidad de mantener un cierto control jurídico sobre la proyección externa de la persona y la información personal destinada a ser compartida con terceros. Inicialmente no tuvo la consideración de derecho. Bastaba con imponer límites a los pocos operadores que podían tratar esa información a gran escala para proteger de forma suficiente la privacidad de una ciudadanía, a la que, además, se comenzó a reconocer ciertas facultades de actuación en relación con los datos que estaban siendo tratados, singularmente, la de poder conocerlos (acceder a ellos) y rectificarlos si la información era errónea.

Ese poder para controlar y disponer de los datos referidos a uno tiene una conexión directa con la dignidad de la persona y el libre desarrollo de la personalidad. El reconocimiento por el TCFA del derecho a la autodeterminación informativa así lo confirmaba y, con el tiempo, ese derecho de autodeterminación, acabará adoptando el nombre de derecho a la protección de datos.

Una historia y una transformación que nos recuerdan la condición variable de los derechos individuales, de la que nos habló el maestro García-Pelayo, así, su contenido viene «condicionado por la defensa de la personalidad humana frente a los poderes o métodos que en cada ocasión la amenacen» (García-Pelayo, 1984, p. 152). En el caso del derecho a la protección de datos, fue la amenaza de una indebida utilización de la información personal la que dio lugar a la necesidad de reconocer, como derecho, la facultad individual de disposición y control de aquellas informaciones personales que comportaban una proyección externa del ser.

En efecto, «los derechos fundamentales son la respuesta ("reacción"), según la experiencia histórica, a las amenazas fundamentales para el hombre (derechos del hombre) y al ciudadano (derechos civiles) en

el Estado constitucional; dado que las situaciones específicas de peligro mudan históricamente. Y nuevos instrumentos para combatirlos deben ser desarrollados» (Häberle, 2003, p. 205).

Hay derechos inherentes a la idea misma de constitución, cuyo propósito es implantar un orden de convivencia liberal y democrático, y hay otros derechos, posteriores, que son consecuencia de los desarrollos y de las nuevas necesidades que surgen dentro del modelo de convivencia democrática previamente establecido. Estos derechos no son, como los primeros (libertad personal, de expresión, de creencias, acceso al juez y a un proceso con todas las garantías, asociación y reunión,…), una suerte de catálogo rupturista frente al universo cultural anterior, sino una consecuencia, una decantación lógica, del orden democrático ya establecido. Por esta razón, primero la preocupación ciudadana se transforma en un mandato a los poderes públicos y, particularmente, al legislador y, solo tiempo después, cuando la amenaza persiste o cuando, a pesar de las medidas adoptadas, se acrecienta, se considera necesario "fundamentalizar" el derecho, para su mejor protección.

A este esquema evolutivo obedece el derecho a la protección de datos, cuya caracterización y regulación jurídica precede al momento de su "constitucionalización". Este particular modo de alumbramiento como derecho fundamental, presenta, sin embargo, algunas consecuencias contaminantes a la hora de individualizar el derecho e identificar su sustantividad propia. Es necesario acotar el contenido del derecho y deslindarlo de aquellas otras previsiones conexas, nacidas cómo remedios instrumentales mediante los que evitar las consecuencias no deseadas que del tratamiento de los datos personales pudieran derivarse para otros derechos fundamentales distintos (la intimidad, la libertad ideología, la salud, etc.).

El legislador no ha realizado esfuerzo alguno en esa dirección, regulando la protección de datos como si fuese una especie de "garantía-paraguas" al servicio de un amplio conjunto de derechos fundamentales, más que como un derecho dotado de una entidad específica y diferenciada.

Probablemente, ello se deba al hecho de que una vez superada la imbricación inicial entre este derecho y los derechos a la vida privada y a la intimidad, la preocupación principal se focalizase en la seguridad de los tratamientos y en la eficacia de las medidas a adoptar, de suerte que la

iusfundamentalización del derecho solo adquirió interés con la llegada de la digitalización.

En todo caso, las bases para la confusión del todo con la parte estaban sentadas. Y, a mayor abundamiento, la recién conquistada autodeterminación informativa acabaría adoptando una denominación que, en principio, todo lo abarca: protección de datos.

Un solo nombre para muchas realidades. Sin embargo, por complejo que resulte y por más que puedan coincidir en ocasiones, corresponde al jurista descubrir las señas de identidad del derecho, máxime cuando es considerado como fundamental. Lo que se incorpora al plano de la constitucionalidad como "derecho fundamental" no es, ni puede ser, el contenido recogido en toda la regulación jurídica concerniente a la protección de datos personales. Por tanto, resulta obligado diferenciar entre las previsiones normativas generales y el derecho fundamental propiamente dicho, especialmente cuando las primeras incluyen elementos que, en puridad, responden a la protección de otros bienes jurídicos distintos.

7. La externalidad, la reserva de lo privado y la contextualidad del derecho a la protección de datos

La utilización de la información personal siempre ha estado acompañada de una preocupación por su uso, es decir, por los impactos que su conocimiento por terceros pudieran tener sobre la persona a la que está referida. La pérdida de la individualidad y la dispersión de la identidad personal en una comunidad de la información gobernada por claves aún desconocidas, explican el miedo y la consiguiente reacción. La inquietud expresada por Warren y Brandeis se convirtió, con la llegada de los tratamientos automatizados de datos, en fundado pavor.

Fue la separación de lo público y lo privado propia de la revolución liberal, la que animó, hacia finales del siglo XIX, los primeros estudios generales sobre la *privacy* y la intimidad[148]. Es en ese momento cuando la

[148] Las normativas sectoriales existentes solo se ocupaban de regular la confidencialidad y el deber de secreto en determinados ámbitos profesiones. Tenían un carácter particularizado y no tomaban en consideración la existencia de una pretensión de autorrealización del individuo que fuese digna de protección.

disponibilidad de un espacio personal, propio y seguro, comienza a reivindicarse como un elemento imprescindible de la idea de libertad. La consolidación de una esfera reservada al conocimiento ajeno debía completarse con el dominio de la información a uno referida. La construcción de una esfera privada, de un ámbito reservado, imponía un proceso de delimitación de espacios y la definición de los círculos de información, incluida la proyección exterior.

La transformación del modo de concebir al individuo en su dimensión comunitaria demandaba la garantía de un espacio libre de intromisiones. Ese cambio de paradigma implica un replanteamiento completo del modo de estar y relacionarse con el mundo. Al identificarse como valiosas determinadas informaciones personales, la proyección exterior de la personalidad adquiere una nueva dimensión que ha de ser especialmente protegida.

Defender la existencia de una esfera reservada, implica reconocer que hay una esfera pública. Las personas toman una mayor conciencia de su imagen y de los riesgos que les comporta el hecho de cómo son percibidas. De la mano de lo privado vino un incremento en la importancia del individuo en su proyección social. Saber qué se quiere detraer del conocimiento ajeno implica asumir que habrá un conjunto de informaciones que serán de dominio público o, al menos, que tendrán una proyección exterior mayor que aquellas consideradas como reservadas.

No importa que «no se tenga nada que ocultar»[149]. La determinación de espacios, de lo reservado y de lo que no lo es, resulta esencial para definir la proyección exterior del ser. El control de la transparencia es la única forma de asegurarse un ámbito cierto de privacidad.

En la era digital, las inferencias permiten conocer aquello que se quiere mantener reservado. Aunque la información que ofrezcan no tenga una fiabilidad absoluta, tendrá consecuencias como si realmente lo fuera. Así operan hoy muchos algoritmos cuyo cálculo es determinante para adoptar decisiones sobre una persona. A partir de estas informaciones se puede intentar sugestionar a los ciudadanos para que voten de un determinado modo (como hizo *Cambridge Analytica*, por ejemplo) o influir en sus expectativas profesionales o vitales (al contratar un seguro, pedir un

[149] Sobre lo pernicioso de la expresión nada que ocultar, vid. (Solove, 2007) y, de manera más detallada y amplia, en la monografía: *Nothing to Hide. The False Tradeoff between Privacy and Security*, (Solove, 2011).

préstamo, solicitar un trabajo o determinar la valía de la formación académica recibida[150]). En definitiva, pueden afectar a sus derechos y al libre desarrollo de la personalidad.

Los medios digitales facilitan los medios para revertir las tradicionales garantías de lo privado. La externalidad del ser, al transitar por el tamiz de las tecnologías de la información, excreta un avatar de cada uno de nosotros, con la diferencia contextual de que, ahora, se han incrementado las posibilidades de influir y condicionar el comportamiento de los individuos y de truncar su libertad individual, mediante sistemas, generalmente, difusos. No solo la libertad, la dignidad y el libre desarrollo de la personalidad corren el riesgo de verse afectadas, la democracia misma está amenazada.

El tratamiento de la información en la era digital ha generado un efecto perverso, al anudar el control de lo externo y la garantía de lo interno. La intimidad, la libertad ideológica o el derecho a la salud, ya no se protegen suficientemente con las tradicionales medidas de garantía jurídica. Es necesario el control de la proyección externa de la persona; el control de los datos personales. El derecho a la protección de datos personales opera como un factor de persuasión, como una línea anticipada de defensa frente a potenciales intromisiones ilegítimas. Pero una cosa es la prevención del daño y otra, bien distinta, su reparación. Para esto último, es imprescindible individualizar el derecho efectivamente conculcado y examinar sus específicas formas de reparación.

Al igual que los derechos a la intimidad o a la vida privada se ocuparon de asegurar un espacio libre de intromisiones ajenas, el derecho a la protección de datos vendría a garantizar un poder de control y disposición sobre, la información a uno referida, ajustándola a las preferencias y a la realidad de cada individuo. No solo es una facultad de libre ejercicio, sino que es el principal dique de contención frente a la

[150] Sirva como ejemplo lo acontecido con el algoritmo que, en Reino Unido, determina las calificaciones de acceso para acceder a formación superior, cuya decisión de reajustar las calificaciones de los estudiantes generó una notable polémica y, finalmente, hubo de ser enmendada, por los sesgos que se intuían en su decisión, sobre el particular, vid. https://www.theguardian.com/education/2020/aug/13/almost-40-of-english-students-have-a-level-results-downgraded. (Última consulta: 20/10/2021).
Por su parte, la utilización de algoritmos para determinar la capacidad financiera y la probabilidad de impagos de un consumidor de crédito es más que conocida, como lo es, el uso de estas herramientas en los seguros de salud. Y, cada vez se utilizan más en el ámbito laboral para la selección de personal.

capacidad disolvente de las esferas personales que los ingenios de la era digital facilitan.

Además, los usos de la información exteriorizada no solo afectan a ese derecho de control sobre la proyección externa del ser, que el TCFA denominó derecho a la autodeterminación informativa. Muchos otros derechos fundamentales también son susceptibles de verse afectados por ellos.

De hecho, antes del derecho a la protección de datos, surgió la cuestión concerniente a la protección de los derechos (la vida privada o la intimidad, pero también otros, como la libertad ideológica, la religiosa o el derecho a la salud, por mencionar los más significativos) frente al tratamiento de los datos. Que estas regulaciones fuesen consideradas como una proyección de la intimidad no es casual, pues, entre los derechos amenazados por el tratamiento de datos, el de la vida privada era el más evidente. Sobre el mismo objeto, la información personal, concurren diferentes derechos, expectativas y amenazas, lo que dio lugar a una regulación omnicomprensiva como respuesta a esa situación.

El derecho a la protección de datos es una pieza más, acaso la principal, de los sistemas de protección frente a la utilización de información personal por terceros, sean particulares, empresas o los estados. Es un derecho que se integra en la legislación preexistente, que toma de ella los elementos que lo caracterizan, pero que no los absorbe por completo. No hace desaparecer los peligros y los riesgos, pero condiciona el enfoque y el modo en que se han de afrontar esos desafíos.

Así, la actual concepción del derecho a la protección de datos es un precipitado de respuestas legislativas y judiciales que ponen de manifiesto la importancia que, en este derecho, tiene el contexto, tanto en su aplicación, como en su propia definición. La autonomía personal, en su vertiente de autodeterminación informativa, se ha canalizado, a lo largo de los años, de diferentes modos, adoptando diferentes fisionomías en función del momento y de la cultura jurídica sobre la que se proyecta. Las diferencias entre la concepción europea y la estadounidense, son el reflejo más elocuente.

La densidad de la regulación europea, su esfuerzo constante por configurar un sistema de facultades, principios, garantías y sanciones comunes, es el producto de un modo particular de entender el derecho, vinculado a la idea de estado social y a una dimensión más comunitaria o

republicana del mismo. Además, también trae causa de la necesidad de compaginar ese modelo garantista con el aprovechamiento de las oportunidades económicas que el tratamiento masivo de la información supone. Tanto las Directrices de la OCDE, como el Convenio 108 –también en su versión actualizada– responden a esta doble lógica.

A nivel global, es previsible que la necesidad de convergencia y la búsqueda de puntos de intercambio y encuentro que permitan mantener el flujo de datos imprescindible para alimentar la creciente industria digital, fuercen el entendimiento y termine por aproximar las diferentes realidades jurídicas.

CAPÍTULO III. EL ECOSISTEMA EUROPEO DEL DATO Y SU IDIOSINCRASIA

«Europa puede hacer suya esta transformación digital y establecer las normas mundiales en materia de desarrollo tecnológico. Y, lo que es más importante, puede hacerlo a la vez que garantiza la inclusión y el respeto de todos. La transformación digital solo puede funcionar si está al servicio de todos, y no solo de unos pocos. Será un proyecto auténticamente europeo —una sociedad digital basada en los valores europeos y en las normas europeas— que pueda inspirar en verdad al resto del mundo»[1].

1. El modelo[2] europeo de protección

Un estudio meramente abstracto del derecho a la protección de datos nos llevaría, en el mejor de los casos, a un conocimiento hipotético y poco realista del mismo. Para este derecho, el momento, el espacio y el contexto son factores tan determinantes que obligan a seleccionar previamente el marco de referencia en el que se sitúa. En nuestro caso, el sistema de protección jurídica frente al tratamiento de datos diseñado por la Unión Europea será nuestro objeto de estudio. Por esta razón, cuando, a partir de este momento, se haga mención a otros modelos de protección de origen europeo, como el Convenio 108, se explicitará expresamente.

La noción europea del derecho a la protección de datos es claramente deudora de su configuración inicial. Su desarrollo normativo viene pautado por la sucesiva implementación de fórmulas legales de protección de los derechos de la ciudadanía, frente a las amenazas derivadas del tratamiento de datos personales y un uso inadecuado o abusivo de los mismos. El dato, era y sigue siendo, el eje central de la regulación, lo que ocasionó una acusada tendencia hacia la especialización normativa.

La protección de datos en Europa se configuró como el derecho destinado a asegurar la administración de la proyección externa de la identidad que se realiza a través de datos de carácter personal. Con esta base regulatoria como premisa, se ha convertido en el principal modelo de referencia en la materia. Es el más completo y garantista, así como el más

[1] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al comité Económico y Social Europeo y al Comité de las Regiones. Configurar el futuro digital de Europa.

[2] A lo largo de esta Tesis, se utilizarán los conceptos "modelo de protección" y "sistema de protección" como sinónimos. Ambos harán referencia al conjunto de previsiones normativas destinadas a ofrecer un marco de protección frente al tratamiento de datos personales.

influyente a escala global, al punto de inspirar la regulación de otros muchos países no pertenecientes a la Unión.

La UE ha articulado, y sigue desarrollando, un entramado normativo cuya finalidad es constituir «un modelo de referencia de una sociedad empoderada por los datos para tomar mejores decisiones, tanto en el ámbito empresarial como en el sector público»[3].

En el marco de la Estrategia Digital de la UE[4], se reserva un espacio destacado para la Estrategia Europea de Datos[5], así como para las medidas destinadas a disciplinar el uso de la inteligencia artificial. Las bases del futuro digital se están creando ahora (en la segunda y tercera década del siglo XXI). La UE pretende aprovechar este momento de transformación para consolidarse como una referencia mundial en la economía y el desarrollo digital, sin que la calidad de vida y la garantía de los derechos de sus ciudadanos se vean damnificados en el proceso.

En el ecosistema europeo de tratamiento de la información, el Reglamento General de Protección de Datos ocupa una posición privilegiada. Su ascendencia como referencia normativa es innegable, sin embargo, no es una *rara avis*, ni la única norma a considerar; existe todo un entramado regulatorio cuya importancia no debe verse eclipsada por su fulgor.

---

[3] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. Puede consultarse en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066. (Última consulta: 20/10/2021).
La información, personal o no, es el centro de la economía digital. Su uso y potencialidades se han convertido en un elemento estratégico de primer orden en la lucha por la hegemonía en la era digital. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. Puede consultarse en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066. (Última consulta: 20/10/2021).

[4] Tanto la Estrategia Digital Europea, como los objetivos digitales de la Década Digital de Europa están disponibles en el siguiente enlace: https://www.consilium.europa.eu/es/policies/a-digital-future-for-europe/. (Última consulta: 20/10/2021).

[5] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. Puede consultarse en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066. (Última consulta: 20/10/2021).

Con todo, el acervo legislativo europeo dista mucho de ser una obra cerrada. Como Martínez Martínez atinadamente apunta, «las tecnologías de la información […] generan nuevas realidades en ocasiones impredecibles salvo para la ciencia ficción. Ello obliga a un doble esfuerzo en materia regulatoria. De una parte, resulta imprescindible sujetar estos procesos de innovación al marco normativo preexistente. […] De otra parte, resulta evidente que se requieren adaptaciones que vienen determinadas por distintos factores. […] [Consecuentemente] las delegaciones normativas específicas y las necesarias adaptaciones que son admisibles en el límite del margen de apreciación, multiplican la producción normativa» (Martínez Martínez, 2021b, párrs. 2 y 3).

El conjunto de normativas que inciden en el tratamiento de la información personal es un conglomerado vivo, de volumen creciente y en evolución/revisión constante. Esa necesidad de ajuste alcanza, incluso, a normativas relativamente recientes, como es el caso del RGPD. El dinamismo de la era digital se proyecta sobre el ordenamiento jurídico, obligando a un trabajo de permanente adecuación, revisión y ampliación del campo de actuación normativo.

Sin embargo, «no es posible adoptar una nueva cultura ya confeccionada. Uno ha de esperar a que crezca la hierba que alimentará a las ovejas que darán la lana con la que se hará un abrigo nuevo» (Eliot, 2003, p. 186). La adopción de una medida normativa ajena a la práctica jurídica habitual siempre entraña un riesgo. Los actores a los que se dirige pueden tener dificultades para asimilar –al menos en los primeros compases– el nuevo paradigma introducido por el cambio regulatorio, por resultarles extraño a su bagaje cultural y tradición jurídica. La regulación no tiene un efecto taumatúrgico.

En este sentido, cabe preguntarse cuál es la «cultura constitucional»[6] europea respecto del derecho a la protección de datos y, por tanto, si existe un sustrato común cuya alteración pueda suponer una desnaturalización del modelo. Si fuese así, habrá cambios que debieran ser evitados para no introducir elementos extraños a la idiosincrasia europea. Interrogarse acerca de las bases de la cultura jurídica común en materia de protección

[6] Conforme al planteamiento Häberle, «la Constitución no es tan sólo un texto jurídico o una regla normativa de trabajo, sino también expresión de un proceso cultural en desarrollo, medio para la expresión cultural de un pueblo, espejo de su herencia cultural y fundamento de sus esperanzas» (Häberle, 2008, p. 349).

de datos y por los elementos nucleares que la integran no es, en consecuencia, un mero ejercicio de retórica.

Como hemos ido viendo (Capítulo II), hay ciertos elementos que caracterizan al sistema europeo de protección de datos. El reconocimiento de este derecho como un derecho autónomo, y no como una manifestación de la vida privada o como parte de un macroderecho, como la *privacy* estadounidense. La regulación europea tiene carácter general, y busca establecer un sustrato común aplicable a todo tipo de tratamientos (en oposición a sistemas eminentemente autorregulatorios), además, su aplicación es horizontal, teniendo efecto también sobre las relaciones *inter privatos* (en contraposición a modelos exclusivamente verticales). La protección de los derechos y libertades o la atribución de un poder de control y disposición son otros rasgos identificadores que dan forma y contenido al derecho fundamental.

No cabe duda de que, a la hora de diseñar el modelo de protección, cuestiones como el concepto de dato o el rol que desempeñaran las categorías especiales –en caso de reconocerse– son decisiones estratégicas con un impacto real en la garantía del derecho de toda persona «a la protección de los datos de carácter personal que la conciernan» (art. 8.1 CDFUE).

Pero, como Kahn ha puesto de manifiesto, «*all of law's text are works of fiction. Each sustains an imaginative world by representing it as our world. To every such imagined world, we can, and often do, imagine alternative worlds. The turn to fiction is not, then, a turn away form law, but only another way of examining the constructed character of our political universe and of our identity within that universe. What we know something to be sets the discursive moves we are prepared to make or accept about it. This is true of individuals and of institutions. Fiction can show us the contingent character of these beliefs; it show us that we can always imagine the world differently. At best, however, it also shows us the difficulty of shedding our perceptions and changing our settled expectations*» (Kahn, 1999, pp. 126-127).

El Derecho también es la representación de una identidad, de un modo de entender y afrontar la realidad. Las normas son un reflejo de los contextos en los que se insertan y permiten identificar las características

del marco cultural que las ha generado (Häberle, 2001, pp. 11-16)[7]. Por este motivo, con independencia del necesario respeto formal al contenido sustantivo del derecho, no deben dejar de valorarse la compatibilidad de los cambios que se quieran introducir, con el fin de evitar efectos no deseados. Una reforma mal diseñada puede hacer inoperantes las medidas introducidas.

La viabilidad de realizar algún tipo de cambio en relación con el concepto de dato o las categorías especiales, precisa de la cognición de la idiosincrasia del modelo europeo de protección. Para ello, se examinarán los elementos definitorios del RGPD. Adicionalmente, se evaluará el modo en que otras normativas europeas abordan la protección frente al tratamiento de la información personal.

2. La "europeización"[8] del derecho a la protección de datos. Los tratados y la Carta de Derechos Fundamentales

2.1. La creación de un sistema europeo de protección

2.1.1. La construcción del mercado interior como impulso. Primeros pasos en la forja del sistema europeo de protección de datos: Schengen

La Unión Europea ha sido/es un agente dinamizador y transformador del modo de entender el derecho a la protección de datos. En los últimos años, su papel en la evolución de este derecho es equiparable, en muchos sentidos, a la función de creación y consolidación que, en los años setenta y ochenta, tuvieron las normativas y pronunciamientos jurisprudenciales comentados en el Capítulo II. Desde

[7] Si bien Häberle plantea esa vinculación entre la cultura y la ciencia jurídica en el marco de su teoría de la Constitución, lo cierto es que como doctrina resulta plenamente trasladable al plano legislativo, especialmente en materia de derechos.

[8] Como Olsen ha puesto de manifiesto, la denominación europeización tiene diferentes significados y usos, (Olsen, 2002). En este caso, se utiliza para reflejar la capacidad de la UE para establecer, con carácter vinculante, el marco normativo de una materia concreta.
Sobre el proceso de europeización del derecho a la protección de datos, vid. el sistemático y detallado artículo de Martínez López-Sáez, (Martínez López-Sáez, 2018a).

los años ochenta[9], la UE ha ido cobrando protagonismo como motor de cambio e impulso de los sistemas de protección frente al tratamiento de datos. Inicialmente, se ha circunscrito a su territorio, si bien, tras la aprobación del RGPD, puede afirmarse que su modelo se ha convertido en parámetro de referencia global.

El rol desempañado por la UE tiene como motor de impulso la consolidación del mercado interior, reforzado por la función vital que la libre circulación de datos desempeña en la estrategia digital europea[10]. La aproximación normativa, el establecimiento de unos parámetros comunes, han sido/son la razón de ser de los diferentes productos normativos que han ido moldeando el sistema de protección de datos europeo. En este sentido, el Acuerdo Schengen[11] (directamente) y el Convenio 108 (por

[9] Pese a que sería el Acuerdo Schengen (1985) con el que se comenzaría a regular en serio sobre protección de datos, no debe dejar de señalarse que, desde la segunda mitad de los años setenta, comienzan a gestarse iniciativas en el seno del Parlamento Europeo (PE) que muestran la preocupación por los efectos de la informática en la garantía de los derechos. Sería el caso de la Resolución del Parlamento Europeo de 21 de febrero de 1975, «*sur la protection des droits de la personne face au developpement des progres techniques dans le domaine de l' informatique*» [sobre los derechos de la persona frente al desarrollo de los progresos técnicos en el ámbito de la informática], puede consultarse, la versión en francés, en, DO C 60 de 13.3.1975, p. 48.
https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1592737792063&uri=CELEX:51974IP0487. (Última consulta: 20/10/2021).
En la misma línea de precedentes de los años setenta se incardina la creación, el 18 de mayo de 1977, de una Subcomisión Informática y derechos de la persona en el marco de la Comisión Jurídica del Parlamento. Sobre esta y otras iniciativas desarrolladas por el PE en los años setenta y la primera mitad de los ochenta, vid. (Guerrero Picó, 2005, pp. 295-296).

[10] Las líneas estratégicas de la UE para afrontar los desafíos de la era digital abarcan diferentes fases temporales y temáticas. Así, la promulgación del RGPD se incardina en la consolidación del *Digital Single Market*, elemento central de la estrategia europea para el período 2014-2019, vid. https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market. (Última consulta: 20/10/2021).
En la actualidad, la UE está trabajando en la conformación del futuro digital de Europa y en el diseño de una transición digital que asegure la «*European technological sovereignty*» (p. 2 del *Shaping Europe's Digital Future*, elaborado por la Comisión Europea, puede consultarse en: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf). (Última consulta: 20/10/2021).
En la consecución de este ambicioso objetivo, los datos desempeñarán un papel crucial:
La Estrategia europea de datos (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066&qid=1606207978191&from=ES),
tiene, como líneas principales de actuación, la gobernanza de los datos (la Comisión ya ha elaborado una propuesta de reglamento sobre la materia, puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020PC0767&from=EN) y la consolidación de un mercado único de datos, cuyos objetivos pueden consultarse en: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es. (Última consulta: 20/10/2021).

[11] Sobre el origen del Acuerdo y el Convenio Schengen, su fundamento e historia, vid. (Van Outrive, 2001).

remisión) constituyen el punto de partida del proceso regulatorio europeo sobre tratamiento de datos personales.

El Acuerdo de Schengen, de 14 de junio de 1985, tenía como finalidad garantizar la libre circulación de personas, mercancías y servicios[12]. En su redacción inicial, no se hacían previsiones en materia de protección de datos personales, más allá de los habituales llamados para reforzar la cooperación y el intercambio de información en la lucha contra la criminalidad organizada. Esta situación cambió notablemente con la firma del Convenio de aplicación del Acuerdo de Schengen, de 19 de junio de 1990 (en adelante, Convenio Schengen)[13] que constituye su complemento indispensable.

La consecución del espacio de libre circulación requería la transmisión de información, incluida la de carácter personal, pues, resulta imprescindible para asegurar el control de los flujos de personas[14] en un amplio territorio sin fronteras interiores. Nació, así, el «Sistema de Información de Schengen» (arts. 92-119 del Convenio Schengen). Este, posibilita que «las autoridades designadas de las Partes contratantes, mediante un procedimiento de consulta automatizado, dispongan de descripciones de personas y de objetos, al efectuar controles en la frontera y comprobaciones y otros controles de policía y de aduanas […], así como, […] a efectos del procedimiento de expedición de visados, de expedición de permisos de residencia y de la administración de extranjeros en el marco de la aplicación de las disposiciones sobre la circulación de personas»[15].

---

[12] Acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985. Diario Oficial n° L 239 de 22/09/2000 p. 0013 – 0018. Puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:42000A0922(01)&from=EN. (Última consulta: 20/10/2021).

[13] El Convenio Schengen entró en vigor en 1995. Diario Oficial n° L 239 de 22/09/2000 p. 0019 – 0062, puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A42000A0922%2802%29. (Última consulta: 20/10/2021).

[14] Los datos transmitidos se utilizarían para cuestiones de seguridad y prevención del delito, pero también para motivos de carácter humanitario, como pueden ser las solicitudes de asilo, vid. art. 38 Convenio Schengen u otras funciones de gestión, como puede ser la expedición de permisos de residencia.

[15] Art. 92.1 Convenio Schengen.

El éxito del Sistema pasaba por la provisión de una serie de informaciones de carácter personal[16], cuyo tratamiento gozase de «un nivel de protección […] que […] [fuese], al menos, igual al que se desprende de los principios del Convenio del Consejo de Europa de 28 de enero de 1981»[17]. Para lograrlo, era necesario homogeneizar las regulaciones en materia de protección de datos, reforzando y ampliando las previsiones de un Convenio 108, al que se tomaba como referencia[18]; además, se requería la implementación de autoridades de control independientes[19].

La consolidación del tratamiento de datos como un elemento estratégico en la construcción del mercado interior motivó el desarrollo de sistemas jurídicos de protección cada vez más uniformes, con los que limitar las disfuncionalidades y facilitar el flujo de información. Si la UE no quería quedar rezagada respecto de las otras potencias globales en la carrera por dominar la era digital[20], la aproximación normativa entre los Estados miembros era ineludible. El Acuerdo y, sobre todo, el Convenio Schengen supusieron un impulso esencial al proyecto europeo de vida en común y, en lo que aquí nos interesa, fueron el catalizador para la generalización de las previsiones en materia de protección de datos[21].

---

[16] El Sistema incluiría, conforme al art. 94.3 del Convenio, las siguientes categorías de datos personales: «a) el nombre y los apellidos; en su caso, los alias registrados por separado; b) los rasgos físicos particulares, objetivos e inalterables; c) la primera letra del segundo nombre; d) la fecha y el lugar de nacimiento; e) el sexo; f) la nacionalidad; g) la indicación de que las personas de que se trate están armadas; h) la indicación de que las personas de que se trate son violentas; i) el motivo de la inscripción; j) la conducta que debe observarse».

[17] Art. 126 del Convenio Schengen. En el mismo sentido apuntan los arts. 38.12, 117.1del Convenio Schengen.

[18] Al punto de ser «un paso más en el contenido del artículo 12 del Convenio de 1981» (Rebollo Delgado, 2010, p. 308), destinado a disciplinar el flujo transfronterizo de datos.

[19] La incorporación de esta garantía institucional por parte de los Estados miembros vino fomentada por el Convenio Schengen (art. 115.1). Este preveía la creación de una autoridad de control común integrada por representantes de aquellos. El modelo de Autoridad común tomó como referencia las previsiones del Convenio 108 y la Recomendación 15 de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía.

[20] Al igual que en los años 90 y en las primeras décadas del siglo XXI la regulación y el tratamiento de datos fueron/son el caballo de batalla global por la hegemonía en la esfera digital. La Inteligencia Artificial lo es y lo será con mayor intensidad en las próximas décadas. Así lo ha puesto de manifiesto la Presidenta de la Comisión Europea, Ursula von der Leyen, en la presentación, el 19 de febrero de 2020, del Libro Blanco sobre Inteligencia Artificial. Pueden consultarse las declaraciones de la Presidenta en:
https://ec.europa.eu/commission/presscorner/detail/en/speech_20_294.
Puede consultarse el Libro Blanco sobre Inteligencia Artificial en:
https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. (Última consulta: 20/10/2021).

[21] La influencia en el desarrollo de legislación sobre protección de datos se refleja en que, durante la primera mitad de los años 90, números países europeos promulgaron, o

2.1.2. La armonización como herramienta: La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995

La remisión al Convenio 108 fue insuficiente para lograr un nivel de uniformidad normativa adecuado, ni siquiera con el estímulo del Convenio Schengen. Se hizo necesaria una norma que precisase, ampliase y actualizase[22] las previsiones del Convenio 108[23] y, sobre todo, ofreciese un marco regulatorio que no generase trabas a la circulación de datos en la esfera comunitaria[24].

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva) fue la respuesta de la UE, amén del primer instrumento genuinamente comunitario sobre la materia. Su fundamento y finalidad están íntimamente conectados con los objetivos generales de

actualizaron, sus normativas sobre la materia. Así, Alemania en 1990; Dinamarca en 1991; también 1991 promulgó Portugal su primera ley de protección de datos; Bélgica se dotaría de una ley sobre la materia en 1992, sobre los procesos legislativos derivados del Convenio 108, vid. (Lazpita Gurtubay, 1994, pp. 404-407).
Entre ese listado de países también se debe incluir a España, donde se promulgó la LORTAD (1992), la primera ley de protección de datos española. Para un análisis de la LORTAD y de la normativa complementaria surgida a su amparo, vid. (Marzal Herce, 1996), también (Heredero Higueras, 1996). Sobre los antecedentes de esta ley, vid. (Santamaría Ibeas, 1994). Sobre su tramitación parlamentaria, vid. (Navarro Ruiz, 1992).

[22] Era necesaria una actualización y adecuación a una realidad tecnológica más dinámica, que exigía «*a new generation of data protection legislation. In this new generation the static concept "personal data file" will be replaced by the dynamic concept of "processing personal data". Because in a number of situations processing of personal data will take place without (the creation of) a personal data file*» (Bergfeld, 1996).

[23] La Directiva precisa y amplía «los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad» (Considerando 11 de la Directiva).

[24] En esta línea de trabajo debe incardinarse la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, sustituida por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Sobre los motivos que llevaron al reemplazo de la Directiva del 1997, vid. (Guerrero Picó, 2006, pp. 373-374). Aunque la razón principal no es otra que la ausencia de previsiones adecuadas en dicha Directiva sobre Internet, tal sonoro silencio hacía previsible su brevedad. Sobre las características generales de la Directiva 2002/58/CE, vid. (Herrán Ortiz, 2003, pp. 46-52).

quien la promulga: la construcción y consolidación del mercado interior[25]. Para lograr que el flujo de información y datos no se viese obstaculizado por las divergencias normativas existentes[26], se implementó una directiva de máximos, pues su objetivo era lograr una «armonización completa»[27].

Con la Directiva se colmaron dos objetivos básicos. De una parte, permitió la actualización y desarrollo de las previsiones normativas en materia de protección de datos y, consecuentemente, mejoró «la protección de los derechos y libertades de las personas y, en particular, del derecho a la intimidad»[28]. Por otra parte, al operar como parámetro ineludible para las legislaciones nacionales[29], se propició una aproximación de los sistemas normativos de los Estados miembros.

La protección equivalente fue la llave maestra de la Directiva para remover los obstáculos que pudieran restringir la libre circulación de datos personales y, con ello, consolidar el mercado interior. Este último fue el auténtico detonante de la Directiva, que con ella se lograse, además, un

[25] Sobre la construcción del mercado interior, vid. (Quadra-Salcedo Janini, 2011) o (Pérez de las Heras, 2008).

[26] Considerando 5 de la Directiva.

[27] STJUE asunto C-101/01, asunto Lindqvist, 6 de noviembre de 2003, apdo. 96. En este mismo apdo. del pronunciamiento, el TJUE señala que «la armonización de dichas legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una armonización completa. […] [con la que] la Directiva 95/46 trata de asegurar la libre circulación de datos personales, garantizando al mismo tiempo un alto nivel de protección de los derechos e intereses de las personas titulares de dichos datos». En el apdo. 97, el TJUE concreta las posibilidades de actuación de las legislaciones nacionales, incidiendo en «que la Directiva 95/46 reconoce a los Estados miembros un margen de apreciación en ciertos aspectos y que les permite mantener o establecer regímenes particulares para situaciones específicas […]. No obstante, dichas posibilidades deben emplearse tal y como dispone la Directiva».

[28] Considerando 9 de la Directiva 95/46/CE, en la misma línea, Considerandos 10 y 11.

[29] La transposición de la Directiva 95/46/CE, para la que se concedieron 3 años, no fue sencilla, prueba de ello son los retrasos que hubo en su realización, al punto de llevar a la condena del Gran Ducado de Luxemburgo por parte del Tribunal de Justicia de las Comunidades Europeas, STJCE Asunto C-450/00, Comisión c. Luxemburgo, de 4 de octubre de 2001.

En el caso de España, fue necesario llevar a cabo importantes modificaciones en la LORTAD (Alonso Blas, 1997). La principal consistió en la ampliación de su ámbito de aplicación, que se extendió a cualquier tratamiento de datos personales, resultando indiferente que los ficheros estuviesen automatizados, o no. La ampliación de contenidos (Troncoso Reigada, 2010, p. 137), sumado al elevado número de enmiendas (114) supusieron, sin duda, el golpe de gracia para la LORTAD, (Sánchez González, 2015, p. 230) y llevaron a apostar (Heredero Higueras, 2001) por elaborar una nueva ley: *la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (LOPD). Desde el punto de vista de la naturaleza del derecho, supuso extender su objeto más allá de la mera libertad informática o *habeas data*, cuyo ámbito de actuación viene marcado por el «uso ilegítimo del tratamiento mecanizado de datos» (STC 202/1999, de 8 de noviembre, FJ 2).

marco más adecuado de protección para los derechos de los ciudadanos[30] no dejaba de ser un extra, positivo y deseable, pero, en cualquier caso, secundario. Tan es así que, la Directiva, «más que […] una norma protectora de los derechos de los ciudadanos […] parece ser una norma habilitante para que los operadores, fundamentalmente económicos, desarrollen sus actividades» (Arenas Ramiro, 2006, p. 278)[31].

El camino que las Directrices de la OCDE habían apuntado[32], y que el Convenio 108 comenzó a recorrer, se afianzó. El fundamento de las regulaciones sobre protección de datos ya no se limitaba a la protección de los derechos individuales o a asegurar a la ciudadanía un control sobre sus informaciones personales, sino que cobró un valor estratégico, tanto para la gestión de la política interna, como para el comercio, la economía y la geopolítica internacional. Este factor, de importancia creciente, será desarrollado, ampliado y elevado a la categoría de eje definidor del sistema de protección de datos por el RGPD[33], si bien la Directiva ya apuntaba su transcendencia[34].

Desde el punto de vista normativo, la Directiva mantenía una referencia específica a la intimidad, cuya protección era una de sus finalidades definitorias[35], regulaba el derecho a la protección de datos y extendía su objeto a la salvaguarda de «las libertades y de los derechos fundamentales de las personas físicas»[36]. En definitiva, definía un modelo completo de actuación y protección frente al tratamiento de la información personal.

---

[30] En este sentido, *vid*. (Heredero Higueras, 1997, pp. 69-70).
[31] En la misma línea se manifiestan, entre otros, (Troncoso Reigada, 2010, p. 179) o (Sánchez Bravo, 1998, p. 123).
[32] Vid. Capítulo II de esta tesis.
[33] V. gr. Considerandos 3, 6 y 9 del RGPD. Especialmente significativo es el Considerando 13 RGPD, al establecer como límite infranqueable del derecho a la protección de datos la libre circulación de datos personales en la Unión Europea: "El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales"
[34] Cfr. considerandos 2 y 3 de la Directiva.
[35] Como señaló el TJUE en Linqvist, el objetivo de la Directiva «que consiste en mantener un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad», STJUE asunto C-101/01, asunto Lindqvist, 6 de noviembre de 2003, apdo. 97.
[36] Artículo 1.1 de la Directiva.

2.2. Los Tratados

Los Tratados constitutivos no son ajenos al proceso de consolidación del derecho a la protección de datos. Este ha estado expresamente reconocido en ellos desde el Tratado de Ámsterdam, de 2 de octubre de 1997. Este Tratado convirtió a las «instituciones y organismos» en sujetos pasivos del derecho a la protección de datos, sometiéndolos a la aplicación de las previsiones en materia, de la que, hasta ese momento, estaban excluidas.

El establecimiento de una política firme de protección de datos en el seno de la UE se alineaba con las demandas de mayor transparencia y democratización[37]. El sometimiento de la burocracia europea al deber de garantía y respeto de los derechos de la ciudadanía en el tratamiento de sus datos fue una medida más en el proceso de apertura de las instituciones europeas. En la práctica, supuso la habilitación de mecanismos destinados a permitir que los residentes en la UE ejercitasen, frente a las instituciones, las facultades de actuación inherentes al derecho a la protección de datos.

El art. 286.1 del Tratado Constitutivo de la Comunidad Europea (TCE) fue la plasmación positiva del sometimiento de las instituciones y organismos europeos a las normativas europeas relativas al «tratamiento de datos personales y a la libre circulación de dichos datos». De este modo, además de incluir por primera vez en los Tratados el derecho a la protección de datos, se ampliaban los sujetos obligados. Adicionalmente, en el apartado segundo de ese precepto, se establecía la obligación de contar con un «organismo de vigilancia independiente, responsable de controlar la aplicación de […] [las normativas de protección de datos] a las instituciones y organismos de la Comunidad». Exigencia que sería colmada con la instauración del Supervisor Europeo de Protección de Datos (SEPD)[38].

[37] Vid. (Guerrero Picó, 2005, p. 314). La plasmación normativa de esta exigencia sería el Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

[38] Sobre el Supervisor Europeo de Protección de Datos y sus funciones, además de su web institucional: https://edps.europa.eu/, vid. (Papakonstantinou y De Hert, 2014) o (Hijmans, 2006).

El Tratado de Lisboa sería la siguiente[39] y, por el momento, última etapa en la regulación del derecho a la protección de datos en los Tratados constitutivos. Este Tratado reconoció a la CDFUE el mismo valor jurídico que los Tratados; revisó, amplió y concretó las previsiones del art. 286 TCE, al establecer que «toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan» (art. 16.1 TFUE); residenció en el Parlamento Europeo (PE) y el Consejo la competencia para elaborar «las normas sobre protección de datos de las personas físicas respecto del tratamiento de datos carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos» (art. 16.2 TFUE); y mantuvo la exigencia de contar con autoridades de control del cumplimiento de las normativas de protección de datos (16.2 TFUE *in fine*).

2.3. La Carta de Derechos Fundamentales de la Unión Europea

El derecho a la protección de datos fue, en origen, una pieza al servicio de la consolidación de las políticas comunitarias. Las primeras regulaciones relativas al tratamiento de los datos de carácter personal tienen un marcado contenido económico y político. Las medidas adoptadas por el Acuerdo y el Convenio Schengen, así como por la Directiva 95/46/CE, responden a la consecución de sus objetivos estratégicos, principalmente, el afianzamiento del mercado interior. Con todo, no puede desconocerse el éxito de la Directiva a la hora de lograr cierto grado de armonización normativa –sobre todo en los primeros años– y su enorme utilidad como guía para la efectiva implantación de un modelo propio de protección de datos (Rallo Lombarte, 2019, p. 24).

[39] No se toma en consideración el Tratado por el que se instituye una Constitución para Europa, por no haber llegado a entrar en vigor y, consecuentemente, producir efectos en el estatus jurídico del derecho a la protección de datos.
Con todo, más allá de la posición que dicho Tratado otorgaba a la CDFUE, debe reseñarse que, en el mismo, se situaba a la protección de datos como uno de los elementos definitorios de la vida democrática de la UE (Parte I, Título VI, art. I-51 del Tratado por el que se instituye una Constitución para Europa).
Puede consultarse todo su *iter* legislativo en: https://www.europarl.europa.eu/about-parliament/es/in-the-past/the-parliament-and-the-treaties/draft-treaty-establishing-a-constitution-for-europe. (Última consulta: 20/10/2021).

Sería una *Recommendation*[40] del «grupo de protección de las personas en lo que respecta al tratamiento de datos personales», creado al amparo de la Directiva, (Grupo de Trabajo del artículo 29, GT29)[41], la que pondría la primera piedra en el proceso que culminaría con la inclusión de este derecho en la Carta de Derechos Fundamentales (CDFUE), aprobada en Niza el 7 de diciembre del 2000[42].

El rol de los derechos humanos en la UE, su protección y salvaguarda, ha ido ganando en importancia al compás del fortalecimiento de las instituciones y de la relevancia de las funciones asumidas por la UE[43]. La CDFUE constituye un salto cualitativo en el desarrollo de un sistema europeo de protección de los derechos[44]. Su proclamación en Niza, por más que no fuera jurídicamente exigible, por ser meramente declarativa, no le restó valor como referencia interpretativa para jueces y tribunales[45].

Sin embargo, el verdadero cambio de paradigma se produce con el Tratado de Lisboa (13 de diciembre de 2007), en él se concede a la CDFUE

---

[40] Recomendación 4/99, de 7 de septiembre de 1999 del GT29, *on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights*. Puede consultarse en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp26_en.pdf. (Última consulta: 20/10/2021).

[41] Artículo 29 de la Directiva.

[42] Esta versión inicial puede consultarse en el Diario Oficial de la Unión Europea C 364, de 18 de diciembre del año 2000. El derecho a la protección de datos se regula en el art. 8. Pese a que la CDFUE ha sido actualizada, el contenido de este precepto no ha variado. El texto consolidado puede consultarse en el Diario Oficial de la Unión Europea Nº 53, C 83/01, de 30 de marzo de 2010, p. 389 y ss.

[43] Desde finales de los 60 y, sobre todo, en la década de los 70, la preocupación por los efectos que el proceso de integración pudiera tener en la garantía de los derechos fundamentales ha sido cada vez mayor. Los pronunciamientos del TJUE dan cuenta de ello, v. gr. SSTJUE, asunto C-29/69, Stauder, de 12 de diciembre de 1969; asunto C-4/73, J. Nold, de 14 de mayo de 1974. Además de, por supuesto, la saga Solange, SSTJUE asunto C-11/70, Internationale Handelsgesellschaft mbH c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, de 17 de diciembre de 1970 (Solange I) y asunto C-69/85, Wünsche Handelsgesellschaft GmbH & Co. c. Federal Republic of Germany, de 5 de marzo de 1986 (Solange II) (en ambos la doctrina del TCFA, venía a asegurar el papel de los Estados miembros como garantes de los derechos fundamentales frente a los riesgos derivados de la conformación del mercado interior).
Mangas Martín realiza una detallada descripción de las diferentes fases y peso normativo y simbólico que han tenido los derechos humanos en el proceso que llevaron al Tratado de Lisboa y a la actual Unión Europea, vid. (Mangas Martín, 2008). Sobre la evolución de la defensa de los derechos en la UE, resulta igualmente recomendable, por su claridad, el trabajo de Gill-Pedro, vid. (Gill-Pedro, 2019, pp. 95-205).

[44] Para una exégesis de la misma, de su valor jurídico y simbólico de la Europa de los derechos, vid. (Martín-Retortillo Baquer, 2010).

[45] Prueba de ello es el pronunciamiento del TJUE, STJUE, asunto C-275/06, Promusicae, de 28 de enero de 2008, apdo. 63. La influencia de la CDFUE también se dejó sentir en los Estados miembros, desde el primer momento, como demuestra la STC 292/2000, de 30 de noviembre, en la que el TC español la esgrime como argumento para reforzar la condición de derecho autónomo de la protección de datos (FJ 8).

el «mismo valor jurídico que los Tratados» (art. 6.1 TUE)[46]. Este reconocimiento refuerza su posición en el ordenamiento jurídico europeo, y la eleva por encima de otras previsiones normativas destinadas a la consolidación del mercado interior. El cambio en el estatus jurídico de la CDFUE es evidente, ya no se trata, como con su aprobación en el año 2000, de «mostrar los derechos sin destruir la Unión» (Rubio Llorente, 2002)[47], sino de un compromiso vinculante con su defensa, por más que no haya alcanzado los niveles de exigibilidad y condicionalidad de la actuaciones del TJUE que pudieran esperarse de este *bill of rights* europeo[48]. A los efectos que aquí interesan, en la UE, la protección de datos no es una mera orientación político-jurídica, sino un derecho fundamental.

[46] La posición jurídica de la Carta habría estado aún más reforzada, en el caso de haberse ratificado el Tratado por el que se instituye una Constitución para Europa (puede consultarse todo su *iter* legislativo en: https://www.europarl.europa.eu/about-parliament/es/in-the-past/the-parliament-and-the-treaties/draft-treaty-establishing-a-constitution-for-europe). (Última consulta: 20/10/2021).
De haber entrado en vigor, «la Carta, Parte II del mismo, no sólo se convertiría en instrumento jurídico vinculante, sino en parte sustancial del Derecho originario de la Unión y, por tanto, en parámetro de validez del Derecho» (Díaz Crego, 2005). En lo referente al modo en que se regulaba el derecho a la protección de datos en el Tratado por el que se instituye una Constitución para Europa, vid. (Guerrero Picó, 2005).

[47] Rubio Llorente realiza una exégesis del valor jurídico de la CDFUE tras su aprobación en Niza, además de señalar las opciones posibles que podía llegar a tener en el futuro, vid. (Rubio Llorente, 2002). Sobre el estatus jurídico de la CDFUE, su importancia creciente y el ámbito de aplicación en su configuración actual, vid. (Carmona Contreras, 2016); (Rodríguez-Piñero y Bravo-Ferrer, 2019) o (Linde Paniagua, 2008).

[48] Leczykiewicz llega a calificar a la Carta como «*a lost opportunity to strengthen the EU's constitutional credentials*» (Leczykiewicz, 2019, p. 154). En una línea similar, no tan crítica, pero igual de contundente, se pronuncia Tajadura Tejada, «el contenido de la Carta constituye realmente la traducción jurídica y la expresión política de los principios de legitimidad de la Unión, esto es, del orden material de valores sobre el que la integración europea se fundamenta, [por ende] resulta también evidente que la Carta debería formar parte del cuerpo del Tratado de la Unión Europea. Y, sin embargo, […] se cedió para evitar el veto de» Estado antieuropeístas y nacionalistas [(en aquel momento, Reino Unido y Polonia)]» (Tajadura Tejada, 2010, p. 277), de modo tal que se debilitó su posición jurídico-política y, con ello, su fuerza.
En términos similares se manifiestan Monereo Atienza y Monereo Pérez consideran que, la exclusión de la CDFUE «del Sistema de los Tratados Fundamentales revisados por el Tratado de Lisboa […] no deja de entrañar un debilitamiento del papel garantista de la Carta, a pesar de ser elevada a rango de norma equiparable a los Tratados de la Unión» (Monereo Atienza y Monereo Pérez, 2012, p. XIII).
A pesar de todo, como apunta, acertadamente, López Castillo, «la Carta, se integre formalmente o se siga considerando referente hermenéutico sin mayor énfasis, deviene parte significativa del parámetro de *ius* fundamentalidad» (López Castillo, 2019, p. 57) del ordenamiento jurídico europeo.

La CDFUE singulariza al derecho a la protección de datos como un derecho con características propias, por más que pueda estar «íntimamente ligado al derecho al respeto de la vida privada»[49].

Su artículo 8 establece que:

«1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente».

Ha de resaltarse el hecho de no configurar al derecho a la protección de datos como uno de los contenidos posibles del artículo 7 de la CDFUE –del mismo modo que lo hace en CEDH en su art. 8, relativo a la vida privada y familiar, a la inviolabilidad domiciliaria y al respeto de las comunicaciones personales–. Esta decisión es toda una declaración de intenciones, y la constatación del carácter autónomo del derecho a la protección de datos, a pesar de existir una identidad literal absoluta entre lo previsto en el art. 7 de la CDFUE y el art. 8.1 del CEDH[50]. Este reconocimiento expreso supone un salto cualitativo para el derecho a la protección de datos.

El conjunto formado por el art. 16 del TFUE, complementado con lo previsto en el artículo 39 del Tratado de la Unión Europea (TUE)[51], y el art. 8 de la CDFUE, es el anclaje "constitucional" de la pléyade de previsiones

[49] STJUE asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke y Eifert c. Land Hesse, de 9 de noviembre de 2010, apdo. 47. Sobre la distinción entre el objeto de los arts. 7 y 8 de la CDFUE existe una profusa doctrina, sirvan para ilustrarla los trabajos de: (Blume, 2010); (González Fuster y Gellert, 2012); (Kokott y Sobotta, 2013); (Tzanou, 2013)o (Dalla Corte, 2020) .

[50] Tanto art. 7 CDFUE como el art. 8.1 CEDH establecen que, «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia».

[51] Art. 39 TUE: «De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes».

normativas (reglamentos, directivas, recomendaciones y protocolos técnicos) que conforman el entramado jurídico-normativo de la UE en esta materia. Son el fundamento jurídico sobre el que se erige el régimen «*omnibus*» (Klamert, 2019, p. 407) destinado a disciplinar el tratamiento de la información personal.

El derecho a la protección de datos ha pasado de ser un elemento necesario para «el establecimiento y funcionamiento del mercado interior» (Considerando 3 de la Directiva 95/46/CE), a un derecho fundamental autónomo proclamado en las bases "constitucionales" de la UE. El art. 8 de la CDFUE y el art. 16 del TFUE son el fundamento del RGPD y el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, (en adelante, Reglamento 2018/1725)[52].

En lo esencial, el derecho a la protección de datos ha dejado de ser una materia a disciplinar por los Estados miembros para convertirse en «un derecho exclusivamente europeo sometido a la excluyente normación de la Unión Europea y a la fijación de canon hermenéutico por el TJUE» (Rallo Lombarte, 2019b, p. 70). Los dos Reglamentos[53] mencionados regulan sus elementos basilares, lo concretan y precisan. No es un mero cambio de rol (hacia una posición más activa de la UE), ni la confirmación de la teoría de la «*reverse Solange*» propuesta por von Bogdandy, Kottman, Antpöhler Dickschen y Hentrei[54]. Es una auténtica traslación del centro normativo del derecho.

[52] Tanto el Considerando 1 del RGPD como el Considerando 1 del Reglamento 2018/1725 señalan que: «La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan». Convirtiendo a dichos preceptos en sus normas habilitantes.

[53] Cuando se utilice Reglamentos en mayúscula estará referido al RGPD y al Reglamento 2018/1725.

[54] Estos autores proponen, con el art. 2 del TUE como fundamento, una reversión de la doctrina Solange. Conforme a su teoría, en caso de que los Estados miembros no respetasen el contenido de los derechos fundamentales, aun cuando se tratase de un supuesto que no fuese subsumible en el ámbito de aplicación de la CDFUE, los ciudadanos podrían acudir a los tribunales nacionales y al TJUE pues estaría en juego la «*substance*» de la ciudadanía europea (von Bogdandy, Kottmann, Antpöhler, Dickschen, y Hentrei, 2012).

El RGPD culmina la «mutación […] [d]el sistema constitucional de fuentes al producirse una auténtica abducción del derecho constitucional» (Rallo Lombarte, 2019b, p. 70). Los Estados miembros pueden legislar sobre aquellos aspectos de su competencia, sin embargo, lo nuclear, los estándares de protección, ya se han fijado por la UE[55].

Estamos ante un devenir pionero, que puede no ser el único[56] (el secreto de las comunicaciones acaso pudiera ser el siguiente, a tenor de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre privacidad y comunicaciones electrónicas))[57].

La Unión se presenta, en el espacio digital y frente a las entidades transnacionales que lo dominan, como el poder más apropiado para «asegurar […][una] libertad igual, efectiva y para todos» (Requejo Pagés, 2016, p. 265), acaso como el ¿único? Leviatán capaz de contener al Ciberleviatán.

[55] Para Lucas Murillo de la Cueva, la configuración europea del derecho a la protección de datos va a operar como parámetro mínimo también en aquellos ámbitos a los que no se extienda el Derecho de la UE, si bien mantiene un punto de prudencia, al indicar que «es la conclusión más segura» (Lucas Murillo de la Cueva, 2021, p. 312).
Jurídicamente, sería posible que los Estados miembros configurasen un sistema paralelo para aquellos espacios de su exclusiva competencia, sin embargo, en la práctica no sería efectivo no operativo. No solo sería entrañaría una dificultad aplicativa enorme derivada de la confusión que generaría dos concepciones diferentes del mismo derecho fundamental, sino que los problemas comenzarían en su origen, pues se antoja una tarea titánica articular un modelo de protección que fuese constitucionalmente aceptable en un estado democrático y que, a la vez, tuviese la suficiente singularidad como para diferenciarse de la configuración europea.

[56] Como apunta De Gregorio, nos encontramos en una «*new constitutional phase in the EU* […] *based, first, on the codification of the CJEU's efforts to protect fundamental rights in the information society and, second, on the limitation of online platforms' powers through the implementation of legal instruments aimed at increasing the degree of transparency and accountability in online content moderation and data processing*» (De Gregorio, 2021, p. 58).

[57] Puede consultarse en la Propuesta de Reglamento sobre privacidad y comunicaciones electrónicas en:
https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf. (Última consulta: 20/10/2021).

3. El Reglamento General de Protección de Datos: la plasmación normativa de la cultura jurídica europea

3.1. El RGPD, el buque insignia del modelo europeo de protección de datos

Desde su entrada en vigor en el año 2016 y, sobre todo, desde que es aplicable (25 de mayo de 2018), el RGPD se ha convertido en la norma de referencia en materia de protección de datos en la Unión Europea. Es la previsión normativa que ha alcanzado mayor relevancia y *auctoritas* en el amplio espectro de las regulaciones sobre tratamientos de datos, «*the new gold standard for data protection*» (Mantelero, 2020)[58], un parámetro de referencia global. Es el producto de todas las necesidades, retos y exigencias estratégicas de las que trae causa[59], aunque, formalmente, se presente como la respuesta normativa al agotamiento de una Directiva que, transcurridos más de veinte años, resultaba poco adecuada para hacer frente a una realidad mucho más compleja que aquella que buscaba regular en 1995; baste con señalar que Google ni siquiera existía[60].

Renovar la Directiva y establecer «un marco más sólido y coherente para la protección de datos en la Unión Europea» (Considerando 7 RGPD) era ineludible[61]. La Directiva, tan útil en los primeros años para la consolidación del espacio de libertad, seguridad y justicia (Sánchez Domingo, 2017, pp. 23-27), resultaba ahora un obstáculo para el desarrollo

---

[58] En la misma línea apuntan (Gobeo, Fowler, y Buchanan, 2018).

[59] El proceso de reforma de la Directiva que culminaría con la aprobación del RGPD comenzó con el Commissión Staff Working Paper Impact Assessment de 2012 (SEC/2012/0072 final), puede consultarse en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0072. (Última consulta: 20/10/2021).
En ese primer documento ya están presentes las carencias de la Directiva que llevarían a la adopción del RGPD, así, se pone el acento en la inseguridad jurídica que genera la fragmentación del marco normativo, se señalan las dificultades de los individuos para mantener el control sobre las informaciones a ellos referidas y se incide en las barreras que la regulación de la Directiva representa para el aprovechamiento económico del uso de la información personal.
Sobre los objetivos del RGPD y su proceso de elaboración del RGPD, vid. (AA. VV., 2015), (Piñar Mañas, 2016b) y (Pérez Miras, 2018, pp. 340-350).

[60] Google fue fundado el 27 de septiembre de 1998. El fenómeno de las redes sociales es de mediados de la primera década del 2000 (v. gr. Facebook: 2004; Twitter: 2006).

[61] A las consecuencias del inexorable paso del tiempo han de agregarse otras de naturaleza estrictamente jurídica, como las dificultades que, para el flujo de datos en el espacio europeo, generaban las divergencias normativas entre los Estados miembros; o la ausencia de un marco regulatorio adecuado para hacer frente al crecimiento exponencial de los flujos de datos con terceros estados, con el riesgo adicional que comporta que los datos se traten en un país con un nivel de protección menor. Para una descripción y justificación detallada de cada uno de los males que acuciaban al marco normativo europeo pre-RGPD, vid. (Troncoso Reigada, 2012, pp. 30-68)

del mercado interior y la economía digital[62]. Era imperativo disponer de una solución jurídica que, desde el respeto a los derechos fundamentales, reforzase la estrategia digital europea y diese respuesta a los nuevos desafíos.

El reglamento era el instrumento jurídico más adecuado para remover los obstáculos y hacer frente a los retos de la era digital. Ese instrumento normativo, merced a su aplicabilidad directa y obligatoria (art. 288.2 TFUE)[63], permitía homogenizar la protección en todos los Estados miembros mediante el establecimiento de un modelo común[64]. Con él se favorecía la libre circulación de datos y se facilitaba el aprovechamiento económico de la gestión de la información (considerando 9 RGPD). Además, el RGPD permitió incorporar al derecho positivo el fructífero acervo jurisprudencial del TJUE.

El RGPD es la normativa europea de referencia para todos los Estados miembros. Sus previsiones constituyen un parámetro obligatorio[65] y sistematizado. Su manto protector se extiende, incluso, a los tratamientos llevados a cabo por compañías residenciadas en terceros estados, cuando estas operen con datos personales de ciudadanos europeos[66]. En definitiva, el RGPD es lo más parecido a una representación normativa de la concepción europea del derecho a la protección de datos.

---

[62] Considerando 2 del RGPD, en el mismo sentido, y más fundamentado, vid. (Díaz Díaz, 2016).

[63] Sobre la eficacia de los Reglamentos existen multitud de trabajos, en general, cualquier manual de derecho de la Unión Europea hace referencia a su aplicabilidad directa y vinculante, v. gr. (Mangas Martín y Liñán Nogueras, 2020, pp. 420-470) o (Urbaneja Cillán, Ferrer Lloret, Soler García, y Requena Casanova, 2020, pp. 192-201).

[64] Como pone de manifiesto Lynskey (Lynskey, 2020, pp. 355-356), la disparidad en la aplicación del derecho a la protección de datos en los diferentes Estados miembros antes del RGPD era notable. Así, no se constataban menciones específicas al derecho previsto en el art. 8 de la CDFUE ni en Bulgaria, ni en Hungría, ni en Polonia. En Eslovenia su invocación era poco frecuente, especialmente si se compara con la frecuente apelación al art. 8 del CEDH.

[65] Si bien es cierto que la Directiva también supone un límite a la discrecionalidad de los estados miembros (especialmente si se tiene en cuenta que es directamente aplicable en caso de no existir trasposición), la realidad es que un Reglamento, por su aplicabilidad y nivel de exigibilidad, supone un salto cualitativo significativo en el *statu quo* en materia de protección de datos, quedando la normativa estatal como mero complemento de la norma europea, que se convierte en el auténtico marco regulador de referencia. Además de que, «seguramente por primera vez, la regulación de un derecho fundamental […] va a estar contenido en un Reglamento europeo. […] [En una norma que aborda] la práctica totalidad de su disciplina, incluido su contenido esencial» (Piñar Mañas, 2016, pp. 17-18).

[66] Art. 3 del RGPD. Sobre el ámbito de aplicación del RGPD vid. (Voigt y von dem Bussche, 2017, pp. 9-30) o (Palma Ortigosa, 2018a).

3.1.1. El necesario complemento estatal y la idiosincrasia del modelo

El RGPD no es un reglamento al uso, anida en él el alma de una directiva (Medina Guerrero, 2019, p. 256), pues concede a los Estados miembros cierto «margen de maniobra» (Considerando 10 RGPD) en una amplia variedad de temáticas[67]. Las numerosas materias susceptibles de concreción, desarrollo o matización hacen ineludible analizar, conjuntamente, el RGPD con las previsiones nacionales destinadas a complementarlo.

Solo desde un análisis dual será posible comprender, en toda su magnitud y extensión, el marco normativo europeo relativo a la protección de los datos personales. Con todo, la capacidad para establecer previsiones más o menos imaginativas por parte de los Estados ha quedado, en lo esencial, cercenada por el RGPD. Los Estados pueden concretar cuestiones de detalle, pero el núcleo del derecho, sus elementos basilares, han sido fijados por el regulador europeo.

La transversalidad de materias que son susceptibles de verse afectadas por el tratamiento de datos hace de su regulación un juego de equilibrios. Cuestiones como la imposición de sanciones penales, la regulación de las relaciones labores, la consideración de qué es interés público, la afectación de la seguridad nacional, la respuesta frente a catástrofes o problemas de salud pública, la consecución de intereses económicos esenciales o la organización del sistema institucional en el que se han de integrar las autoridades de control exceden las competencias de la UE y, por tanto, el derecho comunitario no puede entrar a disciplinarlas en su totalidad. En esos supuestos, el RGPD o bien ha evitado por completo su regulación o ha dejado en manos de los Estados miembros la capacidad para fijar los límites y alcance de las medidas. En definitiva, hay ciertas cuestiones en las que el RGPD no tiene más remedio que operar como una Directiva.

No obstante, la cautela necesaria para evitar sobrepasar los límites competenciales solo justifica una parte de los, casi, tres centenares de apelaciones al Derecho de los Estados miembros. El legislador europeo es plenamente consciente de que su regulación se proyecta sobre ordenamientos nacionales con características propias. Esto hace que, en ocasiones, tenga cierta deferencia con los Estados miembros y les deje

[67] Sobre los diferentes aspectos en los existen "vacíos regulatorios" susceptibles de ser colmados por los legisladores nacionales vid. (García Mexía, 2016).

margen para establecer limitaciones al tratamiento de determinados datos, como la señalada respecto de los datos genéticos, biométricos y los relativos a la salud (art. 9.4 RGPD) o la eventual limitación del ejercicio de las facultades de actuación previstas en el art. 23.1 RGPD[68]. Otras veces, posibilita que puedan regular una determinada materia –con las previsiones del RGPD como guía– (v. gr. la habilitación para regular el tratamiento de opiniones políticas por los partidos, Considerando 56 RGPD) o, incluso, difiere a los legisladores nacionales la concreción de determinados tratamientos, como sería el caso de los referidos a personas fallecidas (Considerando 27). También deja margen para que puedan establecer ciertos límites al ejercicio de algunos derechos (v. gr. el derecho de supresión art. 17.3.b RGPD), o les habilita a articular los equilibrios y relaciones entre el derecho a la protección de datos y las libertades de expresión e información (Considerando 153 y art. 85 RGPD) o el secreto profesional (Considerando 164 y art. 90 RGPD).

En definitiva, a pesar de disciplinar el contenido nuclear del derecho a la protección de datos y de articular un modelo destinado a establecer unas condiciones comunes en todo el territorio europeo, el RGPD no elimina por completo las singularidades de los derechos internos.

---

[68] Art. 23.1 RGPD: «1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:
a) la seguridad del Estado;
b) la defensa;
c) la seguridad pública;
d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;
e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;
f) la protección de la independencia judicial y de los procedimientos judiciales;
g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;
h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);
i) la protección del interesado o de los derechos y libertades de otros;
j) la ejecución de demandas civiles».

Así, aunque el marco de actuación del RGPD sirve, en gran medida, para alcanzar los fines armonizadores que lo motivaron, cada eventual divergencia regulatoria supone un escollo a superar. Cuestiones como la edad de consentimiento de los menores (que pueden oscilar entre los 13 y los 16 años[69]) generan disonancias[70] que, seguramente, serán objeto de revisión para lograr una mayor cohesión y homogeneidad en los tratamientos y favorecer el flujo de información.

Sin embargo, esas discrepancias son la válvula de escape de los Estados, el método de expresión de su modo de concebir el tratamiento de la información personal y la protección de los derechos. Una eventual reforma deberá considerar los equilibrios entre el mantenimiento de una cierta singularidad nacional y la homogeneidad que el mercado interior demanda.

Por otra parte, en tanto el derecho a la protección de datos es un diamante con múltiples facetas, los Estados, además de poder desarrollar aquellos elementos que la normativa europea les habilita, podrían llegar a reconocer nuevas facultades de actuación a sus ciudadanos, siempre que sean compatibles con las previsiones europeas y, sobre todo, no rebasen los límites por esta definidos.

Con todo, cualquiera que sea la regulación desarrollada por los Estados miembros, habrá de ser compatible con los principios del RGPD, así como con el resto de medidas que marcan la orientación del modelo. Por lo tanto, aunque los Estados pueden –y deben– regular ciertos aspectos del tratamiento de la información personal, no tienen capacidad para alterar su idiosincrasia.

---

[69] Art. 8.1 RGPD

[70] En la Comunicación de la Comisión al Parlamento Europeo y al Consejo acerca de la protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos, de 24 de junio de 2020, la edad es uno de las factores en los que se observa un grado de fragmentación no deseable, por generar incertidumbre. Otros aspectos que incluye esta Comunicación son la conciliación entre libertad de expresión, derecho a la información y protección de datos o las regulaciones relativas a los usos de las categorías especiales. Puede consultarse la Comunicación en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0264&from=EN. (Última consulta: 20/10/2021).

3.2. Los dos pilares del RGPD: La protección de los derechos y la libre circulación de la información

Desde un punto de vista estructural, la salvaguarda de los derechos y la libre circulación de los datos, son los pilares del RGPD[71]. Sin embargo, en la disyuntiva –y eventual conflicto– entre esos dos límites, el segundo de ellos (la libre circulación de datos) parece tener cierta preferencia. Así se puede deducir del apartado tercero del artículo 1 del RGPD: «La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales». «El buen funcionamiento del mercado interior [así lo] exige» (Considerando 13).

Ahora bien, esa posición preferente de la libre circulación ha de entenderse en su debido contexto y dimensión. La prohibición de restringirla no es, en puridad, un criterio interpretativo que pueda hacerse valer ante un eventual conflicto de derechos, sino que se trata de un mandato de optimización dirigido al legislador, especialmente al de los Estados miembros. La libre circulación opera como límite a la capacidad de los legisladores estatales para complementar las disposiciones del RGPD, por lo que su propósito se circunscribe al aseguramiento de la homogeneidad del modelo, sin perjuicio de que los legisladores estatales puedan introducir garantías adicionales o nuevos derechos a los interesados, siempre que no supongan un obstáculo para el fin perseguido.

El RGPD no privilegia la libre circulación. Tan solo la convierte en un límite a las capacidades creativas de los legisladores estatales.

3.3. Un ámbito de aplicación con aspiración de influencia global. La fuerza condicionante del RGPD

En Capítulos precedentes, hemos visto como la ubicuidad de Internet ha propiciado la emergencia de auténticos «continentes virtuales» (Lucena-Cid, 2014, p. 16) que quiebran la base territorial de protección de los derechos. En la realidad virtual, los datos, incluidos los personales, son

[71] Son la piedra de Rosetta con la que ha de interpretarse un modelo destinado a «garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión» (Considerando 10 RGPD).

la moneda de cambio y la materia prima con que se alimenta la Red[72]. No resulta extraño que los estados tengan la tentación de convertir a sus regulaciones en parámetros de referencia global.

Naturalmente, el nivel de impacto e influencia de una determinada regulación dependerá, en última instancia, de la entidad, tamaño e importancia en el mercado, del país o región. Las exigencias jurídicas de un estado pequeño, especialmente si es poco relevante económicamente, difícilmente alterarán las dinámicas globales o inquietarán a las grandes entidades transnacionales que dominan la Red, sin embargo, el marco de actuación fijado por un sujeto geoestratégicamente relevante sí puede afectar a los modos en que se opera con la información personal en el macrocosmos virtual. La UE es uno de los pocos actores con capacidad condicionante real.

El RGPD representa un cambio en el modo de enfocar la protección. Los sujetos intervinientes son el centro de atención, pues, a diferencia de los datos, su lugar en el mundo es más constante. Se transitó de una «Directiva […] centra[da] en dónde están los datos, algo que tenía sentido en 1995 pero que carece de valor en la era de Internet […][a un enfoque focalizado en] dónde está el interesado o dónde tiene su establecimiento principal el responsable del tratamiento, [quedando relegado a un segundo plano el lugar][…] donde se encuentra la información» (Troncoso Reigada, 2012, p. 36).

En esta línea ha de situarse la sentencia Schrems I[73]. Este pronunciamiento supuso un golpe de atención y el espaldarazo definitivo del TJUE al cambio de modelo representado por el RGPD. La invalidez del *Safe Harbour,* y la necesidad de adoptar un nuevo acuerdo que disciplinase las transferencias de datos entre la UE y EEUU[74], reafirmó a la UE como símbolo y expresión de un modo específico de afrontar el tratamiento de la información personal, en el que los derechos de los ciudadanos ocupan un papel central. El mensaje fue claro y contundente: para operar con datos de personas residentes en la UE se ha de garantizar un nivel de protección

[72] Sobre el importante papel de la protección de datos en un mundo globalizado ya había escrito, mucho antes del RGPD, Teresa Freixes, con relación a la Convención de Prüm (Freixes Sanjuán, 2007).
[73] STJUE, Asunto C-362/14, Maximillian Schrems y Data Protection Commissioner, 6 de octubre de 2015.
[74] Sobre las consecuencias de Schrems I y la adopción del *Privacy Shield* vid. (López Aguilar, 2017) y (Ortega Giménez, 2016).

adecuado. El desarrollo digital no puede hacerse a costa de los derechos de la ciudadanía europea.

El ámbito de aplicación territorial del RGPD (art. 3 y capítulo V del RGPD) constituye la constatación de la apuesta de la UE por establecer un sistema de protección que asegure europeos un marco de garantías respetuoso con los derechos de la ciudadanía. No importa quién trate los datos, ni dónde los quiera tratar[75]. Si el tratamiento tiene por objeto datos de personas que residan en la UE, se aplicarán las reglas establecidas en el RGPD o, cuando menos, se ha de asegurar un estándar de protección equivalente.

Con todo, es el apartado segundo del art. 3, el que refuerza la proyección internacional e influencia global del RGPD[76]. Este precepto

[75] Con todo, el RGPD establece que su ámbito de aplicación se extiende a los tratamientos de todas aquellas entidades que tengan un establecimiento. El concepto de establecimiento se establece en el Considerando 22 RGPD, cuando se estipula que «un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto».
La jurisprudencia del TJUE ha ido perfilando el concepto, desde la STJUE asunto 168/84, Bergholz, de 4 de julio de 1985, apdo. 14, donde se consideraba que debía que era necesario que «tanto los recursos humanos como los técnicos necesarios para la prestación de determinados servicios estén disponibles de forma permanente» para considerar que había un establecimiento; hasta la STJUE asunto C-230/14, Weltimmosro c. Nemzeti, de 1 de octubre de 2015, donde se acepta que la presencia de un solo representante del responsable puede ser suficiente. En un término intermedio estaría lo previsto en la STJUE asunto C 131/12, asunto Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014.
Por su parte, en el articulado (art. 4.16 RGPD) se estipulan las características que permiten identificar cual es el establecimiento principal. Este, será «el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal».
Asimismo, el RGPD será de aplicación a los tratamientos en que se utilicen datos de personas que «residan en la Unión». Si bien es cierto que, en este caso, está condicionado a la concurrencia de alguno de los supuestos previstos en el apartado segundo del art. 3, esto es, que el tratamiento esté relacionado con: «a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión».
Finalmente, se incluyen, como susceptibles de regirse por el RGPD, aquellos tratamientos en los que pudiera ser de aplicación el Derecho de los Estados miembros «en virtud del Derecho internacional público». Como puede constatarse, el RGPD incorpora tanto criterios de atribución competencial de base territorial como otros fundados en el elemento subjetivo. Sobre el ámbito de aplicación del RGPD, vid. (Amérigo Alonso, 2019) y (Delgado Caravilla y Puyol Montero, 2018, pp. 19-22).

[76] Art. 3.2 RGPD: «El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

condiciona el uso de información de las personas residentes en la UE al cumplimiento de la normativa europea, aunque, quien trate los datos, no tenga presencia en la UE. A esa previsión debe adicionársele otra, no menos relevante, la relativa a las transferencias de datos a terceros estados y la exigencia de que estos estados cuenten con una protección adecuado (arts. 44-50 RGPD).

Al exigir a las compañías que, al menos para los datos de las personas residentes en Europa, establezcan sistemas de tratamiento con un determinado nivel de protección, se está introduciendo un incentivo para que adopten esas prácticas por defecto. De este modo, la UE aprovecha su posición estratégica en el mercado global[77] para, por un lado, proteger los derechos de su ciudadanía frente a los eventuales abusos de las grandes corporaciones transnacionales que operan en el mercado digital (p. ej. Amazon; Apple; Alphabet Inc.; Facebook; Huawei o Xiaomi) y, por otro, intentar hacer valer su visión (más garantista y protectora de los derechos) respecto al modo en que han de tratarse los datos personales.

Pese a las resistencias (Ryngaert y Taylor, 2020, p. 8) y obstáculos (López Calvo, 2017, pp. 108-109) que pueda encontrar la aplicación extraterritorial de la regulación europea, no cabe dudar de su influencia global, así como de su condición de estándar de referencia para cualquier regulación relativa al tratamiento de los datos personales. Así lo acredita la importante cantidad de modificaciones de los sistemas de tratamiento surgidas a raíz de la aprobación del RGPD. Sirvan para ilustrar esa oleada de cambio, las normativas de Australia (Goggin, Vromen, Weatherall,

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión».

[77] La UE es un mercado de casi 450 millones de usuarios. Además, conforme al I-DESI (*The International Digital Economy and Society Index*), tiene un desarrollo notable de las estructuras digitales. El I_DESI, compara la situación de los 27 estados de la UE con la de otros 18 estados de todo el mundo (Australia, Brasil, Canadá, Chile, China, Islandia, Israel. Japón, México, Nueva Zelanda, Noruega, Rusia, Serbia, Corea del Sur, Suiza, Turquía, Reino Unido y Estados Unidos). En las variables analizadas, (conectividad, habilidades digitales, uso de internet, tecnología digital y servicios públicos digitales) la UE, como conjunto, ocupa una buena posición. Si bien es cierto que, por la heterogeneidad de estados que la conforman, en el cómputo global, no es la mejor (excepto en habilidades digitales). Por otra parte, los 4 estados de la UE que presentan mejores resultados (Finlandia, Dinamarca, ambos con 65 puntos; Luxemburgo y Países Bajos con 62) compiten, cuando no superan, a los mejores a nivel global. España obtiene 47 puntos en este índice, Italia 37, Portugal 41, Francia 51 y Alemania 52. Pueden consultarse todos los datos y el informe completo en: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72352. (Última consulta: 20/10/2021).

Martin, y Sunman, 2019) [78]; Canadá (Benjamin, 2020)[79]; Brasil (Iramina, 2020)[80] o la India, si bien, en este caso, su *Personal Data Protection Bill*, de 11 de diciembre de 2019, «*adopts and further develops many existing principles of EU-style data processing regulation and some aspects of US-style data privacy laws*» (Determann y Gupta, 2019, p. 513). En Chile se está trabajando en la elaboración de una normativa que tiene claras reverberaciones del RGPD (Contreras Vásquez y Trigo Kramcsák, 2019) o (Bauzá Martorell, 2019)[81].

En Estados Unidos, la *California Consumer Privacy Act of 2018*, especialmente desde su modificación por la *California Privacy Rights Act of 2020*[82], es la punta de lanza en la aproximación del modelo estadounidense al europeo (Padín, 2020), pues «*has taken the view that substantive data protection regulations are essential to safeguard the rights and freedom of individuals in a democracy*» (Heward-Mills y Turku, 2020, p. 319). Además, desde el gobierno federal, se está trabajando en la elaboración de una ley federal sobre la materia[83]. Incluso en China se ha dejado sentir la influencia del RGPD, si bien de manera muy atenuada. La *Cyber Security Law of the People's Republic of China* establece un estándar nacional en el que se fomenta el tratamiento de datos conforme a unos principios claramente inspirados en el RGPD. Aunque su finalidad, servir como orientación para las empresas –no para el gobierno–, hace de él un instrumento débil en la salvaguarda de la privacidad, vid. (Chen, Han, y Kipker, 2020)[84].

---

[78] La Privacy Act de 1988 ha sido enmendada en julio de 2020 (Act. Nº. 11, 2020).

[79] La *Personal Information Protection and Electronic Documents Act* de 13 de abril del 2000, ha sido modificada en diversas ocasiones, incluida la modificación de 18 de junio de 2015, por la *Digital Privacy Act*, que incluyó algunas modificaciones, p. ej. en materia de brechas de seguridad, en el sentido que apuntaba el RGPD –en ese momento en tramitación–. No obstante, la normativa canadiense siempre ha sido bastante respetuosa con los derechos de la ciudadanía en el tratamiento de los datos y ha ofrecido una protección similar a la europea.

[80] *Lei* Nº 13.709, de 14 de agosto de 2018, *Lei Geral de Proteçao de Dados Pessoais* (LGPD).

[81] Puede consultarse el texto del Proyecto de Ley que regula el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, en: https://www.senado.cl/appsenado/index.php?mo=transparencia&ac=doctoInformeAsesoria&id=7045. (Última consulta: 20/10/2021).

[82] Como han puesto de manifiesto (Federman, 2020) o (Dhar, 2021).

[83] En septiembre de 2020 comenzaron las primeras audiencias para determinar la necesidad una regulación federal sobre privacidad de los datos (*Federal Data Privacy Legisation*), pueden consultarse en: https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation. (Última consulta: 20/10/2021).

[84] Con todo, las últimas actuaciones legislativas de la República Popular China apuntan a una mayor preocupación por la protección de los derechos de la ciudadanía en la Red, como pone de manifiesto la aprobación de una Ley de Seguridad de Datos (Ortega Giménez, 2021) y de una Ley de Protección de la Información Personal. Esta última tendría como cometido

No obstante, como Schrems II[85] ha puesto de manifiesto, no deben relajarse las medidas y ni la vigilancia constante de las transferencias de datos a terceros países y, en general, sobre las actuaciones de los responsables[86] que operan con datos de residentes en la Unión.

3.3.1. Las transferencias internacionales de datos

La fuerte presencia del modelo europeo también se refleja en su capacidad para condicionar la regulación y las condiciones que canalizan el flujo de información entre la UE y terceros países u organizaciones internacionales. El RGPD dispone dos modalidades de transferencia: las basadas en una decisión de adecuación (art. 45) y las que se producen mediante garantías adecuadas (art. 46).

Las primeras requieren que la Comisión aprecie que el nivel de protección que proporciona un «tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o […] [una] organización internacional» (art. 45.1 RGPD) es el adecuado. Las decisiones de adecuación son actos jurídicos vinculantes de la UE, mediante las que se informan a los Estados miembros acerca de aquellos terceros con los que pueden realizar transferencias internacionales de datos. Son flexibles en su contenido (pueden abarcar la totalidad de las transferencias o solo para sectores concretos) y, una vez adoptadas ofrecen un marco seguro de actuación a los operadores de datos (Gonzalo Domenech, 2019, p. 355).

Sin embargo, presentan ciertos problemas prácticos que no pueden desconocerse. El principal, la complejidad administrativa y la enorme dificultad que entraña lograr una decisión de adecuación por parte de la

reforzar el consentimiento y evitar que las personas deban facilitar el acceso a su información personal para obtener determinados servicios. Al menos, así la han descrito desde el gobierno Chino, vid. http://www.xinhuanet.com/english/2021-08/20/c_1310138698.htm. (Última consulta: 20/10/2021).

[85] STJUE asunto C-311/18, Facebook Ireland & Maximillian Schrems, de 16 de julio de 2020. Sobre los efectos y consecuencias de Schrems II, vid. (Neiazy, 2021), (Tracol, 2020), (de Miguel Asensio, 2020), (Sobrino García, 2020) y (von Danwitz, 2020).

[86] A efectos del RGPD, se entiende por responsable a « la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros» (art. 4.7 RGPD).

Comisión, como lo acredita el escaso número de decisiones existentes[87]. A su vez, la saga Schrems, y la consiguiente invalidez de las dos Decisiones destinadas a regular el flujo de datos entre la UE y Estados Unidos, no deja de suponer un cuestionamiento de la pertinencia de este mecanismo jurídico como cauce general para la regular las transferencias internacionales de datos.

En el caso de las transferencias mediante garantías adecuadas (art. 46 RGPD) es necesario tener presente que, bajo esa denominación, se acoge a un conjunto variado de opciones (art. 46.2 RGPD): la adopción de un instrumento jurídicamente vinculante; las normas corporativas vinculantes (art. 47 RGPD); las cláusulas contractuales tipo, ya sean adoptadas por la Comisión[88] o por una autoridad de control; los códigos de conducta (art. 40 RGPD)[89]; los mecanismos de certificación (art. 42) acompañados de compromisos vinculantes del responsable de implementar las garantías adecuadas. A estas medidas, que no requieren del consentimiento expreso de una autoridad de control, han de adicionarse dos supuestos para los que sí es necesaria esa autorización: las cláusulas entre responsables o encargados del tratamiento y los acuerdos administrativos entre autoridades públicas (art. 46.3).

Todos estos instrumentos han de asegurar, además, «que los interesados cuenten con derechos exigibles y acciones legales efectivas» (art. 46.1 RGPD). Si la saga Schrems pone en cuestión la efectividad de las

---

[87] Son pocos los países que tienen reconocido por la Comisión un nivel de protección adecuado: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Japón. Asimismo, la Comisión Europea ha elaborado un borrador para la futura decisión de adecuación respecto de los flujos de datos con el Reino Unido, este borrador puede consultarse en: https://ec.europa.eu/info/files/draft-decision-adequate-protection-personal-data-united-kingdom-general-data-protection-regulation_en. (Última consulta: 20/10/2021).
Lista de la que se ha caído Estados Unidos a raíz del pronunciamiento del TJUE, Schrems II. Salvo que se funden en normas corporativas vinculantes o sobre la base de Cláusulas Contractuales Tipo (CCT), siempre que superen la evaluación del nivel de protección. Para más información, vid. FAQ document on CJEU judgment C-311/18 (Schrems II) elaborado por el Comité Europeo de Protección de datos (EDPB), puede consultarse en: https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_en. (Última consulta: 20/10/2021).

[88] Sobre las cláusulas contractuales tipo, la Comisión ha adoptado una Decisión de ejecución destina a establecer las condiciones para la adopción de este tipo de instrumentos, incluyendo modelos que sirvan como referencia. Vid. Decisión de ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

[89] Sobre los códigos de conducta, la situación actual (2021) de su uso en la UE y el recorrido que este instrumento jurídico puede tener, vid. (Vander Maelen, 2021).

decisiones de adecuación como método general para canalizar las transferencias internacionales de datos, bien puede decirse que Schrems II ha supuesto la puesta en valor de los mecanismos de garantía adecuada, al ser, algunos de ellos, los únicos estimados válidos y respetuosos con el derecho a la protección de datos[90]. Siendo cierto que cada una de las opciones habilitadas para llevar a cabo una transferencia mediante garantías adecuadas tiene su singularidad[91], no lo es menos que, en términos generales, todas ellas permiten configurar marcos de protección personalizados y adaptados a las características de cada tratamiento, lo que, en última instancia, redunda en la adopción de medidas más idóneas y, por ende, en una mejor protección de las personas.

Finalmente, el RGPD contempla una serie de situaciones excepcionales en las que admite la viabilidad de la transferencia internacional, aunque no se vehicule a través de los mecanismos normativamente previstos a tal fin. Sin embargo, del análisis de los supuestos habilitantes, se infiere que todos ellos se fundamentan en la concurrencia de alguna circunstancia particular que, para un tratamiento concreto, justifique que se efectúe la transferencia.

Así, el art. 49.1 RGPD establece como supuestos habilitantes aquellos en los que la persona interesada haya prestado un consentimiento explícito; las transferencias sean necesarias para la ejecución de un contrato (sea por solicitud de la interesada o, por interés de la persona responsable); cuando concurran razones de interés público, se precisa para la formulación, ejercicio y defensa de reclamaciones, sirva para la protección de intereses vitales (en caso de no poder prestar el consentimiento) o, finalmente, cuando la transferencia se realice desde un registro público.

La mayoría de las condiciones coinciden con los supuestos habilitantes para el tratamiento de los datos especiales (los previstos en el 9.2 del RGPD), lo que conecta a las transferencias no amparadas en los mecanismos generales (Decisiones de adecuación o garantías adecuadas)

[90] Serán válidos los tratamientos que se funden en normas corporativas vinculantes o que se lleven a cabo sobre la base de Cláusulas Contractuales Tipo (CCT), siempre que superen la evaluación del nivel de protección. Para más información, vid. FAQ document on CJEU judgment C-311/18 (Schrems II) elaborado por el Comité Europeo de Protección de datos, puede consultarse en: https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_en. (Última consulta: 20/10/2021).

[91] Para un análisis singularizado de cada una de ellas, sus virtudes y defectos, vid. (Recuero Linares, 2019, pp. 422-426) y (Fernández-Samaniego y Fernández-Longoria, 2021).

con la existencia de un riesgo mayor. Ello explica por qué se incrementan las exigencias adicionales. El riesgo se erige en un factor determinante a la hora de concretar las condiciones de uso de los datos personales[92].

Las fórmulas que se acaban de reseñar en relación con la transferencia de datos personales toman como parámetro de referencia el RGPD en su configuración actual; consecuentemente, exigen tomar en consideración la naturaleza de los datos como uno de los criterios que han de observarse para decidir la adecuación de un marco normativo o el establecimiento de garantías necesarias[93].

Ahora bien, no puede dejar de constatarse el éxito de aquellos mecanismos de garantía que priman la personalización y la atención a las circunstancias del tratamiento (el sector en que se produce, sus finalidades, sus riesgos y particularidades). Asimismo, como el Comité Europeo de Protección de Datos (EDPB) ha remarcado, los responsables tienen un papel determinante en la evaluación de los riesgos y la determinación del nivel de seguridad de la operación, pues a ellos corresponde la decisión acerca de la continuidad de la transferencia y la valoración sobre la adecuación del nivel de protección[94]. El contexto se nos presenta como un

---

[92] Además de los supuestos específicos, también se incluye una cláusula general destinada a disciplinar posibles situaciones no subsumibles en los presupuestos anteriores. Así, el párrafo segundo del artículo 49.1 de RGPD establece que «cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos».

[93] El TJUE se ha pronunciado en reiteradas ocasiones acerca de la importancia de incrementar las cautelas cuando «*the particular category of personal data that is sensitive data is at stake*» en TJUE Opinion 1/15, de 26 de julio de 2017, sobre los acuerdos entre Canadá y la UE, especialmente en lo referente al PNR. En la misma línea, STJUE asuntos C-293/12 y C-594/12, Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014, apdos. 54 y 55; STJUE asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB, de 21 de diciembre de 2016, apdos. 109 y 117.

[94] Apartados 70 a 72 de las *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* del EDPB. Sirva para ilustrar la idea central de las Recommendations lo afirmado en el apartado 72, donde el EDPB señala que: «*where you are not able to find or implement effective supplementary measures that ensure that the transferred personal data enjoys an essentially equivalent level of*

factor decisivo a la hora de asegurar el éxito de las medidas y, por consiguiente, la protección de los derechos de los interesados.

3.3.2. Globalidad e idiosincrasia del modelo

«*The EU is at the forefront of data protection worldwide. The GDPR represents the most comprehensive and advanced regulatory framework for data privacy*» (Fabbrini y Celeste, 2020, p. 25). Esa privilegiada condición le ha servido para convertirse en parámetro de influencia global o, cuando menos, lo ha situado en una posición de fortaleza suficiente como para intentar preservar su modelo de protección de datos frente a los múltiples intereses del mercado digital global, especialmente, en relación con los actores transnacionales. Como la Comisión ha puesto de manifiesto: «*high data protection standards thus become an advantage in the global digital economy*»[95].

La pretensión de globalidad del modelo europeo es «*a more sophisticated expression of digital constitutionalism called digital humanism,* […] *should not be seen just as the imperial extension of legal provisions outside the territory of the Union but as the reaction of European constitutionalism against the challenges for human dignity coming from new technologies in the algorithmic society. In this scenario, the evolution of digital constitutionalism would oppose to techno-determinist solutions and contribute to promoting EU values as a sustainable constitutional model for the development of automated technologies on a global context*» (De Gregorio, 2021, p. 70).

---

protection, you must not start transferring personal data to the third country concerned on the basis of your chosen transfer tool. If you are already conducting transfers, you are required to promptly suspend or end the transfer of personal data». Pueden consultarse las *Recommendations* en:
https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en. (Última consulta: 20/10/2021).

[95] *Communication from the Commisión to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, de 10 de enero de 2017, p. 16. Puede consultarse en:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.
(Última consulta: 20/10/2021).

3.4. Los derechos del derecho a la protección de datos

El RGPD reconoce, en los artículos 15 a 18 y 20 a 22, los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y el derecho a no ser objeto de decisiones individuales automatizadas. Su regulación es la plasmación positiva de los diferentes cauces de actuación necesarios para asegurar el dominio de la proyección exterior del individuo.

Además de concretar las facultades[96] en que se materializa el poder de disposición y control, el RGPD establece las circunstancias que han de concurrir para hacerlo efectivo. Los derechos del derecho a la protección de datos son facultades de actuación con efectos individualizados.

Su accionamiento es un acto personal del interesado que, si no concurre ninguna circunstancia que lo impida, obliga al responsable a realizar algún tipo de actuación (desde facilitar al interesado el conocimiento de qué datos a él referidos están siendo objeto de tratamiento hasta la finalización de la operación).

Con todo, el ejercicio de estos poderes jurídicos no es absoluto. Cada uno de ellos tiene límites y condicionantes. Con carácter general, los principales agentes moduladores serán los intereses de los responsables, las finalidades, el contexto del tratamiento o la presencia de interesados con voluntades contrapuestas.

Las facultades de actuación son la principal proyección externa del derecho a la protección de datos. Su importancia en la configuración del modelo de protección es indudable, pues son el elemento personalísimo del sistema general de protección. Cada uno de ellos, por sí solo, justificaría un estudio monográfico, sin embargo, a los efectos que aquí interesa, y en la medida en que cualquier eventual propuesta de reforma sobre el concepto de dato o las categorías especiales no les afectaría, no precede detenernos en sus características específicas, bastando, en este punto, con enunciar qué aporta cada uno de ellos a la garantía general del derecho fundamental.

Así, el derecho de acceso es el mecanismo jurídico a través del que el interesado puede «obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen» (art. 15.1

[96] Si se ha optado por calificar a esos derechos como facultades de actuación es, precisamente, por el modo en que son accionados –previa solicitud de su titular–.

RGPD) [97] y, de ser la respuesta afirmativa, conocer el destinado de la información a él referida[98].

Al facilitar la cognición de la realidad del tratamiento, estamos ante un derecho capital para el ejercicio de otros derechos[99] (como pueden ser los de rectificación o supresión). Al ser la antesala del resto de derechos, es una facultad de actuación especialmente resistente frente a eventuales limitaciones[100] a su ejercicio[101].

Finalmente, sin ser una limitación *stricto sensu*, el apartado tercero del artículo 15 señala que las peticiones de copia subsiguientes a la primera podrán ser objeto de «un canon razonable basado en los costes

[97] El artículo 15.1 del RGPD establece un listado bastante amplio de informaciones a las que interesado puede acceder:
«a) los fines del tratamiento;
b) las categorías de datos personales de que se trate;
c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
f) el derecho a presentar una reclamación ante una autoridad de control;
g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado».
También tendrá derecho a una copia de la información (art. 15.3 RGPD).

[98] Sobre el desarrollo normativo del derecho de acceso en el RGPD (art. 15), vid. los detallados análisis de Arenas Ramiro (Arenas Ramiro, 2021a) y Zanfir-Fortuna (Zanfir-Fortuna, 2020c).

[99] STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017, apdo. 57.

[100] Aun cuando se le aplican las limitaciones generales previstas en el Considerando 73 RGPD. Estas permiten «imponer restricciones» a los derechos cuando «sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública […] [así como por] objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero […], o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios». Con todo, este tipo de limitaciones habrán de cumplir las exigencias del 52.1 de la CDFUE, esto es, implementarse mediante ley, respetar el contenido esencial del derecho y el principio de proporcionalidad

[101] En esta línea, el apartado cuarto del art. 15 del RGPD y, con mayor profusión y detalle, el Considerando 63 del RGPD, señalan que la afectación negativa de los derechos y libertades de terceros puede operar como límite, sin que por ello deban «tener como resultado la negativa a prestar toda la información al interesado». No obstante, cuando este derecho suponga la quiebra de un deber de secreto o afecte «negativamente a […] los derechos de propiedad intelectual» podría llegar a limitarse su ejercicio (Considerando 63 RGPD).

administrativos». Si bien es una potestad del responsable el solicitar ese pago (siempre que esté justificado), el eventual coste de un ejercicio reiterado del derecho no deja de ser un modo de evitar abusos pero, a su vez, puede llegar a desincentivar segundos y terceros ejercicios del derecho (IT, 2019, pp. 57-58).

Junto al derecho de acceso, la otra facultad expresamente reconocida en el art. 8 de la CDFUE, es el derecho de rectificación. Este tiene como finalidad el asegurar la correspondencia entre el dato y el interesado al que se refiere[102]. Así, de no existir esa concordancia entre la información gestionada y la realidad del sujeto, este podrá «obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan […] [asimismo, podrá solicitar] que se completen los datos personales que sean incompletos» (art. 16 RGPD)[103].

Además de concretar los derechos enunciados en la CDFUE, el RGPD amplía el conjunto de posibilidades de actuación del interesado mediante el reconocimiento de un conjunto variado de facultades que permiten a los interesados defender sus intereses jurídicos.

En este sentido, el derecho de supresión[104] es la facultad de actuación que permite lograr la eliminación de ciertos datos personales[105],

---

[102] Un dato erróneo no deja de ser un dato personal, pero es un dato que no refleja la realidad de la persona y, consecuentemente, la prioridad debe ser corregirlo para restablecer el vínculo dato-persona.

[103] La activación de este derecho ha de ir acompañada de la información que se pretende modificar –por lo que, habitualmente, se habrá ejercitado previamente el derecho de acceso–, así como el sentido del cambio y las referencias que acrediten la exactitud de los nuevos datos o la incorrección o incompletitud de los existentes. Estas exigencias resultan muy pertinentes, pues minoran los eventuales conflictos derivados de pareceres discordantes entre el responsable y el interesado sobre la exactitud de una determinada información.

[104] Es una versión mejorada del derecho al olvido, porque busca «la efectividad del derecho no sólo respecto de los responsables, sino también sobre los terceros destinatarios de datos, sean cesionarios o encargados del tratamiento» (Díaz Díaz, 2021, p. 1592). Para un análisis más detallado de este derecho, vid. los diversos trabajos de Martínez López-Sáez sobre este derecho, entre otros, son especialmente recomendables para el conocimiento del derecho de supresión: (Martínez López-Sáez, 2017a), (Martínez López-Sáez, 2017b), (Martínez López-Sáez, 2020).

[105] El asunto Mario Costeja suele considerarse el caso fundante del derecho al olvido, STJUE asunto C 131/12, asunto Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014. Para un análisis de esta sentencia y del modo en que se concebía el derecho al olvido en esos momentos, vid. (Rallo Lombarte, 2014) y (Arenas Ramiro, 2014).

Con todo, pueden encontrarse precedentes tanto en instrumentos internacionales, como en la normativa europea, vid. el detallado estudio realizado por Martínez López-Sáez en (Martínez López-Sáez, 2017b, pp. 237-259), en el que, además, se pone el foco en el

siempre que se reúnan los requisitos jurídicamente previstos[106]. Es la respuesta normativa al «resurgimiento perjudicial que puede suponer un clic instantáneo y una memoria digital que nunca olvida» (Martínez López-Sáez, 2017, p. 260).

Aunque generalmente se activará por parte de los interesados cuando teman los efectos dañosos de una determinada información, lo cierto es que, en la medida en que es una manifestación subjetiva del derecho fundamental, no se exige que los datos tengan un carácter nocivo para poder accionar este derecho, incluso frente a informaciones que sean de acceso público[107].

El derecho de supresión no es la única vía para lograr que dejen de utilizarse datos personales. Así, cuando el tratamiento esté fundado en el

importante papel desarrollado por la jurisprudencia, tanto del TEDH como del TJUE, en la consagración de este derecho. No menos detallado, si bien más focalizado en el desarrollo en el marco de la UE y en la realidad española, es el trabajo de Díaz Díaz en (Díaz Díaz, 2021, pp. 1563-1580).

[106] En lo referente a su ejercicio, si bien ninguna de las facultades de actuación es ilimitada, el derecho de supresión es, seguramente, el que cuenta con más condicionantes. Solo será efectivo si, sobre los datos objeto de tratamiento, concurre alguna de las circunstancias previstas en el apartado 1 del artículo 17 del RGPD. Esto es, caundo: «a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1».

Adicionalmente, el RGPD prevé (art. 17.3) una serie de supuestos en los que no sería de aplicación el derecho de supresión. La imposibilidad de ejercicio del derecho trae causa de la concurrencia de alguna circunstancia que exija el tratamiento de esa información: el ejercicio del «derecho a la libertad de expresión e información»; el «cumplimiento de una obligación legal […] o […] de una misión realizada en interés público o […] el ejercicio de poderes públicos conferidos al responsable»; cuestiones de salud pública; «fines de archivo en interés público, fines de investigación científica o histórica o fines estadístico»; así como «para la formulación, el ejercicio o la defensa de reclamaciones» (art. 17.3 RGPD).

Para una ampliación de los límites al ejercicio del derecho de supresión en el modelo europeo, vid. (Martínez López-Sáez, 2017a, pp. 169-171). Asimismo, en la STJUE asunto 398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni, de 9 de marzo de 2017, se excluyó, con carácter general, al registro de sociedades del ámbito de actuación del derecho al olvido.

[107] En estos casos, el responsable deberá hacer todo lo que sea técnicamente posible para eliminar cualquier ruta que posibilite el acceso a la información. Se puede cumplir con las exigencias del derecho de supresión sin necesidad de destruir los datos, bastaría con implementar medidas que impidan su conocimiento por los demás, esto es, hacer que lo que antes era público deje de serlo.

«cumplimiento de una misión realizada en interés público» (art.6.1.e RGPD) o sea «necesario para la satisfacción de intereses legítimos perseguidos por el responsable» (6.1.f RGPD), el interesado podrá ejercitar el derecho de oposición[108].

Con todo, no existe un derecho general de oposición[109] (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2018, p. 258). Para poder ejercitar este derecho, habrán de concurrir algún tipo de razón personal que les permita instar al responsable a cesar en la utilización de su información (Arenas Ramiro, 2021, p. 1718)[110].

Sin llegar al nivel de intensidad de los derechos de oposición y supresión[111], el derecho a la limitación del tratamiento[112], positivizado en el artículo 18 del RGPD, atribuye al interesado la facultad de restringir el

[108] El derecho de oposición está profusamente regulado en el artículo 21 del RGPD. La finalidad principal del mismo es ofrecer al interesado una vía de actuación mediante la que lograr que dejen de utilizarse sus datos personales cuando el tratamiento esté fundado en el «cumplimiento de una misión realizada en interés público» (art.6.1.e RGPD) o sea «necesario para la satisfacción de intereses legítimos perseguidos por el responsable» (6.1.f RGPD). Es decir, el derecho de oposición es el mecanismo a través del que el interesado puede evitar que se utilicen sus datos en tratamientos que no deberían producirse, pues concurren circunstancias personales que justificarían que no se lleven a efecto. Sobre el derecho de oposición, vid. (Arenas Ramiro, 2021b) y (Zanfir-Fortuna, 2020d).

[109] No ocurre así en el caso del consentimiento, donde el interesado tiene el derecho de retirarlo «fácilmente» (EDPB, Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 4 de mayo de 2020, p. 21). Tampoco cuando el tratamiento es necesario para la ejecución de un contrato, el interesado toma parte del mismo y, por lo tanto, el tratamiento está ajustado a las necesidades del caso concreto. Si el tratamiento tiene como justificación la protección de intereses vitales del interesado o de un tercero, la valoración de los intereses en concurso es inherente a la base de legitimación. Lo mismo acontece en aquellos tratamientos que se basan en la existencia de una obligación legal, pues esta ha de considerar los riesgos y consecuencias del tratamiento (Considerando 45 RGPD).

[110] Cuando el tratamiento se funda en alguna de las dos bases que habilitan el ejercicio del derecho de oposición –misión en interés público o interés legítimo–, el análisis de las circunstancias del tratamiento es abstracto y apriorístico, pudiendo concurrir razones subjetivas que justifiquen que los datos de un determinado interesado no tomen parte del mismo. No se cuestiona el tratamiento, sino que se aducen las circunstancias personales que permiten eludirlo.

Junto a las previsiones generales, se regulan una serie de situaciones específicas. Así, el derecho de oposición se habrá de aplicar de manera automática tanto en los tratamientos que tengan fines de mercadotecnia directa (art. 21.3 RGPD), como en los realizados para la prestación de servicios de la sociedad de la información (21.5 RGPD). En el caso de los tratamientos que tengan «fines de investigación científica o histórica o fines estadísticos», el derecho de oposición será viable, salvo que el tratamiento en cuestión «sea necesario para el cumplimiento de una misión realizada por razones de interés público» (21.6 RGPD).

[111] De hecho, sirve como opción alternativa al ejercicio del derecho de supresión, cuando, pese a estar produciéndose un tratamiento ilícito, el interesado no quiera eliminar la información. Para evitar vulneraciones innecesarias, es preciso que el interesado sea convenientemente informado de las consecuencias de optar por una opción u otra.

[112] Para un análisis más detallado de este derecho y sus implicaciones, vid. (Pascual Huerta, 2021a) y (González Fuster, 2020a).

tratamiento de sus datos, constriñéndolo, solo, a aquellas acciones por él autorizadas, así como, a las necesarias para defender posibles reclamaciones, proteger derechos de terceros (sean personas físicas o jurídicas), o los que sean necesarios por razones de interés público (sea de la UE o de un Estado miembro) (18.2 RGPD).

El interesado tendrá éxito en su ejercicio cuando se esté ejercitando el derecho de rectificación o se esté produciendo el proceso de confirmación de la verosimilitud de las razones por las que se ejercita el derecho de oposición. También podrá aplicarse cuando, a pesar de que el responsable ya no necesite los datos para alcanzar los fines del tratamiento, el interesado precise que se mantengan disponibles para algún tipo de reclamación. En este caso, la limitación actúa como una garantía que permite conservar la información, reducir los daños y, a la vez, velar por los intereses del propio interesado.

El derecho a la protección de datos es un derecho vivo, es como un diamante con facetas por descubrir. Muestra de ello es la inclusión del derecho a la portabilidad de los datos (art. 20 del RGPD)[113]. Esta facultad de actuación permite al interesado exigir del responsable la transmisión de los datos, bien al propio interesado, bien a otro responsable[114].

Este derecho conecta con la libre circulación de información y supone un incentivo para que los responsables implementen sistemas

[113] Art. 20 RGPD: «1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
b) el tratamiento se efectúe por medios automatizados.
2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros».
Para una ampliación del contenido de este derecho, así como de sus límites, vid. (Martínez López-Sáez, 2019) y (Santamaría Ramos, 2021a).

[114] Los traslados de datos entre responsables habrán de realizarse directamente entre ellos, evitando que deba ser el interesado el que primero los reciba de uno y luego los transmita al otro. Para una ampliación del contenido de este derecho, así como de sus límites, vid. (Martínez López-Sáez, 2019) y (Santamaría Ramos, 2021).

interoperables que permitan proporcionar los datos personales «en formatos con un alto nivel de abstracción en relación a cualquier formato» (Santamaría Ramos, 2021, p. 1675).

Con todo, su ejercicio tiene importantes limitaciones: solo es posible cuando la base de legitimación sea el consentimiento, o la firma de un contrato[115] o estar circunscrito a los tratamientos automatizados[116] (art. 20.1.b RGPD), conformándolo como una faceta del derecho a la protección de datos circunscrita al entorno digital. Además, aun concurriendo todas las condiciones necesarias, este derecho no será de aplicación si el responsable precisa de esos datos para llevar a cabo un tratamiento en «cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos» (art. 20.3 RGPD).

Al igual que la portabilidad, el derecho a no ser objeto de decisiones individuales automatizadas también está estrechamente conectado al tratamiento mecanizado de la información. Es una facultad pensada para hacer frente a los efectos perniciosos del decisionismo algorítmico[117]. Este

---

[115] Esta exigencia resulta, hasta cierto punto, coherente, pues son los dos supuestos de tratamiento en que existe una certeza absoluta de que los datos proceden del interesado y, además, son los dos casos en que el tratamiento trae causa de un acto de autodeterminación personal directo por parte del interesado. Consecuentemente, con su transmisión no se ponen en riesgo «los derechos y libertades de otros», tal como exige el apartado cuarto del artículo 20 RGPD.
Sin embargo, deberían haberse incluido aquellos tratamientos que fuesen necesarios para la protección de intereses vitales del propio interesado, especialmente cuando se diesen las circunstancias del art. 9.2.c) del RGPD. En ese supuesto, la portabilidad serviría para preservar la vida de un interesado que no se encontraría en condición de prestar consentimiento. La utilidad de esta medida para la asistencia sanitaria, especialmente en supuestos transfronterizos, no es desdeñable (Jove Villares, 2019).

[116] En el caso de las transmisiones entre responsables, los datos han de encontrarse «en un formato estructurado, de uso común y lectura mecánica» (art. 20.1 RGPD). La circunscripción de este derecho a los tratamientos automatizados (art. 20.1.b) se justifica desde la viabilidad de su realización efectiva, mucho más sencilla que en los tratamientos manuales. De hecho, «el derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles» (Considerando 68 RGPD). Sin embargo, no deja de ser una ablación de las posibilidades de actuación del interesado el no extender este derecho, al menos en el plano jurídico, a todo tipo de tratamiento, dejando que sean las circunstancias del tratamiento las que determinen las posibilidades de materialización fáctica.

[117] El GT29 ha señalado en sus Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 3 de octubre de 2017 y revisadas el 6 de febrero de 2018, p. 23 qué se entiende por producción de «efectos jurídicos». Así, en aquellos tratamientos que afecten «a los derechos jurídicos de una persona, como la libertad de asociarse con otras personas, de votar en unas elecciones o de entablar acciones legales. Asimismo, un efecto jurídico puede ser algo que afecte al estatuto jurídico de una persona o a sus derechos en virtud de un contrato. [Por ejemplo] […] la cancelación de un contrato, el derecho o la denegación de una prestación […] o […] la denegación de admisión en un país o la denegación de ciudadanía».

derecho es útil en el presente, pero será crucial en el futuro, debido a la popularización del uso del *big data* y a las posibilidades –y comodidades– que supone derivar la toma de decisiones a lo determinado por un análisis algorítmico, especialmente, cuando este se reviste de la credibilidad de la certeza matemática[118].

Conforme al modelo europeo de protección, «los interesados no deben ser objeto de decisiones automatizadas [incluida la elaboración de perfiles[119]] que surtan efectos legales o tengan efectos de similar importancia. Si es posible que dichas decisiones tengan un impacto significativo en las vidas de las personas físicas a las que conciernen puesto que, por ejemplo, hacen referencia a la solvencia, la contratación en red, el rendimiento profesional, el análisis de la conducta o la fiabilidad, será necesario establecer una protección especial para evitar consecuencias negativas» (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2018, p. 263).

Además de circunscribirse, en exclusiva, a decisiones totalmente automatizadas e individuales[120] (Brkan, 2019, p. 99), el ejercicio de este derecho tiene toda una serie de condicionantes. El interesado no podrá valerse de este derecho cuando haya consentido explícitamente el uso de dicha técnica (22.2.c RGPD), ni cuando la decisión automatizada sea «necesaria para la celebración o la ejecución de un contrato» del que él sea parte (22.2.a RGPD). Finalmente, tampoco podrá hacer uso de esta facultad cuando tal actuación esté «autorizada por el Derecho de la Unión o de los Estados miembros» y se contemplen las garantías adecuadas para salvaguardar tanto los derechos y libertades como los intereses legítimos del interesado (22.2.b RGPD).

En los supuestos de afectación significativa son aquellos en los que, «incluso cuando no se produzca ningún cambio en sus obligaciones o derechos jurídicos, el interesado puede verse suficientemente afectado como para exigir protección».

[118] El ejercicio de este derecho tiene como presupuesto fáctico que el interesado haya sido «objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente» (art. 22.1 RGPD). Sobre este derecho y su alcance, vid. (Bygrave, 2020) y (Sancho Villa, 2021).

[119] Conforme a lo dispuesto en el art. 4.4 del RGPD, se entiende por elaboración de perfiles: «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física».

[120] Supone una limitación de partida significativa, al no incluir los supuestos en los que el resultado algorítmico es un apoyo, un criterio a considerar dentro de la decisión final (Medina, 2021, párr. 5).

La exigencia de garantías en los procesos automatizados de decisión es el otro elemento regulado en el art. 22 del RGPD. Como se ha apuntado, para el supuesto en que no pueda hacerse uso de este derecho por existir una previsión normativa que habilite al responsable a valerse de estas innovaciones, han de preverse las garantías adecuadas y se deberá prestar especial atención al cumplimiento de los deberes de información (Sancho Villa, 2021, pp. 1740-1744).

Por otra parte, en aquellos casos en que medie el consentimiento del interesado o el tratamiento sea necesario para la celebración de un contrato, se impone al responsable el deber de implementar «las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, [y] como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión» (art. 22.3 RGPD). Es decir, el interesado tendrá la posibilidad de contrastar y cuestionar la decisión. Ello le permitirá, por ejemplo, aducir por qué no encaja en el perfil que se le ha hecho o cuestionar alguna de las variables empleadas.

Con todo, no es una solución perfecta, pues hace recaer sobre el interesado el deber de demostrar los motivos que le llevan a cuestionar el resultado probabilístico obtenido. Ese deber de motivación puede resultar, en ocasiones, de difícil realización, tanto por la complejidad de su cognición, como por la dificultad para lograr un nivel de transparencia adecuado respecto del diseño de los algoritmos (Ananny y Crawford, 2018)[121].

En términos generales, el derecho a no ser objeto de decisiones individuales automatizadas regulado en el RGPD es un instrumento valioso para afrontar los desafíos del decisionismo algorítmico[122]. Sin embargo, se antoja insuficiente para responder al complejo escenario planteado por las decisiones automatizadas en la era digital[123].

---

[121] En lo referente al resto de medidas a implementar por el responsable, estas han de ser adecuadas al contexto del tratamiento, de ahí que no puedan establecerse previsiones más concretas. Cualquiera que sea la garantía prevista ha de respetar las normativas antidiscriminatorias y, en general, todo el ordenamiento jurídico. La realidad digital puede parecer un mundo diferente, pero la normativa existente también rige para ella, pues, en última instancia, los efectos –negativos y positivos– se producen sobre personas reales.

[122] Sobre el alcance, importancia y modo de explicar las decisiones automatizadas, vid. (Kaminski, 2019) y (Bayamlıoğlu, 2021).

[123] El trabajo de Wachter et. al. sobre esta cuestión es, seguramente, el más claro y contundente al respecto, (Wachter, Mittelstadt, y Floridi, 2017).

En todo caso, y más allá del margen de mejora que alguna de las facultades pueda tener, es indudable que los residentes en la UE cuentan con un buen arsenal para defender sus intereses jurídicos frente al tratamiento de sus datos.

3.5. Un modelo de resolución de conflictos

La economía digital se funda, en gran medida, en el tratamiento de datos por entidades privadas. Además, la estructura técnica, el soporte que permite el funcionamiento de la sociedad digital depende, en gran medida, de un puñado de grandes empresas. No resulta extraño, por tanto, que el RGPD sea una norma que, preferentemente, disciplina las relaciones *inter privatos*, sin perjuicio de las previsiones reservadas al tratamiento de la información por entidades públicas.

El conjunto de equilibrios que es necesario realizar es mayúsculo. El tratamiento de datos implica la convergencia de diversos intereses sobre un mismo objeto. Sobre una información determinada concurren expectativas de todo tipo y entidad jurídica[124].

No debe extrañar que el RGPD sea, también, una normativa de resolución de conflictos[125]. Esta condición queda patente en el caso de las relaciones entre los responsables y los interesados. En estos casos, la normativa disciplina el modo de establecer las preferencias jurídicas y posiciones prevalentes respecto del destino de la información, acotando, en función del contexto y características del tratamiento, las capacidades de actuación de cada una de las partes.

Al legislador corresponde establecer los criterios y definir el modo en que se conjugan los intereses de la persona a la que están referidos los

[124] Imaginemos una información que es dato personal de más de una persona y cada una de ellas pretende hacer un uso distinto de la misma. Además, cuando esa información pasa a ser tratada, aparecen nuevos actores, generando nuevos intereses y expectativas, con los consiguientes problemas derivados de afrontar la regulación de una realidad tan diversa como la pluralidad de operaciones que pueden realizarse.

[125] Ningún derecho es absoluto, tampoco el derecho a la protección de datos, «que debe ser considerado en relación con su función en la sociedad». STJUE asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke GbR c. Land Hessen y Eifert c. Land Hessen y Bundesantalt fur Landwirtschaft un Ernahrung, de 9 de noviembre de 2010, apdo. 48. En la línea ya apuntada, años antes por STJUE asunto C-112/00, Eugen Schmidberger, Internationale Transporte und Planzüge y Republik Österreich, de12 de junio de 2003, apdo. 80. El Considerando 4 del RGPD también se pronuncia en idénticos términos.

datos. Por su parte, el interesado, en la medida en que el tratamiento puede poner en riesgo sus derechos, así como en ejercicio de su poder de disposición y control, podrá exigir/esperar que se implementen determinadas cauciones (reconocimiento de garantías, establecimiento de medidas de seguridad) y podrá ejercitar las facultades de actuación que correspondan (si bien mediatizadas por los otros intereses en concurso).

El RGPD ofrece ciertas claves para la resolución de otras situaciones de conflicto de derechos, como es el caso de la relación entre tratamiento de datos y libertad de expresión e información (Considerandos 4, 65, 153; arts. 17.3 y 85 RGPD) o el secreto profesional (Considerandos 50, 53, 75, 85; art. 14.5 o art. 90 RGPD)[126]. Sin embargo, no proporciona, al menos de un modo directo y expreso, reglas de actuación para los casos en los que una misma información sea dato personal de más de una persona, y los interesados tengas voluntades contrapuestas[127]. En esa clase de supuestos, los criterios que permitirán resolver los conflictos serán: las circunstancias, el contexto del tratamiento, los riesgos o la afectación y menoscabo que suponga para el ejercicio de los derechos de los interesados[128].

Los peligros, o la ausencia de los mismos, condicionan el ejercicio de las facultades de actuación. A menor riesgo, más posibilidades de que los derechos mediante los que se manifiesta el poder de disposición y control cedan frente a otros intereses con los que pueda entrar en conflicto. Simplificando las variables en concurso, puede decirse que, cuanto menor sea el riesgo, mayores son las posibilidades de llevar a cabo el tratamiento y el margen de actuación del responsable. Sin que, por ello, se deba olvidar que estamos ante una realidad dinámica, sujeta a cambios, pues nuevos riesgos demandarán una adecuación del *statu quo*.

Los efectos que el tratamiento pueda producir en los sujetos intervinientes serán un criterio determinante a la hora de resolver los conflictos entre interesados e, incluso, entre interesado y responsable, por más que esta relación esté mucho más reglada. Con todo, la identificación

[126] El RGPD no aborda en toda su extensión estas cuestiones (relación derecho de información-protección de datos o este último y secreto profesional) remitiendo gran parte de su desarrollo a la regulación de los Estados miembros.

[127] Por ejemplo, por querer un interesado que el dato sea objeto de tratamiento y otro interesado no; o uno querer suprimirlo y el otro continuar con el tratamiento

[128] Como ocurrió en el asunto Nowak, donde los intereses del Sr. Nowak entraban en conflicto con los del examinador, pues las anotaciones subjetivas en el examen eran datos personales de ambos. Vid. STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017, especialmente apdos. 42 a 58.

del interés preponderante no deja de fundarse en un ejercicio hipotético, pues se basa en las consecuencias previsibles. La determinación de las posibilidades reales de actuación de los sujetos intervinientes no deja de ser el resultado de una ponderación abstracta acerca de las consecuencias posibles de un determinado tratamiento. El legislador, al regular las relaciones entre responsables e interesados, está positivizando el resultado de su valoración. En el caso de las relaciones entre interesados, ese ejercicio corresponderá, en buena medida, a los tribunales, sin perjuicio de que puedan articularse criterios relacionales[129].

Las situaciones en las que la afectación ya se haya producido constituyen un escenario diferente. En esos casos habrá de valorarse el daño efectivamente producido, así como las circunstancias que lo motivaron. Son dos momentos distintos. El primero corresponde al conflicto de intereses entre interesados o entre interesado y responsable y se focaliza en las posibilidades de ejercicio de las facultades de actuación o, incluso, en la posibilidad de realizar el tratamiento[130]. En esta fase, los criterios valoración son: el riesgo, los posibles efectos derivados de las decisiones adoptadas, la proporcionalidad de las medidas existentes, así como las garantías implementadas.

La segunda fase se produciría cuando, a raíz del tratamiento, se ha vulnerado algún derecho o libertad –distinto del derecho a la protección de datos–. En este caso, se ha de valorar si concurre alguna circunstancia que pudiera justificar la injerencia efectivamente producida en los bienes jurídicos del afectado. De no ser así, se habrán de adoptar las medidas de reparación correspondientes al derecho efectivamente vulnerado.

En este último escenario, ¿qué papel puede desempeñar el derecho a la protección de datos? La adopción de las medidas jurídicamente exigibles podría constituir una atenuante. Siendo determinante la capacidad para acreditar que hubo diligencia en las actuaciones y no medió voluntad de generar daño. La responsabilidad proactiva se presenta como

[129] El derecho a no saber (Gómez Sánchez, 2011) sería un ejemplo de solución jurídica para este tipo de situaciones.

[130] Por ejemplo, porque una persona quisiese que los datos se tratasen y otra estuviese en contra, siendo ambos interesados y, consecuentemente, estando la información referida a ambos y, pudiendo considerarse dato personal de los dos. Sobre este tipo de problemáticas, en relación con los datos genéticos, he tenido ocasión de pronunciarme, en coautoría con de Miguel Beriain, en (De Miguel Beriain y Jove Villares, 2021).

la herramienta mediante la que tratar de lograr cualquier minoración de las sanciones y reparaciones que deban afrontarse.

En todo caso, con estas reflexiones, con un punto de elucubración en lo referente a los efectos balsámicos que la responsabilidad proactiva pudiera tener, se busca poner de manifiesto una serie de características del modelo europeo de protección de datos. En primer lugar, es un sistema eminentemente preventivo, focalizado en evitar los efectos dañosos que el tratamiento de la información pudiera ocasionar. En segundo lugar, el RGPD es una normativa de resolución de conflictos, pues, o bien establece el sentido en que las divergencias han de resolverse, o proporciona las herramientas para hacerlo[131] (v. gr. la atención al riesgo, los posibles efectos nocivos que pudiera tener la actuación que se vaya a ejercitar). En tercer lugar, la protección de datos no puede absorber los daños efectivamente producidos en otros derechos. En esos casos, se habrá vulnerado el derecho que corresponda y, a lo sumo, habrá que valorar si también ha habido afectación del derecho fundamental a la protección de datos, pero serían dos desvalores distintos.

En un escenario ideal, el derecho a la protección de datos personales debería ser capaz de prevenir gran parte de los daños que pudieran producirse en los demás derechos. Sin embargo, muchos de los conflictos, reales o potenciales, se resuelven a partir de análisis apriorísticos y bajo hipótesis de posibles consecuencias, con lo que una efectividad absoluta de las medidas de prevención es materialmente imposible. No obstante, las disposiciones normativas existentes, y la orientación de las mismas, resultan, a mi modo de ver, adecuadas para resolver las fricciones que se generen entre los sujetos que tomen parte en el tratamiento de la información.

3.6. Los principios como elemento vertebrador del tratamiento

Los principios establecidos en el art. 5 del RGPD son «la bóveda del sistema de protección de datos» (Troncoso Reigada, 2021: 851). A través

[131] STJUE asunto C-101/01, asunto Lindqvist, 6 de noviembre de 2003, apdo. 82, en la que se señala a la legislación europea (la Directiva en ese entonces) y a la de los Estados miembros como el lugar en que están residenciados y regulados los «mecanismos que permiten ponderar los diferentes derechos e intereses» que puedan entrar en conflicto en un determinado tratamiento.

de ellos, el legislador europeo ha adoptado decisiones clave: a) qué modelo de protección quería implementar –anticipatorio y preventivo–; b) estrechamente conectada con la anterior, su apuesta decidida por el principio de responsabilidad proactiva, que orienta todo el modelo y asegura su observancia (art. 5.2 RGPD) y, c) que la vulneración de los principios siempre comporta una infracción muy grave[132].

Los principios constituyen el mínimo común que todo tratamiento debe reunir para asegurar el respeto al derecho a la protección de datos[133]. Disciplinan el modo en que ha de transcurrir el tratamiento (Muñoz Ontier, 2018, p. 347), estableciendo las condiciones en que se ha de operar con los datos e imponiendo a los responsables (de manera directa) y al resto de operadores de datos[134] (en la medida en que tomen parte del tratamiento), una serie de deberes de actuación destinados a asegurar que el uso de la información personal no suponga una injerencia en los bienes jurídicos del interesado[135].

Su transversalidad les sitúa en el núcleo del sistema de protección. Con la responsabilidad proactiva como el elemento vertebrador[136], los

[132] Consecuentemente, las sanciones derivadas de la infracción de lo previsto en el artículo 5 del RGPD llevan aparejadas las multas de mayor cuantía, remarcando, de ese modo, la centralidad de los principios. Las multas por incumplimiento de lo dispuesto en el art. 5 del RGPD serán «de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía» (83.5 RGPD).

[133] Son ineludibles para quienes pretendan operar con datos de carácter personal y, también, para los legisladores nacionales que hagan uso de sus competencias regulatorias en la materia (p. ej. vía obligación legal o regulación de un interés público que justifique el tratamiento (6.1. c) y e) RGPD).

[134] Entendiendo por tales a los sujetos que intervienen en el tratamiento sin ser los responsables, p. ej. encargados del tratamiento (art. 4.8 RGPD: «"encargado del tratamiento" o "encargado": la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento») o los terceros (art. 4.10 RGPD: «"tercero": persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado»).

[135] Denominación con la que se identifica en la versión en español del RGPD a la persona física a la que se refiere la información objeto de tratamiento.

[136] El principio de responsabilidad proactiva condiciona y orienta a los demás principios y, a su vez, estos contribuyen a su realización plena.

principios conforman un entramado de obligaciones agregadas que dan como resultado un modelo garantista, anticipatorio y preventivo. Desde un mínimo ineludible, posibilitan la adopción de medidas acomodadas a la realidad de cada tratamiento, son como un fresno, resistentes, pero extraordinariamente flexibles.

Pese a su denominación, algunos principios se asemejan a reglas[137] (v. gr. el de licitud, el de limitación del plazo de conservación, el de exactitud o el de minimización), alejándose de la concepción alexiana de los principios, como mandatos de optimización que admiten cierta graduación en su nivel de cumplimiento (Alexy, 1993. pp. 83-87). Otros, incluida la responsabilidad proactiva o la transparencia, sí gozan de un carácter abierto y modulable, capaz de dar cabida a un conjunto de comportamientos posibles dentro de los límites por ellos fijados.

La complejidad de los tratamientos, así como la variedad de los mismos, ha hecho que, al menos en el modelo europeo, lo que en los comienzos eran guías de actuación o meras recomendaciones, se hayan transformado en el fundamento jurídico del sistema. Su carácter vinculante, el aparato sancionador que los ampara, ha convertido a los principios relativos al tratamiento de datos previstos en el RGPD en las obligaciones básicas del sistema.

Los principios son la respuesta a la necesidad de salvaguardar determinados intereses jurídicos. Algunos de ellos, como el de responsabilidad proactiva, son la plasmación de una política pública concreta, en este caso, la necesidad de establecer un modelo anticipatorio y de prevención de riesgos. Otros, como el principio de licitud, son la

[137] Partiendo de la distinción de Hart entre reglas y principios como una cuestión de grado, en el que las reglas serían «cuasi concluyentes en las que, salvo contadas excepciones (en que sus disposiciones pueden ser incompatibles con otra regla que se considera más importante), [por lo que] el hecho de satisfacer los requisitos de aplicación es suficiente para determinar las consecuencias jurídicas, y, por otro lado, [los] principios generalmente no concluyentes, que se limitan a señalar una decisión, pero que a menudo no la determinan» (Hart, 1997, p. 250).

plasmación de los mandatos de optimización inherentes al derecho a la protección de datos. Son el desarrollo de su dimensión objetiva.

Cada uno de los principios facilita y enriquece el ejercicio de los demás. Individualmente considerados resultan valiosos y útiles en su cometido, pero es en su aplicación conjunta donde cobran verdadera fuerza, al generar las condiciones adecuadas para que los tratamientos transcurran conforme a las exigencias del derecho fundamental a la protección de datos.

Por este motivo, y con la excepción del principio de responsabilidad proactiva, cuyo impacto en la caracterización general del modelo europeo de protección de datos obliga a analizarlo de manera particularizada, del resto de principios establecidos en el artículo 5 del RGPD (licitud, lealtad, limitación de la finalidad, transparencia, minimización de datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad) apenas si apuntaremos las aportaciones singulares que realizan al conjunto del sistema.

Esta elección metodológica no niega su importancia, al contrario, cada uno de ellos es una pieza vital del modelo, con enjundia suficiente como para justificar trabajos monográficos sobre su contenido, límites e implicaciones. Sin embargo, en la medida en que un estudio detallado de los mismos excede los objetivos de este trabajo, y tomando en consideración que, cualquier eventual propuesta de reforma sobre el concepto de dato o las categorías especiales no les afectaría, consideramos apropiado centrarnos en dilucidar, exclusivamente, sus implicaciones respecto del modo en que se ejecutan los tratamientos.

3.6.1. Las aportaciones singulares de cada principio a la caracterización del modelo

El principio de licitud[138] demanda que el tratamiento que se pretenda llevar a efecto cuente con un título habilitante[139]. Esta exigencia entronca con la idea de diseño previo del tratamiento y de atención a las particularidades del contexto y de los sujetos intervinientes[140].

Del principio de licitud deben destacarse dos elementos: la obligación de contar con un título habilitante, constituye una exigencia para los terceros y la heterogeneidad de las circunstancias que aseguran la licitud del tratamiento[141], pero necesariamente debe existir alguna, en caso contrario, el tratamiento no es jurídicamente aceptable.

El principio de lealtad[142], por su parte, es eminentemente subjetivo. Se materializa en un específico deber de conducta, que impone el acatamiento de las normativas sobre tratamiento de la información personal, amén de la adecuación de las actuaciones a las particularidades de cada tratamiento concreto.

Este principio preside el conjunto del tratamiento, aunque se proyecta con especial intensidad sobre el binomio responsable[143]-interesado[144]. Con él se busca propiciar las condiciones adecuadas para que

---

138 Art. 5.1.a) RGPD: «tratados de manera lícita, leal y transparente en relación con el interesado».

139 El responsable, al diseñar el tratamiento, ha de identificar el título –o títulos– que lo habilitan y, además, merced a la exigencia de proactividad, ha de ser capaz de probarlo.
Las bases de legitimación previstas en el RGPD, art. 6, son: consentimiento, contrato, obligación legal, protección de intereses vitales, misión realizada en interés público o ejercitando poderes públicos y, finalmente, la concurrencia de algún interés legítimo del responsable o de un tercero que prevalezca sobre los intereses del interesado.

140 Por ejemplo si es una entidad pública la que quiere tratar los datos o si el interesado está en una situación en la que el tratamiento es necesario para preservar su vida o salud

141 Los motivos que dan fundamento al consentimiento son diferentes a los del contrato o los intereses vitales.

142 Art. 5.1.a) RGPD: «tratados de manera lícita, leal y transparente en relación con el interesado».

143 El IT Governance Privacy Team concreta los deberes de actuación que el principio de lealtad impone al responsable. Así, este tiene que ser: «*open and honest about its identity; obtains data from someone who is legally authorised/required to provide it; only handles data in ways the data subject would reasonably expect; does not use data in ways that might unjustifiably have a negative effect on them*» (IT, 2019, p. 33).

144 Algún autor se ha preguntado si el interesado también estaría sometido a este deber de actuar de un modo honesto y transparente (Palma Ortigosa, 2018, p. 43) y en qué grado.
En la práctica, son contadas las ocasiones en que tendría que acomodar sus actuaciones a esta exigencia, con excepción del momento de facilitar la información, en el que se le podría exigir que esta fuese real y actualizada. En todo caso, las normativas de desarrollo no prevén sanciones directas al interesado. La falta de lealtad del interesado no parece tener más

los individuos puedan desplegar sus facultades de actuación, amén de generar confiabilidad respecto del modo en que se opera con la información[145]. Esta dimensión informativa entronca la exigencia de tratamiento leal con el principio de transparencia[146].

El deber de tratar los datos de un modo «transparente», impone al responsable un modo específico de proceder, que se proyecta sobre todas las fases del tratamiento[147]. Con él se busca hacer cognoscible el tratamiento (sus implicaciones, sus riesgos, las garantías implementadas, etc.), facilitando su fiscalización y el ejercicio de las facultades de actuación por parte de la ciudadanía.

Para asegurar su cumplimiento, se establece un deber general de información que, además, ha de reunir ciertas características en cuanto al modo de transmitirse[148]: ser fácilmente accesible, concisa, comprensible en

---

consecuencias para él que las que pudieran derivarse de un tratamiento fundado en datos incorrectos.
Cuestión distinta es determinar si el responsable puede ver minorada su responsabilidad en aquellos casos en los que estuviese operando con datos erróneos porque así se los ha proporcionados por el interesado. Así lo ha entendido, por ejemplo, el legislador español, a la hora de establecer excepciones al incumplimiento del principio de exactitud de los datos (art. 4.2 LOPDGDD). A su vez, esa previsión muestra la interconexión entre principios.
En el modelo europeo de protección de datos, y merced al principio de exactitud que los Reglamentos establecen, no basta con acreditar que la información incorrecta provenía del interesado, sino que deberá demostrarse cierta diligencia al tratarla, en el sentido de que el responsable está obligado a detectar la información incongruente.

[145] Al imponer que el responsable actúe con razonabilidad y previsibilidad, se termina por generar un entorno más seguro y propicio para que los datos fluyan, lo que, en última instancia, refuerza el modelo europeo de tratamiento.

[146] Sobre los principios de lealtad y transparencia, sus efectos, sus diferencias y cómo se complementan, vid. (Berrocal Lanzarot, 2019, pp. 151-162), (Muñoz, 2018).

[147] El deber de transparencia, al igual que el derecho de acceso, «*lays down a general technical and procedural principle of enabling the exercise of*» *data subjects rights* (Polčák, 2020, p. 410).

[148] Además de la forma, también se granula la cantidad de información a facilitar en atención al grado de participación en el tratamiento. Así, el primer nivel de información, está destinado al conocimiento de toda la ciudadanía. En él, se describen las características del tratamiento que se lleva a efecto, las medidas de seguridad que se adoptan, los sujetos que intervienen (quien es el responsable, si hay, o no, delegado de protección de datos, si hay transferencias a terceros…), los tipos de datos que se recaban, las finalidades que se persiguen, las bases de legitimación con las que se opera o los derechos que se podrían llegar a ejercitar. Las políticas de privacidad o los registros de tratamiento son la plasmación de ese deber de información que, a su vez, está estrechamente vinculado con el principio de transparencia.
El segundo nivel de información está focalizado en la relación responsable-interesado. En coherencia, la información que se transmite tendrá un mayor grado de detalle y, sobre todo, de personalización. Ya no bastarán las descripciones generales, sino que habrán de facilitarse los detalles específicos del tratamiento y, habrá de hacerse en relación con el sujeto afectado. Así, habrá de informarse sobre cuestiones como el modo en que se han obtenido de los datos, qué datos concretos se están utilizando y para qué o a quién se han transferido (en caso de haberlo hecho).

sus términos y visible (con un tamaño de letra apropiado) (Considerando 39 RGPD)[149].

Además, extiende sus efectos más allá de los tratamientos efectivamente realizados, al reforzar la base informativa en la que los potenciales interesados fundarán su decisión de consentir, o no, el tratamiento. Conectando, de este modo, con el principio de licitud (Aparicio Salom y Vidal Laso, 2019, p. 54) y justificando, en parte, el tratamiento sistemático que realiza el RGPD (art. 5.1.a), pese a las diferencias de contenido[150].

Al dar publicidad a las condiciones del tratamiento, se logra condicionar el modo en que se lleva a cabo. Ese efecto condicionante es su principal valor, pues contribuye a generar una cultura y conciencia jurídicas en torno al tratamiento de los datos personales y, por lo tanto, a consolidar el cambio hacia un modelo más proactivo.

Por su parte, el principio de limitación de la finalidad (art. 5.1.b))[151] exige que los datos sean «recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines». El cumplimiento de estas obligaciones requiere del diseño previo del tratamiento, así como la atención a las consecuencias del mismo[152]. Con él se busca asegurar que el tratamiento obedezca a razones

---

[149] El Grupo de Trabajo del Artículo 29 (GT29) elaboró las *Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679*. Estas ofrecen un compendio de todas las condiciones que han de reunirse para considerar que un tratamiento se está llevando a cabo con la transparencia debida, así como una exégesis detallada de los deberes de información de los artículos 13 y 14 del RGPD.
Puede consultarse, la versión en castellano en:
https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/wp260rev01_es-transparencia.pdf. (Última consulta: 20/10/2021).

[150] Recuérdese que el principio de transparencia se enuncia junto a los principios de licitud y lealtad. Art. 5.1.a) RGPD «Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)».

[151] Art. 5.1.b) RGPD: «recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales». Para un análisis más detallado, vid. (Palma Ortigosa, 2018, pp. 43-45) y (Troncoso Reigada, 2021b, pp. 858-872) quien realiza una exégesis detallada los cuatro elementos que conforman el principio de finalidad.

[152] Vid. GT29, Dictamen 03/2013 sobre limitación a la finalidad, de 2 de abril de 2013. Puede consultarse en:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. (Última consulta: 20/10/2021).

justificadas y legítimas; asimismo, hace que el tratamiento sea previsible[153].

Como puede colegirse, este principio está estrechamente conectado con el principio de licitud, además de contribuir a la materialización de la proactividad por la que apuesta el modelo europeo de protección de datos[154].

Con todo, esa exigencia de previsibilidad y certeza puede rozar, en ocasiones, con el dinamismo propio de la era digital[155]. A pesar de ello, «*requiring prior determination of the purpose of processing may be one way to prevent overly enthusiastic data harvesting, and as a legal stipulation it may have more force than an ethical principle to stick to context*» (Hildebrandt, 2013, p. 38). Estamos ante un principio mediante el que se modula y condiciona el diseño de los tratamientos, aunque ello comporte una mayor complejidad de los procesos.

Conforme al principio de minimización de datos, las informaciones que se traten han de ser «adecuad[a]s, pertinentes y limitad[a]s a lo necesario» (art. 5.1.c)) para la consecución de los objetivos que se

---

153 El RGPD prohíbe los tratamientos ulteriores de unos mismos datos, cuando sean incompatibles con los fines originarios y conocidos por el interesado. La limitación a la finalidad opera como una barrera para los segundos y terceros usos de la información. Nuevos fines, nueva justificación.
Al excluir todo tratamiento ulterior cuyos fines sean incompatibles, el RGPD abre la puerta para que aquellos tratamientos que tengan fines compatibles (Considerando 50 RGPD) puedan llevarse a efecto con apoyo en la base de legitimación originaria. La legislación europea regula una serie de supuestos en los que la compatibilidad es una opción viable (Considerando 50 RGPD), si bien es cierto que, previamente, habrá de evaluarse previamente si es posible alcanzarlos sin utilizar datos personales (Considerando 156 RGPD). En todo caso, como ha apuntado el GT29, «further processing for a different purpose does not necessarily mean that it is incompatible: compatibility needs to be assessed on a case-by-case basis», GT 29, Dictamen 03/2013 sobre limitación a la finalidad, de 2 de abril de 2013, p. 3.
En los casos de tratamientos ulteriores, los deberes de información deberían de acentuarse (Cavoukian, Dix, y El Emam, 2014); en caso contrario, se dificultaría, de manera injustificada, la utilización de los instrumentos de defensa que el derecho a la protección de datos proporciona (Barbará i Fondevila, 2014, p. 10).

154 Conocer el propósito de los tratamientos facilita la selección de la base de legitimación más adecuada y, sobre todo, permite evaluar si la finalidad perseguida justifica las eventuales afectaciones de bienes jurídicos que pudieran producirse.

155 Este es uno de los déficits que presenta el RGPD, pues no dispone de ningún instrumento –ni de criterios interpretativos– que permitan compatibilizar la limitación a la finalidad con la utilización de sistemas de tratamiento masivo de información. Como apunta Hildebrandt «*the value of Big Data can only be set free if we admit the novelty of the inferred knowledge and rethink purpose binding in line with the innovative potential of its outcomes*» (Hildebrandt, 2013, p.36). Auque, en el Considerando 50 del RGPD, se apuntan las condiciones que debe reunir un tratamiento ulterior para ser considerado como compatible, no parecen suficientes para afrontar la multiplicidad de posibles usos que del *big data* se derivan.

persiguen[156]. Con él se busca evitar la utilización indiscriminada y desproporcionada de informaciones personales. No basta con determinar qué finalidades se persiguen, ha de alcanzarse el objetivo con el menor grado de afectación de los derechos. La ausencia de «diferenciación, limitación o excepción [a la hora de recabar datos] en función del objetivo» conlleva la vulneración de este principio[157].

La proposición de partida es sencilla, a menor información en manos de un responsable, menor riesgo (Zarsky, 2017, p. 1010). Con todo, la minimización de los datos no debe entenderse solo en un sentido cuantitativo, tiene, también, un componente cualitativo. En la media en que resulte posible lograr unos resultados equivalentes, deberá priorizarse la utilización de aquellos datos que, *a priori*, entrañen un menor riesgo para los bienes jurídicos de los interesados.

Este principio entronca con la exigencia de adecuación a los fines y a la realidad de los tratamientos, imponiendo al responsable un deber de autocontención y previsión[158].

En esa línea de asegurar la concordancia dato-persona y «evita[r] que el afectado sea tratado de forma desigual respecto a los demás ciudadanos» (Troncoso Reigada, 2021b, p. 887), resulta crucial el principio

[156] Como puede intuirse, la minimización de datos resulta difícilmente compatible, incluso «*antithetical*» (Bennet y Bayley, 2016, p. 210), con el *big data*Sobre las dificultades para compatibilizar el respeto a este principio y la utilización del técnicas de tratamiento masivo de información, vid. (Rouvroy, 2016, p. 14) o (van der Sloot y van Schendel, 2016, p. 119).

[157] Así lo ha considerado el TJUE en el asunto Digital Rights Ireland, STJUE asunto Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, 8 de abril de 2014, apdo. 57.

[158] En consonancia con el principio de minimización, el art. 11.1 del RGPD establece que cuando no sea necesaria «la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional» para dicha finalidad. Es decir, podrá prescindir de conservar ciertos datos identificativos, siempre que pueda alcanzar las finalidades del tratamiento sin ellos. Por otra parte, no puede dejar de constatarse el carácter voluntario de este precepto –en contraste con la obligación de minimizar– (Georgieva, 2020, p. 392). En última instancia, más que una minimización, estamos ante un modo indirecto de seudonimizar la información, que tiene como consecuencias la reducción del riesgo y la posibilidad de denegar el ejercicio de ciertas facultades de actuación.

de exactitud[159] exige que los datos sean «exactos y, si fuera necesario, actualizados» (art. 5.1.d RGPD)[160].

La exactitud de los datos conecta con el deber de tratar la información personal para fines concretos y, sobre todo, con la protección de los bienes jurídicos del interesado frente su uso. En efecto, si la materia prima no es la correcta, el resultado no será el perseguido, ni se alcanzarán los objetivos que justificaron el tratamiento y, consecuentemente, se producirá una injerencia en el derecho a la protección de datos.

En esa línea de prevención de efectos no deseados a raíz del tratamiento de datos personales, se incardina el principio de limitación del plazo de conservación[161] (art. 5.1.e) RGPD)[162]. Conforme a este principio, el responsable del tratamiento solo podrá operar con los datos durante el tiempo necesario para la consecución de los fines para los que fueron recabados[163].

Establecer que el tratamiento de información personal se realice «durante no más tiempo del necesario» (art. 5.1.e RGPD) implica que será la finalidad del tratamiento, y no la voluntad del responsable, la que

---

[159] Conforme a este principio, los datos habrán de ser «exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan» (art. 5.1.d) del RGPD).

[160] Sin perjuicio de las eventuales excepciones que, en atención a las circunstancias en que se recabó la información, pudieran establecer los Estados miembros. Por ejemplo, en el caso de España, se han previsto, en el art. 4.2 de la LOPDGG, cuatro situaciones que generan una presunción de exactitud: 1. Que la información hubiera sido facilitada del interesado; 2. Que los datos provinieran de un mediador o intermediario que los hubiera recabado en nombre propio; 3. Cuando el responsable los hubiese recibido de otro a raíz del ejercicio del derecho a la portabilidad por parte del interesado; 4. Cuando tuvieran su origen en un registro público. Para una ampliación de estas excepciones y sus implicaciones, vid. (Garriga Domínguez, 2019).

[161] La limitación del plazo de conservación tiene una conexión directa con la idea de reducción de riesgos. Al acompasar la conservación de la información y la consecución de los objetivos, se minoran las posibilidades de afectación de los derechos.

[162] El art. 5.1.e) RGPD dispone que los datos serán «mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado».

[163] No supone, necesariamente, que una vez alcanzados los objetivos, esa información no se pueda utilizar de ningún modo. En efecto, existe una alternativa que posibilita cumplir con las exigencias del principio de limitación del plazo de conservación sin eliminar la información: la anonimización (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2018, p. 147).

determine el período de conservación[164]. Convirtiendo a este factor en un elemento dinámico. Al responsable no le bastará con remitirse a plazos previamente fijados; será la realidad del tratamiento la que deba guiar sus actuaciones. Si ya nada justifica el tratamiento, este no puede continuar, de hacerlo, supondría una injerencia directa en el derecho a la protección de datos.

Finalmente, los principios de integridad y confidencialidad también tienen en la seguridad del tratamiento y la reducción de riesgos su razón de ser[165]. En última instancia, son los mecanismos de los que el modelo europeo se vale para ofrecer seguridad a los interesados. Son la contrapartida que los responsables han de "pagar" por poder utilizar información personal.

El principio de integridad de la información se enfoca en la vertiente física de la gestión de la información, esto es, en los soportes con los que se opera y en las medidas de seguridad que se implementan[166].

En lo relativo a la exigencia de confidencialidad, si bien se ve beneficiada por las medidas que el principio de integridad demanda, se proyecta, especialmente, sobre la esfera subjetiva del tratamiento de datos. Todos aquellos operadores[167] que tomen parte en el tratamiento de datos

---

[164] La previsibilidad, la anticipación y el derecho/obligación de información que preside el modelo europeo hacen necesario anticipar el período de tiempo durante que cuál se va a gestionar la información. Además, cuando el tratamiento obedezca, «exclusivamente», a razones de «archivo en interés público, fines de investigación científica o histórica o fines estadísticos» (5.1.e RGPD), se admitirán «períodos más largos» de conservación. Con esta excepción, el RGPD está estableciendo una relajación del nexo causal: consecución del objetivo → finalización del tratamiento → supresión o anonimización de los datos.

[165] El modelo europeo exige que los datos sean «tratados de tal manera que se garantice una seguridad adecuada […], incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas» (art. 5.1.f RGPD).

[166] Se han de adoptar las medidas técnicas y organizativas que mejor se ajusten a la realidad del tratamiento, tomando en consideración cuestiones como si los datos están digitalizados o se encuentran en soporte analógico, el entorno en que se gestionan, o quién va a tener acceso a los mismos.

Estas exigencias incluyen el diseño de una política específica de tratamiento de datos, un análisis de los riesgos y la implementación de las medidas más adecuadas para reducirlos. Son ejemplos de medidas posibles, la seudonimización, la encriptación de la información, las verificaciones en dos pasos, la formación de los empleados que gestionarán la información o la adhesión a códigos de conducta. En todo caso, el responsable deberá acompasar los instrumentos de protección a las características y contexto del tratamiento, así como a los peligros específicos que puedan derivarse de eventuales brechas de seguridad o pérdidas de información.

[167] Esencialmente, los responsables, los encargados, los destinatarios, los delegados de protección de datos.

son sujetos obligados por el deber de confidencialidad. Ese deber de reserva no se agota con el tratamiento, sino que pervive en el tiempo. Su objetivo es evitar los efectos derivados de la utilización de esa información fuera del contexto específico en que el tratamiento tuvo lugar. Por otra parte, en aquellos casos en que esta obligación concurra junto al deber de secreto profesional[168], este último no lo sustituye, sino que se complementan. El secreto profesional constituye un refuerzo del deber de confidencialidad y reserva[169].

3.7. El alma del Reglamento General de Protección de Datos: proactividad y riesgo

3.7.1. El responsable del tratamiento

El éxito o el fracaso del modelo europeo de protección de datos europeo no depende, en exclusiva, del ejercicio por parte del interesado de sus facultades de actuación. Antes bien, la buena marcha de los tratamientos, su adecuación a las exigencias normativas y el respeto a los derechos fundamentales pende, fundamentalmente, del diseño y ejecución de las operaciones de tratamiento o, dicho con otras palabras, del responsable del tratamiento. Este es el «principal sujeto obligado por la normativa […][,] es el que decide sobre el tratamiento» (Durán Cardo, 2021, pp. 637 y 638), sobre sus características, sobre los datos necesarios, las finalidades a lograr o el modo en que se actuará (los medios personales y técnicos).

Por lo tanto, el responsable del tratamiento es, en cierto modo, el autor intelectual del mismo. No tiene por qué ejecutarlo, ni su persona tiene por qué coincidir con la encargada de gestionar los datos personales. El responsable puede decidir que sean otros los que lo lleven a efecto (p. ej. los encargados del tratamiento[170]), pero siempre será él quien determine «los fines y medios» (art. 4.7 RGPD) que lo definen.

---

168 Sobre el concepto de secreto profesional, vid. (J. García Sanz, 2005).

169 La seguridad adicional que el secreto profesional proporciona tiene tal entidad que sirve como causa habilitante para permitir el tratamiento de datos especiales cuando sea «necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social» (art. 9.2.h)) en conjunción con el art. 9.3 del RGPD.

170 Los encargados del tratamiento son aquellos sujetos/entidades que traten «datos por cuenta del responsable del tratamiento» (art. 4.8 RGPD). Su figura se desarrolla con más

El RGPD elabora un concepto autónomo[171] de responsable, que ha de ser interpretado en sentido amplio[172]. Así lo sugiere el EDPB en sus Directrices, al señalar que la condición de responsable «*may be defined by law or may stem from an analysis of the factual elements or circumstances of the case*»[173]. Por tanto, más allá de apreciaciones formales, será la realidad del tratamiento y quien determine el «*why and how*»[174] del mismo, lo que permita identificar al responsable.

En consonancia con ello, pueden ser responsables del tratamiento tanto personas físicas como jurídicas, así como autoridades, servicios u organismos públicos. No se ha preestablecido un «límite al tipo de entidad que puede asumir el rol de responsable del tratamiento» (Durán Cardo, 2021, p. 645). Son las acciones y no las condiciones del sujeto las que determinan la condición de responsable[175].

Además, el responsable puede actuar conjuntamente con otro, dando lugar a supuestos de corresponsabilidad, caracterizados por la determinación conjunta de «los objetivos y los medios del tratamiento» (art. 26.1 RGPD). Con todo, cuando se hable de corresponsabilidad debe tomarse en consideración que, «responsabilidad conjunta no implica idéntica responsabilidad» (Caamaño Domínguez y Jove Villares, 2021, p.

---

detalle en el artículo 28 del RGPD. Sobre el encargado del tratamiento, vid. (Núñez García, 2016), (Farré Tous, 2021) y (García del Poyo Vizcaya, 2021).

171 La condición autónoma del concepto «responsable» se refiere a su carácter eminentemente europeo. Es un concepto que ha de «interpretarse fundamentalmente con arreglo a la legislación sobre protección de datos», es decir, a la normativa europea, sin que otras previsiones legales alteren sus condiciones basilares.

172 STJUE asunto C 131/12, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014, apdo. 34. En el que señala que la Directiva, pretende garantizar «mediante una definición amplia del concepto de "responsable", una protección eficaz y completa de los interesados El concepto de responsable del tratamiento no debería verse afectado por otros conceptos —con los que a veces colisiona o se solapa— de otros ámbitos del Derecho, como el de autor o titular de derechos de propiedad intelectual», GT29, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», de 26 de febrero de 2010, p. 10. Puede consultarse, en:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf. (Última consulta: 20/10/2021).

173 EDPB, Directrices 07/2020 sobre los conceptos de responsable y encargado en el RGPD, versión 1.0, adoptada el 2 de septiembre de 2020. Puede consultarse su versión en inglés en: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf, p. 3. (Última consulta: 20/10/2021).

174 Ibídem.

175 Si bien es cierto que, «preferentemente[,] debe considerarse responsable del tratamiento a la empresa o al organismo como tal antes que a una persona concreta dentro de la empresa o el organismo», en GT29, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», de 26 de febrero de 2010, p. 17.

1828). En esta línea se ha pronunciado el TJUE, al señalar que pueden existir, «distintos grados [de responsabilidad], de modo que […] [las consecuencias para cada responsable deben] evaluarse teniendo en cuenta todas las circunstancias pertinentes del caso concreto»[176].

Sea de manera individual, o conjuntamente con otros responsables, no cabe duda de la centralidad del responsable[177] en la lógica inherente al modelo articulado por el RGPD.

3.7.2. La proactividad. Elemento central del modelo

En la configuración del marco de actuación del responsable existían dos líneas de actuación posibles. «Los medios para estimular la responsabilidad pueden ser proactivos o reactivos. En el primer caso, consisten en garantizar la aplicación efectiva de las medidas de protección de datos y unos medios suficientes para que los responsables del tratamiento puedan rendir cuentas de su actividad. En el segundo caso, los medios pueden abarcar la responsabilidad civil y sanciones para garantizar que se indemnicen los perjuicios de cierta consideración y se adopten las medidas pertinentes para subsanar posibles errores o irregularidades»[178]. El RGPD, sin prescindir de los elementos reactivos, tiene en la proactividad su línea maestra.

Resulta, cuanto menos curioso, que la responsabilidad proactiva, pese a ser un elemento definitorio del sistema de protección de datos europeo, solo aparezca expresamente mencionada en dos ocasiones. Una en el articulado (art. 5.2 RGPD), donde se la reconoce como principio, y otra en el Considerando 85, para señalar uno de sus efectos: que su cumplimiento puede permitir no tener que notificar una violación de

---

[176] STJUE asunto C-210/16, Wirtschaftsakademie Schleswig-Holstein, de 5 de junio de 2018, apdo. 43.

[177] Del responsable del tratamiento solo se han señalado los elementos definitorios de la figura, pues, a los efectos que aquí interesa, no es necesario entrar en detalles acerca de sus cometidos concretos o de quien puede ostentar dicha condición, así como otras características más específicas. Para un estudio más detallado sobre esta figura me remito a la extensa y detallada monografía de Durán Cardo, (Durán Cardo, 2016); así como el comentario sobre la regulación en el RGPD de los responsables del tratamiento realizado por la misma autora, (Durán Cardo, 2021). También resultan de interés por su grado de detalle y claridad, los trabajos de (Núñez García, 2019) y (Bygrave y Tosoni, 2020).

[178] GT29, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», de 26 de febrero de 2010, p. 7.

seguridad[179]. Sin embargo, el principio de responsabilidad proactiva[180] es el que define y condiciona el modelo de protección de datos.

Hasta el RGPD, el método de protección era eminentemente reactivo, se «ponía el acento en el establecimiento de reglas y estándares mínimos en la gestión de la información, y [se] contemplaba[n] vías de reparación a posteriori, esto es, cuando ya se había producido la vulneración de la privacidad» (Medina Guerrero, 2020, p. 42). El modelo actual hace honor a esa condición proactiva[181], pues insta a los operadores de datos a tomar activamente el control y decidir qué hacer en cada momento. García Mexía y Perete Ramírez, apuntan cuál sería el de esta apuesta por la proactividad: «propiciar un cambio de mentalidad en las empresas, pasando de un enfoque reactivo a un enfoque preventivo basado en la reducción de cargas administrativas y en un mayor nivel de responsabilidad de las empresas» (García Mexía y Perete Ramírez, 2018, p. 173).

En el plano normativo, la proactividad supone que el responsable habrá de cumplir con los demás principios previstos en el 5.1 RGPD y que, además, ha de ser capaz de demostrarlo. Este modo de afrontar el tratamiento de la información personal, además de reforzar la vertiente procedimental del derecho, aproxima su ejecución práctica a los modelos de *compliance* penal (López Calvo, 2017, pp. 81-88).

La positivización del principio de proactividad implica asumir e implementar un modelo de protección con unos rasgos muy definidos: la anticipación a los problemas; la definición de toda una política de prevención de riesgos; la exigencia de cauciones a la hora de diseñar y ejecutar los tratamientos; la atención a la realidad de cada tratamiento; y

[179] El elemento clave será la capacidad para demostrar que esa brecha de seguridad es improbable que «entrañe un riesgo para los derechos y las libertades de las personas físicas». La ausencia de notificación de brechas de seguridad, si no está debidamente justificada, puede suponer importantes sanciones, p. ej., en diciembre de 2020, la *Irish Data Protection Commission* impuso a Twitter una sanción de 450 000€ por no notificar en plazo (72 horas) una quiebra en la seguridad de los datos que gestiona. Toda la información sobre el proceso puede consultarse en: https://edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_en#. (Última consulta: 20/10/2021).

[180] El primer antecedente de la proactividad configurada en el RGPD sería, con todas las distancias en cuanto a fuerza vinculante e impacto en el sistema, el principio de responsabilidad previsto en el art. 14 de las Directrices de la OCDE de 1980, «A todo inspector de datos se le deberían pedir responsabilidades por el cumplimiento de las medidas que permiten la aplicación de los principios antes expuestos».

[181] Conforme a la definición de proactivo de la RAE, «que toma activamente el control y decide qué hacer en cada momento, anticipándose a los acontecimientos».

la información, la transparencia y la rendición de cuentas, como exigencias inexcusables.

El principio de responsabilidad proactiva es la palanca de la que se vale el legislador europeo para propiciar un cambio –cultural y práctico– en el modo de entender y regular el tratamiento de datos personales y fomentar un entorno que facilite su protección y defensa.

Desde un punto de vista jurídico, el principio de responsabilidad proactiva impone, al responsable del tratamiento, el deber de examinar las actuaciones que lleva o pretende llevar a efecto, evaluarlas y adoptar las medidas necesarias para asegurar el cumplimiento de los principios del tratamiento y, en general, de las previsiones y obligaciones del RGPD[182]. La responsabilidad proactiva exige del responsable la atención a las particularidades del tratamiento, a «la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas» (art. 24.1 RGPD), debiendo estar en condiciones de acreditar que ha obrado con la debida diligencia. Por lo tanto, la vigilancia y la actualización de las medidas implementadas son determinantes para verificar el cumplimiento de este principio[183].

Pero no solo eso. La responsabilidad proactiva es la respuesta jurídica que la UE ha encontrado para hacer frente a la mayoría de los problemas derivados del dinamismo que caracteriza a la realidad digital. Es la pieza que permite equilibrar el establecimiento de unas reglas comunes de obligado cumplimiento y la existencia de un ámbito de flexibilidad suficiente que permita a quienes diseñan los tratamientos operar, con un mínimo de seguridad, en las turbulentas aguas del desarrollo tecnológico. La principal misión de este principio es evitar que el Derecho no vaya muy por detrás de la realidad (Martínez Martínez, 2019, 340).

[182] En esa línea interpretativa apunta (Berrocal Lanzarot, 2019, p. 168).
[183] Para un análisis más detallado del principio de responsabilidad proactiva, vid. (Martínez Martínez, 2019b) y (Nuñez García, 2019, pp. 353-348).

3.7.2.1. Una breve digresión acerca de la autorregulación y la responsabilidad proactiva

Apostar por la responsabilidad proactiva supone priorizar la atención al contexto, a los riesgos y a las condiciones de cada tratamiento. Si se apurase este enfoque, podría alcanzarse la conclusión de que la proactividad es una especie de seudoautorregulación. Sin embargo, no es así. El RGPD no prevé autorregulaciones en sentido estricto, como las que pueden existir en Estados Unidos respecto de las relaciones *inter privatos*.

No puede hablarse, en puridad, de autorregulación porque la proactividad no deja exclusivamente al albur del responsable la selección y determinación de las medidas de protección y tratamiento. Las posibilidades de actuación de los responsables están circunscritas al cumplimiento de las previsiones del RGPD y a los derechos de los interesados.

Su flexibilidad se traduce, fundamentalmente, en la mayor capacidad de los operadores de datos para evaluar, seleccionar y disponer aquellas medidas de protección más adecuadas a las particularidades de cada tratamiento.

Así, el RGPD admite –incluso incentiva– que se adopten códigos de conducta (arts. 40-41 RGPD) y mecanismos de certificación (arts. 42-43 RGPD)[184]. En efecto, los códigos de conducta y fórmulas similares no dejan de ser una forma de «autorregulación regulada» (Serrano Pérez, 2021). Al adecuar el cumplimiento de la normativa a las particularidades de un sector, ofrecen seguridad a las entidades que los han adoptado, además de a los propios interesados[185]. La granulación y precisión que los códigos de

[184] Acerca de la importancia de los códigos de conducta y los mecanismos de certificación, sus límites y posibilidades, vid. (Prieto Hergueta, 2019), (Sáiz Peña, 2019) y (Díaz-Romeral Gómez, 2016).

[185] Seguramente el mejor ejemplo de la utilidad de los códigos de conducta sea la STJUE asunto C-311/18, Facebook Ireland & Maximillian Schrems, de 16 de julio de 2020. Mientras el *Privacy Shield* es declarado contrario a los estándares europeos en materia de protección de los derechos por no ofrecer una protección adecuada, tanto las cláusulas contractuales tipo, como los tratamientos fundados en códigos de conducta, perviven si se acredita su adecuación a las exigencias normativas europeas, por ejemplo, por adecuarse a las *Directrices 1/2019 sobre códigos de conducta y organismos de supervisión con arreglo al Reglamento (UE) 2016/679* del Comité Europeo de Protección de Datos, pueden consultarse en: https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-12019-codes-conduct-and-monitoring-bodies-under_es. (Última consulta: 20/10/2021).
Sobre los efectos y consecuencias de Schrems II, vid. (Tracol, 2020), (de Miguel Asensio, 2020), (Sobrino García, 2020) y (von Danwitz, 2020).

conducta permiten resulta imposible de prever normativamente en una regulación general[186].

En todo caso, no es obligatorio que el responsable se adhiera a códigos de conducta o cuente con certificaciones en materia de protección de datos para cumplir con las exigencias derivadas del RGPD. Estamos ante «una solución complementaria y no puede ser la garantía única sobre la que descanse la privacidad de los usuarios» (Troncoso Reigada, 2012, p. 53).

3.7.3. El riesgo[187] como factor modulador y condicionante del sistema

El temor atávico a los efectos derivados del tratamiento de datos ha operado como motor de cambio e impulso de las normativas sobre la materia, también del RGPD. El diseño de todo tratamiento ha de considerar los riesgos que entraña[188].

La importancia del riesgo en el RGPD también se refleja desde un punto de vista cuantitativo. Su presencia se ha multiplicado por nueve (de 8 menciones en la Directiva 95/46/CE a 73 en el RGPD), mientras que el

---

[186] Como apunta Martínez Martínez, «el nivel de exigencia de un Código de Conducta es enorme, y sin embargo deberían impulsarse. Junto con las certificaciones son un instrumento dotado de criterios, de listas de verificación y controles. Pero, sobre todo, nacen desde abajo, desde los responsables del tratamiento y los encargados. Adherirse a un pacto es reseñable, adoptar un código de conducta supone un esfuerzo valioso» (Martínez Martínez, 2021a).
Por su utilidad, resulta sorprendente que, en el caso de España, solo conste un único código en el Registro de la AEPD. El código de conducta que consta es el de tratamiento de datos en actividad publicitaria (autocontrol). Puede consultarse en, https://www.aepd.es/es/informes-y-resoluciones/codigos-de-conducta. En el registro del EDPB constan solo tres, uno de ellos, el registrado en la AEPD. Puede consultarse el registro del EDPB en: https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_es. (Última consulta: 20/10/2021).

[187] Como Luhmann ha señalado, el riesgo, como concepto, admite diferentes interpretaciones, grados, límites y distinciones respecto de términos conexos, como puede ser el de peligro, (Luhmann, 1996). En este sentido, a los efectos de este trabajo se utilizará el concepto de riesgo definido por el GT29 en las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para
determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del
Reglamento (UE) 2016/679, de 4 de abril de 2017 (se utiliza la versión revisada de 4 de octubre de 2017). Conforme a estas Directrices, un riesgo «es un escenario que describe un acontecimiento y sus consecuencias, estimado en términos de gravedad y probabilidad», p. 7.

[188] El riesgo es un parámetro de actuación de los operadores de datos. Así, el Considerando 83 RGPD señala que, «a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos».

RGPD tiene una extensión apenas dos veces superior a la que tenía la Directiva 95/46/CE.

El riesgo, como parámetro modulador del tratamiento, está estrechamente conectado con el resto de elementos caracterizadores del modelo europeo de protección: la proactividad, la adecuación a las características del tratamiento que los principios demandan (atención a la finalidad, la minimización de los datos o el ajuste de los plazos) o la protección de datos desde el diseño y por defecto. Ese conjunto de actuaciones se ven enriquecidas por la atención al riesgo, que opera como acicate, mejorando la adecuación de los tratamientos a la realidad y logrando una mayor precisión de las medidas de protección.

En la sociedad del riesgo, «*the past loses its power to determine the present. Its place as the cause of present-day experience and action is taken by the future, that is to say, something nonexistent, constructed and fictitious. We are discussing and arguing about something which is not the case, but could happen if we were not to change course*» (Beck, 2000). En el caso del derecho a la protección de datos, son las probabilidades de un daño futuro lo que determina la fisonomía presente del tratamiento.

El riesgo es consustancial a todo tratamiento de datos personales. No hay un tratamiento seguro *per se*. Los riesgos pueden tener orígenes diversos, desde cuestiones puramente técnicas, como las brechas de seguridad o la destrucción de los datos, hasta usos indebidos de la información facilitada. Si variadas son las causas, las consecuencias gravosas para el interesado no lo son menos. A título ejemplificativo: «problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo»[189].

Si bien es cierto que hay un riesgo consustancial a todo tratamiento, no todos entrañan el mismo grado de peligrosidad. Entre los objetivos del RGPD se cuenta, el establecer las medidas apropiadas para minorar esos riesgos y hacer los tratamientos de datos jurídicamente aceptables. En consonancia con los deberes de responsabilidad proactiva, el responsable

[189] Considerando 75, en la misma línea se manifiesta el Considerando85.

será quien deba valorar el nivel de riesgo, concretar las medidas que puedan servir para minorarlo y decidir si el nivel de riesgo es asumible[190].

El RGPD proporciona una serie de criterios, exigencias y mínimos comunes que todo tratamiento debe cumplir. Gradúa las medidas a implementar en función de la probabilidad de riesgo y establece un régimen más severo cuando el tratamiento suponga un «alto riesgo». La noción de alto riesgo resulta clave, de ella depende la necesidad de llevar a efecto ciertas actuaciones. Consecuentemente, es necesario determinar el nivel de riesgo para todo tratamiento. Por ejemplo mediante matrices de riesgo como la de la Figura 1.

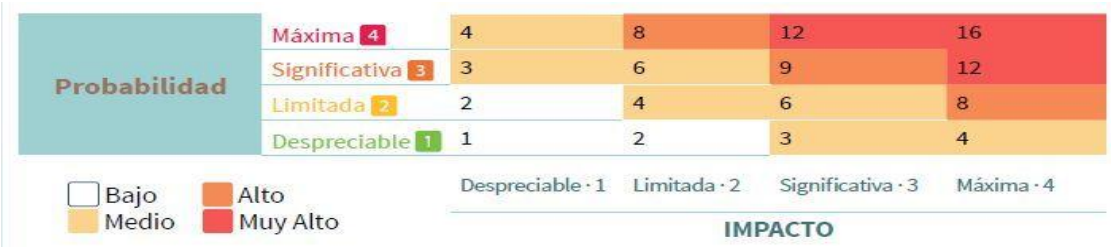

Figura 1: Matriz de riesgo tomada de la Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD de la Agencia Española de Protección de Datos

El RGPD no contiene una definición expresa de alto riesgo, pero sí apunta ciertos elementos que permiten identificarlo. Serán tratamientos de alto riesgo aquellos que comporten una amenaza de mayor entidad para los derechos, o puedan hacer más difícil su ejercicio (Considerando 91), por ejemplo, porque empleen nuevas tecnologías[191] o por el «alcance, contexto

[190] Las posibilidades de llevar a cabo el tratamiento están estrechamente vinculadas al modo en que este se va a ejecutar, no dependen en exclusiva de los objetivos que se persigan. En última instancia, el responsable ha de realizar un ejercicio de ponderación entre los riesgos que el tratamiento supone, las finalidades que persigue y las medidas que debe, y puede, adoptar, pues no siempre tendrá lo medios económicos y técnicos para implementar la más segura de las opciones que el mercado ofrezca.

[191] Entendiendo por tales cualquiera de las tecnologías de la era digital, pero también en su sentido literal por ser ingenios de «una nueva clase» (Considerando 89). Aunque la expresión "nuevas tecnologías" acostumbra a referirse a tecnologías que, como puede ser el caso de Internet, poco tienen de nuevo en el sentido de novedoso, aquí el adjetivo nuevo sirve tanto para recoger esa tradición denominativa como para abrir espacio a las creaciones futuras, conformando, de ese modo, una fórmula abierta capaz de abarcar lo pasado, lo presente y lo que en un futuro la técnica pueda crear.

o fines» de la operación (art. 35.1 RGPD, en la misma línea, Considerandos 76 y 89).

Esa capacidad adicional de incidencia lleva aparejada la exigencia de actuaciones preventivas más severas e implementación de medidas de seguridad y protección más firmes. Por ejemplo, el responsable verá limitada su capacidad de decisión respecto de la viabilidad del tratamiento, pues deberá consultar con las autoridades de control de datos (art. 36 RGPD).

El riesgo es un factor condicionante del diseño y viabilidad del tratamiento, haciendo de las medidas de seguridad la llave maestra del sistema. Entre las actuaciones específicas que han de implementarse y que tienen en el riesgo su principal motivación destacan: la protección de datos desde el diseño y por defecto (art. 25); la llevanza de un registro de actividades (art. 30); la notificación de brechas de seguridad (art. 34); la realización de evaluaciones de impacto (art. 35); el deber de consulta previa con las autoridades de control en caso de que se acredite un riesgo alto (art. 36) o la designación de un delegado de protección de datos (art. 37).

A las medidas de prevención señaladas, ha de añadirse el cumplimiento de los deberes generales de información que, sin ser una actuación que tenga como finalidad directa reducir el riesgo efectivo, sí permite a los interesados tomar conciencia de las potenciales consecuencias gravosas del tratamiento y actuar en consecuencia, por ejemplo, mediante la activación de sus facultades de actuación.

3.7.4. Medidas específicas de prevención de riesgos

El cumplimiento de los principios del tratamiento de datos es el mecanismo básico de reducción de riesgos. Si se minimizan los datos, si se acotan los períodos de conservación, si se actúa con proactividad y anticipando los problemas que puedan surgir, las probabilidades de afectación de los bienes jurídicos del interesado se reducen considerablemente. Sin embargo, los principios del artículo 5 del RGPD no son las únicas previsiones jurídicas destinadas a configurar un entorno seguro para el tratamiento de datos.

3.7.4.1. Protección desde el diseño y por defecto[192]

La protección de datos desde el diseño y por defecto (art. 25 RGPD) es el instrumento normativo mediante el que se pretende lograr la implementación de «medidas técnicas y organizativas apropiadas». Este dúo de actuaciones, «si bien se configuran y desarrollan como obligaciones, bien podría tratarse realmente de principios aplicables al cumplimiento» (Miralles López, 2021, p. 1814).

Conforme a este conjunto de medidas, el responsable debe evaluar los diferentes riesgos del tratamiento, así como las medidas de seguridad que está en condiciones de aplicar, tomando en consideración la estructura organizativa de su entidad, el «estado de la técnica [o] el coste de la aplicación» (art. 25.1 RGPD). La protección de datos desde el diseño y por defecto supone que, tanto en el plan previo al tratamiento, como en su realización fáctica, se habrán de cumplir las exigencias derivadas de los principios de protección de datos (art. 25 RGPD). Es una objetivación de las técnicas de autorregulación, pues ha convertido posibilidades de actuación en obligaciones del responsable (Troncoso Reigada, 2012, p. 51).

El deber de proteger los datos desde el diseño y por defecto no es una cuestión exclusivamente técnica, sino que representa un modo de entender el derecho a la protección de datos. Si se analizan los principios fundantes de la *privacy by desing*, conforme a su conceptualización por Ann Cavoukian[193], se constata que se caracteriza por ser proactiva en lugar de reactiva; por ser preventiva en lugar de reparadora; por ser transparente en lugar de opaca; y por ser funcional, evitando dicotomías (como podría ser protección de datos vs seguridad) al priorizar aquellos diseños que permitan compatibilizar diferentes realidades, sin establecer preferencias.

Cavoukian incluye, entre las particularidades de la *privacy by design*, ciertas características que, en el RGPD, se vinculan a la protección de datos por defecto. Extiende el conjunto de deberes de actuación más allá del diseño del tratamiento, incidiendo en el rol del responsable a lo largo de todo el proceso, cualquiera que sea la naturaleza del mismo (Cavoukian, 2009).

[192] Aunque se trata dos realidades con características propias, a los efectos que aquí interesan se analizarán sus efectos generales sobre la fisonomía del modelo.
[193] Ann Cavoukian fue la *Information & Privacy Commissioner* en Ontario, Canadá y una referencia en la conceptualización de la *privacy by design*.

En el caso de la normativa europea, el legislador ha escindido protección desde el diseño y la protección por defecto. En el caso de la protección «por defecto», el responsable deberá regir sus decisiones buscando la menor afectación de los derechos y la reducción de los riesgos (Ježová, 2020, p. 133). En el cumplimiento de dicho objetivo, y en coherencia con el principio de minimización de datos, se exige que solo se traten «los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento» (25.2 RGPD).

Cada responsable habrá de determinar las medidas que mejor se adapten a las características del tratamiento que pretende realizar[194] y, merced al principio de responsabilidad proactiva, deberá ser capaz de demostrar que ha actuado con la diligencia de debida y ejecutado las actuaciones más adecuadas para asegurar la integridad del tratamiento[195].

En definitiva, la protección desde el diseño y por defecto implica prever los riesgos que cada tratamiento concreto pueda entrañar[196], adoptar las medidas, técnicas y organizativas adecuadas para prevenirlos y sostener ese nivel de vigilancia y seguridad a lo largo de todo el proceso.

3.7.4.2. Notificación de violaciones de seguridad

En caso de producirse una brecha de seguridad[197] que deje expuestos los datos personales que se están tratando –ya sea por causas

[194] El RGPD ofrece, en el art. 32.1, un listado abierto de medidas que, si las circunstancias del tratamiento lo hacen oportuno, son susceptibles de ser implementadas. Entre otras, destacan: «la seudonimización y el cifrado de datos»; la incorporación de sistemas que aseguren «la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas»; implementar mecanismos que permitan «restaurar la disponibilidad y el acceso a los datos personales de forma rápida», acompañados de sistemas de alerta temprana frente a eventuales destrucciones, pérdidas o brechas de seguridad o contar con procesos «de verificación, evaluación y valoración regulares».

[195] Por su capacidad para aportar certezas en el cumplimiento de las exigencias jurídicas en torno al tratamiento de datos, resulta muy adecuada la «adhesión a un código de conducta […] o a un mecanismo de certificación» (32.3 RGPD).

[196] La exigencia de protección de datos desde el diseño y por defecto se extiende a cualquier operación con datos personales, desde la recopilación de datos, hasta la determinación del plazo de conservación, pasando por la extensión del tratamiento o la implementación de medidas que aseguren que «los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas» (art. 25.2 RGPD).

[197] El RGPD, art. 4.12, define a las violaciones de seguridad como: «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos».

internas (filtraciones), ya por agentes externos[198]–, el responsable debe comunicarlo[199], tanto a las autoridades de control («sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella[200]» (art. 33.1 RGPD)), como a los interesados («sin dilación indebida» (art. 34.1 RGPD)). No obstante, esta exigencia puede eludirse en caso de concurrir determinadas circunstancias, que el responsable deberá acreditar.

En concreto, el responsable no tendrá que poner en conocimiento de las autoridades de control aquellas brechas en las que el riesgo de afectación de los derechos y libertades sea «improbable» (33.1 RGPD). Para acreditar que se cumple tal condición, serán determinantes las medidas de seguridad que se hubiesen implementado, por ejemplo, seudonimizar los datos[201].

Por lo que se refiere al deber de notificación a los interesados, el RGPD solo exige que se comunique la brecha a las personas cuyos datos han sido objeto de una violación de seguridad, si tal evento entraña «un alto riesgo para los derechos y libertades» (art. 34.1 RGPD). Si se compara con las exigencias de comunicación a las autoridades de control, se colige que, para que se genere la obligación, la entidad de la violación ha de ser de

---

198 El GT29, en sus Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, de 3 de octubre de 2017 (se ha utilizado la versión revisada de 6 de febrero de 2018), clasifica las brechas de seguridad en tres tipos: «"Violación de la confidencialidad": cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos. "Violación de la integridad": cuando se produce una alteración no autorizada o accidental de los datos personales. "Violación de la disponibilidad": cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales, o la destrucción de los mismos» (p. 8). También es posible cualquier combinación de las tres.

199 Cómo hacer frente a las quiebras en la seguridad de la información, y medir el nivel de impacto que las mismas puedan tener, es una preocupación inherente al tratamiento de la información personal, no es una particularidad exclusiva del modelo europeo (P. M. Schwartz y Janger, 2006). Sobre la regulación en el RGPD, vid. (Davara Fernández de Marcos, 2021).

200 Cualquier retrase en el cumplimiento de este plazo deberá estar debidamente justificado (art. 33.1 RGPD).

201 Una violación de seguridad en la que se filtren datos seudonimizados, pero la clave para identificarlos permanezca segura, se trataría de un supuesto con un bajo nivel de riesgo, en el que las medidas técnicas han reducido considerablemente las posibilidades de afectación de los derechos. Ese sería, probablemente, un supuesto en que no habría que notificar la brecha de seguridad.

No obstante, como advierte el GT29, «incluso cuando los datos estén cifrados, una pérdida o alteración puede tener consecuencias negativas para los interesados cuando el responsable del tratamiento no disponga de copias de seguridad adecuadas», en Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, de 3 de octubre de 2017 (se ha utilizado la versión revisada de 6 de febrero de 2018), p. 20.

mayor («alto riesgo» frente a cualquier brecha que comporte un riesgo, salvo aquellas en que la afectación de derechos sea «improbable»). Consecuentemente, el margen de actuación del responsable se incrementa[202], siendo posible que se produzcan brechas de seguridad que, habiendo sido puestas en conocimiento de las autoridades de control, no se trasladen a los interesados.

No obstante, en la medida en que las autoridades de control tendrán conocimiento de las mismas, el margen de actuación discrecional del responsable se ve sustancialmente reducido, pues las autoridades de control validarán si es necesaria, o no, la comunicación a los interesados. De este modo, se conjuran las posibles tentaciones de eludir la comunicación a los interesados y, con ello, evitar los efectos negativos que tal circunstancia pudiera tener en su reputación.

3.7.4.3. Las evaluaciones de impacto

Las evaluaciones de impacto están estrechamente vinculadas a la idea de gestión del riesgo[203]. En tanto los niveles de riesgo son variables, no siempre se exige una evaluación formalizada. Sin embargo, al vincular su obligatoriedad a la existencia de una probabilidad significativa de alto riesgo (35.1 RGPD), provoca que, el responsable, cualquiera que sea el tratamiento que pretenda llevar a efecto, deba hacer una valoración preliminar/no oficial de los riesgos que este pueda entrañar, así como mantener el nivel de atención frente a nuevas amenazas[204].

---

[202] Solo tendrá que realizar la comunicación cuando la naturaleza de los datos filtrados, así como la cantidad y trazabilidad de los mismos, confieran a la brecha de seguridad un potencial dañoso considerable. Del mismo modo, tampoco habrá de realizar una notificación individualizada cuando fuera desproporcionada la comunicación personalizada, en cuyo caso, bastará con realizar una comunicación pública (Platero Alcón, 2019, p. 68).

[203] Por gestión de riesgos se entiende al conjunto de «actividades coordinadas para dirigir y controlar una organización respecto al riesgo», en GT29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, de 4 de abril de 2017 (se utiliza la versión revisada de 4 de octubre de 2017), p. 7.

[204] Así lo entiendo el GT29 al señalar que, «en la práctica, esto significa que los responsables deben evaluar continuamente los riesgos creados por sus actividades de tratamiento a fin de identificar cuando es probable que un tipo de tratamiento entrañe "un alto riesgo para los derechos y libertades de las personas físicas"», en GT29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, de 4 de abril de 2017 (se utiliza la versión revisada de 4 de octubre de 2017), p. 7.

Las evaluaciones de impacto tienen un carácter eminentemente preventivo (R. M. Miralles López, 2021, p. 2139). Buscan anticiparse a los peligros. Con todo, la aproximación inicial para determinar si es necesario realizar una evaluación de impacto no está formalizada. Serán las circunstancias concretas del tratamiento, así como las medidas que el responsable esté en condiciones de implementar, lo que dilucidará la necesidad, o no, de proceder con la evaluación de impacto.

No obstante, la decisión final acerca de la necesariedad de una evaluación de impacto no es completamente discrecional. Las autoridades de control publican listados con las tipologías de tratamiento para las que se exigirá su realización (35.4 RGPD). Además, y siempre que lo estimen oportuno, pueden establecer relaciones no taxativas de tratamientos en los que este tipo de actuación no es obligatoria (35.5 RGPD). Este tipo de enumeraciones[205], por más que tengan un carácter eminentemente orientativo, resultan especialmente útiles para disipar las dudas que pudieran asaltar al responsable en supuestos dudosos. Con todo, será la realidad del tratamiento la que tenga la última palabra.

Por otra parte, el RGPD establece una serie de supuestos que, de concurrir, harían necesaria una evaluación de impacto: «evaluación sistemática y exhaustiva de aspectos personales […] que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten de un modo similar»; «tratamiento a gran escala de las categorías especiales de datos […] o de lo datos personales relativos a condenas e infracciones penales» y «observación sistemática a gran escala de una zona de acceso público» (art. 35.3 RGPD).

Las razones por las que estas tres tipologías de tratamiento requieren de evaluación de impacto resultan evidentes. La primera de ellas (la elaboración de perfiles) pone el acento en el riesgo derivado del uso de

---

[205] Pueden consultarse los dictámenes del EDPB sobre los listados de cada uno de los Estados miembros de las operaciones de procesamiento de datos que exigen evaluación de impacto, así como de aquellas que no lo necesitan, en: https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en. (Última consulta: 20/10/2021).
En el caso de la AEPD, ha publicado el listado de tratamientos que demandan de evaluación de impacto: https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en y otra, de carácter orientativo, con los que no: https://www.aepd.es/es/documento/listasdpia-35.5l_0.pdf. (Última consulta: 20/10/2021).

técnicas algorítmicas en la toma de decisiones. En esos casos, por la técnica utilizada y la pluralidad de posibilidades decisorias que este tipo de instrumentos posibilita[206], se considera que el riesgo de afectación de los derechos del interesado se incrementa sustancialmente.

El segundo de los escenarios, el tratamiento masivo de datos especiales o datos relativos a condenas e infracciones penales, tiene, en el elemento cuantitativo, el factor multiplicador del riesgo. El régimen particularizado de las categorías especiales tiene como fundamento de su existencia «que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos» (Considerando 51 RGPD). Por consiguiente, a aquellos casos en que se requieren grandes cantidades de información personal especialmente sensible, se les atribuye una probabilidad significativa de ser de alto riesgo.

El tercero de los supuestos está vinculado con los riesgos de la videovigilancia masiva. Los peligros de este tipo de tratamientos son muy variados. Desde las dificultades que los interesados puedan tener para detectar que están siendo objeto de observación, hasta la imposibilidad evitar el tratamiento, por estar jurídicamente fundado en, por ejemplo, un interés público[207]; pasado por las consecuencias que este tipo de prácticas tienen para la vida diaria, al impactar y condicionar el modo de vivir y comportase de la ciudadanía, con el consecuente riesgo de afectación del derecho a la libre circulación o el libre desarrollo de la personalidad. Además, la videovigilancia, establecida como política de estado, puede llevar a sociedades de vigilancia y control, inaceptables en sociedades democráticas.

Las evaluaciones de impacto, «*the GDPR's most practical tool*» (Bieker, Martin, Friedewald, y Hansen, 2017, p. 207), posibilitan una objetivación y cuantificación del riesgo, y permiten decidir si es asumible o no. En ellas se valoran cuestiones como las operaciones que se van a llevar

[206] El GT29 ha elaborado directrices específicas acerca de cómo se han de realizar los tratamientos de información que impliquen tanto la elaboración de perfiles, como la adopción de decisiones automatizadas. En las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 3 de octubre de 2017 (se ha utilizado la versión revisada de 2018) establece las condiciones específicas que debe incluir una evaluación de impacto en este ámbito, pp. 33-34.

[207] Esta es la razón aducida por el GT29 en las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, de 4 de abril de 2017 (se utiliza la versión revisada de 4 de octubre de 2017), pp. 10-11.

a efecto, la proporcionalidad y adecuación del tratamiento para alcanzar los objetivos perseguidos o las medidas de seguridad (técnicas y organizativas) destinadas a minorarlos (35.7 RGPD).

Si, a pesar de las medidas de seguridad implementadas, la evaluación de impacto determinase la existencia de un alto riesgo, el responsable deberá consultar con la autoridad de control correspondiente para que le autorice el tratamiento y le aconseje medidas tendentes a minorar el riesgo y hacerlo asumible (art. 36 RGPD). Aunque, naturalmente, podrían darse situaciones en que el tratamiento de datos no fuese posible de ningún modo, por entrañar un riesgo jurídicamente inaceptable.

Finalmente, existe un conjunto de tratamientos en los que la evaluación de impacto viene dada: aquellos supuestos en los que el tratamiento de datos tenga como base de legitimación «el cumplimiento de una obligación legal» (art. 6.1.c RGPD). En ellos, no será necesario realizar una evaluación de impacto, «excepto si los Estados miembros [lo] consideran necesario» (art. 35.10). Los motivos de esta exclusión radican en la asunción de que, el legislador, al regular el tratamiento, ya ha realizado la debida valoración de riesgos y previsto las garantías adecuadas, tal como exige toda regulación legal que afecta a derechos fundamentales (art. 52.1 CDFUE).

3.7.4.4. Medidas no exclusivamente vinculadas a la reducción del riesgo

Junto a las medias generales de prevención, el RGPD establece ciertas exigencias que, sin ser obligatorias en todo caso, tienen en los riesgos del tratamiento uno de sus detonantes. Entre ellas destacaremos, a título puramente ejemplificativo, la llevanza de un registro de actividades o contar con un delegado de protección de datos.

El registro de actividades conecta con la idea de responsabilidad proactiva (Kotschy, 2020, p. 618), al implicar el control documentado y ordenado de los tratamientos que cada responsable lleva a efecto. Con él se obtiene una radiografía de los tratamientos realizados por el responsable.

Esta medida sigue una lógica similar a la de la evaluación de impacto, pero, a diferencia de aquella, no la hace depender de la existencia de un alto riesgo, sino que la objetiva, al establecer un conjunto de criterios que, de

producirse, hacen necesario documentar los tratamientos de manera mucho más detallada[208].

Por su parte, la inclusión del delegado de protección de datos[209] supone incorporar al modelo de protección una figura cuyo cometido es velar por el correcto transcurso del tratamiento (asesorando al responsable y mediando entre éste y los interesados). Si bien no es obligatorio contar con un delegado de protección de datos en todo caso, si lo será cuando los tratamientos «requieran una observación habitual y sistemática de interesados a gran escala» así como, en aquellos que impliquen «el tratamiento a gran escala de categorías especiales de datos personales […] [o] de datos relativos a condenas e infracciones penales» (art. 37.1 RGPD)[210].

Aunque el riesgo no aparece expresamente recogido como detonante del nombramiento de esta figura, los supuestos obligatorios concuerdan con los que permiten identificar la existencia de un alto riesgo y hacen exigible la evaluación de impacto. Además, en el ejercicio de sus funciones, el delegado de protección de datos debe prestar «la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento» (39.2 RGPD) y asesorando al responsable en la realización de la evaluaciones de impacto (35.2 y 39.1.c RGPD).

3.7.5. Seguridad y riesgo

La seguridad de los tratamientos de datos es una característica del modelo europeo. El desarrollo histórico del sistema de protección de datos, desde sus primeras manifestaciones normativas, demuestra que siempre ha estado impulsado por la preocupación –cuando no el temor– a los

[208] La llevanza de este registro es obligatoria tanto por razones cuantitativas (más de 250 trabajadores) como cualitativas (riesgo para los derechos, uso de categorías especiales o datos de condenas e infracciones penales) (30.5 RGPD).

[209] Como apunta Santamaría Ramos, «esta figura no es nueva ya se encontraba prevista y regulada en la Directiva 95/46/CE y fueron no pocos estados miembros los que decidieron transponerla a su Derecho interno y sí, España no fue una de ellas» (Santamaría Ramos, 2021, p. 2242).

[210] Sobre las condiciones de designación (facultativa u obligatoria) del delegado de protección de datos, vid. (Botella Pamies, 2019) y (Santamaría Ramos, 2021b).

efectos que el tratamiento de información personal por terceros pudiera tener sobre los bienes jurídicos de la ciudadanía.

La atención al riesgo o la adopción de medidas técnicas y organizativas adecuadas para incrementar la seguridad de los datos son exigencias tanto del derecho a la protección de datos, como de los demás derechos y libertades que, en su caso, pudieran verse afectados. El elemento técnico no debe oscurecer esta realidad.

La atención al riesgo y la adopción de las medidas adecuadas para cada tratamiento son la manifestación de un modelo contextual y casuístico. El modelo europeo cuenta y fomenta el uso de herramientas que, por centrarse en la prevención y la anticipación a los problemas, hacen viable cualquier propuesta que se incardine en esa línea de acción.

3.8. Un modelo complejo e híbrido

El RGPD es la consecuencia de años de evolución y desarrollo normativo. Sus preceptos establecen una orientación y un modo específico de entender el derecho a la protección de datos, acomodado a los intereses y necesidades europeas (la estrategia digital europea, la consolidación del mercado interior y, sobre todo, la garantía de libre circulación de la información).

Desde un punto de vista jurídico, las operaciones en las que se utiliza información personal son complejas y los efectos derivados de su uso variados. Dar respuestas predefinidas, que sirvan a la generalidad de situaciones posibles, es cada vez más difícil, y su porcentaje de éxito menos elevado. Frente a esta realidad, el modelo de protección diseñado por la UE es poliédrico y transversal. Aborda las diferentes variables en concurso y ofrece la solución jurídicamente más adecuada o, al menos, el modo de determinarla.

No es una mera normativa de desarrollo del derecho a la protección de datos, sino una regulación omnicomprensiva, destinada a configurar el marco normativo europeo para el tratamiento de datos. El nombre completo del RGPD no engaña, Reglamento «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».

Los tratamientos de datos personales no afectan, en exclusiva, al derecho fundamental a la protección de datos, hay otros intereses en concurso. Los riesgos no se circunscriben a la afectación de un único derecho y, consecuentemente, las medidas a implementar tampoco son unidireccionales. Resulta coherente que, si sobre una misma información, confluyen diferentes intereses y se pueden ver afectados diversos derechos, la normativa refleje esa complejidad.

El RGPD proporciona los asideros jurídicos necesarios para ofrecer protección frente a los riesgos e injerencias que el tratamiento de datos personales pudiera entrañar, suministra las herramientas para disciplinar los intereses en conflicto y establece preferencias jurídicas que posibilitan resolver las disputas entre los diferentes sujetos que tomen parte del tratamiento. Además, aporta ciertos elementos valorativos que contribuyen a resolver las eventuales colisiones entre el derecho a la protección de datos y otros derechos.

Constituye, por tanto, un modelo de protección proactivo y flexible, capaz de hacer frente a la miríada de tratamientos que pueden tener lugar. Este sistema de protección posibilita la adecuación a las diferentes realidades y problemas que cada operación plantea. En la era de la individualización, la personalización y el perfilado, el RGPD tiene los mimbres para facilitar una protección igualmente singularizada, conjugando la protección de los derechos con la flexibilidad y subjetivación que la era digital demanda. En definitiva, es un modelo dinámico y funcional (Lucas Murillo de la Cueva, 2021, p. 316).

Sin embargo, aunque prevalente, la orientación contextual, proactiva y focalizada en las circunstancias y riesgos del tratamiento, no es absoluta. En efecto, el RGPD no renuncia ciertas características estáticas que, si bien aparentemente ofrecen seguridad y certeza, también pueden provocar disonancias, como es el caso de las categorías especiales de datos.

En cierto sentido, el RGPD es un híbrido. En él confluyen elementos de los modelos de protección reactivo y rígido con otros eminentemente proactivos y flexibles. El resultado es un modelo heterogéneo, perfectamente válido e, incluso, adecuado para cambios de etapa. Sin embargo, por esa transitoriedad, está condenado a ser temporal, al menos en aquellos elementos incapaces de ofrecer respuesta a los retos futuros.

La era digital, con la velocidad que imprime a las transformaciones sociales, culturales y técnicas, es refractaria a las respuestas jurídicas

excesivamente rígidas, pues terminan por quebrar a la menor innovación. Ante ese escenario, más pronto que tarde los elementos rígidos del RGPD habrán de ser revisados, pues, en caso contrario, las dinámicas tecnológicas les llevarán a la obsolescencia, por ser incapaces de hacer aquello para lo que fueron positivizados.

4. Más allá del RGPD. La regulación europea de la información

4.1. El tratamiento de datos por las instituciones europeas

El 2018 no solo es el año en que comenzó a aplicarse el RGPD. También es el momento en que se produjo la renovación de la otra normativa de referencia en la interpretación y desarrollo del art. 8 de la CDFUE: el Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos fue reemplazado por el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE.

El objeto de este Reglamento es la protección de «los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales» (Art. 1.2 Reglamento 2018/1725) frente a los tratamientos de datos llevados a cabo por las instituciones y organismos de la Unión[211]. En términos generales, y más allá de las adecuaciones técnicas motivadas por las características de los sujetos a los que está dirigido («las instituciones y organismos de la Unión» (art. 2.1 Reglamento 2018/1725)) (p. ej. no se incluye el interés legítimo como base de legitimación[212] y la autoridad de control de referencia es el Supervisor Europeo de Protección de Datos[213]), el Reglamento 2018/1725

[211] En esa línea apuntan los arts. 1.1 y 2 del Reglamento (UE) 2018/1725.

[212] La no inclusión del interés legítimo obedece a la diferente posición de las instituciones y organismos de la UE, los tratamientos que estas lleven a cabo habrán de justificarse en la existencia de un interés público debidamente justificado.

[213] El Supervisor Europeo de Protección de Datos es la autoridad de control «responsable de la vigilancia de los tratamientos de datos personales efectuados por las instituciones y los organismos de la Unión». Sobre esta autoridad y las novedades en sus funciones

contiene unas previsiones equivalentes –cuando no idénticas– a las del RGPD. Tanto el modo de afrontar el tratamiento de la información personal (proactividad e importancia de las medidas de seguridad vinculadas al riesgo), como la conceptualización de lo que es un dato personal o la regulación de las categorías especiales siguen la misma lógica jurídica.

En relación con el uso de datos por las instituciones europeas, no puede dejar de mencionarse el Reglamento (UE, Euratom) 2019/493 del Parlamento Europeo y del Consejo, de 25 de marzo de 2019, por el que se modifica el Reglamento (UE, Euratom) n.° 1141/2014 en lo que respecta a un procedimiento de verificación relativo a las infracciones de las normas de protección de los datos personales en el contexto de las elecciones al Parlamento Europeo.

El Reglamento 2019/493 establece medidas profilácticas tendentes a garantizar la limpieza del proceso electoral en las elecciones al Parlamento Europeo. Para ello, califica como «infracción no cuantificable»[214] que un partido político o fundación política europeas influyan, o traten de hacerlo, de manera deliberada «en el resultado de las elecciones al Parlamento Europeo aprovechándose de una infracción, cometida por parte de una persona física o jurídica, de las normas aplicables en materia de protección de datos personales»[215].

Estamos ante una adecuación del marco regulatorio con el objetivo de prevenir una amenaza específica: la eventual subversión de los procesos electorales mediante el uso de información personal. Es la respuesta europea a escándalos como el de *Cambridge Analytica*[216]. Al reforzar el aparato sancionador, el legislador apuesta por un modelo de prevención basado en una medida eminentemente reactiva, pues la sanción se generaría frente a actuaciones ya ejecutadas (influir o tratar de hacerlo).

---

incorporadas por el Reglamento 2018/1725, vid. (Costa, Peris Brines, y Cervera Navas, 2020).

[214] Art. 27.2.a del Reglamento (UE, EURATOM) Nº 1141/2014 del Parlamento Europeo y del Consejo, de 22 de octubre de 2014, sobre el estatuto y la financiación de los partidos políticos europeos y las fundaciones políticas europeas. En concreto, para el caso que estamos analizando, sería el apartado VII).

[215] Art. 10 bis, incorporado por el Reglamento (UE, Euratom) 2019/493 al del Reglamento (UE, EURATOM) Nº 1141/2014.

[216] El caso *Cambridge Analytica* es un ejemplo paradigmático de las potencialidades del tratamiento masivo de datos. Sobre cómo se utilizaron los datos acerca de gustos y preferencias para realizar perfiles individualizados a partir de los que enviar publicidad segmentada, vid. (Manokha, 2018) o (Villalobos Guízar, 2018).

Desde el punto de vista de la caracterización del modelo, esta opción legislativa puede interpretarse de varios modos. Una primera opción sería considerar que, en tanto la proactividad y las medidas anticipatorias están aseguradas (los partidos políticos habrán de respetar el marco normativo en materia de protección de datos conformado por el RGPD y el Reglamento 2018/1725). Ello supone que solo queda margen para reforzar el aparato sancionador y, consecuentemente, la solución pasa por la positivación de medidas específicas capaces de disuadir a los partidos políticos de la ejecución de actuaciones vulneradoras del derecho a la protección de datos.

Por otra parte, es posible entender que la medida adoptada en el Reglamento 2019/493 es el reflejo de una preferencia legislativa por las medidas reactivas, ya sea por desconfianza de la efectividad de las actuaciones proactivas o porque, para este caso concreto, se consideran las más adecuadas.

Personalmente, me inclino por el primer escenario, esto es, por la suficiencia de las medidas preventivas y necesidad de reforzar el aparato represivo en este caso concreto. En todo caso, se constata la necesidad de conjugar la anticipación y la prevención con la adopción de sanciones con entidad suficiente como para evitar que sea "rentable" vulnerar los derechos de los ciudadanos mediante el uso de datos personales.

4.2. El tratamiento de los datos no personales. El RDNP

En la era digital, la información, su uso, gestión e interconexión, son claves[217]. No toda información es un dato personal, de hecho, la mayoría no lo es[218]. Los datos personales son muy relevantes[219], sin embargo, desde una perspectiva global, estratégica y economicista, no dejan de ser una más pieza del tablero. Un mar en los océanos de la información.

---

[217] Los datos no personales constituyen el elemento más importante de la economía digital europea. En 2020 representaron el 4% del PIB de la UE, vid. https://digital-strategy.ec.europa.eu/en/library/free-flow-non-personal-data. (Última consulta: 20/10/2021).

[218] Los datos de las personas jurídicas, los datos anonimizados, los datos referidos a objetos, los datos estadísticos (por ejemplo sobre gastos o consumos), la mayoría de la información financiera y de producción, los datos climáticos, los referidos a máquinas, etc.

[219] permiten la segmentación y la personalización de las ofertas y de los productos (lo que resulta valioso para el mercado) y, a la vez, su uso tiene un impacto directo en los derechos y libertades, así como en la pervivencia de las sociedades democráticas.

De la regulación de la infinidad de datos no personales[220] se ocupa el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea (RDNP). Este, no solo disciplina el uso de esa tipología de información definida por exclusión –serán datos no personales: «los datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679» (art. 3.1 RDNP)–, sino que regula el régimen de protección de los tratamientos mixtos, esto es, de las operaciones en las que, de manera conjunta, se utilizan datos personales y aquellos que no lo son (art. 2.2 RDNP)[221].

El RDNP es un instrumento normativo crucial. Proporciona anclaje jurídico y certezas en un ámbito esencial para la economía y el funcionamiento de las sociedades contemporáneas: el flujo de información.

La regulación de los tratamientos mixtos y las sinergias con el RGPD tienen un impacto directo sobre el modo en que se utiliza la información personal en la UE. La condición no personal de una información ni es perpetua, ni es inmutable. De una parte, los datos anónimos de hoy pueden no serlo mañana[222], de otra, «si los datos no personales pueden relacionarse con una persona de alguna manera, haciendo que sean identificables directa o indirectamente, los datos deben considerarse datos personales»[223] y, por lo tanto, habrán de aplicárseles las exigencias del RGPD.

Los datos rara vez se utilizan aisladamente, tienden a utilizarse en conjunción con otros, de tal manera que la agrupación de diversos datos no personales podría dar como resultado la obtención de información

---

[220] Sobre las potencialidades del tratamiento de datos no personales, vid. (Somaini, 2020).

[221] Art. 2.2 RDNP: «En el caso de un conjunto de datos compuesto por datos personales y no personales, el presente Reglamento se aplicará a los datos no personales del conjunto de datos. Cuando los datos personales y los no personales de un conjunto de datos estén inextricablemente ligados, el presente Reglamento se aplicará sin perjuicio del Reglamento (UE) 2016/679».

[222] El RDNP señala, en su Considerando 9, que «si los avances tecnológicos hicieran posible transformar datos anónimos en datos personales, dichos datos se deben tratar como datos personales y, en consecuencia, se debe aplicar el Reglamento». Como se recordará, las posibilidades de reidentificación están en competencia constante con las capacidades de anonimización.

[223] Comunicación de la Comisión al Parlamento Europeo y al Consejo. Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea, de 29 de mayo de 2019. Puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52019DC0250&from=EN#footnote28. (Última consulta: 20/10/2021).

personal[224], incluso de carácter sensible. Los datos, su condición y naturaleza, incluso el hecho mismo de si son personales o no, no es algo estático que vaya a poder predeterminarse de una vez y para siempre. Son una realidad viva y modulable.

Consecuentemente, las previsiones del RDNP resultan especialmente útiles como mecanismo de defensa frente a la lógica algorítmica y su capacidad inferencial. Si un tratamiento que tiene como materia prima datos no personales termina generando una conexión con algún individuo concreto, podrá exigirse la aplicación de las medidas protectoras y preventivas del RGPD.

El RDNP es una advertencia constante a los operadores para que no caigan en la complacencia que pudiera generar el operar con datos anonimizados[225]. La finalidad y efectos del tratamiento, así como el contexto tecnológico en que tiene lugar, introducen matices en la información raíz, que hacen mutar la naturaleza del dato en cada operación concreta. Más que de naturaleza del dato personal habría que hablar de naturalezas, en plural.

Además de la transubstanciación de los datos no personales en personales, existe otra pasarela relevante entre el RDNP y el RGPD, la referida al tratamiento de los datos mixtos, esto es, de los conjuntos de datos personales y no personales. Este tipo de agregados son muy habituales «en la economía de datos […] debido a desarrollos tecnológicos como el Internet de las cosas (es decir, objetos que se conectan digitalmente), la inteligencia artificial y las tecnologías que permiten el análisis de macrodatos»[226].

---

[224] Sería el caso de los metadatos, los cuales, «considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan», STJUE asuntos C-293/12 y C-594/12, Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014, apdo. 27. En la misma línea, STJUE asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB, de 21 de diciembre de 2016, apdo. 99.

[225] Pues, «si los avances tecnológicos hicieran posible transformar datos anónimos en datos personales, dichos datos se deben tratar como datos personales y, en consecuencia, se debe aplicar el Reglamento (UE) 2016/679» (Considerando 9 RDNP)

[226] Comunicación de la Comisión al Parlamento Europeo y al Consejo. Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea, de 29 de mayo de 2019. Puede consultarse en:

Frente a la presencia conjunta de datos personales y no personales, el art. 2.2 RDNP plantea dos escenarios posibles. El primero de ellos es aquel en que los datos están «inextricablemente ligados» (art. 2.2 RDNP). Aunque no se proporciona una definición legal del concepto «inextricablemente ligado», las Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea elaboradas por la Comisión[227] consideran que dicha noción hace referencia al «conjunto de datos […][que contenga] datos personales así como datos no personales […][en que] la separación de ambos [sea] imposible o sería considerada por el responsable del tratamiento como económicamente ineficiente o no viable desde el punto de vista técnico. […] También […] [encajarían aquellos supuestos en que] la separación del conjunto de datos disminuya significativamente el valor del conjunto de datos. Además, la naturaleza cambiante de los datos […] hace que sea más difícil diferenciar claramente y, por lo tanto, separar entre diferentes categorías de datos»[228].

En el segundo de los escenarios se opera con ambas tipologías a la vez, pero se les da un tratamiento diferenciado, esto es, resulta posible segregar unos datos de otros. En este caso, a cada dato se le aplica la normativa que le corresponde por su condición, es decir, a los datos no personales el RDNP y a los datos personales el RGPD. Con todo, los responsables no están obligados a separar los datos. La opción de operar con dos normativas es estratégica. Si decidiese tratarlos conjuntamente, habría de aplicar las mismas condiciones que los supuestos de inextricabilidad.

Tanto en los supuestos en que el responsable considere que es más eficiente no operar separadamente con datos personales y no personales, como en los que se dé alguno de los supuestos de inextricabilidad, el RDNP «se aplicará sin perjuicio del Reglamento (UE) 2016/679» (art. 2.2 RDNP). Dicho de otro modo, la normativa de datos no personales solo será de

---

https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52019DC0250&from=EN#footnote28. (Última consulta: 20/10/2021).

[227] Las Orientaciones pueden consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52019DC0250&from=EN#footnote28. (Última consulta: 20/10/2021).

[228] Comunicación de la Comisión al Parlamento Europeo y al Consejo. Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea, de 29 de mayo de 2019.

aplicación en aquellos aspectos en los que no contravenga al RGPD. Es una cuestión cualitativa, la protección de los datos personales, por su impacto en los derechos fundamentales, tiene cierta *vis atractiva*, arrastrando hacia su normativa, más garantista, la regulación del conjunto[229].

Item más, como el RGPD comparte con el RDNP la finalidad de asegurar el flujo de la información, la aplicación del mismo a los datos no personales no representa un obstáculo inasumible que haga económicamente ineficiente la aplicación de sus previsiones a los datos no personales entreverados con los personales. En este sentido, la regulación europea de los datos no personales encierra unas lógicas muy similares a las del RGPD. En ambas, la libre circulación de la información es un motor de impulso.

En definitiva, los dos reglamentos (RDNP y RGPD), cada uno a su manera, hacen hincapié en la necesidad de una vigilancia constante del devenir del tratamiento, pues su *statu quo* puede variar en cualquier momento (en el caso de los no personales, la reidentificación y la conmixtión de los datos serán las vías más habituales). En ambos anida un espíritu refractario de las aplicaciones mecanizadas y las falsas seguridades basadas en la condición original de la información.

4.3. Cuando la finalidad es el elemento determinante: La prevención, investigación, detección o enjuiciamiento de infracciones penales y la ejecución de sanciones penales

Paralela al RGPD[230], se elaboró la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en relación con el tratamiento de datos personales por parte de las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento penal delitos o la ejecución de sanciones penales, y sobre la libre circulación de dichos datos,

[229] Las Orientaciones de la Comisión señalan que «los derechos y obligaciones de protección de datos derivados del Reglamento general de protección de datos se aplicarán completamente a todo el conjunto de datos mixtos, incluso cuando los datos personales representen solo una pequeña parte del conjunto»

[230] Prueba de ello son las 21 referencias al RGPD que realiza en su texto, pese a ser de la misma fecha, el 27 de abril. Sobre la tramitación y elaboración conjunta de ambas normativas, vid. (Agencia de los Derechos Fundamentales de la Union Europea, 2018, p. 14).

y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva 2016/680).

Si la consolidación del mercado interior es el acicate del RGPD, la conformación del espacio europeo de libertad, seguridad y justicia[231] lo es de la Directiva 2016/680. Esta, se incardina dentro de la política de cooperación policial y judicial en materia penal (Fiodorova, 2021). La Directiva 2016/680 tiene como objetivo «asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados miembros» (Considerando 7 Directiva 2016/680). Para ello, establece un régimen particularizado y más detallado, en el que los márgenes de actuación de los responsables de los tratamientos están mucho más acotados.

Por su objeto, la Directiva 2016/680 opera como ley especial respecto del RGPD y del Reglamento 2018/1807. Estos constituyen la referencia general bajo cuyas directrices habrán de ejecutarse los tratamientos que, aun teniendo por objeto los mismos datos, no tengan finalidades concurrentes con la Directiva 2016/680[232]. De este modo, el RGPD se aplicaría a aquellos tratamientos que no sean realizados por autoridades competentes ni instituciones europeas (Considerando 12 de la Directiva)[233]. Además, el RGPD opera norma subsidiaria en todos aquellos elementos no previstos por la Directiva 2016/680[234].

Por su denominación, pudiera pensarse que la razón de ser de esta norma es disciplinar el tratamiento de los datos personales relativos a condenas e infracciones penales, completando, de ese modo, lo dispuesto en el artículo 10 del RGPD con relación a este tipo de datos[235]. No debemos

---

[231] Sobre la importancia estratégica que la lucha contra la delincuencia y la cooperación policial y judicial han tenido en la conformación del espacio de libertad, seguridad y justicia, vid., por su pertinencia para para enmarcar el tratamiento de los datos sobre condenas e infracciones penales, el trabajo de Remotti Carbonell, en (Remotti Carbonell, 2020).

[232] Si los mismos datos se utilizan, además, para otros fines, en esos tratamientos será de aplicación el RGPD, salvo que «se efectúe[n] como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión» (art. 9.1 Directiva 2016/680).

[233] Un supuesto de este tipo sería aquel en que la información sobre antecedentes penales fuese utilizada, por ejemplo, por entidades financieras para protegerse frente a posibles fraudes.

[234] Considerando 9 de la Directiva 2016/680: «el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (2) establece las normas generales para la protección de las personas físicas en relación con el tratamiento de los datos personales y para garantizar la libre circulación de datos personales dentro de la Unión».

[235] Esta tipología de datos tiene en el artículo 10 RGPD su principal regulación: «El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de

llevarnos a engaño. El elemento definitorio de la Directiva 2016/680 no es la naturaleza de los datos que regula, pues no es una norma destinada a disciplinar, en exclusiva, los datos relativos a condenas e infracciones penales, sino que su cometido es otro: regular los tratamientos que tengan como finalidad la «prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública» (Art. 1.1 Directiva 2016/680), siempre que sean llevados a efecto por las autoridades competentes para alcanzar tales fines[236].

Son las finalidades, los sujetos intervinientes, así como el ámbito en que se produce el tratamiento, los que fijan el objeto de la Directiva 2016/680. En cuanto a la naturaleza de los datos sobre los que se aplica, lo cierto es que no excluye ninguna tipología. Ello no obsta para que, debido a su particular objeto, las informaciones relativas a condenas e infracciones penales sean la principal categoría de datos a la que será de aplicación la Directiva, pero no la única. En la lucha contra la delincuencia y en la cooperación policial y judicial se utiliza una variedad mucho más amplia de datos personales, por ejemplo, los que revelan los rasgos físicos o el número de identificación personal oficial (v. gr. el DNI).

En esta línea, destaca el particular modo en que la Directiva 2016/680 afronta el tratamiento de las categorías especiales. El artículo 10 de la Directiva[237] no parte de la prohibición del tratamiento como premisa,

---

seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas».
No obstante, la Directiva 2016/680, por su objeto, regula determinados usos de los datos de esta naturaleza.

[236] A efectos de la Directiva 2016/680, se entiende por autoridad competente: «a) toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, o
b) cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública» (art. 3.7 Directiva 2016/680).

[237] Artículo 10 Directiva 2016/680:
«El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física solo se permitirá cuando sea estrictamente necesario, con sujeción a

sino que acota las situaciones en que las tipologías de datos consideradas sensibles pueden ser utilizadas por las autoridades competentes.

Así, mientras el RGPD prevé un conjunto tasado de bases de licitud (art. 6 RGPD) exige y, para el tratamiento de las categorías especiales, la concurrencia de alguna de las circunstancias del 9.2 RGPD como condición para enervar la prohibición de tratamiento; la Directiva 2016/680 adopta una aproximación diferente. Vincula la licitud a la necesidad del tratamiento[238].

Será posible utilizar datos especiales, pero solo «cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando: a) lo autorice el Derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos» (art. 10).

La combinación de causa fundante y sujetos responsables (autoridades públicas), tiene como resultado que la regulación legal será la base de licitud en todos los casos, aunque formalmente se prevén tres. Las otras dos, son situaciones que los Estados miembros podrían reconocer[239].

De este modo, en la medida en que todo tratamiento ha de ser lícito, y las condiciones de licitud han de estar legalmente reguladas, la habilitación legal se convierte en la constante de todo tratamiento realizado al amparo de la Directiva 2016/680, también la de aquellos que incluyan datos especiales[240]. Con todo, el tratamiento de esas tipologías de

---

las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando:
a) lo autorice el Derecho de la Unión o del Estado miembro;
b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o
c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos».

238 «Los Estados miembros dispondrán que el tratamiento solo sea lícito en la medida en que sea necesario» (art. 8 Directiva 2016/680).

239 La mera situación fáctica (v. gr. que los datos sean manifiestamente públicos) no será suficiente, sino que su validez como base de legitimación depende de que una previsión normativa le haya reconocido dicha capacidad respecto de los tratamientos que se pretenden realizar.

240 Los legisladores no tienen una libertad de actuación absoluta para configurar las condiciones del tratamiento, pues la Directiva 2016/680 impone el deber de identificar, normativamente, los objetivos y finalidades, así los datos personales que se vayan a utilizar. Este conjunto cumulativo de exigencias resulta coherente con el criterio de necesidad adoptado, pues proporciona los parámetros que permitirán valorar la necesariedad del tratamiento y la adecuación de las condiciones previstas para su realización.

datos tiene un régimen más agravado. Así, mientras para el resto de datos personales basta con justificar la necesidad de su tratamiento, en el caso de los datos sensibles esa exigencia es cualitativamente superior, pues ha de ser «estrictamente necesario» (art. 10)[241].

Además de esos deberes positivos, la Directiva 2016/680 –diferenciándose, también en este aspecto, del RGPD– excluye al consentimiento como base de legitimación habilitante para los tratamientos realizados a su amparo[242]. En la medida en que los tratamientos de la Directiva 2016/680 se basan en la existencia de un interés público legalmente reconocido y con entidad suficiente como para hacer necesario el tratamiento de la información, no queda margen para la autodeterminación personal que el consentimiento representa.

Con todo, el consentimiento voluntario podría llegar a operar «como salvaguarda adicional»[243] –nunca como causa habilitante única– en aquellos tratamientos que pudieran resultar más incisivos, como sería el caso de «la realización de pruebas de ADN en las investigaciones penales o el control del paradero del interesado mediante dispositivos electrónicos para la ejecución de sanciones penales» (Considerando 35 de la Directiva 2016/680).

Las evidentes diferencias en el modo de afrontar el tratamiento de los datos especiales en la Directiva 2016/680 ponen de manifiesto que la opción legislativa del RGPD no es la única posible; y demuestra que no es necesario partir de la prohibición del tratamiento para ofrecer un marco de actuación con todas las garantías. En este caso, la justificación legal de la necesariedad del tratamiento y la necesaria atención a sus condiciones

---

[241] En la medida en que la Directiva 2016/680 reconoce el principio de minimización de datos (art. 4.1.c)[241]) y que, «conforme a la jurisprudencia reiterada del Tribunal de Justicia, […] las excepciones a la protección de los datos personales y las restricciones a dicha protección se […] [han de establecer] sin sobrepasar los límites de lo estrictamente necesario»[241], consideramos, en la misma línea que apunta el GT29, que esa diferente graduación «debe entenderse como un llamamiento a prestar especial atención al principio de necesidad», en GT29, Dictamen sobre algunas cuestiones fundamentales de la Directiva sobre protección de datos en el ámbito penal (UE 2016/680), de 29 de noviembre de 2017, p. 8.
Estas precauciones, se complementan con la exigencia de adoptar «las salvaguardias adecuadas» (art. 10 de la Directiva 2016/680), debiendo realizar las actuaciones precisas para minorar los riesgos y hacer el tratamiento jurídicamente aceptable.

[242] Considera que, «cuando se exige al interesado que cumpla una obligación jurídica, este no goza de verdadera libertad de elección, por lo que no puede considerarse que su respuesta constituya una manifestación libre de su voluntad» (Considerando 35).

[243] GT29, Dictamen sobre algunas cuestiones fundamentales de la Directiva sobre protección de datos en el ámbito penal (UE 2016/680), de 29 de noviembre de 2017, p. 9. En la misma línea, (Quintel, 2018, p. 106.

específicas, unido a la adopción de las medidas de protección adecuadas para reducir los riesgos inherentes al tratamiento, proporciona resultados equivalentes[244].

Junto al particular modo de afrontar el tratamiento de las categorías especiales, debe destacarse la fundamentación de la Directiva, pues pone de manifiesto la preeminencia del quien (las autoridades competentes) y del para qué (la cooperación policial y judicial), por encima del qué (la tipología de datos a utilizar), al punto de justificar una regulación específica sobre la materia.

Si las finalidades, los sujetos intervinientes o el contexto/ámbito en el que se produce el tratamiento tienen enjundia suficiente como para justificar la producción de legislación específica, ¿no deberían ser factores con una posición equivalente a la naturaleza del dato a la hora de determinar las medidas a implementar?, ¿tiene sentido privilegiar a unos criterios sobre otros cuando el tratamiento de datos se produce en contextos tan diversos?

4.4. La interoperabilidad, el tratamiento y la gestión de la información personal en la circulación de personas por el espacio europeo

La consolidación y perfeccionamiento del espacio de libertad, seguridad y justicia de la UE también es la causa que subyace a los Reglamentos 2019/817 y 2019/818, relativos, respectivamente, al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo; y al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se

[244] Salami considera que la Directiva 2016/680 ofrece una protección más adecuada que la que podría ofrecer la Directiva 95/46/CE, sin embargo, respecto del RGPD, cree que el estándar de protección es un poco inferior, circunstancia que achaca a los equilibrios que ha sido necesario realizar para lograr un equilibrio entre la protección de datos y la consecución de los objetivos que la Directiva 2016/680 persigue (Salami, 2017, p. 14).
Pajunoja, aunque valora positivamente la regulación de la Directiva 2016/680, señala que serán las regulaciones de los Estados miembros las que definan el nivel real de protección, mostrando su preocupación por las disparidades que ello pueda generar (Pajunoja, 2017).

modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816.

Si el buen funcionamiento del espacio de libertad, seguridad y justicia es la razón de ser de los mencionados reglamentos, el flujo seguro de la información es el cauce para lograrlo. La libre circulación de la información se presenta como un instrumento necesario para la construcción de ese proyecto colectivo de vida en común que es la UE.

Asegurar la interoperabilidad de los sistemas de información[245] es crucial para la rápida transmisión de información entre los Estados miembros. La principal línea de acción de los Reglamentos 2019/817 y 2019/818 es la remoción de las fronteras que el uso de diferentes sistemas operativos comporta, para lo que establecen pautas comunes de actuación en el modo de recabar y transmitir la información. No son meras regulaciones técnicas, sino que buscan generar una dinámica de actuación común, fundada en valores y criterios compartidos.

Los Reglamentos 2019/817 y 2019/818, pese a su especialización temática, tienen elementos de conexión, como explícitamente apunta el artículo 1.1 del 817/2019[246]. La confluencia en los medios técnicos, así como de algunos de sus preceptos y conceptos[247], es perfectamente comprensible. Ambos tienen como finalidad asegurar el control de las entradas y movimientos de personas en la UE. Las diferencias, por su parte, traen causa de las razones del desplazamiento, y las particularidades del mismo: control de fronteras y visados (Reglamento 2019/817) vs cooperación policial y judicial, asilo y migración (Reglamento 2019/818)).

Desde un punto de vista jurídico, estos reglamentos son leyes especiales, con unos objetivos muy marcados y un ámbito de aplicación

[245] Conforme a la segunda acepción del Diccionario panhispánico del español jurídico, se entiende por interoperabilidad «la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos». Puede consultarse en: https://dpej.rae.es/lema/interoperabilidad. (Última consulta: 20/10/2021).

[246] Artículo 1.1 del 817/2019: «El presente Reglamento, junto con el Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo (34) establece un marco para garantizar la interoperabilidad del Sistema de Entradas y Salidas (SES), el Sistema de Información de Visados (VIS), el Sistema Europeo de Información y Autorización de Viajes (SEIAV), Eurodac, el Sistema de Información de Schengen (SIS) y el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN)».

[247] Por ejemplo, comparten definiciones (art. 4 en ambos reglamentos); mandatos de no discriminación y respeto de los derechos fundamentales (art. 5 de ambos reglamentos) y hasta algunas de las medidas, como el portal europeo de búsqueda (art. 6 de ambas reglamentos).

muy delimitado. Consecuentemente, en todo aquello no previsto por ellos, serán de aplicación las previsiones del RGPD[248] y, allí donde corresponda por razón de materia, el Reglamento 2018/1725 y la Directiva 2016/680[249]. En la práctica, el RGPD será la norma de referencia en el diseño y ejecución de los tratamientos, como demuestran las constantes remisiones a sus preceptos, especialmente en relación con los principios del tratamiento, los derechos del interesado o en materia de responsabilidad[250].

En lo referente al tratamiento de las categorías especiales de datos, la normativa aplicable será la que corresponda en función del caso concreto. Pudiendo producirse situaciones problemáticas en aquellos supuestos en que se dude entre aplicar alguno de los reglamentos (el RGPD o el Reglamento 2018/1725) o la Directiva 2016/680, pues su régimen jurídico tiene, como hemos visto, diferencias significativas.

A los efectos de identificar la idiosincrasia del modelo europeo de tratamiento de la información, los Reglamentos sobre interoperabilidad ponen de manifiesto la relevancia de la libre circulación y corroboran la importancia de la finalidad[251] del tratamiento y de los sujetos que intervienen en él.

Las finalidades son las que dictan qué datos se van a precisar. Por su parte, el agregado de informaciones y el modo en que se tratan (cómo, para qué, por quién) son agentes de cambio y modulación de una importancia capital en la fisonomía final del tratamiento. Los mismos datos, usados para un fin diferente, serían tratados de otro modo. Estas regulaciones sectoriales ponen de manifiesto la necesidad de adecuación a la realidad de cada tratamiento. En este caso, el ajuste ha sido realizado por el legislador;

---

[248] Sirva como ejemplo, por su claridad, el Considerando 53 del Reglamento 2019/817, en el que se establece que «el Reglamento (UE) 2016/679 se aplica al tratamiento de datos personales con fines de interoperabilidad por parte de las autoridades nacionales en virtud del presente Reglamento, a menos que sean las autoridades designadas o los puntos de acceso central de los Estados miembros quienes lleven a cabo dicho tratamiento por razones de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves».

[249] Como apunta el Considerando 55 al señalar que «el Reglamento (UE) 2018/1725 o, en su caso, la Directiva (UE) 2016/680 se aplican también a las transferencias de datos personales a terceros países u organizaciones internacionales realizadas de conformidad con el presente Reglamento».

[250] Vid. Considerando 69 (derechos), Considerando 70 (principio de minimización), art. 40 (responsabilidad) del Reglamento 2019/818 o el Considerando 58 del Reglamento 2019/817 respecto del establecimiento de garantías institucionales.

[251] La importancia estratégica de los objetivos que se persiguen, así como la valía del conjunto de datos con los que se opera, son el acicate para implementar las medidas de seguridad necesarias.

sin embargo, en otros ámbitos no regulados con este nivel de detalle, serán los operadores de datos quienes, a partir del marco jurídico existente, definan las condiciones específicas del tratamiento.

En este sentido, los legisladores, sea el europeo o los de los Estados miembros, habrán de velar por asegurar la existencia de un marco jurídico adecuado, con las garantías pertinentes, que permita a los responsables del tratamiento adoptar las medidas que mejor se adecúen a los tratamientos que pretenden llevar a efecto.

El RGPD no siempre será suficiente y, en ocasiones, habrán de establecerse regulaciones sectoriales que colmen las ausencias y ofrezcan garantías específicas a aquellos tratamientos que sean especialmente delicados, bien por suponer un riesgo más elevado o por llevarse a cabo en un ámbito con características diferenciales (ya sea por su importancia estratégica (como ocurre con los reglamentos de interoperabilidad) o por los datos con los que se opera y el ámbito en que se emplean (como es probable que ocurra con la creación de un espacio europeo de datos sanitarios[252]).

4.5. Entre el presente y el futuro: la gobernanza de datos y las comunicaciones electrónicas

4.5.1. Datos abiertos, reutilización y el desafío de la gobernanza de datos

Caminamos hacia una «sociedad basada en datos»[253], estos son el núcleo y combustible de la economía digital. La regulación y el aprovechamiento de los datos, personales o no, está en la base de la Estrategia Europea de Datos.

La conformación de la sociedad de los datos requiere que se facilite el acceso al caudal de información existente al mayor número de entidades y particulares, así como crear generar sinergias e incrementar el flujo de

[252] Este proyecto «es una de las prioridades de la Comisión para el período 2019-2025», así se declara en la web de la Comisión Europea: https://ec.europa.eu/health/ehealth/dataspace_es#:~:text=Espacio%20europeo%20de%20datos%20sanitarios,para%20el%20per%C3%ADodo%202019%2D2025. Desde el 3 de mayo de 2021, el proyecto está abierto a consulta pública: https://ec.europa.eu/commission/presscorner/detail/es/ip_21_2083. (Última consulta: 20/10/2021).

[253] Considerando 11 de la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público.

datos, para ampliar las posibilidades de uso y las potencialidades de cada información existente. La lógica subyacente es sencilla, cuantas más personas y empresas puedan acceder a una misma información, más posibilidades de encontrarle nuevas utilidades que reporten beneficios y contribuyan al progreso de la sociedad (p. ej. generando nuevos servicios e innovaciones).

Como puede comprenderse, una política de datos abiertos entraña riesgos. Que los datos[254] estén «abiertos»[255] puede tener consecuencias negativas para la ciudadanía, al propiciar usos que generasen nuevas formas de afectación de los derechos y libertades, incluido el derecho a la protección de datos[256].

La Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (en adelante, Directiva 2019/1024) es el instrumento normativo que, en la actualidad, establece los mecanismos mediante los que conciliar los diferentes intereses y derechos en concurso. Esta Directiva es una versión refundida de la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público. Estamos, por tanto, ante la actualización de una materia que viene formando parte de las políticas europeas desde hace años[257]. Su cometido último es generar sinergias entre el sector público y el privado, estimulando, de ese modo, «la innovación de los productos y servicios» (art.1.1 Directiva 2019/1024), tanto para fines comerciales como no comerciales (art. 2.11 Directiva

---

[254] entendidos aquí en sentido amplio, esto es, como «toda representación digital de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual» (artículo 2.1) de la propuesta de Reglamento sobre gobernanza de datos). Puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52020PC0767. (Última consulta: 20/10/2021).

[255] «Por datos abiertos como concepto se entiende en general los datos en formatos abiertos que puede utilizar, reutilizar y compartir libremente cualquier persona con cualquier fin» (Considerando 16 de la Directiva 2019/1024).

[256] Una política de datos abiertos en las que se incluyan informaciones personales tiene un peligro extraordinario de afectación del derecho a la protección de datos, pues, el incremento de los sujetos que operan con los datos podría mermar la capacidad de las personas para mantener el control sobre los datos a ellas referidos.

[257] En la actualidad, y solo en el portal oficial de datos europeos, hay casi millón y medio de conjuntos de datos abiertos y disponibles. Estos abarcan todo tipo de materias, desde agricultura a ciencia y tecnología, pasando por medio ambiente, energía, educación, economía, transporte, salud, información poblacional y social, justicia, datos del sector público o asuntos internacionales. Puede accederse al portal europeo de datos en: https://data.europa.eu/es. (Última consulta: 20/10/2021).

2019/1024)[258], mediante la reutilización[259] de la información que obra en poder de los organismos y empresas del sector público[260].

La taxonomía de la Directiva 2019/1024 viene condicionada por su objeto (la reutilización y la accesibilidad a las informaciones), por los sujetos a los que está dirigida (el sector público) y por las garantías y precisiones técnicas destinadas a hacer efectivos los fines que la inspiran. Así, se establecen tanto las condiciones de reutilización (desde los formatos a utilizar[261] a las tarifas a aplicar (arts. 6 y 7 Directiva 2019/1024, en este último precepto se impone un deber de transparencia respecto de su cálculo y fijación), pasando por la convergencia y cooperación entre los Estados miembros en la utilización de dispositivos que diluyan las barreras (idiomáticas y de operatividad) y faciliten el libre uso de las informaciones (art. 9), el uso de licencias tipo (art. 8) o la «disponibilidad de los datos de investigación» (art. 10)).

Desde el punto de vista del tratamiento de datos personales, la Directiva 2019/1024 adopta una posición muy cautelosa y respetuosa con el derecho a la protección de datos. Prueba de ello es que, con carácter general, la Directiva «no afecta a la protección de las personas en lo que respecta al tratamiento de datos personales» (Considerando 52)[262].

---

[258] Reutilización es, conforme a los dispuesto en el art. 2.11) de la Directiva 2019/1024: «el uso por personas físicas o jurídicas de documentos que obran en poder de:
a) organismos del sector público, con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos en la misión de servicio público para la que se produjeron, excepto para el intercambio de documentos entre organismos del sector público en el marco de sus actividades de servicio público, o
b) empresas públicas, con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos de prestar servicios de interés general para el que se produjeron, excepto para el intercambio de documentos entre empresas públicas y organismos del sector público que se realice exclusivamente en el desarrollo de las actividades de servicio público de los organismos del sector público»

[259] A efectos de la Directiva sobre datos abiertos, se entiende por reutilización, «el uso por personas físicas o jurídicas de documentos que obran en poder de: a) organismos del sector público […] b) empresas públicas» (art. 2.11 Directiva sobre datos abiertos).

[260] Para un análisis de las novedades de la Directiva sobre datos abiertos, vid. (Salinas Alcega y Fernández-Rodríguez Fairén, 2019, pp. 167-170).

[261] Los formatos mediante los que se facilitarán los documentos habrán de ser «electrónicos, […], abiertos, legibles por máquina, accesibles, fáciles de localizar y reutilizables, [y habrán de aportarse] conjuntamente con sus metadatos» art. 5.1 de la Directiva 2019/1024.

[262] Sus exigencias en materia de reutilización y datos abiertos no se aplican a «los documentos cuyo acceso esté excluido o limitado en virtud de regímenes de acceso por motivos de protección de los datos personales, y las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales o como un menoscabo de la protección de la intimidad y la integridad de las personas» (art. 1.2.h).

En los supuestos en que la reutilización de los datos personales sea posible, su uso ha de cumplir con las exigencias «del Derecho nacional y de la Unión relativas a la protección de datos personales, en particular del Reglamento (UE) 2016/679 y la Directiva 2002/58/CE»[263]. Esto supone que cualquier reutilización en la que se vean envueltos datos de carácter personal ha de cumplir con las exigencias del modelo europeo de protección de datos[264].

En el caso de los datos especiales, no podrán ser objeto de reutilización, salvo que, por ley, se habilite tal posibilidad. Tomando en cuenta la importancia de este tipo de informaciones, es bastante habitual que las normativas sectoriales incluyan previsiones específicas respecto de la reutilización y la política de datos abiertos en ámbitos en los que se utilicen datos sensibles con regularidad, y su uso persiga fines de interés general[265], como ocurre con la investigación biomédica.

En términos generales, la Directiva, guiada por la máxima «tan abiertos como sea posible, tan cerrados como sea necesario» (art. 10), establece las condiciones en que resultaría factible la reutilización de los datos personales, apostando por la confidencialidad, la seguridad y, sobre todo, la anonimización (art. 6), como mecanismos de protección. La ruptura del nexo dato-persona y la consecuente desaparición de las obligaciones que conlleva el tratamiento de datos personales, es la principal medida de seguridad de la Directiva de datos abiertos, con ella, además, facilita el aprovechamiento de la información, al reducir las exigencias de protección.

---

[263] El art. 1.4 de la Directiva 2019/1024 señala que «la presente Directiva se entiende sin perjuicio» de las normativas existentes en materia de protección de datos.

[264] Han de respetarse los principios del tratamiento (incluida la responsabilidad proactiva, la limitación a la finalidad y el tratamiento lícito, por lo que la reutilización habrá de contar con una base de legitimación que le fundamente y ha de circunscribirse a los fines establecidos); asimismo, habrá de reconocerse y facilitarse el ejercicio de los derechos del interesado y se adoptarán las medidas necesarias para que el tratamiento sea jurídicamente aceptable, por ejemplo, efectuando evaluaciones de impacto allí donde proceda.

[265] La propia Directiva 2019/1024 pone como ejemplo la posible reutilización de información en el sector de la salud, respecto del que señala que «de la salud, podrá ser necesario efectuar evaluaciones de impacto» (Considerando 53).

Sirvan como ejemplo de ese regulación sectorial y particularizada la disposición adicional decimoséptima (apartado 2 letra c)) y la disposición transitoria sexta de la LOPDGDD, destinadas a establecer las condiciones en que será lícita la reutilización de los datos personales con fines de investigación en salud e investigación biomédica (de todos los datos, especiales o no).

4.5.1.1. La gobernanza del dato. Una mirada al futuro

La Directiva 2019/1024 es la plasmación positiva de una estrategia geopolítica: el aprovechamiento económico y social de los documentos e informaciones en poder de las administraciones y entidades públicas. Sin embargo, deja fuera de su ámbito de aplicación importantes tipologías de información[266], entre ellas los conjuntos de datos excluidos por cuestiones vinculadas a la protección de datos (art. 1.2.h)).

La UE, como parte de su Estrategia Europea de Datos, está trabajando en la elaboración de un futuro Reglamento relativo a la gobernanza europea de datos[267]. Con él, busca facilitar la reutilización de algunas de las categorías de información en manos del sector público[268] a las que no se aplica la Directiva 2019/1024. En concreto, la propuesta incide sobre las informaciones que estén protegidas por razones de confidencialidad, sea comercial o estadística, así como sobre los conjuntos de datos respecto de los que terceros gocen de derechos de propiedad intelectual. Finalmente, también se aplica a aquellas informaciones protegidas por motivos relacionados con la protección de datos personales (art. 3.1 de la propuesta de Reglamento sobre gobernanza de datos).

Además de la reutilización, la propuesta de Reglamento sobre gobernanza de datos regula la cesión altruista de datos[269] (art. 1.1.c. y arts. 15 a 22 de la propuesta de Reglamento) y establece marcos de actuación reglados para ciertas actividades[270] vinculadas al intercambio de datos (art. 1.1.b.).

---

[266] Vid. el extenso listado de exclusiones previsto en el art. 1.2 de la Directiva 2019/1024.

[267] Propuesta de Reglamento sobre gobernanza de datos de 25 de noviembre de 2020. Puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52020PC0767. (Última consulta: 20/10/2021).

[268] A diferencia de la Directiva 2019/1024, la propuesta de reglamento excluye de su ámbito de aplicación «los datos conservados por empresas públicas» (art. 3.2.a) de la propuesta de Reglamento).

[269] La propuesta de reglamento define la cesión altruista de datos como «el consentimiento que otorga un interesado para que se traten sus datos personales, o el permiso que otorga otro titular de datos para que se usen sus datos no personales, sin ánimo de obtener una gratificación, con fines de interés general como la investigación científica o la mejora de los servicios públicos» (art. 2.10) de la propuesta de Reglamento).

[270] Esencialmente, establece las condiciones de prestación de los servicios de intercambio de datos, poniendo especial énfasis en el control y la supervisión de los proveedores de este tipo de servicios (arts. 9 a 14 de la propuesta de Reglamento).

La opinión conjunta del EDPB y del Supervisor Europeo de Protección de Datos ha puesto de manifiesto[271] que, la actual propuesta de Reglamento, presenta ciertas inconsistencias y contradicciones con el marco normativo europeo en materia de protección de datos y, singularmente, con el RGPD. Lo que resulta consistente con una propuesta que aún se encuentra en discusión y sobre la que existen importantes dudas, tanto de forma[272] como de fondo.

Así, el texto de la propuesta no termina de clarificar la relación que tendría con el RGPD, pudiendo provocar problemas de interpretación que derivasen en una afectación del derecho a la protección de datos[273].

Sirva como ejemplo la regulación de la figura del titular de datos[274]. Se trata de un sujeto al que se reconoce «derecho a conceder acceso a determinados datos personales o no que estén bajo su control, o a compartir tales datos». Esta figura no tiene equivalente en el RGPD. No es el interesado (además, en el caso de la propuesta de Reglamento se señala que puede ser una persona jurídica), tampoco es el responsable del tratamiento, pues no termina de encajar, pues en el RGPD no existe un «derecho a conceder acceso».

Además de los problemas de imbricación existentes entre la propuesta de Reglamento sobre gobernanza de datos y la normativa europea vigente, la Opinión conjunta del EDPB y el Supervisor Europeo de Protección de Datos, añade otros, como la necesidad de clarificar el marco

---

271 EDPB y Supervisor Europeo de Protección de datos, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, de 9 de marzo de 2021. Puede consultarse en: https://edps.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. (Última consulta: 20/10/2021).
Para un análisis más detallado de la Opinión conjunta, así como de la propuesta de Reglamento, vid. (Fernández, 2021).

272 En estos momentos, la propuesta normativa tiene forma de reglamento, si bien es cierto que, en la misma, se admite la posibilidad de que finalmente esa no sea la forma final del acto legislativo.

273 Muestra de ello es la ambigüedad con la que se afronta la exigencia de una base de legitimación para operar con datos personales, dejando abierta la puerta a posibles tratamientos que, a luz del RGPD, serían considerados ilícitos. Además, existen incongruencias terminológicas entre las definiciones de la propuesta y las del RGPD, lo que podría generar cierta confusión e, incluso, inducir a error. Vid. Párrs. 47 a 56 de la EDPB y Supervisor Europeo de Protección de datos, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, de 9 de marzo de 2021.

274 *Data holder* en la versión en inglés.

jurídico aplicable a los conjuntos mixtos (personales y no personales)[275] o concretar el papel que las autoridades de control en materia de protección de datos han de realizar en la supervisión de las actividades realizadas al amparo de la propuesta de Reglamento sobre gobernanza de datos[276].

Ante la entidad de las dudas suscitadas, parece razonable evitar el análisis de las previsiones concretas de la propuesta de Reglamento, pues seguramente sufrirán algunas modificaciones y adecuaciones antes de su aprobación. No obstante, existen aspectos de la propuesta que sí vale la pena considerar, y cuya valoración puede coadyuvar a la identificación de los elementos caracterizadores y la orientación político-jurídica que la UE quiere adoptar en relación con el tratamiento de la información.

En primer lugar, al promover la gobernanza de datos, la UE apuesta por implementar una metodología de actuación y una cultura específica en el modo de operar con la información (Abella García, 2020, pp. 167-175). Gobernar los datos supone «abandonar una posición reactiva para centrase en determinar bajo qué condiciones podemos definir usos de los datos al servicio de un desarrollo centrado en el ser humano y en la garantía de sus derechos» (Martínez Martínez, 2021ª, párr. 7).

En segundo lugar, el dato, en sentido lato y libre de adjetivos, es la realidad en torno a la que se configura la normativa. Sin embargo, las condiciones iniciales de la información, aun siendo relevantes, quedan en un segundo plano en comparación con otros factores que la atañen, como, por ejemplo, quién la detenta, cómo se utiliza y para qué o la capacidad para monitorear y fiscalizar sus usos. Consecuentemente, la viabilidad de cada operación vendrá determinada, principalmente, por elementos exógenos al dato (v. gr. las condiciones en que se opere con la información, las medidas de seguridad que se implementen, las finalidades que se persigan o la relevancia que el tratamiento tenga para la consolidación del mercado interior); y, en menor medida, por la condición endógena de la información (su naturaleza).

---

[275] También inciden en la necesidad de distinguir el régimen a aplicar a los datos personales y no personal. Vid. párrafos 57 a 62 de la EDPB y Supervisor Europeo de Protección de datos, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, de 9 de marzo de 2021.

[276] Párrafos 63 y 64 de la EDPB y Supervisor Europeo de Protección de datos, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, de 9 de marzo de 2021.

En definitiva, «ya no basta identificar el riesgo, se […] exige gobernarlo» (Martínez Martínez, 2021ª, párr. 8). El aprovechamiento de la información, sus posibilidades de utilización, dependerán de las medidas y garantías que se implementen.

Finalmente, la propuesta de Reglamento sobre gobernanza de datos pone en valor la importancia de la legislación. Pero no como manual de instrucciones, sino como guía. Si el legislador pretende anticipar todos los escenarios posibles estará condenado al fracaso, ningún frenesí normativo sería capaz de regular con detalle los diferentes contextos que las tecnologías y usos de la información generan. Aun cuando tal hiperproducción legislativa fuese posible, no sería deseable, pues adicionaría, a la hercúlea tarea de someter la realidad digital a la lógica jurídica, la dificultad de selección de la normativa aplicable.

En última instancia, una densidad regulatoria excesiva podría terminar siendo inoperante, al no ser capaz de proporcionar las respuestas rápidas y flexibles que el dinamismo e inmediatez de la vida en la Red exigen. Como apunta Martínez Martínez, «en lugar de una alocada carrera en la producción de documentos, de ser el primero en tener algo distintivo, se necesitan criterios homogéneos, compartidos y horizontales» (Martínez Martínez, 2021a).

La legislación, el modo en que se ejecute, será determinante para la pervivencia del ecosistema europeo de protección de datos. Si se focaliza en establecer las condiciones generales, los procedimientos, orientaciones y garantías que permitan dar una respuesta coherente a los diferentes escenarios que se puedan plantear, si tiene la flexibilidad suficiente para adaptarse a situaciones no previstas sin denuedo de los derechos y libertades, la regulación será la herramienta definitiva en el éxito de la Estrategia Europea de Datos. Si, por el contrario, se enroca en fijar condiciones concretas de ejercicio y dar soluciones a situaciones específicas en lugar de ser coherente con los principios, valores e idiosincrasia del modelo europeo, estará condenada al fracaso, pues no será reconocible internamente, ni podrá exportarse/imponerse en el plano internacional.

4.5.2. Las comunicaciones electrónicas

Internet no solo ha mejorado las formas de interconexión previamente existentes (v. gr. las videollamadas o mensajería instantánea y gratuita, o a bajo coste), sino que ha propiciado nuevas formas de relacionarse, como las «comunicaciones *one to many*, donde la información transita hacia varios comunicantes simultáneamente» (Ocón García, 2021, p. 17).

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[277] es la normativa de referencia en la UE en lo referente a la garantía del secreto de las comunicaciones (art. 7 CDFUE[278]). Como se desprende de su nombre, presta una atención especial a los efectos que las formas de interconexión mediatizadas por la tecnología pudieran tener sobre el derecho a la protección de datos.

Los medios técnicos, el canal a través del que se produce el proceso comunicativo, han hecho emerger nuevas amenazas para los derechos (desde la integridad de la comunicación, hasta riesgos para el derecho a la protección de datos o la intimidad merced al modo en que operan los servicios avanzados de comunicación, especializados en extraer y generar datos e informaciones adicionales al propio contenido del mensaje intercambiado, p. ej. mediante metadatos).

Los avances técnicos de las últimas décadas, la necesidad de adecuar el marco jurídico a una realidad copada por la prestación de servicios a través de Internet, así como la pertinencia de hacer converger la regulación sectorial sobre comunicaciones electrónicas con los cambios normativos operados en el ecosistema europeo de tratamiento de la información –y con su orientación proactiva– hacen perentoria la actualización de la Directiva sobre la privacidad y las comunicaciones electrónicas[279]. Así lo entienden

---

[277] Puede accederse a su versión consolidada, en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:02002L0058-20091219. (Última consulta: 20/10/2021).

[278] Art. 7 CDFUE: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones».

[279] Así lo considera la propuesta de Reglamento e-*privacy* (Considerando 6), en la que señala la necesidad de establecer un marco de protección que imponga a los servicios de comunicación electrónica unas exigencias y garantías equivalentes a las de los servicios tradicionales. Vid. Propuesta de Reglamento e-*privacy*, aprobada por el Consejo de la UE en

las instituciones europeas, que vienen trabajando, desde hace años[280], en la elaboración de un Reglamento sobre privacidad y comunicaciones electrónicas (Reglamento e-*privacy*)[281].

Sin embargo, la conformación de un marco jurídico apropiado para las comunicaciones mediatizadas por sistemas electrónicos no es sencilla, especialmente en lo relativo a la salvaguarda del derecho a la protección de datos.

El primer escollo a superar conecta con los supuestos de afectación derivada. Esto es, aquellos casos en que la quiebra de la integridad de las comunicaciones, además de suponer la vulneración del secreto de las comunicaciones, afecte a otros derechos fundamentales, como la intimidad[282] o la protección de datos. No hay, en estos casos, una relación causa-efecto automática, dependerá del caso concreto, pues no siempre las comunicaciones involucran datos personales, como ocurre, por ejemplo, en una transmisión de información de máquina a máquina, o en una cadena de correos entre empresas. Con todo, incluso en supuestos de ese tipo, es posible llegar a establecer conexiones con personas físicas, pues la autoría última de los mensajes podría conducir a un individuo concreto, salvo en

febrero de 2021. Puede consultarse el texto aprobado por el Consejo en: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf. (Última consulta: 20/10/2021).

[280] La Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una estrategia para el Mercado Único Digital de Europa, de 6 de mayo de 2015 incluía, entre las normativas necesitadas de revisión, a la Directiva sobre la privacidad y las comunicaciones electrónicas, señalando su inadecuación para dar respuesta a las particularidades de un sector en el que la mayor parte de los prestadores de servicios de la sociedad de la información usan Internet como medio operacional. Vid. punto 3.4 de la Comunicación, puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192&from=ES. (Última consulta: 20/10/2021).

[281] La Propuesta de Reglamento, actualmente, lleva por título: Reglamento del Parlamento EUROPEO Y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE. Sobre las líneas básicas de esta propuesta, vid. (Gil González y De Hert, Paul Papakonstantinou, 2020).

[282] Derecho a la intimidad entendido como «aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados a su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros» (Romeo Casabona, 2002, p. 521).

La vulneración del derecho a la intimidad a raíz de una comunicación electrónica es un escenario posible solo bajo ciertas circunstancias. En efecto, no siempre el contenido transmitido tiene una conexión con la persona con entidad suficiente para considerar que su conocimiento puede suponer una vulneración de la intimidad.

aquellos casos de respuestas generadas automáticamente y canalizadas a través de programas informáticos, p. ej. mediante bots[283].

Más allá de las dudas planteadas, no puede dejar de reseñarse que, al menos en algunos casos, el derecho al secreto de las comunicaciones proporciona una garantía adicional a otros derechos que pudieran verse violados en una eventual pérdida de integridad del proceso comunicativo. En cierto sentido, el secreto de las comunicaciones opera como un derecho instrumental de protección, si bien ese no es su cometido definitorio.

No obstante, los verdaderos riesgos para el derecho a la protección de datos no proceden de las brechas en el proceso comunicativo, sino de las particulares características de los servicios comunicación prestados a través de Internet[284], o mediante sistemas electrónicos que, además de conectar al emisor y al receptor, son capaces de generar y recabar otras informaciones adicionales.

Entre las fuentes de riesgo que se generan, o cobran verdadera magnitud, con los servicios de comunicación digitales, destacan los metadatos y las *tracking tools*. Por lo que respecta a los metadatos[285], estos

---

[283] Bot: «Acortamiento por aféresis de la palabra, ya también española, *robot*— se usa en referencia a un programa informático que efectúa automáticamente determinadas tareas». Observatorio de palabras de la Real Academia Española. https://www.rae.es/observatorio-de-palabras/bot. (Última consulta: 20/10/2021).

[284] Bajo la denominación servicios de comunicación se están considerando tanto los servicios de comunicaciones electrónicas, como los de comunicaciones interpersonales entendidos conforme a las definiciones de la Directiva (UE) 2018/1972 del Parlamento y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, arts. 2.4) y 2.5), respectivamente.

Art. 2.4). «"servicio de comunicaciones electrónicas": el prestado por lo general a cambio de una remuneración a través de redes
de comunicaciones electrónicas, que incluye, con la excepción de los servicios que suministren contenidos transmitidos
mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos».

Art. 2.5) ««servicio de comunicaciones interpersonales»: el prestado por lo general a cambio de una remuneración que permite un intercambio de información directo, interpersonal e interactivo a través de redes de comunicaciones electrónicas entre un número finito de personas, en el que el iniciador de la comunicación o participante en ella determina el receptor o receptores y no incluye servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio».

Aunque ambas definiciones señalan que la condición lucrativa de este tipo de servicios, lo cierto es que, en algunas casos la remuneración por los mismos tiene un carácter simbólico, cuando no son prestados gratuitamente. En otros, como son los servicios de acceso a internet, sí es habitual que lleven aparejado un coste reseñable.

[285] Los metadatos en el ámbito de las comunicaciones electrónicas son las informaciones generadas y/o descriptivas del proceso comunicacional (p. ej. la duración de la comunicación,

tienen una utilidad operativa evidente para el prestador del servicio, pues le permiten obtener una imagen real del proceso. Pero, además, se trata de datos valiosos para terceros, ya sean entidades públicas (en investigación policial y penal, pero también para la planificación de obras y servicios públicos[286]) o privadas (usos de servicios o ubicaciones para realización de ofertas personalizadas).

La utilización de este tipo de informaciones, en determinados contextos y para según qué finalidades, puede entrañar un riesgo para los derechos y libertades de las personas. De tal manera que, un conjunto de datos no generado por las personas de manera consciente y que, al menos en origen, no se refiere a individuos específicos, sino a un proceso mecanizado, termina proporcionando información específica sobre personas determinadas[287]. En definitiva, los metadatos pueden operar, bajo las circunstancias adecuadas, como datos personales y, consecuentemente, han de adoptarse las precauciones que dicha condición exige (Polo Roca, 2021, p. 222).

Junto a los metadatos, las *tracking tools* (v. gr. *cookies*, *spyware* o los identificadores ocultos) son el otro gran desafío para la regulación de las comunicaciones realizadas a través de sistemas electrónicos. Aunque, si se toman en consideración sus implicaciones económicas y su importancia estratégica, son el reto principal, debido a su capacidad para recabar datos de los dispositivos en que se instalan.

Naturalmente, no todas las herramientas de este tipo tienen funciones extractoras, algunas son necesarias, incluso imprescindibles, para asegurar el correcto funcionamiento del servicio electrónico (p. ej. las *cookies* técnicas utilizadas para asegurar un rendimiento constante de la web o servicio en cuestión). En la distinción en función de las finalidades perseguidas radica el primero de los desafíos. No parece razonable dar el mismo trato, por más que técnicamente sean similares, a herramientas que cumplen funciones tan desiguales como mantener el funcionamiento del

cuándo y dónde se produjo o el número de interacciones producidas en una determinada zona en un momento dado).

[286] En España, a lo largo del año 2019 se realizaron varios estudios de movilidad poblacional a partir de datos anonimizados derivados del uso de telefonía móvil. Para más información, vid. https://www.ine.es/experimental/movilidad/experimental_em.htm. (Última consulta: 20/10/2021).

[287] Se ha demostrado que es posible, a partir de los metadatos de una llamada, obtener información sobre el estado de salud de una persona, sin escuchar el contenido de la conversación (Mayer, Mutchler, y Mitchell, 2016).

servicio o extraer datos que permitan perfilar al usuario y realizarle ofertas publicitarias.

Como puede deducirse, las comunicaciones mediatizadas por tecnologías digitales no solo sirven al cometido originario que les identifica (la interconexión personal), sino que son la base de todo un sector de la economía digital, a la que nutren con los datos que logran recabar y generar.

La necesidad de establecer unos niveles de protección adecuados, sin hacer inoperantes o deficitarios unos servicios que resultan esenciales tanto para la posición estratégica de la UE, como para preservar la calidad de vida de la ciudadanía europea, dificulta sobremanera la elaboración de un marco regulatorio adecuado, capaz de conciliar los muchos intereses en conflicto. La complejidad de la materia, unida a su importancia económica, justifica las constantes dilaciones[288] en la aprobación de un Reglamento e-*privacy* que, al igual que Godot, no termina de llegar.

Con todo, la propuesta de Reglamento e-*privacy* aprobada por el Consejo en febrero de 2021, sin ser definitiva[289], sí está lo suficientemente avanzada en su tramitación[290] como para, con la prudencia que exige abordar una materia en la que se han producido tantos *impasses*, extraer ciertas conclusiones respecto de la orientación político-jurídica adoptada en relación con el tratamiento de la información personal[291].

---

[288] La Propuesta de Reglamento e-*privacy* inició su andadura legislativa con la propuesta de la Comisión, en enero de 2017, esta puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010.
No ha sido hasta 4 años después, en febrero de 2021, que el Consejo ha aprobado un texto que será enviado al Parlamento Europeo para continuar con la tramitación. Puede consultarse el texto aprobado por el Consejo en: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf. (Última consulta: 20/10/2021).

[289] Como ponen de manifiesto las recomendaciones y modificaciones propuestas por el EDPB en relación a la conservación de datos, la confidencialidad de las comunicaciones o la necesidad de desterrar, de una vez y para para siempre prácticas que supediten «el acceso a los servicios y funcionalidades a que el usuario consienta que se almacene o se acceda a información» personal. En EDPB, Declaración 03/2021, relativa al Reglamento sobre la privacidad y las comunicaciones electrónicas, adoptada el 9 de marzo de 2021. Puede consultarse en:
https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_es.pdf. (Última consulta: 20/10/2021).

[290] Puede seguirse toda la tramitación de este futuro reglamento en: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010. (Última consulta: 20/10/2021).

[291] Los retos en materia de integridad y las particularidades de la garantía del secreto de las comunicaciones, así como la eventual afectación de otros derechos como la vida privada,

Así, en primer lugar, la propuesta de Reglamento e-*privacy* constituye una regulación sectorial, especializada por razón de materia, pero condicionada por la normativa de protección de datos, al punto que su contenido no puede reducir el nivel de protección que el RGPD proporciona (Considerando 2a de la propuesta de Reglamento e-*privacy*).

El RGPD se erige en el mínimo a respetar en la articulación del régimen jurídico de las comunicaciones electrónicas, debiendo prestarse especial atención al cumplimiento de los principios del tratamiento de datos (Considerando 2a de la propuesta de Reglamento e-*privacy*). Además, opera como legislación supletoria en lo no previsto por el futuro Reglamento e-*privacy*, por ejemplo, para la realización de evaluaciones de impacto (art. 6a.2 de la propuesta de Reglamento e-*privacy*) o los deberes de confidencialidad (Considerando 15 de la propuesta de Reglamento e-*privacy*).

Por su parte, las recomendaciones de mejora y los llamados de atención del EPDB[292] inciden en la pertinencia de establecer condiciones más claras con relación a los plazos de conservación, en consonancia con los criterios que la jurisprudencia del TJUE ha venido estableciendo desde el asunto Digital Rights Ireland[293] y reiterado posteriormente en La Quadrature du Net y otros[294]. En esas sentencias, el TJUE señala que los plazos de conservación ilimitados son incompatibles con el derecho a la protección de datos; además, reitera la obligatoriedad de aplicar criterios de proporcionalidad, necesidad y adecuación a la hora de fijar los períodos de conservación de los datos personales recabados a raíz de la comunicación electrónica.

En lo referente a los metadatos, la principal apuesta de la propuesta de Reglamento e-*privacy* es la anonimización y la reducción de los riesgos derivados de posibles usos de las informaciones asociadas a los procesos

---

exceden el cometido de este capítulo y se alejan del objeto de esta tesis. No obstante, existen excelentes trabajos que abordan los desafíos para dichos derechos en el ámbito de las comunicaciones electrónicas, a título puramente ilustrativo, (Ocón García, 2021); (Rodríguez Lainz, 2016); (Zoco Zabala, 2015).

[292] EDPB, Declaración 03/2021, relativa al Reglamento sobre la privacidad y las comunicaciones electrónicas, adoptada el 9 de marzo de 2021. Puede consultarse en: https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_es.pdf. (Última consulta: 20/10/2021).

[293] STJUE asuntos C-293/12 y C-594/12, Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014.

[294] STJUE asuntos C-511/18, C-520/18 y C-520/18, La Quadrature du Net y otros, de 6 de octubre de 2020, especialmente apdos. 58 a 68.

comunicacionales (vid. Considerando 17aa, arts. 6b, 6c.2 o art. 7.1[295] de la propuesta de Reglamento e-*privacy*). Además de la anonimización, para aquellos tratamientos en los que se opere con datos personales, se aplicarán todas las medidas de reducción de riesgos que la normativa de protección de datos impone, amén de reconocer y facilitar el ejercicio de las facultades de actuación que caracterizan al derecho a la protección de datos.

Serán los usos que se den a los metadatos, y no el contenido del metadato en sí, los que determinen las posibilidades de llevar a efecto el tratamiento pretendido. Así, el uso de la información relativa a la ubicación geográfica se ha de evitar, incluso vedar, cuando tenga como finalidad elaborar los perfiles de los usuarios (Considerando 17aa de la propuesta de Reglamento e-*privacy*). Pero, por el contrario, se admite, incluso se incentiva, cuando sirva «*for the protection of vital interest of the end-user* […] [*or*] *for humanitarian purposes, including for monitoring epidemics and their spread or in humanitarian emergencies, in particular natural and man-made disasters*» (Considerando 17a de la propuesta de Reglamento e-*privacy*).

Finalmente, por lo que respecta a las medidas adoptadas con relación a las *tracking tools*, se impone, en primer lugar, la especialización y la diferenciación entre las herramientas imprescindibles y las que no lo son. Esto es, el régimen jurídico de las *cookies*, por utilizar el exponente paradigmático de este tipo de herramientas, no viene determinado por el hecho de ser *cookies*, sino por el cometido que van a realizar, la finalidad, su necesariedad y los efectos que puedan provocar en los individuos.

El elemento en torno al que se articula el régimen jurídico de las tracking tools es el consentimiento, sin perjuicio de «*other specific and transparent purposes*» que el futuro Reglamento e-*privacy* pueda prever y que, como del amplísimo listado del artículo 8.1 de la propuesta se deduce, están vinculadas a la ejecución de funciones específicas relacionadas con el correcto funcionamiento del servicio, la actualización del software o cuestiones de seguridad.

El modo en que se obtenga el consentimiento, la claridad de la información proporcionada, los fines que se persiguen o los posibles usos

[295] En el art. 7.1 de la propuesta de Reglamento e-*privacy* se señala expresamente a la anonimización como la alternativa a la eliminación de la información, una vez que esta ha cumplido su finalidad.

ulteriores que pueda tener, son elementos determinantes para la evaluación de la viabilidad del tratamiento. En esa línea de configuración contextual, focalizada en las características del tratamiento y en la transparencia de la información, el EDPB[296] insiste la conveniencia de pulir la propuesta de Reglamento e-*privacy* y establecer la inadmisibilidad de servicios condicionados. Esto es, solicita que se destierren los modelos de "*take it or leave it*", en los que el acceso al producto/servicio depende de la aceptación incondicionada de todas las cookies y herramientas de monitorización que el proveedor implemente.

4.6. La tendencia de las normativas que marcarán el futuro del ecosistema digital europeo

4.6.1. El control del contexto digital. La regulación de los mercados y servicios digitales

La capacidad de las empresas transnacionales[297] para abstraerse al control de los Estados merced a su dominio del mercado, es uno de los grandes retos jurídicos del siglo XXI[298]. El entorno digital no es ajeno a esta realidad, al contrario, en él han emergido algunas de las entidades con mayor capacidad para distorsionar la libertad de mercado, gracias, entre otras razones, a su posición estratégica en el mercado digital, pues ofrecen servicios estructurales, indispensables para el desarrollo del modelo de negocio que la Red posibilita. Alphabet (Google), Amazon, Facebook, Iphone, Twitter, Microsoft, Huawei o Xiaomi son ejemplos del tipo de empresas que, por sus características, dimensión e influencia global, tienen poder suficiente como para desvirtuar la competencia e, incluso, operar como freno a la innovación[299].

---

[296] Vid. EDPB, Declaración 03/2021, relativa al Reglamento sobre la privacidad y las comunicaciones electrónicas, adoptada el 9 de marzo de 2021. Puede consultarse en: https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_es.pdf. (Última consulta: 20/10/2021).

[297] Entendidas estas como aquellos «operadores económicos privados cuya constitución y extinción, así como sus actividades, se encuentran sometidas a una pluralidad de jurisdicciones estatales» (Guamán Hernández y Moreno González, 2018, p. 20).

[298] Así lo han puesto de manifiesto autores como (Bonet, 2008), (Guamán Hernández y Moreno González, 2018) o (AA.VV., 2016).

[299] Este tipo de entidades tienen capacidad para impedir que otros puedan acceder a un mercado que copan de manera oligopolística, cuando no como auténticos monopolios. Sería el caso de Alphabet, objeto de varias multas por parte de la Comisión por incumplir las normas antimonopolio de la UE. Sirvan para ilustrar algunas de esas sanciones, los más de

Para tratar de evitar prácticas desleales y proporcionar un marco de protección adecuado a los consumidores europeos, la UE está trabajando en la Propuesta de Reglamento del Parlamento y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales)[300]. Este Reglamento se focalizaría en el control de las actuaciones de los «guardianes de acceso», esto es, de los proveedores «de servicios básicos de plataforma […] [que tengan] una repercusión significativa en el mercado interior; […] [operen] un servicio básico de plataforma que sirv[a] como puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales; y […] [tengan] una posición afianzada y duradera en sus operaciones o es previsible que alcance dicha posición en un futuro próximo» (art. 3 propuesta de Ley de Mercados Digitales).

Junto al control de las actuaciones de los grandes proveedores, la UE está elaborando –al mismo tiempo[301]– una propuesta de Reglamento del Parlamento y el Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE[302]. Este segundo reglamento tiene como cometido mejorar el funcionamiento del mercado digital, mediante el establecimiento de un conjunto de deberes y obligaciones de actuación y, a la vez, busca «crear un entorno en línea seguro, predecible y confiable, en el que los derechos fundamentales consagrados en la Carta estén efectivamente protegidos» (art. 1.2.b) de la propuesta de Reglamento de Servicios Digitales).

8000 millones de euros que se han impuesto a Alphabet en solo tres multas por abuso de posición de dominio de tres de sus productos:
4340 millones por Android (https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581), 2420 millones por Shopping (https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784) y 1490 por Google (https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770).
Microsoft también ha sido objeto de sanción por este motivo, sentencia del Tribunal de Primera Instancia de la UE, de 17 de septiembre de 2007, asunto T-201/04, puede consultarse en:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62004TJ0201. (Última consulta: 20/10/2021).

[300] La propuesta de Reglamento del Parlamento y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales): https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=COM:2020:825:FIN. (Última consulta: 20/10/2021).

[301] Ambas propuestas se aprobaron el 15 de diciembre de 2020.

[302] Es una traducción propia del nombre oficial, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, el nombre final oficial en castellano podría ser diferente. Por el momento solo puede consultarse la Propuesta en inglés:
https://www.eumonitor.eu/9353000/1/j4nvke1fm2yd1u0_j9vvik7m1c3gyxp/vlenhiua50zj/v=s7z/f=/com(2020)825_en.pdf. (Última consulta: 20/10/2021).

En estos reglamentos, el tratamiento de información personal es una cuestión tangencial lo que, sumado a su carácter provisorio –por encontrarse en fase de tramitación– obligan a tener cierta cautela a la hora de extraer conclusiones respecto de sus efectos e influencia en la conformación del modelo europeo de protección de datos. No obstante, controlar las actuaciones de los grandes detentadores de información, quienes, además, se ocupan de canalizar los flujos de datos (personales o no) (propuesta de Ley de Mercados Digitales); regular los términos y condiciones en que se prestan los servicios (art. 12 de la propuesta de Ley de servicios digitales[303]); u obligar a proporcionar información ante los requerimientos de las autoridades (art. 9 de la propuesta de Ley de servicios digitales[304]), son medidas jurídicas con un impacto directo tanto en el derecho a la protección de datos, como, en general, en el grado de libertad de/en la Red.

Los reglamentos sobre los mercados y los servicios digitales inciden en la apuesta por regulaciones especializadas, sectoriales, capaces de disciplinar las particularidades de cada ámbito. Asimismo, son un reflejo del empeño de la UE en proporcionar un marco seguro de actuación por medio de regulaciones adecuadas a la realidad de cada sector. La especialización normativa y aplicativa es, en definitiva, una de las señas de identidad del modelo europeo.

4.6.2. El gran desafío: la regulación de la Inteligencia Artificial

La regulación de la Inteligencia Artificial (IA) es uno de los campos de batalla más complejos, pues requiere someter la lógica matemático-economicista de los ingenios tecnológicos a los parámetros jurídicos que rigen la vida en sociedad. La determinación de los criterios en que aquella ha de fundar sus decisiones, los mecanismos de fiscalización de los algoritmos que la alimentan, la respuesta frente a decisiones injustas o discriminatorias, así como el respeto a la protección de datos, son variables

[303] La información sobre las condiciones de servicio, abarcará «todo tipo de políticas, procedimientos, medidas y herramientas que se utilicen con fines de moderación de contenidos, incluidas las decisiones algorítmicas y la revisión humana. Se expondrá en lenguaje claro e inequívoco y se hará pública en un formato fácilmente accesible» art. 12 de la propuesta de Ley de servicios digitales.

[304] «Los prestadores de servicios intermediarios, cuando reciban una orden de entrega de un elemento de información concreto acerca de uno o varios destinatarios concretos del servicio […]informarán a la autoridad que haya dictado la orden, sin dilaciones indebidas, acerca de su recepción y aplicación», art. 9 de la propuesta de Ley de servicios digitales.

que han de ser consideradas cuando se pretenda aprovechar las posibilidades y ventajas de su uso.

La Unión Europea viene trabajando, desde hace unos años, en una Estrategia Europea para la IA (2018)[305], de la que han surgido, como producciones más reseñables: el *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y al confianza*[306] y la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas[307].

Además, con el texto propuesto en abril de 2021 por la Comisión Europea, se ha iniciado el proceso legislativo que habrá de culminar, en un futuro no muy lejano, con la aprobación del Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial[308]) y se modifican determinados actos legislativos de la Unión[309].

La necesidad de garantizar que los sistemas de IA sean seguros y respetuosos con los derechos y valores de la UE, la voluntad de promover la inversión y la innovación con esta tecnología como base, la mejora en la efectividad de la IA, así como su gobernanza, amén de la consolidación del mercado interior a través de un marco común que rija la utilización de esta herramienta, constituyen el fundamento de la propuesta de Reglamento

---

[305] La Comisión presentó, el 25 de abril de 2018, sus planes en relación con el uso de la IA, puede consultarse la Comunicación de la Comisión al Parlamento, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones en, https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF. (Última consulta: 20/10/2021).

[306] En el Libro Blanco se establecen las líneas maestras que ha de seguir el desarrollo de esta tecnología. Puede consultarse el Libro Blanco de la Comisión en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf. (Última consulta: 20/10/2021).

[307] Puede consultarse el texto de la resolución en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.pdf. (Última consulta: 20/10/2021).
Un análisis detallado de la propuesta, las principales aportaciones y debilidades de la misma puede consultarse en (Lazcoz Moratinos, 2020).

[308] En la versión en inglés se le denomina *Artificial Intelligence Act*. No deja de ser reseñable esta apuesta nominativa por el término ley para lo que no deja de ser un reglamento de la UE. Con todo no parece algo casual, pues las propuestas de reglamentos sobre mercados y servicios digitales también usaban la denominación ley para su denominación.

[309] Al tratarse de una propuesta legislativa en una fase muy inicial es posible que no sea el nombre definitivo, con todo, es el que identifica el texto con el que se está trabajando. Puede consultarse la propuesta de la Comisión, de 21 de abril de 2021, en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206. (Última consulta: 20/10/2021).

IA[310]. El modo en que se articule jurídicamente la consecución de dichas finalidades puede ser especialmente útil para conocer la orientación/morfología futura de las normativas sobre tratamiento de la información, pues la regulación de la IA marcará y condicionará el futuro del ordenamiento jurídico digital europeo.

4.6.2.1. Hacia un modelo de prevención de riesgos más acuciado: La propuesta de Reglamento IA

Tanto el Libro Blanco como la Resolución del Parlamento constituyen referencias valiosas acerca de la idiosincrasia el modelo europeo de IA. Sin embargo, a efectos de estudio, resulta más clarificadora la propuesta de Reglamento de Inteligencia Artificial, pues no deja de ser el resultado de la convergencia de las orientaciones y propuestas del Libro Blanco y la Resolución del Parlamento con las demandas y particularidades de la realidad material.

En el análisis de la propuesta de Reglamento se prestará especial atención a su enfoque, así como a las referencias específicas que realice respecto de la utilización de datos personales. Sin embargo, no se entrará en el detalle técnico de las medidas que propone, pues probablemente sufran cambios a lo largo de la tramitación legislativa, especialmente si se toman en consideración las importantes –y atinadas– críticas y dudas planteadas por autores de la talla de Veale y Zuiderveen Borgesius[311].

Más allá de los problemas, contradicciones y lagunas que dichos autores identifican, hay una característica de la propuesta de Reglamento IA que valoran positivamente: su estructura basada en el riesgo. En efecto, el elemento definitorio de la propuesta de Reglamento IA es su apuesta por la gestión de riesgos como herramienta jurídica mediante la que lograr los objetivos que la impulsan. Para ello, establece una graduación de los sistemas de IA, a los que define de manera amplia[312], clasificándolos en función del riesgo que su uso puede entrañar.

---

310 Vid. Exposición de motivos de la propuesta de Reglamento IA, en concreto, el apdo. 1. Contexto de la propuesta.

311 Vid. (Veale y Zuiderveen Borgesius, 2021).

312 En el art. 3.1) se define como Sistema de inteligencia artificial al «software que se desarrolla empleando una o varias […] técnicas y estrategias […] y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de

En primer lugar, se incluye un grupo de sistemas de IA cuya utilización está prohibida, por suponer un riesgo inaceptable. En segundo lugar, se encuentran profusamente detallados, los sistemas IA de alto riesgo. Finalmente, en un tercer bloque, se agruparían los sistemas de IA que no comportan un alto riesgo. En este último conjunto se puede identificar un subgrupo, definido por su finalidad, en el que se integrarían aquellos sistemas IA que entrañen ciertos riesgos de manipulación, individual o colectiva.

En lo referente a los usos de la IA prohibidos, la propuesta de Reglamento IA incluye cuatro supuestos. De ellos, dos están vinculados a formas de manipulación del comportamiento. Uno focalizado en los sistemas que producen dichos resultados mediante el uso de «técnicas subliminales que transciendan la conciencia de una persona» (art. 5.1.a) de la propuesta de Reglamento IA). El otro, presta atención a los modelos de IA que se aprovechan «de las vulnerabilidades de un grupo específico debido a su edad o discapacidad física o mental» (art. 5.1.a) de la propuesta de Reglamento IA).

En ambos casos, además de esa finalidad de control conductual, se exige que el uso del sistema de IA «provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra» (art. 5.1. apartados a) y b) de la propuesta de Reglamento IA). Esa exigencia de daño ha sido criticada por Veale y Zuiderveen Borgesius, pues impediría aplicar esta prohibición a aquellos sistemas que tuviesen efectos cumulativos[313]. En esos casos, no sería posible vincular el perjuicio a una actuación concreta de la IA y, sin embargo, los efectos gravosos podrían ser igual de

salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa».
Las técnicas y estrategias a las que se refiere la definición aparecen enunciadas en el Anexo I de la propuesta de Reglamento. Se trata de un conjunto abierto, que la Comisión puede actualizar conforme los avances técnicos así lo demanden (art. 4 de la propuesta de Reglamento IA) y que, en la actualidad, incluye: «Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo.
Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico).
Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización». (Anexo I de la Propuesta de Reglamento IA). Pueden consultarse los Anexos de la Propuesta de Reglamento IA en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN. (Última consulta: 20/10/2021).

[313] Por ejemplo, a través de modelos de control coercitivo, en los que se penalicen ciertos comportamientos, condicionando, de ese modo, la manera de vivir y actuar en sociedad.

importantes, no solo en una persona, sino en grupos completos (afectación colectiva que la propuesta tampoco contempla) (Veale y Zuiderveen Borgesius, 2021, pp. 4-5).

La tercera práctica de IA prohibida está vinculada a la utilización de sistemas de evaluación y clasificación social que desemboquen en «un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros» siempre que, además, no sea proporcional ni obedezca a razones justificadas (art. 5.1.c) apartado ii) de la propuesta de Reglamento IA). También se prohíbe la utilización de esos sistemas de *social scoring* cuando sus decisiones se produzcan «en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente» (art. 5.1.c) apartado i) de la propuesta de Reglamento IA).

Con esta medida, se busca vedar prácticas como el sistema de crédito social que se ha implantado en algunas regiones de China[314] y, sobre todo, se trata de atajar situaciones como la acaecida con el sistema SyRI (Sistema de Indicación de Riesgos) utilizado por el gobierno de los Países Bajos para evaluar las probabilidades, "el riesgo", de que una persona cometiese fraude a la seguridad social y/o a hacienda. El tribunal neerlandés que enjuició el caso consideró que, si bien la utilización de sistemas de este tipo no era ilícita en todo caso, sí lo era en el supuesto juzgado, pues no se proporcionaban las garantías adecuadas, ni se superaba el juicio de proporcionalidad[315].

La última de las prohibiciones está referida al «uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de aplicación de la ley» (art. 5.1.d) de la propuesta de Reglamento IA). La interdicción de esta forma de utilización de los sistemas biométricos de identificación radica en su capacidad condicionante, así como en su impacto en la libertad de la ciudadanía, pues haría de los espacios públicos lugares permanentemente controlados, dando lugar a situaciones propias de una sociedad orwelliana[316].

---

[314] Sobre el sistema de crédito social chino, sus orígenes, su grado de implantación y características. vid. (Creemers, 2018), sobre las posibilidades de exportación del modelo a otros países, vid. (Mac Síthigh y Siems, 2019).

[315] Sobre la sentencia del caso SyRI vid. (Cotino Hueso, 2020) y (Lazcoz Moratinos y Castillo Parrilla, 2020). Para una descripción del caso juzgado, vid. (Fernández, 2020).

[316] No obstante, en el caso de la propuesta de Reglamento IA, se prevén tres situaciones en las que el uso de esta posibilidad técnica sí tendría cobertura legal: «la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos; la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las

La propuesta de Reglamento IA dedica buena parte de su contenido a establecer las condiciones en que se pueden utilizar los sistemas de IA de alto riesgo[317]. El nivel de detalle con que se regulan estos sistemas está en consonancia con el nivel de amenaza que representan para los derechos y libertades y, más en general, para el estado de Derecho. La identificación de los sistemas de IA de alto riesgo puede agruparse en dos grandes bloques. El primero de ellos vendría caracterizado por la función que desempeñan. Así, se consideran de alto riesgo aquellos sistemas que operen «como componente de seguridad de uno de los productos contemplados» en alguna de las 19 normas de armonización previstas en el Anexo II de la propuesta de Reglamento IA[318] (art. 6.1 de la propuesta de Reglamento IA).

En el segundo grupo de sistemas de alto riesgo se incardinan aquellos que, por sus características y finalidades, pueden generar perjuicios graves para la ciudadanía. En él se incluyen, de una parte, los sistemas enumerados en el Anexo III (art. 6.2 y 7.1.a) de la propuesta de Reglamento IA) y, de otra, cualquier modalidad de IA que represente un peligro para la salud, la seguridad o los derechos fundamentales, siempre que tenga una entidad igual o superior a la que representan los sistemas enlistados en el Anexo III (art. 7.1.b) de la propuesta de Reglamento IA).

Los ocho sistemas relacionados en el Anexo III conforman un conjunto abierto, susceptible de ampliación y actualización por la Comisión (art. 7.1 en conjunción con el art. 73 de la propuesta de Reglamento IA)[319].

---

personas físicas o de un atentado terrorista; [y] la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos […] [previstos en la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, siempre que] la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años» (apartados i); ii) e iii) del art. 5.1.d) de la propuesta de Reglamento IA).

317 Prácticamente 50 (del art. 6 al 51, pero también el 60 o el 61) de los 85 artículos de que consta la propuesta están dedicados, en exclusiva, a disciplinar la utilización de los sistemas de alto riesgo, a los que habría que adicionar aquellas previsiones que, sin ser específicas, también les son aplicables.

318 Pueden consultarse los Anexos de la Propuesta de Reglamento IA en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN. (Última consulta: 20/10/2021).

319 En la actual propuesta, el listado del Anexo III está integrado por los sistemas que: sirvan para la identificación biométrica y la categorización de personas físicas, sea en tiempo real o en diferido. Los «destinados a utilizarse como componentes de seguridad en la gestión y funcionamiento del tráfico rodado y el suministro de agua, gas, calefacción y electricidad». Aquellos que sirvan para el acceso a centros de educación o evaluar al estudiantado. Los empleados en la gestión de los trabajadores, en cualquiera de las etapas de la trayectoria

Esta cláusula de apertura resulta muy pertinente, pues permite actualizar la normativa y evita que los listados y técnicas previstos queden desfasados e introduzcan rigideces en el modelo de protección.

Pese a lo detallado del listado de sistemas de alto riesgo, lo cierto es que, alguno de los así calificados debieran, por su impacto en los derechos, ser considerados como inaceptables y su uso prohibido; v. gr. los sistemas IA destinados a «la evaluación de rasgos y características de la personalidad o conductas delictivas pasadas de personas físicas o grupos» (Anexo III, apartado 6, letra e) de la propuesta de Reglamento IA). En todo caso, es esperable que, a lo largo del proceso legislativo, se revise esta cuestión[320].

A los efectos que aquí nos interesan, lo relevante es reseñar que la calificación como sistema de alto riesgo y, consecuentemente, todas las medidas, garantías y exigencias a implementar están estrechamente vinculadas a la prevención de los efectos nocivos/discriminatorios que pudieran deparar las decisiones adoptadas por medio de la lógica algorítmica. El carácter protector, proactivo y anticipatorio de la propuesta de Reglamento IA se refleja, especialmente, en sus exigencias precautorias. Impone una política de gestión de riesgos destinada a identificar, evaluar y reducir los peligros del sistema IA que vaya a emplearse, con la que busca

---

laboral, desde la contratación y selección, hasta la promoción o resolución del contrato, pasando por la promoción o la evaluación del rendimiento. Los sistemas utilizados para el acceso a determinados servicios, ya sean públicos (p. ej. prestaciones y servicios de asistencia o para priorizar el envío de servicios de emergencia) o privados (v. gr. los sistemas de evaluación de solvencia y calificación crediticia).
También se incluyen entre los sistemas de IA de alto riesgo aquellos que sirven de apoyo a las autoridades para la aplicación de las leyes, como es el caso de los *software* que miden los riesgos de comisión de infracciones penales o de reincidencia, los que evalúan los rasgos y características de personas o grupos, así como aquellos que sirven para predecir la frecuencia con se cometerá un determinado delito en años futuros o los que permiten recabar y validar pruebas (p. ej. detectando falsificaciones, evaluando la fiabilidad de las evidencias presentadas o detectando relaciones ocultas y comportamientos ilícitos no conocidos). En la misma línea de apoyo a la gestión de los asuntos públicos, se incluyen los modelos de IA «destinados a ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la aplicación de la ley a un conjunto concreto de hechos»; así como los sistemas de IA de apoyo en la gestión y control de fronteras, ya para evaluar los riesgos para la seguridad o la salud, para validar la autenticidad de los documentos presentados o en la detección del estado emocional de las personas que pretenden entrar al país.

[320] En la revisión de la propuesta de Reglamento IA sería interesante que se tomasen en consideración propuestas como las realizadas por Soriano Arnanz, quien, desde la gestión del riesgo como premisa, apunta una categorización del mismo más detallada (incluyendo sistemas de riesgo medio y riego bajo), así como medidas muy interesantes con relación al papel que han de desempeñar las administraciones públicas en el control de los sistemas algorítmicos. Vid. (Soriano Arnanz, 2021a).

evitar que los daños lleguen a materializarse (art. 9 de la propuesta de Reglamento IA).

Por otra parte, si bien se incluye un aparato sancionador en el que se prevén importantes multas administrativas (hasta treinta millones de euros o el 6% del volumen de negocio total anual mundial) (art. 71 de la propuesta de Reglamento IA), no se habilitan canales adecuados para la actuación directa de los individuos. Esta ausencia, que debería subsanarse, sería mucho más dramática si no se hubiesen previsto las obligaciones de diseño y las exigencias de evaluación previa del riesgo, destinadas a evitar que el daño llegue a producirse.

Finalmente, respecto de los usos de la IA que no entrañan un alto riesgo, destacan las obligaciones de transparencia que se imponen a los sistemas de IA «que i) interactúen con seres humanos, ii) se utilicen para detectar emociones o determinar la asociación a categorías (sociales) concretas a partir de datos biométricos, o iii) generen o manipulen contenido (ultrafalsificaciones)» (apartado 5.2.4 de la Exposición de motivos de la propuesta de Reglamento IA). El cometido de esas mayores exigencias en materia de transparencia es evidente: prevenir a la ciudadanía frente a posibles intentos de manipulación, asegurarle el acceso a toda la información posible para que pueda decidir por sí misma y evitar engaños masivos que pudieran afectar a la estabilidad de los países, por ejemplo, a través del uso de informaciones falsas durante los procesos electorales.

Además de adecuarse el uso de la IA a las obligaciones relativas al tratamiento de datos personales, la propuesta de Reglamento IA incide, directamente, en el régimen jurídico de las categorías especiales previsto en el art. 9 del RGPD, pues establece un supuesto específico en el que se puede enervar la prohibición de tratarlas. En efecto, en su artículo 10.5, habilita el tratamiento de las tipologías especiales de datos, cuando «sea estrictamente necesario para garantizar la vigilancia, la detección y la corrección de los sesgos asociados a los sistemas de IA de alto riesgo».

Junto a la necesariedad de la utilización, será imprescindible haber implementado «las salvaguardias adecuadas para los derechos y las libertades fundamentales de las personas físicas, lo que incluye establecer limitaciones técnicas a la reutilización y la utilización de las medidas de seguridad y protección de la privacidad más recientes, tales como la

seudonimización o el cifrado, cuando la anonimización pueda afectar significativamente al objetivo perseguido».

Sin embargo, más allá de esas previsiones concretas, lo verdaderamente valioso para la garantía del derecho fundamental a la protección de datos es que la propuesta de Reglamento IA, merced a su enfoque eminentemente preventivo y anticipatorio, ahuyenta muchos de los problemas que amenazaban la eficacia de las normativas de protección de datos. La propuesta de Reglamento IA anticipa las medidas de control y evaluación a una fase previa a la ejecución del tratamiento y, con ello, evita que se produzcan situaciones en las que, el uso de informaciones personales por parte de sistemas IA, pueda terminar provocando algún tipo de discriminación o vulneración de derechos. De este modo, complementa –y completa– las cauciones preliminares que toda operación con datos personales debe aplicar, merced a la exigencia de responsabilidad proactiva.

Por otra parte, la propuesta de Reglamento IA también sirve, por contraposición, para poner de manifiesto que el enfoque del RGPD, pese a incorporar la atención al riesgo y la proactividad como criterios, aún tiene margen de desarrollo. El RGPD no aprovecha toda la potencialidad de las finalidades y los efectos como los mecanismos con los que hacer frente al dinamismo y variedad de posibilidades técnicas y aplicativas de la era digital.

5. Un modelo eminentemente preventivo y proactivo

La era digital es la era de la información, los datos son su materia prima –sean personales o no–. Articular un sistema jurídico que posibilite su gestión y transferencia, garantizando un elevado nivel de protección de los derechos y libertades de la ciudadanía es uno de los grandes desafíos del siglo XXI. La UE ha asumido, merced a sus competencias en la consolidación del mercado interior, un papel protagónico en la construcción de un marco jurídico adecuado para la gestión de la información.

La CDFUE, los Tratados y el RGPD son la base normativa del modelo. Sin embargo, no se agota en ellos el sistema de protección europeo. La UE ha ido construyendo –y continúa haciéndolo– un entramado normativo

destinado a asegurar un marco de garantía y protección para la ciudadanía frente a los peligros derivados de la gestión de la información en la era digital. Para lograr un nivel de protección similar en todos los Estados miembros, ha objetivado los elementos basilares del sistema mediante una estandarización (vía reglamento o directiva, según el caso) que, más allá de su aplicación europea, no oculta su pretensión de universalizar el modelo.

El ecosistema europeo de tratamiento de la información personal, con el RGPD como buque insignia[321], es la plasmación de un modo concreto de afrontar los desafíos del desarrollo tecnológico y la construcción de un mercado digital, en el seno del mercado interior. El equilibrio de intereses y el diseño de mecanismos ágiles de resolución de los inevitables conflictos, han llevado a la UE a apostar por un sistema articulado en torno a los riesgos y efectos del tratamiento, en el que la proactividad sitúa a los operadores de datos como la primera línea de defensa.

Con todo, para no caer en los problemas e inseguridades de la autorregulación, se han establecido unas bases comunes, jurídicamente exigibles y que vinculan a todos –desde los operadores a los legisladores–. Un mínimo común que tiene en la garantía de los derechos y libertades su guía, y en los principios del tratamiento y las facultades de actuación del interesado sus principales instrumentos para hacerlo efectivo.

A ello debe adicionarse la puesta en valor de la privacidad –en sentido amplio–, y los incentivos que un sistema coactivo potente, generan a la hora de desarrollar una cultura de la prevención que oriente los comportamientos hacia modelos de actuación más respetuosos y menos peligrosos para la ciudadanía.

El elemento central de todo ese entramado jurídico es el RGPD. Sus previsiones son cruciales para el sistema de protección frente al tratamiento de la información, pues disciplinan el tratamiento de los datos de carácter personal; los cuáles, por su conexión directa con la persona, constituyen el principal riesgo para los intereses jurídicos de los ciudadanos. Sin perjuicio de que, ingenios tecnológicos como el *big data* o la inteligencia artificial, puedan generar niveles de riesgo equivalentes sin valerse de esa materia prima.

[321] Como apunta Gascón Marcén, el RGPD no solo es la cara más visible del modelo europeo, sino que constituye una referencia para el desarrollo de la «legislación digital europea» (Gascón Marcén, 2021).

La atención al riesgo y la exigencia de responsabilidad proactiva son los principales mecanismos de los que se sirve el RGPD para lograr los dos objetivos que le fundamentan: la libre circulación de la información y la protección de «los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales» en el tratamiento de sus datos personales (art. 1.2 RGPD). La anticipación a los problemas, la documentación de los tratamientos, el diseño de medidas técnicas y organizativas adecuadas, la aplicación por defecto de las prácticas más protectoras con los derechos e intereses son la plasmación fáctica del espíritu preventivo y proactivo del sistema europeo.

El tratamiento de la información personal es una realidad en constante cambio y transformación, que la normativa destinada a disciplinarlo goce de un nivel de flexibilidad y adaptabilidad equivalentes no debería resultar extraño, al contrario, se antoja conveniente, y hasta necesario, para evitar una obsolescencia absoluta de sus presupuestos. En este sentido, la apuesta por un modelo eminentemente contextual encaja con una concepción del derecho a la protección de datos como algo vivo[322], esto es, como un derecho capaz de adaptarse a las circunstancias del caso y de evolucionar para hacer frente a la realidad que disciplina (Resta, 2008).

No obstante, el sistema actual, eminentemente preventivo y proactivo, no debería entenderse como un modelo puro o definitivo. En el RGPD conviven previsiones en las que se combinan las medidas anticipatorias y contextuales, con formas rígidas de protección en abstracto. Así, frente a la libertad dispositiva para ajustar las medidas a la realidad del tratamiento, la previsión de unas categorías especiales de datos, cuya presencia condiciona el margen de decisión de los responsables, se presenta casi como un elemento extraño, contrario a la corriente que parece impulsar la regulación europea relativa al tratamiento de la información.

Más allá del ejemplo concreto de las categorías especiales, cuya configuración predefinida es la antítesis de la adaptabilidad a la realidad del tratamiento, no pueden dejar de señalarse las dinámicas reactivas que genera «la relación entre finalidad y proporcionalidad en conexión con la

[322] En el sentido del Diritto vivente formulado por Resta (Resta, 2008). Si bien las teorías del *living Law* son muy anteriores, pudiendo situar el trabajo de (Ehrlich y Isaacs, 1922) «The Sociology of Law» como referencia inicial. Sobre el *living Law*, sus orígenes, características y referentes, vid. (Messner, 2012).

evaluación del riesgo […] [y que han llevado a] una corriente de pensamiento políticamente correcto centrado en la prohibición» (Martínez Martínez, 2021b).

En definitiva, el sistema de protección configurado por el RGPD es un híbrido. Una normativa que quiere implementar las prácticas más adecuadas para responder a los retos que la era digital plantea, pero que no ha sido capaz de desprenderse completamente de las dinámicas históricas que han ido dando forma al modelo europeo de protección de datos (el carácter defensivo, las categorías especiales, las definiciones tasadas y acotadas, las respuestas predefinidas para aportar seguridad desde la previsibilidad y la aplicación mecanizada).

El RGPD es el producto de un interregno entre lo viejo que no termina de morir y lo nuevo que no termina de consolidarse[323]. Con todo, en la evolución de la normativa de protección de datos se atisban indicios fuertes de un cambio de paradigma. El legislador europeo parece haberse liberado de ciertos temores atávicos, y está apostando por generar una cultura de la protección de datos más flexible, acaso menos previsible *prima facie*, pero no por ello menos segura en sus resultados finales.

Las normativas que integran –o integrarán en un futuro próximo– el ecosistema europeo de tratamiento de la información personal, reflejan esa tendencia hacia la personalización y la protección especializada y sectorializada de los intereses de las personas. Del conjunto de normativas que inciden en el tratamiento de datos se constata la centralidad de ciertos elementos: la libre circulación, la consolidación del mercado interior y la voluntad de no sacrificar los derechos y libertades en el altar de digitalización.

Se percibe, en todas las regulaciones que, de algún modo, inciden en el tratamiento de datos, un esfuerzo por humanizar las lógicas técnicas, así como por racionalizarlas y regularlas jurídicamente, hasta un punto en que se logren conciliar el progreso y el aprovechamiento de los beneficios con la pervivencia de las democracias liberales.

En esa búsqueda del equilibrio, las renuncias a ciertas opciones que la tecnología permite, en aras de preservar los derechos y libertades de la ciudadanía, son un escenario a considerar. Por ejemplo, puede que sea

[323] Parafraseando la frase atribuida al dramaturgo alemán Bertolt Brecht «lo nuevo no termina de nacer y lo viejo no termina de morir», así como la muy similar de Gramsci referida a la muerte del viejo mundo sin que el nuevo termine de aparecer.

posible espiar a todo el mundo, todo el tiempo e incluso saber qué piensa y siente (o al menos establecer una probabilidad cercana al 100%), pero no es jurídicamente aceptable.

La defensa de los derechos y libertades en el espacio digital es una de las señas de identidad más marcadas del modelo europeo. Esta apuesta parte de una convicción clara, «sin unas garantías sólidas de protección de datos, se corre el riesgo de que no sea sostenible una economía digital de confianza» (Fernández, 2021). La defensa de los derechos se alinea con los otros objetivos de la UE: la consolidación del mercado interior y el aprovechamiento estratégico de la economía de datos. Un marco normativo que proporcione seguridad y certeza, evitando la materialización de los riesgos inherentes al tratamiento de datos, es la mejor respuesta que, desde el plano legislativo, se puede ofrecer.

Además de esa filosofía común, los diversos reglamentos y directivas que inciden en el tratamiento de datos ponen de manifiesto la transversalidad de un derecho que «lleva camino de consolidarse como una materia […] con autonomía y perfil propios. Este ámbito del Derecho se caracterizará por disponer de principios, valores, reglas e institutos propios y, a la vez, por una constante apertura a la interacción instrumental con el conjunto del Ordenamiento» (Martínez Martínez, 2021b).

Con todo, la especialización regulatoria no será capaz de dar respuesta a todas las problemáticas que el desarrollo tecnológico plantea. Por ello, es imprescindible que la normativa de referencia (el RGPD) sea lo suficientemente clara, flexible y garantista como para poder afrontar problemas de naturaleza diversa, sin que, por ello, el derecho a la protección de datos deje de ser reconocible.

La orientación proactiva, anticipatoria, centrada en el riesgo y en la personalización de las respuestas normativas, a la que parece tender el modelo europeo, es la que debe inspirar las respuestas jurídicas a los problemas que puedan plantearse en relación con el concepto de dato, o con la rigidez de las categorías especiales.

CAPÍTULO IV. DATO, TRATAMIENTO Y LA COMPLEJA NATURALEZA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

«*Privacy is not something that I'm merely entitled to, it's an absolute prerequisite*».
Marlon Brando. 1960

1. Dato personal y tratamiento como objeto primario de estudio

El derecho a la protección de datos se proyecta sobre una realidad material determinada, los datos personales. Son el objeto de protección del derecho (v. gr. art. 8.1 de la CDFUE o 16.1 del TFUE) y, por ende, resulta esencial determinar cuáles son los criterios que permiten considerar que una información debe ser considerada como dato personal.

El alcance y aplicación efectiva del derecho a la protección de datos depende, en última instancia, de la conceptualización del centro de imputación sobre el que actúa, del «espacio de autodeterminación» (Jiménez Campo, 1987, p. 38) que todo derecho fundamental busca salvaguardar.

Esta aparente inversión metodológica (primero la definición jurídica de dato y después la caracterización del derecho) obedece al proceso de formación del derecho, en el que su reconocimiento constitucional es tardío, al ser el resultado último de una secuencia regulatoria fraguada en el seno de democracias avanzadas.

Responder a la pregunta: ¿qué es, desde un punto vista jurídico, un dato personal?, entraña una dificultad mucho mayor de la que, intuitivamente, pudiera suponerse. Se trata de un concepto en constante evolución y que está salpicado de matices necesitados de concreción y clarificación.

Desde la *Datalag* sueca (1973)[1], que circunscribía los datos personales a la «información relativa a una persona»[2] (1 §), hasta el concepto vigente en el RGPD, se puede constatar una sucesiva ampliación

[1] No se parte de la Ley de Protección de Datos del *Land* de Hesse de 1970 debido a que esta no se circunscribe a los datos personales. En ella, «la protección de datos abarca todos los documentos creados para el procesamiento de datos informáticos, así como todos los datos almacenados y los resultados de su procesamiento» (§ 1). Traducción del original: «*Der Datenschutz erfaBt alle für Zwedce der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten*».
[2] *Datalag* 1973, *SFS*: 289, § 1: «*Personuppgift: upplysning som avser enskild person*».

en los elementos que ha de reunir una determinada información para ser considerada dato personal[3]. Mayor precisión descriptiva que, sin embargo, no ha ido en detrimento del alcance y dimensión del concepto. Al contrario, la inclusión de nuevas adjetivaciones (v. gr. "identificable") ha servido para ampliar las posibilidades de subsunción de una determinada información en la categoría de los datos personales.

No obstante, sin desconocer que el vínculo fuerte es el que se produce entre la persona y el dato, no puede descartarse que, el tratamiento, por sus características, también ocasione algún efecto condicionante sobre los derechos en concurso. No porque los datos utilizados sean erróneos, sino porque se hayan procesado de un modo tal que resulte contraproducente o nocivo para la persona a la que se refieren.

Pensemos en un tratamiento realizado sin las debidas medidas de seguridad, facilitando el acceso a la información por cualquier tercero. En este caso, la afectación de los derechos se deriva directamente del tratamiento, y no de la adecuación de la información. Otro escenario posible es el derivado de inferencias algorítmicas que generen un perfilado equivocado, no porque los datos que utilice sean incorrectos, sino porque no se hayan tomado en consideración variables necesarias o porque el algoritmo obedezca a determinados sesgos que expliquen la generación de perfiles que no se compadezcan con la realidad del sujeto afectado[4].

En definitiva, el tratamiento de datos personales es la condición fáctica que activa la aplicación del derecho a la protección de datos. Consecuentemente, conocer sus elementos caracterizadores resulta determinante para comprender la naturaleza del derecho fundamental.

---

[3] En la evolución del concepto destaca la aportación de la Ley alemana de 1977 para la protección del mal uso de los datos personales a través de su tratamiento (*Gesetz zum Schutz von Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz*)). Esta amplía notablemente el alcance del concepto de dato personal, al establecer que «los datos personales son detalles individuales sobre circunstancias personales o fácticas de una persona física específica o identificable (sujeto de datos» (§ 2).Traducción del original: «*sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)»*

[4] Son bien conocidos los sesgos raciales de los perfilados algorítmicos, vid. (Mogensen, 2019); pero este tipo de problemáticas se extienden a todo tipo de realidades y prácticas, incluidas algunas tan comunes como los seguros de vehículos, vid. (Kiviat, 2019).

2. El concepto de dato personal

2.1. Elementos clave

Cualquier aproximación al derecho del art. 8 de la CDFUE exige que los elementos que le dan forma –el dato y su tratamiento– sean comprendidos en su particular contexto normativo. En el caso del dato personal, esto supone acudir al RGPD, cuyo art. 4.1 se contiene la definición más completa del mismo, sin perjuicio de los matices que la jurisprudencia del TJUE ha ido realizando a lo largo de los años.

La conceptualización del dato personal conlleva ineludiblemente la concreción de las condiciones de aplicación del derecho, al ser aquél la materia sobre la que se proyecta. El art. 4.1 del RGPD establece que será dato personal «toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona». La definición del RGPD es heredera directa de las previsiones de la Directiva 95/46/CE (art. 2.a)), con la que comparte dicción literal, con la excepción de los ejemplos ilustrativos que añade el RGPD. Estos, más allá de su valor referencial, en nada afectan a la determinación de qué es un dato personal.

En la definición legal destacan una serie de componentes: información, persona física y la exigencia de que esta esté identificada o sea identificable. Estos elementos basilares serán examinados individualmente en los próximos apartados. No así el enlace «referido a» que, por sus características, ha sido considerado como un factor que permea a los demás, por lo que ha de ser interpretado como condicionante del conjunto[5].

[5] El Dictamen 4/2007, sobre el concepto de datos personales, de 20 de junio de 2007, del GT29, sí incluye un elemento como una variable singular.

2.2. Información

Los datos personales son información[6]. Cualquier tipo de información puede ser considerada, al menos a priori y de manera descontextualizada, dato personal[7]. Será la conexión con un individuo lo que permita atribuirle tal condición. La no inclusión de condicionantes previos[8] posibilita que, al menos potencialmente, todo género de información pueda llegar a ser dato personal, siempre que cumpla con los demás requisitos del art. 4.1 RGPD.

Esa condición, abierta y amplia, podría no haberlo sido tanto si el legislador hubiese establecido tipologías de información en atención, por ejemplo, al formato en que estuviese contenida (v. gr. solo información digitalizada), a su procedencia (v. gr. solo información proporcionada, directa o indirectamente, por la ciudadanía), a quien la trate (solo datos de bases gubernativas), al volumen (solo conjuntos de información, excluyendo datos singulares) o a la tipología (solo informaciones sobre determinadas realidades, por ejemplo, solo datos íntimos).

Sin embargo, al requerir la conexión con una persona, en realidad, se está estableciendo una concreta tipología: la información personal. Ahora bien, para poder apreciar esa condición, es necesario considerar la realidad específica de cada dato y su contexto, por lo que no cabe una exclusión apriorística en sentido estricto. El adjetivo "verde", por sí solo, puede ser, o no, un dato personal. Si aparece referido al color de pelo en el listado de características físicas de alumnos de un instituto, probablemente será un dato personal. Pero, si ese mismo adjetivo, se refiere al color que simboliza a una conocida marca de cervezas, no lo será. Por lo tanto, la condición personal no es inherente a la información, a veces, será la consecuencia del contexto en que esta se utilice.

---

[6] El concepto información es entendido, en esta tesis, como conocimiento sobre una realidad.

[7] Sobre la heterogeneidad de las informaciones susceptibles de ser consideradas dato personal, vid. SSTJUE asuntos acumulados C-465/00, C-138/01 y C-139/01, Rechnungshof c. Osterreichischer Rundfunk, de 20 de mayo de 2003, apdo. 43; asunto C-101/01, asunto Lindqvist, 6 de noviembre de 2003; apdo. 88 y asunto C-553/07, Coliege van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer, de 7 de mayo de 2009, apdo. 59.

[8] La Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) contiene una definición de «datos» en la que los caracteriza como: «toda representación digital de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual» (art. 2.1 de la Propuesta). Al circunscribirlo a las representaciones digitales está condicionando el marco de aplicación posible.

La adopción de un concepto no excluyente de información, su no condicionalidad morfológica, resulta apropiada para la compleja realidad sobre la que se proyecta el derecho del art. 8 de la CDFUE, pues no establece apriorismos que, merced a la evolución técnica, dejen al derecho obsoleto. Los deberes de protección a que obliga el derecho a la protección de datos personales se construyen en torno al vínculo dato-persona. Cualquier condicionante que se pretenda incorporar a la definición debe ser valorado con suma cautela. El establecimiento de restricciones previas a la condición de dato personal puede operar en denuedo del derecho fundamental, al excluir ciertas informaciones de su ámbito de protección.

El vínculo dato-persona no solo posibilita la identificación de los datos personales, sino que, una vez reconocida dicha condición, permite adecuar el nivel de protección, tal como ocurre con las categorías especiales de datos del art. 9 del RGPD. El mayor o menor grado de conexión con el individuo, la naturaleza de la información y lo que revele del sujeto al que se refiere, son variables a considerar a la hora de establecer las condiciones del tratamiento, y las medidas de seguridad a implementar.

2.3. Persona física

La exigencia de conexión entre la información y una persona física conforma la base sobre la que se asienta el elemento subjetivo del derecho. Los datos personales son el centro de imputación del derecho; en ellos se produce la conexión entre el elemento material y el personal. Ese vínculo refrenda la condición de derecho de la personalidad de la protección de datos[9], y permite seleccionar, del conjunto de informaciones existentes, aquellas sobre las que se proyectan las obligaciones y se ejercitan las facultades inherentes al derecho.

Al establecerse de manera taxativa que solo las informaciones referidas a personas físicas serán objeto de protección, se apuesta por una concepción antropocéntrica de su titularidad, excluyendo, por omisión, a

[9] A estos efectos, se considera derechos de la personalidad aquellos destinados a proteger los intereses más personales del individuo. Sobre las características que justifican la condición de derecho de la personalidad, vid. (Encabo Vera, 2012).

las personas jurídicas del ámbito de aplicación del derecho[10]. Esta previsión diferencia a la CDFUE y, en general, a la normativa europea, del CEDH[11]. En relación con este último, el Convenio 108, en su versión modernizada, deja abierta la posibilidad a que los estados, por vía legislativa, extiendan su protección a las personas jurídicas[12].

Es importante incidir en que el elemento condicionante en el modelo europeo es la conexión entre la información y el sujeto al que se refiere. Serán datos de personas físicas aquellos que aporten algún conocimiento sobre ellas. El elemento identificador es el vínculo relacional, y no quien provea la información. Para considerar un dato como personal, resulta indiferente si ha sido obtenido del sujeto al que se refiere o de un tercero[13]. También es irrelevante quién opere con esa información, es decir, aunque las personas jurídicas traten con datos referidos a personas físicas, quienes los gestionen e, incluso, quienes hagan negocio con ellos; esos datos no son de la persona jurídica, sino de la persona física a la que conciernen.

Al acotar la protección a los datos relativos a personas físicas, todas aquellas informaciones que no gocen de tal condición pasarán a integrar una categoría creada por exclusión: los datos no personales. En ese grupo de informaciones, además de los datos referidos a personas jurídicas, se integrarían «los conjuntos de datos agregados y anonimizados utilizados para análisis de datos a gran escala, los datos sobre agricultura de precisión que pueden ayudar a controlar y optimizar la utilización de plaguicidas y

[10] La exclusión de las personas jurídicas, con excepción de la Ley del Land de Hesse de 1970, ha sido una constante en la regulación de las normativas de protección frente al tratamiento de la información personal.

[11] Así, en el asunto Liberty y Otros c. Reino Unido, el TEDH consideró que la ausencia de un procedimiento de examen, intercambio, conservación y destrucción de la información interceptada, que fuese accesible al público, suponía una vulneración del art. 8 del Convenio. Reconociendo, consecuentemente, que las organizaciones demandantes eran titulares de derechos protegidos por el art. 8 del CEDH. Vid. STEDH Liberty y Otros c. Reino Unido, de 10 de junio de 2008.

[12] Vid. Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apdo. 30: «*While the Convention concerns data processing relating to individuals, the Parties may extend the protection in their domestic law to data relating to legal persons in order to protect their legitimate interests*». Puede consultarse en: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a. (Última consulta: 20/10/2021).

[13] Prueba de ello son los deberes de información establecidos en el art. 14 del RGPD en aquellos casos en que «los datos personales no se hayan obtenido del interesado». Como puede constatarse, no se niega la condición de dato personal, cuestión diferente serán los derechos que pueda ejercitar, pero estos no derivarán de la condición de dato, sino de los intereses en conflicto en el tratamiento concreto.

de agua, o los datos sobre las necesidades de mantenimiento de máquinas industriales»[14].

Para disciplinar el tratamiento de toda la amalgama de datos no personales, la Unión Europea aprobó, como hemos visto, el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (Reglamento Datos No Personales). La finalidad primordial de esta norma es «garantizar la libre circulación en la Unión» de este tipo de información. Para ello, establece una serie de requisitos en cuanto a la localización de estos datos, disponibilidad por las autoridades competentes o la portabilidad entre profesionales (art. 1 RDNP).

Estrechamente vinculados a la conceptualización de los datos como información sobre una persona física surge una serie de desafíos jurídicos de difícil solución: la protección de datos como derecho colectivo, la propiedad de los datos y la salvaguarda de los datos de personas fallecidas.

2.3.1. La "individualidad" de los datos

Pese a la exigencia de conexión dato-individuo, esa obligada ligazón no es excluyente. El art. 4.1 del RGPD establece que será considerada dato personal «toda información sobre una persona física». Este requisito sirve, de una parte, para identificar al conjunto de datos sobre los que se aplicarán las previsiones normativas del sistema de protección y, de otra, permite identificar al titular del derecho. Sin embargo, nunca puede servir como coartada para desnaturalizar el contenido objetivo de la información.

Los datos, al igual que la realidad, son complejos y no siempre unívocos. Desde el punto de vista de la titularidad de la información, un mismo dato puede estar referido a más de una persona física («interesado», en la denominación española del RGPD[15]). En la práctica, esto implica que,

[14] Considerando 9 RDNP. Dicho Considerando apunta al Internet de las cosas, a la inteligencia artificial y al *machine learning* como principales generadores de datos no personales en la era digital.

[15] «*Data subject*» en la versión en inglés, esto es sujeto de los datos o incluso afectado habrían sido denominaciones más adecuadas para referirse a las personas cuyos datos son objeto de tratamiento. Interesado resulta demasiado genérico en un contexto en el que, precisamente, la concurrencia de intereses diversos es la tónica dominante.

sobre una misma información, pueden concurrir diferentes titulares[16], con intereses no necesariamente coincidentes. La interrelación entre sujetos forma parte de la vida en sociedad (v. gr. direcciones postales compartidas con convivientes, mismo lugar o puesto de trabajo o la condición de usuario de una determinada plataforma). Además, existen ámbitos específicos en los que la convergencia de interesados es consustancial al dato (v. gr. los datos genéticos de parientes biológicos[17]).

Debido a esa convergencia de intereses, se ha planteado la posibilidad del ejercicio colectivo del derecho. Esta opción se ha propuesto para ámbitos muy variados. En unos, el vínculo entre los integrantes es evidente, como pueden ser los grupos genéticos[18] o la salvaguarda de los intereses de los pueblos indígenas[19]. En otros, la interrelación entre los sujetos es más difusa, aunque la unidad de acción derivaría de la suma de voluntades en la consecución de una finalidad común. Ejemplo de ello, serían las propuestas que buscan compensar la capacidad condicionante y la posición de dominio de las entidades que tienen, en el tratamiento de datos, la base de su negocio[20], o las que tratan de garantizar y proteger el valor de la información obrante en los sistemas nacionales de salud. En este último caso, esa información se presentaría como el producto resultante de los datos generados por la ciudadanía y del trabajo de los profesionales de la salud (Ballantyne, 2020).

No obstante, desde el punto de vista de la garantía del derecho, esa colectivización de los datos no resulta jurídicamente apropiada. La condición de dato personal concede, a la persona a la que esté referida, una serie de prerrogativas sobre esa información, cuyo fundamento es el

---

16 Así lo ha refrendado el TJUE al señalar que «unos mismos datos pueden concernir a varias personas físicas y, por lo tanto, ser datos personales de cada una de estas», STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017, apdo. 45.

17 Compartimos el 12,5% de nuestro ADN con nuestros primos, la proporción con padres, hermanos o hijos es sustancialmente mayor (Bioinformatics, s. f.).

18 Hallinan y de Hert realizan una propuesta de los mecanismos que se podrían implementar en la defensa de los intereses legítimos de los grupos genéticos, vid. (Hallinan y de Hert, 2017). Kuru plantea los problemas que de implementación de una protección grupal de los datos genéticos en el actual RGPD, si bien plantea ciertos mecanismos con los que los individuos podrían verse resarcidos frente a eventuales lesiones en sus derechos, vid. (Kuru, 2021).

19 La protección de la *indigenous data sovereignty* se plantea como un mecanismo de defensa frente a los riesgos de discriminación y aprovechamiento que pudiera derivarse de la utilización de este tipo de informaciones (Network, s. f.; Sulston, 2002).

20 En este sentido, destaca el § 3º del art. 42 de la Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados Pessoais de Brasil, en la que se establece una previsión específica de reparación de daños colectivos derivados del tratamiento de datos.

vínculo dato-persona. La visión colectiva del dato condiciona el ejercicio individual del derecho, y supone negar que, respecto del destino y usos de una misma información, pueda haber intereses individuales contrapuestos.

Parece evidente que estamos ante problemas diferentes con un sustrato común: el uso de información personal. Consecuentemente, deben distinguirse las acciones destinadas a la protección de colectivos, de intereses generales[21] o de bases de información especialmente valiosas (como pueden ser los archivos de salud), de la titularidad del derecho a la protección de datos.

El art. 8 de la CDFUE reconoce un derecho individual. El ejercicio colectivo del mismo podrá realizarse mediante la suma de voluntades particulares que libremente concurran en una misma dirección. Pero negar la individualidad del derecho equivaldría a desvirtuar la manifestación de la personalidad que cada dato personal encierra.

2.3.2. Sobre la "propiedad" de los datos

Estrechamente relacionado con lo anterior, está la consideración de los datos como una forma de propiedad[22]. Para la resolución de esta cuestión ciclotímica[23], resulta crucial el modo en que se establezca el nexo de unión persona-dato.

Como se ha señalado, para que una determinada información sea considerada dato personal basta con que esté referida a una persona física. El derecho a que esos datos sean protegidos (art. 8 CDFUE) se funda en el vínculo personal, y proporciona al afectado una serie de facultades de

[21] Como podría ser velar por la limpieza de los procesos electorales en aras de evitar injerencias derivadas del uso de información personal, es decir, para evitar casos como el de Cambridge Analytica. Sobre las posibilidades de actuación de los estados frente a los riesgos de afectación de los procesos electorales, vid. el minucioso estudio de Sánchez Muñoz sobre la regulación de las campañas electorales en la era digital (Sánchez Muñoz, 2020).

[22] En los últimos años, sin embargo, más que como un mecanismo de protección, la propiedad de los datos se ha planteado como un mecanismo, complementario a los derechos de protección, destinado a posibilitar la obtención de cierta remuneración por el uso de la información, sin que ello suponga una «*full alienation of all control power over the data*» (Purtova, 2011, p. 280).

[23] El derecho de propiedad como mecanismo de protección de la ciudadanía frente al tratamiento de los datos ha venido debatiéndose, en la doctrina estadounidense, desde los años 70 (Purtova, 2009). En realidad, la inadecuación del derecho de propiedad para ofrecer protección a las intromisiones en la vida privada ya está presente en el artículo de Warren y Brandeis (Warren y Brandeis, 1890).

actuación destinadas a asegurar el poder de control y disposición sobre esa información a uno referida (derecho a la protección de datos, entendido como autodeterminación informativa).

Sin embargo, su posición jurídica respecto del destino de los datos puede ceder o verse condicionada por factores como la fuerza del vínculo con la información, el grado en que le afecte y le exponga, los efectos que su tratamiento pueda tener, o la posición jurídica de otros interesados, o de terceros que precisen de esos datos para la consecución de sus propios objetivos[24].

Expresiones como "mis datos", u otras equivalentes, inducen a error. Llevan a considerar que esa información es patrimonio exclusivo de una persona, que tiene un dominio absoluto sobre el dato concreto. No es cierto. Mis datos no son míos, solo están referidos a mí y reflejan una parte de mi identidad[25]. La posición de los interesados respecto de los datos personales no se compadece bien con el uso adjetivos y pronombres posesivos. La relación con los datos personales es la de un sujeto que, merced a la conexión que existe entre la información y algún aspecto de su vida, tiene determinadas expectativas jurídicas, cuya materialización vendrá condicionada por las de terceros (ya sean otros interesados, el legislador o sujetos que pretendan utilizar esos datos para fines propios)[26].

Si el derecho de propiedad no se compagina bien con la protección de los datos personales[27], la idea de enajenar la información, teniendo en cuenta que dicha venta no podría ir acompañada de una renuncia al

[24] Son muchos los autores que consideran que el la propiedad no el derecho de propiedad no es adecuado para afrontar la protección de ese particular objeto que es la información (Samuelson, 2000); (Litman, 2000) o (Solove, 2002). Una posición intermedia, en la que se apuntan ventajas e inconvenientes de la concepción de los datos como un objeto susceptible de propiedad sería (Prins, 2006). Curiosamente, por razones que nada tienen que ver con su idoneidad para ofrecer protección, Posner llega a una conclusión similar. Para él, no deben extenderse los derechos de propiedad a la información personal, pues esto generaría distorsiones en los datos que se utilizan en el mercado (Posner, 1977).

[25] Como apunta Adsuara Varela, «la "identidad" no es "lo que tú eres" […], sino "lo que sirve para que los demás te identifiquemos"» (Adsuara Varela, 2018, p. 167).

[26] Si, a lo largo de la tesis, se utiliza en alguna ocasión el posesivo en relación con los datos, debe entenderse en el sentido de estar referidos y no como una concepción patrimonial y de dominio absoluto sobre la información.

[27] Incluso aquellas propuestas pensadas para compaginar ambos derechos como puede ser la de Bergelson (Bergelson, 2003) tienen ciertos problemas, pues terminan configurando un derecho de propiedad que, en última instancia, establece principios, condiciones de ejercicio y facultades equiparables al modelo europeo de protección de datos. Es decir, la idea de propiedad se utiliza solo como mecanismo de conexión y activación de las facultades de actuación, cumple la función que, en el modelo europeo, desempeña que los datos sean objeto de tratamiento

ejercicio de las facultades que el derecho a la protección de datos confiere, resulta difícilmente practicable[28]. A lo sumo, resultaría posible plantear ciertos derechos de propiedad con relación a los ficheros de datos, es decir, no a la información en sí, sino a los elementos que la contienen (Tjong Tjin Tai, 2018).

No se está negando, con lo aquí expuesto, el valor económico de los datos personales[29]. Al contrario, si hay un factor que ha hecho evolucionar los sistemas de protección ha sido, precisamente, la importancia de estos en el mercado. Lo único que se pretende negar es la adecuación del derecho de propiedad como modelo mediante el que disciplinar la relación dato-persona. Consecuentemente, tampoco resulta operativo como fundamento las posibilidades de actuación del interesado respecto de aquellas informaciones que le afectan[30].

Como ha puesto de manifiesto con meridiana claridad la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales, «los datos personales no pueden considerarse una mercancía» (Considerando 24). Sin que por ello deba desconocerse su valor en el mercado, o la función de contraprestación que desempeñan[31]. Con toda probabilidad, será necesario desarrollar, más pronto que tarde, «un marco regulatorio patrimonial […] con normas armonizadas, y […] más allá de las fronteras de la Unión Europea» (Plana Arnaldos, 2020, p. 615).

Sin embargo, cualquiera que sea la regulación acerca del rédito económico de los datos personales, o la obtención de servicios derivados del uso de la información a uno referida, ésta no puede hacerse a costa de convertir en tácitamente renunciable un derecho que, por su propia naturaleza, no lo es. Las medidas que se establezcan deberán ser compatibles con el ejercicio del haz de facultades que el derecho a la protección de datos confiere (incluidas la revocación del consentimiento,

[28] Si bien es cierto que, una concepción del cuerpo humano y los derechos como alienables podría abrir la puerta a un cierto aprovechamiento económico de los datos (Rao, 2000).

[29] Para un estudio de cuál es el valor que los datos tienen para las personas a las que se refieren y por cuanto estarían dispuestos a "vender" determinada información, vid. (Benndorf y Normann, 2018).

[30] En la misma línea, (Adsuara Varela, 2018, p. 167).

[31] La propia Directiva (UE) 2019/770 asume que los datos personales operan como moneda de cambio, al señalar que, «a menudo, los contenidos o servicios digitales se suministran también cuando el consumidor no paga un precio, pero facilita datos personales al empresario».

el derecho de supresión o la minimización de los datos), por lo que, el abanico de opciones, queda sumamente reducido y condicionado.

2.3.3. Los datos de las personas fallecidas

La última de las cuestiones relacionada con la condición de persona física de los titulares del derecho fundamental reconocido en el art. 8 de la CDFUE, radica en determinar si ampara a las personas fallecidas o, por el contrario, se circunscribe a las personas vivas.

El RGPD excluye, de su ámbito de aplicación, a las personas fallecidas (Considerando 27 RGPD)[32]. No obstante, no niega su condición de posibles titulares del derecho –como si ocurre con las personas jurídicas–, dejando abierta la puerta a una posible extensión del derecho a aquellas. La concreción de dicha ampliación queda a expensas de los Estados miembros. Estos, podrán establecer normas específicas destinadas a disciplinar los datos personales de quienes hayan fenecido[33].

Las previsiones destinadas a regular el tratamiento de los datos personales de las personas fallecidas tendrían como objetivo gestionar su «huella digital» (Cerrillo i Martínez, 2021, pp. 529-550) y salvaguardar los intereses de estas frente a los efectos derivados de las aspiraciones, cuando no derechos, que otros sujetos pudieran tener sobre esa información. No obstante, la articulación de los mecanismos de protección de las personas que hubiesen espirado choca con la realidad del tratamiento de datos, en la medida en que el ejercicio activo de las facultades de actuación inherentes al derecho de protección resulta materialmente inviable para la persona fallecida.

Ante este escenario, la única posibilidad de las personas para "ejercitar" sus derechos pasaría por realizar una declaración de voluntad anticipada, esto es, un testamento sobre el destino de los datos[34].

[32] Así lo ha ratificado el TJUE en la STJUE ausnto C-398/15, Manni, de 9 de marzo de 2017.
[33] España o Portugal han regulado, con diferente grado de amplitud, el tratamiento de datos de las personas fallecidas. En el primer caso ha establecido una regulación que abarca todas las tipologías de datos personales (arts. 3 y 96 de la LOPDGDD). Por su parte, la Ley portuguesa otorga cierta protección a los datos especiales de las personas fallecidas (art. 17 Lei nº 58/2019, de 8 de agosto de 2019).
[34] Se utilizado la fórmula "testamento de sobre el destino de los datos" en lugar de la habitual "testamento digital" por resultar más representativa de la realidad regulada (ni el testamento tiene que tener formato digital ni está constreñido a los datos en ese formato, pues también hay datos personales gestionados en papel). La LOPDGDD española ha regulado

Adicionalmente, podrían preverse instrumentos de protección de los intereses de la persona fallecida por parte de familiares, tutores u otros sujetos legitimados (como podrían ser los representantes legales que hubiera tenido el fallecido o, incluso, el ministerio fiscal). En cualquier caso, este tipo de medidas deberá implementarse con mucha cautela y estableciendo mecanismos destinados a asegurar que, en efecto, las actuaciones se ejercitan para la protección de la persona fallecida y sus intereses, y no con otro tipo de motivaciones[35].

Adicionalmente, ha de tenerse presente que las informaciones de la persona fallecida pueden ser, también, datos de otros sujetos[36]. Asimismo, puede ocurrir que los intereses de quienes viven fuesen opuestos a los de la persona que ya no está. Ante supuestos de este cariz, al igual que ocurre con los conflictos entre interesados vivos, habrá de estarse a las circunstancias del caso, y a la afectación de derechos que se produzca. Si bien es cierto que, en general, será la voluntad de los vivos la que prevalezca, pues cualesquiera que fuesen los efectos derivados del tratamiento de la información, lo más probable es que tuviesen un impacto mayor en los bienes jurídicos de quien está en condición de sufrirlos vivamente[37]. De cualquier modo, solo cabe la determinación *ad casum*.

2.4. Identificada o identificable

Dato personal es cualquier información referida a una persona física. Ahora bien, el elemento determinante, el que posibilita conectar a la

expresamente el tratamiento de datos de las personas fallecidas, (arts. 3 y 96). Sobre las características de esta regulación, vid. (Durán Rivacoba, 2020) y (Rebollo Delgado y Zapatero Martín, 2019, pp. 183-204). Para un comentario más crítico, vid. (Ginebra Molins, 2021).

[35] En el caso de la regulación española sobre la materia, se habilita ciertas personas vinculadas al fallecido a ejercitar los derechos de acceso, rectificación y supresión. Esto es, solo medidas tendentes a evitar afectaciones al fallecido mediante la corrección o eliminación de los datos y, consecuentemente, del factor de riesgo que pudiera representar su tratamiento para la honra y reputación de la persona fallecida.

[36] Tal como apunta el GT29, en su Dictamen sobre Datos Genéticos, de 17 de marzo de 2004, p. 8: «*the information on dead individuals may also refer to living persons.* […] *Thus, where the information which is data on the dead can be considered to relate at the same time also to the living*», puede consultarse en:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf. (Última consulta: 20/10/2021).

[37] Un ejemplo de conflicto entre intereses de persona viva y fallecida sería el caso de un sujeto que deja explícitamente previsto en testamento que quiere vedar que se trate su información genética y el interés que puedan tener terceros en conocerla, por ejemplo para determinar la paternidad.

persona física con el sujeto –o sujetos– que podrán ejercitar el derecho, es la exigencia de que esa persona esté identificada o sea identificable mediante la información utilizada. Por tanto, para que pueda ser considerado dato personal es imprescindible que ese dato, o conjunto de datos, pueda conectarse con una persona concreta. El vínculo identificativo es el que genera los derechos del individuo. Hasta que no se produzca la identificación, o se confirme la posibilidad de realizarla, no se considerará dato personal y, consecuentemente, la persona no podrá hacer valer sus prerrogativas. Esta característica viene a reforzar la condición individual del derecho, pues incide en la necesaria conexión dato-individuo.

Aunque la premisa pueda parecer clara: será un dato personal aquella información que esté referida a una persona y la identifique o, al menos, posibilite su singularización (Considerando 26 RGPD), en la práctica, la variable «identificable» supone ampliar el abanico de informaciones posibles de manera notable, haciendo imprescindible conocer sus límites.

2.4.1. Los dos extremos: identificado y anónimo (o dato no personal)

Si para considerar que una información es un dato personal es necesario poder conectarla con una persona, la capacidad para establecer esa conexión, así como las condiciones en las que se considera que dicha actuación es posible, pasan a ser el nudo gordiano del concepto. El RGPD, en el Considerando 26, proporciona ciertas claves que contribuyen a definir una información como dato de una persona identificable. Tomando esas previsiones como referencia, resulta posible establecer los márgenes que lo delimitan. Su base más sólida estaría constituida por las informaciones que identifican a una persona identificada y, a partir de ese suelo, se podrían incorporar otras informaciones menos sólidas hasta el límite a partir del que deben ser consideradas como datos anónimos.

En el caso de los datos referidos a una persona identificada, no hay duda de que son datos personales. En ellos la identificabilidad no es un presupuesto o una condición, sino algo inherente al tipo de dato, ya que,

por sí mismo, designa a la persona. No sería información sobre una persona identificable porque ya estaría identificada. Ejemplo de datos que encajan en esta definición serían los nombres y apellidos, especialmente si van acompañados de una fotografía de la persona. La conexión dato-persona es directa y nítida.

En el polo opuesto se encontrarían los datos no personales. Entre ellos, debe distinguirse entre datos anónimos y los que son no personales porque «*it never [be] realated to an identified or identifiable natural person*» (Finck y Pallas, 2020, p. 13), por ejemplo, las informaciones referidas al uso de abonos sintéticos por la industria agroalimentaria. Los datos anónimos, entendidos como las informaciones que resulta imposible conectar con un sujeto determinado (Considerando 26 RGPD), son los que resultan de interés a efectos de delimitar el concepto de dato personal. En ellos, existió una conexión originaria entre dato y persona, pero concurren razones que imposibilitan descifrar y establecer ese nexo.

Conforme al RGPD, los datos anónimos no son datos personales. Ahora bien, ¿cuándo una determinada información merece esa consideración? Lo fácil sería responder siempre que la identificación no sea viable, esto es, cuando resulte imposible establecer la conexión entre dato y persona. Esta circunstancia puede darse, en esencia, por dos motivos: porque el tiempo, los costes y los medios disponibles conviertan a la identificación en improbable o, bien, porque se haya procedido a la anonimización de la información.

La primera de las circunstancias en las que se considera que no es posible la identificabilidad se funda en criterios de razonabilidad. Por este motivo, el tiempo, los costes y los medios disponibles han de analizarse en función del contexto y la realidad del tratamiento (Considerando 26). El RGPD no exige que sea imposible realizar la conexión dato-persona. Para considerar que no se está ante datos personales basta con que no exista una «probabilidad razonable» de lograr ese cometido. La razonabilidad objetiva de los esfuerzos necesarios para vincular ambos elementos se convierte, así, en la unidad de medida.

Por ello, se comprende que, esta previsión está pensada desde la lógica de quienes operan con los datos, sobre todo la de los responsables, a quienes se está indicando que, si se dan ciertos factores que permitan estimar que la información está suficientemente protegida, no se les va a exigir implementar las medidas que prevé la normativa de protección de

datos[38]. No obstante, esa valoración de la razonabilidad no dependerá de las circunstancias específicas del responsable, sino de la realidad del momento, lo que significa que las condiciones de identificabilidad no se evalúan para el responsable en particular, sino en atención a las posibilidades reales de éxito del proceso[39]. Del mismo modo que, para considerar a un dato como personal, «la mera e hipotética posibilidad de singularizar a un individuo no es suficiente» (Gil González, 2016, p.48), tampoco la imposibilidad puede ser un a priori, sino que se han de constatar las posibilidades efectivas de identificación, sea para negarlas o para reafirmarlas.

Como se apuntó en el Capítulo II, el origen de las normativas de protección de datos está íntimamente ligado a la capacidad del tratamiento automatizado para quebrar las defensas que, el tiempo y el esfuerzo, venían ofreciendo a los intereses de la ciudadanía en relación con el tratamiento de su información. La normativa europea, en última instancia, se limita a refrendar que, allí donde esas salvaguardas "naturales" se mantengan, no hay necesidad de establecer otras medidas adicionales de protección.

Si, pese a todo, mediante esfuerzos desproporcionados, no previsibles y nada razonables, se lograse conectar una información con la persona a la que está referida, automáticamente, esos datos, hasta ese momento no personales, pasarían a ser considerados datos personales, debiendo aplicárseles la normativa de protección de datos.

Ocurre, sin embargo, que las barreras "naturales" pueden verse derribadas por el paso del tiempo y la evolución de la tecnología, de modo que aquello que ayer resultaba imposible realizar –o era altamente improbable– mañana podría lograrse en segundos o minutos, sin más

[38] En la actualidad, existen sistemas de cifrado que se consideran inquebrantables, pues «el tiempo requerido para lograrlo con la potencia de cálculo actualmente disponible ([…] cientos o miles de años) lo convierte en una misión inmanejable» (Merino, 2019), tal sería el caso de los cifrados RSA de 2048 bits. La computación cuántica será un auténtico de desafío, pues Gidney y Ekerå apuntan que un ordenador cuántico podría llegar a romper un sistema así en unas 8 horas (Gidney y Ekerå, 2019).

[39] Así lo acredita la resolución del TJUE en la sentencia del asunto C-582/14, Patrick Breyer contra Bundesrepublik Deutschland, de 19 de octubre de 2016. En este asunto se indicó que las IP dinámicas (cambian en cada conexión) eran datos personales, pues resultaba posible llegar a conocer a los usuarios al poner en conjunción el momento y web visitado por esa IP con las informaciones que podían proporcionar los proveedores de acceso a Internet. Para un análisis detallado de la sentencia y los efectos de Breyer, vid. (Zuiderveen Borgesius, 2017).

esfuerzo que unos golpes de tecla o un simple clic. Son, por lo tanto, barreras con un componente temporal inherente a su condición.

A esa connotación, por así decir, natural, de dato no personal que tienen algunas informaciones por la dificultad de conexión con el individuo, ha de añadirse la posibilidad de crear, "artificialmente", datos anónimos mediante técnicas de anonimización. Esto es, mediante la despersonalización de la información y la quiebra de cualquier posibilidad de reconexión.

La anonimización supone convertir a los datos «en anónimos, de forma que el interesado no sea identificable o deje de serlo» (Considerando 26 RGPD), mediante el uso de ciertas técnicas que impidan la conexión dato-persona. La anonimización es un proceso y, como tal, deberá ejecutarse en atención a las propias características de los datos y los tratamientos. Lograr la anonimidad en la era digital es una tarea mucho más compleja que en épocas pretéritas, como Nissenbaum ha puesto de manifiesto, «*namelessness by itself is no longer suficient for protecting what is at stake in anonymity* […] *When we think of protecting anonymity we must think* […] *not only of how a person can prevent his or her name from being divulged, but how a person can prevent all the crucial bits of information from being divulged, especially the bits of information that when divulged would enable access to him or her*» (Nissenbaum, 1999, pp. 142-143). El anonimato en la era digital implicaría tener la garantía de ser «*unreachable*»[40].

Entre los métodos que asegurarían una mayor certeza de anonimización se encuentran la «*Anonymisation by randomization*» y la «*Anonymisation by generalization*»[41]. Estas serían, conforme al criterio del GT29[42], las técnicas que ofrecerían un mayor éxito en la consecución de un marco de actuación en el que el tiempo y esfuerzo necesario para la

[40] Se ha utilizado la expresión de Nissenbaum por trasladar adecuadamente la idea de no ser aprehensible ni alcanzable (Nissenbaum, 1999).
[41] GT29, Opinion 05/2014 on Anonymisation Techniques, de 10 de abril de 2014, pp. 27 a 37. Puede consultarse en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. (Última consulta: 20/10/2021).
[42] El Grupo de Trabajo del Artículo 29, (GT29) «es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD)» (Comité Europeo de Protección de Datos, s. f.). En la actualidad, sus funciones han sido absorbidas por el *European Data Protection Board* (Comité Europeo de Protección de Datos) (EDPB).

reidentificación permitirían considerar que esa información no es un dato personal.

Hay ciertas prácticas "anonimizadoras", como la utilización de algoritmos de Hash (salvo que se combinase con mecanismos criptográficos), de algoritmos de cifrado, capas de anonimización, la perturbación de los datos o la reducción de los datos[43], que garantizan altos niveles de seguridad y confidencialidad –¿acaso suficientes para hacer del tiempo y costes necesarios una barrera insalvable?–, pero en cuanto a su efectividad en la consecución de esa desvinculación entre dato y persona, hay mayores dudas[44].

	Is Singling out still a risk?	**Is Linkability still a risk?**	**Is Inference still a risk?**
Pseudonymisation	Yes	Yes	Yes
Noise addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenization	Yes	Yes	May not

Figura 2. Fuente: Dictamen GT29 sobre técnicas de anonimización[45]

Como puede constatarse en la Figura 2, ninguna de esas técnicas ofrece una garantía plena de protección frente a los riesgos derivados de las inferencias, poniendo de manifiesto el potencial de injerencia que este método tiene y la dificultad de combatirlo mediante mecanismos de disolución de la conexión dato-persona. Por lo tanto, aun cuando estas técnicas logren altos niveles de seguridad, confiriendo una dificultad mayor que, acaso, asegure, por la vía de los tiempos y costes, que no se produzca la conexión directa dato-persona, sin embargo, lo cierto es que, el riesgo de afectación de la esfera personal del individuo continúa. Las técnicas de la figura 2 no son, por consiguiente, mecanismos de anonimización.

[43] Para una explicación más detallada de estas técnicas, y alguna otra, puede consultarse la detallada guía elaborada por la AEPD, "Orientaciones y garantías en los procedimientos de anonimización de datos personales", especialmente las páginas 14 a 18.
Puede consultarse en: https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf. (Última consulta: 20/10/2021).
[44] GT29, Opinion 05/2014 on Anonymisation Techniques, de 10 de abril de 2014, pp. 23 y 24.
[45] Ibídem, p. 24.

La anonimización es, sobre todo, un «*process of reducing the risk of information disclosure executed through the utilization of various anonymization methods on the original data set*» (Wanvik Stenersen, 2020, p. 13). Esto supone llevar la información personal a un estado en el que el riesgo de conexión con una persona concreta tendería a cero. Como ha advertido el GT29, «*the "art of anonymisation"* […] *is a new scientific branch which is still in its infancy and many practices exist to degrade the power of identification of data sets; however, it has to be clearly stated that the majority of such practices do not prevent linking the processed data with data subjects*»[46].

Al igual que con las barreras naturales, los datos anonimizados de hoy podrían no serlo mañana[47], pues podría descubriese alguna técnica que posibilitase la reversión de la anonimización y/o a la reducción de los costes y esfuerzos necesarios para establecer la conexión dato-persona[48]. Consecuentemente, aun cuando se estén tratando datos considerados no personales, deberá mantenerse una cierta vigilancia respecto de estas informaciones. El paso del tiempo y el desarrollo técnico podría terminar por convertirlas en identificables[49] y, consecuentemente, en informaciones sometidas al derecho y a la normativa de protección de datos personales.

2.4.2. Problemas en torno a la anonimidad de la información

En un futuro hipotético, pero perfectamente posible, pudiera ocurrir que la fácil reidentificación de los datos (Ohm, 2010, pp. 1716-1731) haga del anonimato absoluto (entendido como la irreversibilidad e imposibilidad de conectar la información con la persona) un imposible o, a lo sumo, un producto con una caducidad previsible, aunque no determinada. Por más que se procediese a la anonimización, el *big data*, las

[46] Ibídem, p. 27.
[47] AEPD, 10 malentendidos relacionados con la anonimización, 2021, p. 4. Puede consultarse en: https://www.aepd.es/es/documento/10-malentendidos-anonimizacion.pdf. (Última consulta: 20/10/2021).
[48] No solo se trabaja en técnicas de reidentificación (Slavin, 2021), también en nuevos modos y formas de anonimizar. Es una carrera tecnológica, (Girka, Terziyan, Gavriushenko, y Gontarenko, 2021).
[49] Ejemplo de ello sería el caso de la reidentificación de radiografías anonimizadas, mediante procesos de inferencia y correlación. Así lo han puesto de manifiesto los investigadores de la Universidad de Erlangen-Nurnberg (Wiggers, 2021). Como puede comprobarse, el riesgo de reidentificación abarca todo tipo de datos, también los considerados especiales, con lo que se trata de una realidad que no debe eludirse.

inferencias o el uso de otros ingenios tecnológicos terminarían posibilitando una identificación absoluta o, al menos, una singularización capaz de vincular la información con un sujeto determinado[50]. Vista de ese modo, la anonimización de los datos sería una especie de promesa incumplida (Ohm, 2010), por generar una idea de ausencia total de riesgo para los derechos derivada del uso de la información, que no se compadecería con la realidad.

En línea con lo anterior, han surgido voces que plantean la ineficacia de la distinción entre datos identificables y anónimos (Tene y Polonetsky, 2013)[51]. En consonancia con esta postura, se han realizado diversas propuestas que, con matices, tienen un hilo conector común: la asunción de la re-identificación como una posibilidad real y la apuesta por un marco normativo en que se prescinda de la categoría de los datos anonimizados y se apueste por enfoques basados en el nivel de riesgo de la identificación[52]. En una posición intermedia se encontrarían aquellas propuestas en las que se concilia el mantenimiento de la categorías datos anonimizados, valorando el nivel de seguridad y protección que ofrecen, pero sin negar su carácter fluido y contingente (Stalla-Bourdillon y Knight, 2016).

En última instancia, la condición de dato personal implica la aplicación de la normativa de protección de datos, con todas sus obligaciones y exigencias. La decisión de excluir a los datos anonimizados, así como la de aquellos que por tiempo, costes o esfuerzos no resulta posible conectarlos –en condiciones razonables– con una persona concreta, encierra una enseñanza fundamental acerca de la naturaleza del derecho a la protección de datos: el riesgo es su razón de ser.

Por el momento –y nada impide que esto pueda ser modificado en el futuro–, el sistema europeo ha apostado por la identificabilidad como elemento detonante de la condición de dato personal. Asimismo, ha considerado que las técnicas de anonimización ofrecen un nivel de

[50] Como Sweeney ya puso de manifiesto en el año 2000, resulta posible reidentificar información anonimizada al combinarla con datos personales (Sweeney, 2000). A lo largo de los años, se ha sucedido las demostraciones empíricas de la capacidad de reidentificación de datos anonimizados a partir de datos personales. Así, a partir de las bases de datos de los taxistas de Nueva York se logró determinar si determinadas *celebrities* habían dejado propina o dónde vivían, pese a no haber registro de pasajeros (Trotter, 2014). En 2014, se logró conocer el 90% de las transacciones con tarjeta de crédito llevadas a cabo por una persona durante 3 meses, solo a partir del conocimiento de su ubicación en determinados momentos (Bohannon, 2015).

[51] En sentido contrario (Cavoukian y Castro, 2014).

[52] En esta línea de actuación se incardinarían las propuestas de (Ohm, 2010); (P. M. Schwartz y Solove, 2011).

desconexión entre información y persona que tiene la suficiente entidad como para hacer de esas informaciones datos no personales y, consecuentemente, excluirlas de las obligaciones y de la protección que ofrece el sistema legal que garantiza el buen uso de los datos personales.

2.4.3. La identificabilidad

Entre los datos identificados (datos personales) y los datos anónimos (no personales) se encontraría un amplio conjunto de informaciones que se consideran datos personales por su identificabilidad; es decir, son datos que conectan una información con un sujeto determinado.

Desde esa perspectiva, la dificultad para vincular un dato con una persona es una cuestión de matiz y de contexto. Aspectos como los datos de que se disponga, si están seudonimizados[53], su calidad[54], el tratamiento que se realice o las finalidades que se persigan, serán factores que hagan más o menos fácil la identificación, pero que, en ningún caso, cuestionan la condición personal de la información.

Por este motivo, no se exige que deba haber una conexión directa entre dato y persona, ni «que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona»[55]. Tampoco es necesario que se materialice la identificación[56], pues bastará con constatar que la misma es posible. Resulta imprescindible explorar la realidad técnica existente y barajar las distintas posibilidades que ofrece la combinación de la información. Si es posible, en conjunción con otros datos,

---

[53] Esto es, los datos «que cabría atribuir a una persona física mediante la utilización de información adicional» (Considerando 26). El RGPD apuesta por la seudonimización como mecanismo de reducción de riesgos (Considerandos 28-29). Sobre la seudonimización, su utilidad, y los criterios para distinguirla de la anonimización, además de la Opinion 05/2014 on Anonymisation Techniques del GT29, vid. (Gazizov, Gazizov, y Gazizova, 2020, pp. 1-3); (R. Miralles López, 2017) y (Nieto Manibardo, 2019).

[54] Especialmente significativa es la importancia de operar con datos adecuados, pertinentes y auditables en el ámbito del *big data* (Cai y Zhu, 2015).

[55] STJUE asunto C-582/14, Patrick Breyer contra Bundesrepublik Deutschland, de 19 de octubre de 2016, apdo. 43.

[56] El art. 11.1 del RGPD es una buena muestra de ello, al señalar que, «si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento».

identificar a la persona, estaremos ante un dato personal[57] y se aplicarán las previsiones de la normativa de protección de datos.

El grado de dificultad para relacionar un dato con una persona tiene destacadas consecuencias en el diseño del tratamiento. A mayor dificultad para la identificación, menor riesgo para los interesados y, por consiguiente, menores exigencias a la hora de proceder con el tratamiento. Esta dificultad para establecer la correlación entre dato y persona opera como un mecanismo de defensa de los bienes jurídicos del interesado y reduce, considerablemente, los efectos que pudieran derivarse de la materialización de ciertos peligros inherentes al tratamiento de datos (v. gr. las brechas de seguridad).

2.5. ¿Una ampliación del concepto?

2.5.1. El contenido, la finalidad y los efectos como variables identificativas

La conexión entre dato y persona es el elemento esencial que determina la condición de dato personal. Si bien los extremos están claros, en el conjunto de informaciones que serían susceptibles de ser consideradas identificables, existen algunas en las que resulta dudosa la existencia de una conexión suficiente con la persona como para considerar que es identificable o singularizable.

La jurisprudencia del TJUE se muestra oscilante a la hora de fijar los límites del concepto de dato personal. Existen notables diferencias entre los criterios utilizados en el asunto YS y otros (2014)[58] y lo previsto en el asunto Nowak (2017)[59]. Este último pronunciamiento parece apostar, en la línea de los dictámenes del Grupo de Trabajo del Artículo 29[60], por una consideración más abierta del concepto de dato personal, incorporando

[57] Esta concepción de qué es identificable entronca con la teoría del mosaico de Madrid Conesa, en ella se apuntaba el valor ambivalente de los datos en función del tratamiento y del conjunto de informaciones con que se relacionasen. Si bien pensada para determinar las posibles afectaciones de la intimidad, la idea del mosaico sirve, también, para representar ese potencial identificador de los datos (Madrid Conesa, 1984, pp. 23-77).

[58] STJUE asuntos acumulados C-141/12 y C-372/12, YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie; Integratie en Asiel contra M y S, de 17 de julio de 2014.

[59] STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017.

[60] Dictamen 4/2007, sobre el concepto de datos personales, de 20 de junio de 2007. Puede consultarse en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf. (Última consulta: 20/10/2021).

tres características que, en caso de concurrir alguna de ellas, dotarían a una determinada información de la condición de dato personal.

Para saber si la línea jurisprudencial de Nowak tiene visos de asentarse, o es una excepción no susceptible de crear jurisprudencia, conviene, siquiera someramente, analizar tanto esa sentencia, como la que le precede y que, en cierto modo, contradice la dictada en al asunto YS y otros.

2.5.2. La interpretación restrictiva en el asunto YS

En los asuntos acumulados YS y otros[61], el TJUE tuvo ocasión de pronunciarse acerca de la condición de dato personal de los análisis jurídicos que llevaron a la denegación de la solicitud de un permiso de residencia. En la sentencia, el TJUE enjuició las diferentes informaciones y concluyó que solo tienen la condición de dato personal «los datos relativos al solicitante del documento de residencia que figuran en la minuta[62] y, en su caso, los que figuran en el análisis jurídico incluido en […] [ella]». Sin embargo, el análisis como tal, es decir, la valoración, no tendría la condición de dato personal de los solicitantes del permiso[63].

La diferente consideración se explica porque, para el TJUE, son datos personales del solicitante todos aquellos que lo describen y que reflejan su situación, como sería el caso de «su nombre, fecha de nacimiento, nacionalidad, sexo, etnia, religión e idioma»[64]. Ahora bien, ni el proceso argumentativo, ni los motivos que llevaron a adoptar la decisión final, pueden ser considerados como datos personales del solicitante, dado que no son más que la simple aplicación de lo previsto en las normas.

---

[61] Para un análisis más detallado de la sentencia y sus consecuencias, especialmente para los procesos de solicitud de residencia y asilo, vid. (Brouwer y Zuiderveen Borgesius, 2015).
[62] En este caso el TJUE utiliza minuta como sinónimo de expediente vinculado a la resolución.
[63] Tanto el texto expresamente citado, como la denegación de la condición de dato personal al análisis, constan en el apdo. 48 de la STJUE asuntos acumulados C-141/12 y C-372/12, YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie; Integratie en Asiel contra M y S, de 17 de julio de 2014.
[64] STJUE asuntos acumulados C-141/12 y C-372/12, YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie; Integratie en Asiel contra M y S, de 17 de julio de 2014, apdo. 38.

En la línea interpretativa de la Abogada General Sharpston[65], el TJUE configura un concepto de dato personal acotado a las informaciones relativas a la persona. A su juicio, esta conceptualización de la noción de dato personal es la que mejor se acomoda a los objetivos y estructura de la Directiva[66]. Frente a esta interpretación, la Comisión Europea defendió que el análisis jurídico también debía ser considerado dato personal, en la medida en que «se refiere a una persona física concreta y se basa en su situación y características individuales»[67].

2.5.3. Nowak: las opciones se amplían

En el asunto Nowak[68], el TJUE se pronunció acerca de la viabilidad de la petición del sr. Nowak de acceder a su examen de admisión al Instituto de Auditores Públicos de Irlanda, así como a las anotaciones y valoraciones realizadas por el examinador. Su solicitud se fundamentaba en el ejercicio del derecho a la protección de datos, básicamente del derecho de acceso. El reclamante consideraba su petición adecuada, pues entendía que, tanto el examen, como las valoraciones que el evaluador hubiera realizado, eran datos de carácter personal a él referidos.

En este caso, el TJUE, al igual que en el asunto YS, analizó la condición de dato personal de cada una de las informaciones controvertidas (respuestas, preguntas y anotaciones). Respecto de las respuestas al examen, consideró que son un dato personal del reclamante, por ser la plasmación del nivel de los conocimientos y capacidades de la persona, así como un reflejo del «proceso de reflexión, el discernimiento y la capacidad de análisis»[69] del interesado. Por si las razones aducidas no fuesen suficientes, el TJUE adicionó otro motivo: la expresión caligráfica y la información que del autor se pueda extraer a partir de su estudio, vendría a ratificar la condición de dato personal de las respuestas.

---

[65] Vid. Conclusiones de la Abogada General presentadas el 12 de diciembre de 2013, (ECLI:EU:C:2013:838). Especialmente el apdo. 59.
[66] STJUE asuntos acumulados C-141/12 y C-372/12, YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie; Integratie en Asiel contra M y S, de 17 de julio de 2014, apdo. 41.
[67] Ibídem, apdo. 35.
[68] STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017. Vid. el detallado comentario de Podstawa sobre este pronunciamiento en (Podstawa, 2018).
[69] STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017, apdo. 37.

Contrariamente, las preguntas, en tanto que no informan sobre la persona examinada, no deben ser consideradas como un dato personal suyo[70]. Respecto de ellas, el examinado no podrá valerse de los derechos que la protección de datos le proporciona.

Pero, el aspecto que más interesa a efectos de conceptualizar qué ha de entenderse por dato personal, es el relativo a las anotaciones subjetivas del evaluador. Para el Tribunal, las glosas y valoraciones que los examinadores realizan de los ejercicios son datos personales del examinador y del examinado, pues una misma información puede ser considerada dato personal de más de una persona[71].

Interesa detenerse en el proceso argumental que lleva al TJUE a estimar que las valoraciones realizadas por una persona pueden ser, a la vez, dato personal de otra. Las anotaciones son un dato personal del examinado, por ser informaciones sobre una persona específica (el autor del examen), respecto de la que se hacen evaluaciones sobre sus conocimientos y capacidades y, además, esas valoraciones pueden tener consecuencias sobre sus expectativas laborales y vitales.

Para llegar a esa conclusión, el TJUE acude a los tres criterios que, una década antes, había propuesto el GT29 para interpretar el alcance de la expresión «información sobre una persona» (art. 2.a) de la Directiva y 4.1 del RGPD). El GT29 había considerado que, cuando por contenido, finalidad o resultado, una información se refiriese a una persona, esta habría de calificarse como dato personal. El TJUE acoge ahora esos mismos elementos, con un único matiz nominal, en lugar de resultado adopta el término «efectos»[72]. Así, cuando por contenido, finalidad o efectos una información pueda vincularse a un sujeto concreto, habrá de considerarse dato personal. Estas tres condiciones no son cumulativas, basta con que concurra una de ellas para considerar que esa información es personal[73].

Además de un criterio interpretativo, esas tres variables resultan de gran utilidad a la hora de resolver aquellas situaciones en las que, como ocurría en el asunto Nowak, concurren diversos intereses sobre una misma

[70] Ibídem, apdo. 58.
[71] Ibídem, apdo. 45.
[72] Una información, será dato personal cuando «debido a su contenido, finalidad o efectos, la información está relacionada con una persona concreta», STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017, apdo. 35.
[73] El uso de la conjunción disyuntiva "o" en lugar de la copulativa "y" es muestra elocuente de ello.

información. En este caso, fue la valoración de los fines y, sobre todo, los efectos del tratamiento, lo que permitió anteponer el derecho de acceso del examinado, al interés que pudiera tener el examinador en que no se conociese dicha información –debe recordarse que era dato personal de ambos–.

Como puede constatarse, la diferencia con el asunto YS es significativa. Si en ese caso se hubiesen aplicado los criterios establecidos en Nowak, en tanto el análisis jurídico tuvo efectos sobre el solicitante del permiso de residencia, debería haberse procedido de manera más minuciosa a la hora de precisar qué informaciones podían ser consideradas dato personal y cuales eran meras abstracciones jurídicas[74].

2.5.4. Consecuencias de la ampliación del concepto dato personal

2.5.4.1. El proceso de ampliación conceptual. Primeros pasos

El *overruling* que el asunto Nowak parece apuntar, suscita una serie de cuestiones. ¿A qué se debe este cambio de criterio? ¿Son aplicables, como criterio general, el contenido, la finalidad o los efectos como identificadores de la existencia de un dato personal? ¿Cuáles son las consecuencias que se pueden derivar de esta apertura del concepto? Responder a estas preguntas exige volver al concepto de dato personal y a los factores que lo determinan. Con esta aproximación se pretende poner en perspectiva los diferentes pronunciamientos, y vislumbrar cuál puede ser la interpretación que, finalmente, prevalecerá.

El punto de partida del TJUE acerca de lo que deba entenderse por dato personal, fue el artículo 2.a) de la Directiva[75]. En él se establece una definición de dato personal que se replica en el art. 4.1 RGPD. Esta concomitancia permite que, pese a que la jurisprudencia del TJUE acerca

[74] Sobre el asunto Nowak, sus consecuencias para el concepto de dato, así como la extrapolación de su doctrina a otros ámbitos distintos del de los exámenes, he tenido ocasión de pronunciarme en (Jove, 2019). Una valoración, más cautelosa, del alcance y posibilidades interpretativas de la sentencia es la planteada por Wachter y Mittelstadt en (Wachter y Mittelstadt, 2019, pp. 531-537).

[75] Art. 2.a) Directiva: «"datos personales": toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

del concepto de dato está referida a la Directiva, sea perfectamente trasladable a la interpretación de la normativa actualmente en vigor.

La primera gran aproximación interpretativa al concepto de dato personal –y con seguridad la más detallada– fue la realizada por el Grupo de Trabajo del Artículo 29 en el Dictamen 4/2007, sobre el concepto de datos personales, de 20 de junio de 2007[76]. En este Dictamen, el GT29 analizó, término a término, la definición de la Directiva y propuso tres elementos mediante los que determinar si una concreta información versa o no «sobre» una persona. Esos tres criterios relacionales serían el «contenido», la «finalidad» o el «resultado», que coincidiría con lo que en Nowak se denominó «efectos».

Con el Dictamen 4/2007 del GT29 como referencia, una información sería dato personal en atención a su «contenido», cuando proporcione datos «sobre una persona concreta, independientemente de cualquier propósito que puedan abrigar el responsable del tratamiento de los datos o un tercero, o de la repercusión de esa información en el interesado»[77]. Es decir, «contenido» encajaría con la concepción natural y directa de la relación dato-persona; la información sería una proyección del ser.

Por su parte, la «finalidad» desempeña un rol identificador cuando «los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con […] [el objetivo] de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona»[78]. Ergo, cualquiera que sea el contenido de la información, si su uso está relacionado con una persona determinada, será dato personal.

El tercero de los criterios, el «resultado» o, en términos del TJUE, los «efectos», tienen cierta semejanza con la finalidad. Sin embargo, el nivel de intensidad en la conexión es menor. Así, se consideró que una información es dato personal por este motivo, cuando, en atención a «todas las circunstancias que rodean el caso concreto, es probable que su uso repercuta en los derechos e intereses de determinada persona. Basta con

[76] Puede consultarse el Dictamen 4/2007 en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf.
[77] Ibídem, p. 11.
[78] Ibídem, p. 11-12.

que la persona pueda ser tratada de forma diferente […] como consecuencia del tratamiento de tales datos»[79].

Esta categoría interpretativa amplía notablemente el espectro que un dato personal puede abarcar, pero no es un criterio carente de fundamento, pues conecta el concepto de dato personal con la finalidad de las normativas de protección: la salvaguarda de los derechos y libertades de los individuos.

A pesar del Dictamen del GT29, en el año 2014, al resolver el caso YS, el TJUE adoptó una interpretación del concepto de dato en el que prescindía de esos tres elementos y se centraba únicamente en la existencia de un nexo entre el dato y la persona. Al negar la condición de dato personal a las valoraciones que se pudieran realizar, pues estas estarían fundadas en razones carentes de toda vinculación originaria con el interesado.

2.5.4.2. El RGPD. Un modelo más acorde con una interpretación amplia del concepto

La siguiente etapa del proceso se corresponde con la entrada en vigor del RGPD, el 24 de mayo de 2016. A partir de ese momento, y aunque tardaría dos años en ser de aplicación para los estados miembros (art. 99 del RGPD), la UE contaba con un nuevo marco de referencia en la regulación del tratamiento de la información personal. Aunque desde un punto de vista formal la redacción del concepto de dato era la misma, esta se inscribía en un modelo de protección diferente, más proactivo, presidido por una mayor exigencia de atención al contexto y adecuación a la realidad de cada tratamiento[80].

El cambio interpretativo del TJUE en el asunto Nowak, con la adopción de las variables propuestas por el GT29, encajaría con la idiosincrasia que inspira y promueve el RGPD. Al introducir la finalidad y los efectos como elementos detonantes de la condición personal de la información, se reforzó la obligación del responsable de analizar cada tratamiento, de prever los riesgos y de acomodar las medidas de protección. Así, el responsable, después de confirmar que opera con datos

[79] Ibídem, p. 12.

[80] Como hemos visto, los principios consagrados en el art. 5 del RGPD refrendan esa orientación proactiva. En la misma línea apunta el Considerando 39, entre otros. En realidad, el conjunto del RGPD es un reflejo de esta nueva concepción.

personales, deberá ser capaz de determinar, para cada tratamiento, qué sujetos (identificados o identificables) se pueden ver afectados. La identificación o identificabilidad de la persona adquiere, por esta vía, cierta dimensión proactiva relacionada con la idoneidad y la calidad del tratamiento.

Por lo tanto, la ampliación del concepto dato que se promueve en Nowak encaja con una interpretación sistemática del RGPD. Este criterio identificativo de los datos personales resulta teleológicamente coherente con la consecución de uno de los objetivos nucleares del RGPD: proteger «los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales» (art. 1.2 RGPD) «en lo que respecta al tratamiento de los datos personales» (art. 1.1 RGPD). Al incluir los efectos y la finalidad como factores determinantes, se extiende el conjunto de informaciones susceptibles de ser consideradas dato personal. La consecuencia directa de esta interpretación es la ampliación del número de tratamientos frente a los que se podrá reaccionar mediante los instrumentos jurídicos previstos para hacer frente a los riesgos que, para los derechos y libertades, supone el uso de información personal por terceros.

Frente a esta interpretación justificativa del cambio de criterio del TJUE, puede aducirse que, si la voluntad del legislador europeo era ampliar el concepto, ¿por qué no se incluyó expresamente este cambio en el RGPD? En efecto, nada impedía que, al igual que ocurre con el concepto «identificable», se hubiesen dedicado unas líneas a definir el alcance de la expresión «información sobre una persona física». No se hizo así. Sin embargo, no parece fortuito que el cambio interpretativo del TJUE se produjese poco después de la entrada de en vigor del RGPD. Ni la coincidencia, ni la casualidad, explican que la nueva interpretación encaje tan afinadamente con la línea de actuación y el modelo de protección que se pretende implementar con el nuevo marco jurídico.

Siempre se podrá decir que el legislador europeo, pudiendo hacerlo, no ha señalado a esas tres variables como criterios interpretativos. Sin embargo, tampoco las descarta, situándolas, así, en el ámbito de lo posible. El tenor literal del precepto no impide la utilización de la «finalidad» y los «efectos» como elementos que el intérprete puede utilizar.

3. El tratamiento y la protección frente a los riesgos

3.1. El tratamiento como elemento configurador del sistema de protección

Así como el dato es el centro de imputación del derecho a la protección de datos personales, el tratamiento es la realidad objeto de su regulación. Los datos no están en el vacío, ni desconectados de su entorno. Los datos se protegen por lo que son, por lo que representan y porque su utilización lleva aparejado un riesgo inherente para aquellos a los que se refiere[81]; sin que ello empañe las ventajas y beneficios que un determinado tratamiento pueda suponer para el interesado (p. ej. proporcionándole servicios más adecuados a sus intereses o facilitándole el desempeño de su trabajo diario (gestión de nóminas, clientes, cuentas de correo, etc.)).

Los datos personales se recaban y se opera con ellos para conseguir determinados fines –la licitud de las actuaciones es una cuestión diferente y su materialización dependerá de las condiciones previstas en el ordenamiento jurídico–. Del mismo modo que no hay tratamiento sin datos –personales o no– no hay derecho a la protección de los datos personales sin tratamiento. El tratamiento es consustancial al derecho. Si bien una información puede, en algunos casos, ser considerada dato personal sin que se opere con ella (v. gr. en datos sobre personas identificadas), ello no obsta para que la aplicación del derecho dependa de la utilización de esa información y de cómo se gestione la misma: si no se usa, no hay necesidad de protegerla. Los datos personales, por sí solos, en el vacío, sin contexto, en "estado de naturaleza", no necesitan ser protegidos, porque no están amenazados.

Ahora bien, al igual que en Hobbes o en Locke, el estado de naturaleza de los datos no existe, es una premisa, un presupuesto explicativo para facilitar la comprensión de la realidad conocida. En este caso, que no hay dato personal sin contexto. La materialización de una determinada información siempre tiene alguna causa. Todo dato se genera y se usa por algo, incluso el nombre de las personas obedece a una razón de ser: distinguirlas de las demás, identificarlas. Por lo tanto, el contexto,

[81] La AEPD ha definido el riesgo inherente como «el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición. El riesgo inherente surge de la exposición que se tenga a la operación de tratamiento en particular y de la probabilidad de que la amenaza asociada al riesgo se materialice», en Guía Práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD, de la AEPD, p. 26. Puede consultarse en:
https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

las circunstancias en que una determinada información es utilizada, resulta determinante para comprender los rasgos que caracterizan al art. 8 de la CDFUE.

Junto al contexto, la utilización de la información, esto es, su tratamiento, es el otro factor clave. Si se observan las previsiones normativas mediante las que se pretende garantizar el derecho de toda persona a la protección de los datos de carácter personal, se constata que, en puridad, están regulando medidas de salvaguarda frente a la utilización de información personal. El tratamiento es el detonante aplicativo de la normativa (Arias Pou, 2016), basta con acudir al nombre completo del RGPD para comprobarlo: 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"[82] y a la libre circulación de estos datos. Su objeto incide en esta idea, pues la finalidad del RGPD es «la protección de las personas físicas en lo que respecta al tratamiento de los datos personales» (art. 1.1)[83].

Si hay datos personales sin necesidad de tratamiento, ¿por qué las medidas de protección están inexorablemente unidas a este último? La respuesta radica en el elemento que, desde las primeras regulaciones, lleva impulsando la concreción de los instrumentos de protección: el riesgo, el temor a los efectos que la utilización de una determinada información personal por terceros puede generar en el individuo afectado.

La gestión de los peligros potenciales es el elemento central de las normativas de protección de datos y, en última instancia, uno de los fundamentos del derecho del art. 8 de la CDFUE. Al reconocer el derecho a la protección de los datos personales, el legislador está habilitando una política de prevención mediante un conjunto de medidas precautorias frente a las eventuales consecuencias que, el uso indiscriminado y descontrolado de la información, pudiera tener para los bienes jurídicos de las personas.

[82] Comillas propias. El nombre de la primera Ley federal alemana sobre la materia también resulta muy elocuente: Ley para la protección del mal uso de los datos personales a través de su tratamiento, *Bundesdatenschutzgesetz* (Ley federal de protección de datos)

[83] En la misma línea, el Considerando 14 del RGPD apunta que «La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales».

Si el dato personal es la materia prima de todo tratamiento, y el nexo con la persona, el riesgo y la necesidad de prevención anticipada, hacen que el tratamiento se convierta en la realidad a regular. Sin tratamiento no hay riesgo y, por tanto, no hay necesidad de proteger los datos.

3.2. La definición de tratamiento

El tratamiento de la información aporta los matices necesarios para configurar las principales variables del derecho a la protección de datos. «Los datos como tales no tienen ningún sentido intrínseco. Pero pueden ser portadores de información, y en concreto de información codificada. Se les atribuye un sentido cuando […] se convierten en objeto de comunicación» (Hoffman-Riem, 2018, pp. 51-52).

Como ya se ha puesto de manifiesto, las circunstancias en que se produce el procesamiento de los datos tienen consecuencias sobre su naturaleza. El contexto permite identificar, para un sujeto concreto y en un tratamiento determinado, la existencia de un dato personal. No resulta extraño, por tanto, que el tratamiento sea el ámbito de aplicación material (art. 2.1 RGPD)[84] del derecho a la protección de datos. Su caracterización jurídica es, por consiguiente, crucial.

Así, el art. 4.2 del RGPD dispone que tratamiento es «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no»[85].

A continuación, el precepto enuncia, sin carácter taxativo, diferentes tipos de tratamientos susceptibles de ser subsumidos en la definición descrita. Se consideran operaciones de tratamiento: «la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción».

---

[84] Art. 2.1 RGPD: «El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero».

[85] Sobre el concepto de tratamiento en la normativa europea, su alcance y la jurisprudencia relacionada vid. el análisis de Tosoni y Bygrave en (Tosoni y Bygrave, 2020).

Expresado de otro modo: se estarán tratando datos cuando se realice cualquier tipo de actuación sobre ellos. El tratamiento es la utilización del dato para un fin[86].

Las características del tratamiento determinan las condiciones en que se va a llevar a efecto y, consecuentemente, modulan la materialización efectiva del derecho. El mandato general de protección se ajustará, en cada caso concreto, a las condiciones en que se produzca la gestión de los datos.

La naturaleza del tratamiento (automatizado o no automatizado[87]), el ámbito en que se lleva a efecto (doméstico o no), quién lo realiza (personas físicas, autoridades públicas o personas jurídicas), los datos que se utilizan (especiales o no), el modo en que se hace (almacenar, recabar, consultar, modificar, destruir, etc.), las diferentes fases en que se divida[88], los riesgos que representa o la finalidad que se persiga, son elementos que, inevitablemente, se han de ponderar a la hora de seleccionar la normativa aplicable, las medidas de protección que se han de adoptar o los derechos a ejercitar.

Ahora bien, para determinar la existencia de tratamiento basta un único requisito: que haya una operación en la que medien datos personales[89]. Si hay un dato que un tercero, del modo que sea, puede conocer y/o utilizar, habrá tratamiento.

---

[86] Como ha apuntado el Abogado General del asunto C-40/17, Fashion ID, en sus conclusiones de 19 de diciembre de 2018, «el concepto de "tratamiento", a semejanza del de "responsable del tratamiento", es bastante amplio», apdo. 99.

[87] Davara Rodríguez incluye una tercera categoría, los tratamientos mixtos, que serían aquellos en que «los que unos datos se encuentran en soportes automatizados y otros datos (o copia de los mismos) en soportes no automatizados, pero todos ellos se refieren a datos del mismo tratamiento» (Davara Rodríguez, 2021, p. 594).

[88] Un tratamiento puede ser lo suficientemente complejo como para constar de varias fases o etapas, como puso de manifiesto el TJUE al resolver el asunto Fashion ID. En ese caso, al tener que tener si existía corresponsabilidad en un determinado tratamiento, señaló la existencia de diferentes operaciones de tratamiento, cada una de ellas con su finalidad y cometido. STJUE asunto C-40/17, Fashion ID, de 29 de julio de 2019, especialmente los apdos. 73-76.

[89] Cada operación es un tratamiento, con independencia de las que se hayan llevado a cabo previamente o del carácter de las mismas. En esa línea apunta el TJUE en la sentencia del asunto C-73/07, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy, Satamedia Oy, de 16 de diciembre de 2008.

3.3. La confirmación del riesgo como criterio determinante en la aplicación del derecho de protección frente al tratamiento de la información personal

3.3.1. El ámbito de aplicación del RGPD como punto de partida

La mera existencia de un dato personal no justifica, *per se*, el ejercicio del derecho. Éste debe hacerse valer frente a otros, a quienes se imponen obligaciones de acción o abstención, por lo que resulta imprescindible que exista un tratamiento. Es el tratamiento el que produce las condiciones fácticas que hacen ejercitable el derecho, pues solo él proporciona el marco relacional y permite perfeccionar el requisito personal (que exista ese otro al que imponer obligaciones).

La condición de dato personal, y la de tratamiento, son premisas necesarias para obtener la protección que brindan las regulaciones europeas destinadas a hacer efectivo el derecho del art. 8 de la CDFUE. Que un dato personal esté siendo objeto de tratamiento es condición necesaria, pero no suficiente, cuando menos en la práctica. Basta con acudir al RGPD para comprobar que no todo tratamiento de datos personales cuenta con la protección que le brinda esa norma.

El examen del ámbito de aplicación material del RGPD (art. 2) constata que, junto a las exclusiones aplicativas derivadas de la ausencia de competencia de la UE (arts. 2.2 RGPD letras a) y b))[90] o de la existencia de una regulación específica sobre la materia (art. 2.2 letra d) y los art. 2.3 y 2.4 del RGPD)[91], se prevén ciertos supuestos en los que, pese a tratarse

[90] El art. 2.2.a) se refiere al tratamiento de datos realizado «en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión». Por su parte, la previsión del art. 2.2.b) supone excluir del ámbito de aplicación del RGPD las regulaciones de los Estados miembros en materia de política exterior y de seguridad común. En este caso, confluye una mezcla entre ausencia de competencia completa de la UE (Capítulo 2 del Título V del TUE) y la consideración de esta materia como estratégica, lo que justificaría una regulación particularizada.

[91] En el caso del art. 2.2.d) del RGPD, referido a la exclusión de los tratamiento llevados a cabo «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 de protección frente a amenazas a la seguridad pública y su prevención» se trata de una materia con una atención particularizada, la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
La exclusión aplicativa del apartado tercero del art. 2 obedece a la existencia de una regulación particular para los tratamientos llevados a cabo por las instituciones, órganos y organismos de la Unión Europea, en concreto, el Reglamento (UE) 2018/1725 del

datos personales, el RGPD no se aplica. Ese es el caso de la exclusión de los tratamientos efectuados «por una persona física en el ejercicio de actividades exclusivamente personales o domésticas» (art. 2.2 letra c) RGPD).

Por otra parte, el RGPD dispone, expresamente, que las medidas de protección y sanción en él previstas se aplicarán, también, a los tratamientos no automatizados de datos (art. 2.1 RGPD). No se me oculta que, en última instancia, la exclusión o la inclusión de un determinado tipo de tratamiento, dentro del ámbito de aplicación de la norma es una opción del legislador[92].

No obstante, si se analizan las características de los tratamientos excluidos, así como la inaplicación de los datos de las personas fallecidas (más allá de la habilitación hecha a favor de los Estados miembros), y se comparan con las razones que justificarían la inclusión de los tratamientos no automatizados, se evidencia que, el margen decisorio del legislador, no es tan amplio como, en principio, pudiera pensarse.

Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE. Esta disposición normativa es la sucesora de la mencionada en el RGPD, el Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

En lo referente al art. 2.4 del RGPD, más que una exclusión, se establece una actuación conjunta entre las previsiones del RGPD y de la Directiva 2000/31/CE, para «la responsabilidad de los prestadores de servicios intermediarios» en la sociedad de la información. Debe advertirse que, en este caso, es probable que esta concurrencia aplicativa sufra algún ajuste cuando la Directa 2000/31/CE sea sustituida por el Reglamento de Servicios Digitales. También se está trabajando en una Propuesta de Reglamento del Parlamento y el Consejo sobre el Mercado Único de Servicios Digitales (Reglamento de Servicios Digitales) y enmienda da la Directiva 2000/31/EC. Puede consultarse en, https://eur-lex.europa.eu/legal-content/es/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN.

[92] El legislador español, en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), aposto solo por regular un tipo de tratamiento concreto, el automatizado. En este caso, esa decisión legislativa tuvo un recorrido escaso desde el punto de vista temporal, pues la Directiva 95/46/CE se refería a tratamientos «efectuadas o no mediante procedimientos automatizados» (art. 2.b) y fue necesario ampliar el ámbito de aplicación y modificar la normativa, adoptándose la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Sobre las razones que motivaron el reemplazo de la LORTAD, vid. (Rallo Lombarte, 2017, pp. 652-658) y (Jove, 2018, pp. 87-89).

3.3.2. Tratamiento no automatizado de los datos personales

La inclusión del tratamiento de datos de manera no automatizada obedece a un triple motivo. En primer lugar, su previsión específica evita la "huida" de las exigencias de la normativa de protección de datos (Considerando 15 RGPD)[93] mediante la utilización de ficheros no informatizados. En segundo lugar, y muy conectado con el anterior, la incorporación de esta tipología de tratamientos fomenta la digitalización de las empresas. En efecto, al extenderse las obligaciones a todo tipo de tratamientos, no tendrán el incentivo mantener un tratamiento "manual" de la información y optarán por el modelo que les resulte más eficiente, lo que, habitualmente, les llevará a apostar por sistemas automatizados de tratamiento. Como puede comprobarse, las razones detrás de esta justificación son eminentemente políticas, de estrategia nacional o, en este caso, europea[94].

Finalmente, el tercero de los motivos conecta directamente con el derecho del artículo 8 de la CDFUE y con la idea de prevención frente a los peligros que pudieran derivarse del tratamiento de datos. El Considerando 15 del RGPD afirma que «la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas». En consonancia con esta previsión, se incluye el tratamiento no automatizado de datos. Empero, en contra de las implicaciones de esa aseveración, no todas las operaciones no automatizadas serán objeto de protección, sino que se aplicará, exclusivamente, a aquellas en que «los datos personales figuren en un fichero o estén destinados a ser incluidos en él», y siempre que el modo de gestión de la información esté estructurado (Considerando 15). Si la información no está organizada, no se aplicará la normativa de protección de datos.

¿Por qué en un caso sí y en el otro no? Por los costes, el tiempo y el esfuerzo necesarios. En la raíz de las normativas de protección frente al tratamiento de la información está la ruptura de las barreras del tiempo y el esfuerzo que la automatización de la gestión de los datos trajo aparejada. A ello ha de unirse la reducción exponencial y constante de los costes de los

[93] Considerando 15 RGPD, «A fin de evitar que hay un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual».

[94] El desarrollo de la «economía digital […] en todo el mercado interior» es uno de los objetivos que inspiran el RGPD (Considerando 7)».

ingenios tecnológicos, haciendo accesible a más personas la posibilidad de obtener cada vez mejores resultados en un menor tiempo.

En la misma línea, puede comprenderse que, en aquellos casos en que la información esté bien organizada y estructurada, su aprovechamiento será posible sin necesidad de esfuerzos desproporcionados, o inversiones en tiempo desmedidas, aunque se encuentre en papel y no se gestione de manera mecánica. En definitiva, si los datos relativos a una persona determinada son fácilmente recuperables[95], los riesgos inherentes a toda operación con datos personales están presentes y, consecuentemente, es necesario extender los mecanismos de prevención que el derecho a la protección de los datos proporciona.

A contrario sensu, e independientemente del soporte de la información (digital o papel), si los datos están desestructurados; si realizar conexiones e interrelaciones entre informaciones y personas resulta imposible, o requiere de unos esfuerzos extraordinarios (por ejemplo por estar encriptados), se considera que el tiempo, los costes y el esfuerzo son una barrera de protección suficiente para la información. En suma, existen circunstancias que operan como una garantía suficiente para los derechos de las personas, haciendo innecesario, en esos casos, el derecho a la protección de datos.

3.3.3. La exención doméstica

La exclusión prevista en el art. 2.2.c del RGPD se debe, en esencia, a una doble motivación. De una parte, a la naturaleza eminentemente economicista de la normativa de protección de datos. Prueba de ello es que, cuando el tratamiento sea llevado a efecto por personas físicas[96], el RGPD, solo se aplica a los tratamientos que tengan que ver con alguna «actividad profesional o comercial» (Considerando 18).

[95] Así lo ha puesto de manifiesto el TJUE en la STJUE asunto C-25/17, Tietosuojavaltuutettu, de 10 de julio de 2018, al señalar, en el apdo. 61, que «carece de pertinencia indagar cuáles son en concreto el criterio y la forma empleados para estructurar efectivamente el conjunto de datos personales recogido […], en la medida en que dicho conjunto permita recuperar fácilmente los datos relativos a una determinada persona» será un tratamiento susceptible de serle aplicada la normativa de protección de datos.

[96] Por la propia naturaleza de los sujetos, los tratamientos de personas jurídicas y autoridades públicas no encajarían en excepción doméstica

De otra, como expresamente señala el legislador, al reducido, cuando no inexistente, riesgo que comportan unos tratamientos que, por definición, se circunscriben a la esfera personal del propio interesado. En última instancia el RGPD excluye el "autoconsumo" de los propios datos, esto es, la utilización de las informaciones generadas para beneficio propio –en un sentido no crematístico–. Pese a la aparente claridad del presupuesto fáctico, no siempre resulta sencillo delimitar donde termina el ámbito doméstico del tratamiento[97], debiendo interpretarse el alcance de esta exención de manera restrictiva, sobre todo en lo atinente a la difusión de información[98].

El RGPD ofrece algunos ejemplos, puramente ilustrativos, de actividades susceptibles de ser subsumidas en la excepción doméstica. Es el caso de «la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades» (Considerando 18). Incluso en estos supuestos pueden hacerse matices, pues la actividad en redes sociales no está excluida por defecto[99]. Por último, recordemos que esta excepción no alcanza «a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas» (Considerando 18), lo que resulta coherente, en la medida en que en ellos sí anida un interés económico o comercial[100].

---

[97] En la STJUE asunto C-212/13, František Ryneš c. Úřad pro ochranu osobních údajů, de 11 de diciembre de 2014, el TJUE determinó que, en «la medida en que una vigilancia por videocámara [...] se extiende, aunque sea en parte, al espacio público, abarcando por ello una zona ajena a la esfera privada de la persona que procede al tratamiento de datos valiéndose de ese medio, tal vigilancia por videocámara no puede considerarse una actividad exclusivamente "personal o doméstica"» (apdo. 33).

[98] En la STJUE asunto C-101/01, asunto Lindqvist, 6 de noviembre de 2003, el TJUE consideró que «la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» (apdo. 27), por más que no hubiese en la persona que efectuó una convicción de estar realizando un tratamiento.

[99] Como ha puesto de manifiesto el GT29, «un gran número de usuarios funcionan en un ámbito puramente personal, poniéndose en contacto con personas que forman parte de su ámbito personal, familiar o doméstico» (Dictamen 5/2009 sobre las redes sociales en línea, de 12 de junio de 2009, p. 1). No obstante, cuando se utilicen las redes con fines comerciales (Considerando 18), cuando el tratamiento suponga una difusión «a un grupo indeterminado de personas» (asunto Lindqvist, apdo. 47) o el contenido pueda entrañar un alto riesgo para los derechos y libertades de los afectados por publicarse datos sensibles (Dictamen 5/2009 sobre las redes sociales en línea, de 12 de junio de 2009, p. 7).

[100] Sobre las posibilidades de aplicación de la excepción doméstica, vid. (Santos Morón, 2020, pp. 32-35).

3.4. ¿Qué aporta el tratamiento a la determinación de la naturaleza del derecho a la protección de datos?

La sustracción de determinados tratamientos del ámbito de aplicación del RGPD, unida al particular modo en que se afronta la gestión de los datos de personas fallecidas, confirma que no toda operación con datos personales supone un riesgo relevante para los derechos de las personas y que los datos no se protegen, en exclusiva, por el hecho de serlo, sino, también, por lo que representan, por lo que implica su tratamiento y por los peligros inherentes a su gestión, con independencia de que los daños potenciales se concreten o no.

Sin datos no hay derecho, pero sin tratamiento no existiría un riesgo que justificase su existencia. En consonancia con esa línea argumental, es posible no aplicar el derecho y las exigencias del art. 8 de la CDFUE a ciertos tratamientos, siempre que se constate que no engendran peligro suficiente.

Por otra parte, el tratamiento tiene cierta relevancia a la hora de determinar la existencia de un dato personal. Como ya se ha indicado, cuanto más amplio sea el concepto de dato, cuanto más peso tenga el tratamiento, más se refuerza la hipótesis del derecho a la protección de datos como instrumento de defensa de los intereses de la ciudadanía frente al tratamiento de la información personal, y no solo como una plasmación de la autodeterminación personal mediante el dominio de los datos a uno referidos.

Las variables hasta ahora analizadas (el dato y su tratamiento) parecen indicar que, el derecho fundamental a la protección de datos impone al legislador la exigencia de articular una regulación dirigida a asegurar el cumplimiento efectivo de dicho derecho. De este modo, serían las normativas encargadas de configurar los sistemas de protección las que determinarían cuando un tratamiento de datos personales reúne las características que lo hacen acreedor de las salvaguardas legalmente previstas.

4. Un derecho con un contenido por definir

Cualquier modelo de protección frente al tratamiento de la información personal ha de ajustarse a las exigencias derivadas del derecho fundamental a la protección de datos. Proponer un cambio en la noción de dato personal o prescindir de las categorías especiales, implica un giro de muchos grados, por lo que resulta obligado detenerse y plantear la cuestión en la dirección correcta: del derecho fundamental al modelo de protección.

Hasta este momento, hemos identificado y problematizado con ciertos aspectos que pueden contribuir a perfilar la esquiva naturaleza jurídica del derecho a la protección de datos. Hemos analizado su proceso formación en términos evolutivos e históricos (Capítulo II) e identificado las características del ecosistema europeo de protección de datos y teorizado respecto de su idiosincrasia y tendencia (Capítulo III) y, en este mismo apartado, nos hemos detenido en la exégesis de los conceptos de dato personal y tratamiento, nucleares para su compresión y delimitación. Sin embargo, en todas esas referencias, el derecho fundamental aparecía más como una meta que como un punto de partida. Una vez recorrido ese camino, estamos en condiciones de preguntarnos cuál es la naturaleza jurídica de este derecho, aquello que lo identifica y justifica.

Para ello, y continuando con la misma sistemática expositiva, debemos situarnos en la concepción europea del derecho y adoptar la formulación del derecho fundamental a la protección de datos del art. 8 de la CDFUE como objeto de estudio[101].

Sin embargo, antes de abordar la determinación de la naturaleza del derecho a la protección de datos, considero imprescindible realizar una aclaración con relación a la declaración contenida en el art. 52.1 de la CDFUE. Este precepto establece la existencia de un contenido esencial

[101] Se toma al artículo 8 de la CDFUE como referencia a la hora de analizar el contenido del derecho a la protección de datos, por ser en él donde este derecho se desarrolla de manera más detallada, desde una concepción equivalente a la del art. 16 del TFUE (Ramopoulos, 2019). Adicionalmente, con esta elección se evita reiterar constantemente la dualidad existente entre el art. 8 de la CDFUE y el 16 del TFUE. Con todo, allí donde sea pertinente, también se aludirá al art. 16 TFUE.

como "límite de los límites", es decir un núcleo material indisponible para el legislador, cuya transgresión haría irreconocible al derecho[102].

No puedo negar la dificultad intelectual que, como a otros muchos autores, me genera la idea de un contenido esencial de un derecho fundamental[103], porque, de inmediato, parece conducir, casi intuitivamente, a la existencia de contenidos no esenciales. No resulta extraño que se hayan planteado desde la doctrina diversas interpretaciones acerca de la naturaleza del contenido esencial[104].

Así, pueden encontrarse posiciones absolutas, en las que se establece un núcleo esencial y un contenido accesorio, lo que provocaría tener que deslindar lo esencial de lo que no lo es (Gavara de Cara, 1994, pp. 271-272). Este tipo de aproximación debería descartarse, pues supone un desvalor

---

[102] Soy plenamente consciente de que el límite del contenido esencial se había introducido previamente en la constituciones de algunos Estados miembros de la UE (singularmente art. 19.2 Alemana y, por influencia, art. 53.1 España).
Sobre el origen alemán de la idea de contenido esencial y su traslación a la Constitución de 1949, vid. (Gavara de Cara, 1994). Para la concepción española del contenido esencial, así como sus diferencias con el establecido en la Constitución alemana, vid. (Baura, 1987, pp. 700-723). Con todo, es en la jurisprudencia del TC donde mejor se han explicitado qué es y que implica el contenido esencial. Así, en la STC 11/1981, de 8 de abril, FJ 8, se señala que: «constituyen el contenido esencial de un derecho subjetivo aquellas facultades o posibilidades de actuación necesarias para que el derecho sea recognoscible como pertinente al tipo descrito y sin las cuales deja de pertenecer a ese tipo y tiene que pasar a quedar comprendido en otro desnaturalizándose, por decirlo así. Todo ello referido al momento histórico de que en cada caso se trata y a las condiciones inherentes en las sociedades democráticas, cuando se trate de derechos constitucionales.
El segundo posible camino para definir el contenido esencial de un derecho consiste en tratar de buscar lo que una importante tradición ha llamado los intereses jurídicamente protegidos como núcleo y médula de los derechos subjetivos. Se puede entonces hablar de una esencialidad del contenido del derecho para hacer referencia a aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos. De este modo, se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección.
Los dos caminos propuestos para tratar de definir lo que puede entenderse por "contenido esencial" de un derecho subjetivo no son alternativos, ni menos todavía antitéticos, sino que, por el contrario, se pueden considerar como complementarios, de modo que, al enfrentarse con la determinación del contenido esencial de cada concreto derecho pueden ser conjuntamente utilizados para contrastar los resultados a los que por una u otra vía pueda llegarse».
[103] Para algunos derechos resulta difícil, acaso imposible, averiguar cuál es su contenido esencial. Por ejemplo, el derecho a la igualdad (un derecho de fundamento relacional) o qué no es esencial en el derecho a no ser detenido por más de 72 horas o en el de no declarar contra sí mismo. Pareciera como si el contenido esencial solo existiese en relación con ciertos derechos y que, en otros, lo esencial se identifica con la totalidad del derecho.
[104] Para un estudio más amplio de los diferentes significados del contenido esencial, vid. (Castillo Córdova, 2014).

para una parte de un derecho constitucionalmente reconocido, lo que resulta inaceptable, como Martínez-Pujalte ha puesto de manifiesto (Martínez-Pujalte, 1997, p. 31).

Frente a lo acotado de la interpretación absoluta, se presenta la relatividad de la concepción alexiana, conforme a la que «el contenido esencial es aquello que queda después de una ponderación» (Alexy, 1993, p. 288). En un término medio puede situarse la posición de Häberle, para quien el contenido esencial sería un límite inmanente derivado de las relaciones entre derechos constitucionalmente reconocidos (Häberle, 2003, p. 62).

También se ha identificado la esencialidad de los derechos como una conceptualización finalista de los mismos, de tal manera que su afectación se produciría cuando se impidiese a las personas la satisfacción de los intereses en ellos reconocidos o protegidos. En esta línea argumental se incardinan las propuestas de Stein (Stein, 1973, pp. 249-250) y Krüger[105].

Finalmente, deben reseñarse aquellas aproximaciones a la naturaleza del contenido esencial que encuentran su fundamento en la dignidad humana (Dürig, 1956). Esta postura, coherente con la posición de la dignidad en la Constitución alemana, también sería trasladable a otras realidades normativas, como la española, pues, como señala Martín Huertas, la dignidad es el «catalizador de todas las intervenciones que puedan contribuir al desarrollo encauzado de dichos derechos» (Martín Huertas, 2008, p. 186).

Ante las variadas interpretaciones acerca de lo que el contenido esencial es e implica, se ha optado por una aproximación más pragmática a esta cuestión, siguiendo la línea defendida por el profesor de Otto. En consecuencia, no intentaré desentrañar un, a mi juicio, no desentrañable contenido esencial del derecho, sino que me limitaré a indagar sobre su «contenido sin más» (De Otto y Pardo, 1988, p. 161), es decir, el contenido concreto del derecho respecto de un ordenamiento determinado, para un espacio y un tiempo específicos (De Otto y Pardo, 1988, pp. 158-163).

No se está abdicando del propósito de explorar de la naturaleza jurídica del derecho. Tan solo se prescinde de la búsqueda del Santo Grial

[105] Vid. en (Baura, 1987, p. 704)

de su esencialidad abstracta[106]. Ello comporta que, en las próximas páginas, se tratarán de identificar los parámetros mínimos que ha de respetar cualquier eventual limitación del derecho[107]. En la consecución de dicho objetivo, se transitarán, con asiduidad, las dos vías señaladas por el TC español en la STC 11/1981, de 8 de abril, FJ 8. Así, se valorará, tanto la «naturaleza jurídica o el modo de concebir o configurar cada derecho» como «los intereses jurídicamente protegidos».

Específicamente, para la determinación del contenido del derecho a la protección de datos, se va a «partir de una concepción del derecho y de su función […] [, en la que se consideren tanto sus] facultades reaccionales[, como el modelo de protección implementado, en la medida en que refleja] el peso que se d[á] al elemento libertad o al elemento institución» (De Otto y Pardo, 1988, 163). Es decir, en la identificación del objeto del derecho a la protección de datos, la pregunta clave va a ser ¿cuál es el cometido de este derecho? La respuesta a esta cuestión exige conocer los mecanismos implementados para alcanzar dicho objetivo. Será, en definitiva, una aproximación finalista, en la que el modo de lograrlo opera como guía para definir los contornos reales del derecho, así como sus límites.

Puesto que nuestro propósito principal consiste en examinar la viabilidad jurídica de ciertas reformas e interpretaciones en el modelo de protección del derecho, no será preciso realizar una exégesis completa de todas las manifestaciones del derecho a la protección de datos, sino que, a partir de sus elementos más representativos (los formulados en el art. 8 de la CDFUE), intentaremos precisar cuál es su finalidad última y el bien jurídico que protege.

---

[106] Como ha apuntado Kaufmann, no resulta posible la determinación en abstracto del contenido esencial, pues la realidad del derecho dependerá de su configuración histórica y de su proyección en las relaciones personales (Kaufmann, 1984, pp. 390-394).
Para de Otto tampoco resulta aceptable la aproximación en abstracto al contenido esencial de un derecho, pues en la misma cabrían distintos «contenidos esenciales» (De Otto y Pardo, 1988, p. 161), según como se decidiesen modular.

[107] En consonancia con lo dispuesto en el 52.1 de la CDFUE.

5. Variables interpretativas e interrogantes en torno al derecho fundamental a la protección de datos

5.1. De los nombres y su importancia. Un concepto omnicomprensivo

Que los nombres importan es un hecho que se conoce desde antiguo[108], su valor referencial, simbólico y transformador está acreditado[109]. Los conceptos jurídicos no se generan al azar y requieren de un proceso de consolidación hasta "ganarse" un nombre[110]. En el caso de la denominación "protección de datos", es el fruto del específico desarrollo que ha tenido en Europa[111], y es especialmente deudora de sus orígenes normativos.

La legislación no solo ha sido el origen del derecho, también le ha dado nombre. En efecto, la *Datenschutz*[112] del Land de Hesse (1970) fue la primera ley de protección de datos y el nombre de esta norma marcó el rumbo que acabarían siguiendo, tarde o temprano, el resto de normativas sobre la materia. Puede parecer una cuestión menor, pero, a veces, el llegar primero es una garantía de éxito[113], aunque puedan aparecer a posteriori

---

[108] Sobre la importancia de los nombres y su variabilidad escribió Platón hace años una obra en la que, mediante diálogos, como el que a continuación se transcribe entre Cratilo y Sócrates, se ponía de manifiesto la complejidad de la denominación de las cosas: «CRATILO. — Según mi opinión, Sócrates, su virtud y efecto son los de enseñar, y de una manera absoluta se puede decir que cuando uno sabe los nombres, sabe también las cosas
[…]
SÓCRATES. — ¿Y se confundirá también con ella el descubrimiento de lo que es? Al descubrir los nombres, ¿habrá uno descubierto también los objetos designados por los nombres? ¿O bien hay que hacer de otra manera la investigación y el descubrimiento […]?» (Platón, 1991, p. 548).

[109] Para un análisis de la fuerza vinculante de los nombres y su valor referencial y cognoscitivo, vid. (Vicario, 2004). En realidad, esa condición performativa no es exclusiva de los nombres, sino que es una característica del lenguaje, en tanto «representación con efectos» (Butler, 2004, p. 24) de la realidad.

[110] Por este motivo resulta tan compleja la traducción/traslación de términos y figuras jurídicas de unos países a otros (Bestué Salinas, 2009). Sobre la formación de los lenguajes técnicos o especializados y, en concreto, sobre el español jurídico, (E. Alcaraz y Hughes, 2002).

[111] Por ejemplo, en Estados Unidos, el término que lo acapara todo, de un modo incluso más intenso que en Europa es el de *privacy*. La terminología empleada es consecuencia de la cultura jurídica del país en que despliega sus efectos.

[112] Sobre porqué se utilizó *Datenschutz* para nombrar a la primera ley, así como su uso por la doctrina alemana los meses previos y posteriores a su aprobación, vid. (Pascual Huerta, 2016, pp. 223-225).

[113] Es lo que se ha denominado la «ventaja del pionero», habitual en el mundo de las empresas tecnológicas, sobre lo que supone llegar primero, los riesgos y ventajas, vid. (Usero Sánchez y Fernández, 2006), en el que además se analiza un sector específico para ilustrar todos estos efectos.

mejores y más apropiadas opciones[114] (el sector tecnológico es un buen reflejo de ello; su condición de pioneros ayuda a explicar, en parte, el éxito de productos como Windows, Google, Youtube o WhatsApp).

Sea por los efectos derivados de ser la nomenclatura empleada en esa primera norma, sea por su fuerza expresiva, no cabe duda que el término "protección de datos" ha hecho fortuna, pese a sus «*fails to indicate the central interests served by the norms to which it is meant to apply*» (Bygrave, 2010, p. 168). En el imaginario colectivo[115], y también desde una perspectiva jurídica, se ha asentado como el término de referencia.

Ciertamente, no hay una correlación lineal entre el sentido literal del nombre y la función real del derecho: se protegen intereses personales, y para ello se salvaguardan los datos[116]. Sin embargo, sea por el factor nominal, sea por su origen, sea por la suma de ambos, lo cierto es que "protección de datos" se ha convertido en un término "atrapalotodo".

Que un único vocablo sirva para designar diversas realidades, generales y amplias (en este caso, cualquier aspecto en que medie el uso de datos e, incluso, en su versión extrema y casi desvirtuada, cualquier cuestión vinculada a la informática y al entorno digital), es un problema de comunicación, pero también de identificación jurídica.

El poder de atracción del término protección de datos y su amplitud conceptual dificultan la delimitación de la(s) realidad(es) jurídica(s) que abarca. Con razón se ha dicho de él que es como un «agujero negro que lo

---

[114] A pesar de existir normativas con títulos mucho más descriptivos, precisos y acomodados a la realidad que se estaba regulando. Serían los casos de la Ley Federal alemana de 1977, la Ley para la protección del mal uso de los datos personales a través de su tratamiento. *Gesetz zum Schutz von Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG), vom 27 Januar 1977. BGBl.*, 1.*Februar* 1977, *Teil I*, Nr. 7, S. 201-213; la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Finalmente, la ley de Mecklemburgo-Pomerania Occidental: Ley para la protección de los ciudadanos en el tratamiento de sus datos. *Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz - DSG M-V) Vom 28. März 2002*), cuyo nombre resultaba muy atinado, aunque, al tratarse de una ley de 2002, ya no tenía muchas posibilidades de revertir el proceso de consolidación del término "protección de datos" como denominación de referencia.

[115] El otro gran concepto que ha hecho fama y fortuna en la era digital es el de "privacidad", sobre los problemas de la utilización de este término en el ámbito europeo, me he pronunciado en (Jove, 2020).

[116] En esta línea apunta Adsuara Varela, al señalar que **«**lo que se protege, en realidad, no son los datos, sino las relaciones o asociaciones de esos datos con personas concretas, identificadas o identificables […] la forma de proteger estos es justamente disociando esos datos de esas personas, para proteger su identidad**»** (Adsuara Varela, 2018, p. 168).

absorbe todo y no deja escapar nada de su entorno» (Córdoba Castroverde y Díez-Picazo Giménez, 2016, p. 109)[117]. Esa fuerza expansiva del derecho le ha imbuido de un halo de "omnicompetencia" que le permitiría, incluso, reparar la afectación de otros derechos.

Así, Rodotà ha señalado que los derechos a la intimidad o la privacidad no serían más que «las diversas caras de una categoría que puede considerarse unitariamente y reconducirse, por tanto, a ese general derecho a la tutela de los datos personalizados» (Rodotà, 2014, p. 295). En una línea similar, aunque menos taxativa, se ha pronunciado Rallo Lombarte quien apunta que «la fuerza expansiva […] de este novísimo derecho permite […] reafirmar que la protección, hoy, de la privacidad tiene sus principales manifestaciones en la garantía efectiva del derecho a la protección de datos frente al fenómeno tecnológico que mayor impacto tiene en los usos sociales» (Rallo Lombarte, 2018, p. 158).

Sin embargo, por más que pueda resultar sugerente la reduccionista idea de un derecho omnicomprensivo de privacidad llamado "protección de datos personales", lo cierto es que tan extenso derecho nunca ofrecería una protección adecuada a muchas de las manifestaciones del derecho a la vida privada o a la intimidad[118]. Si esto es así respecto de los bienes jurídicos más emparentados con la protección de datos, tanto más para los otros derechos fundamentales potencialmente afectados por el tratamiento de la información personal (libertad ideológica, libertad religiosa, derecho a la salud, etc.)[119].

5.2. El art. 6 del TUE y el art. 52 de la CDFUE como fundamentos interpretativos del art. 8 de la CDFUE

Conocer los criterios y el modo en que se ha de interpretar el contenido y alcance del art. 8 de la CDFUE constituye una excelente base a partir de la que determinar la naturaleza real del derecho en él reconocido,

[117] En los mismos términos lo ha adjetivado Martínez Martínez, en (Martínez Martínez, 2019a).

[118] La necesidad de mantener «una esfera de actividad personal protegida contra la injerencia de todo poder externo» (Bobbio, 1991, p. 44) no se ha desvanecido.

[119] Todos ellos, incluida la intimidad que pudiera ser el más afectado, tienen ámbitos de protección más allá del tratamiento de la información. Así, la intimidad corporal o la familiar tienen plena vigencia. Sobre el rol de la intimidad en la sociedad actual y sus diversos ámbitos de actuación, vid. (Carrillo, 2016).

especialmente por la singular posición de los derechos fundamentales en la normativa europea[120].

La compresión de la naturaleza del artículo 8 de la CDFUE requiere la toma en consideración del ordenamiento en que se integra, amén de los matices que la jurisprudencia del TJUE aporta. En este sentido, el art. 6.1 del TUE establece que «los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones».

Esto es, la CDFUE cuenta con su propio canon interpretativo, el Título VII. En él se abordan, el ámbito de aplicación de los derechos (art. 51)[121], el nivel de protección que proporciona la CDFUE y su coexistencia con otros textos normativos (art. 53)[122], la prohibición de abuso del derecho (art. 54)[123] y, lo que más interesa a efectos de acotar el contenido del derecho a la protección de datos, el alcance e interpretación de los derechos reconocidos en la CDFUE (art. 52).

El artículo 52 de la CDFUE abarca toda una serie de criterios interpretativos y de desarrollo de los derechos en ella previstos. El

---

120 «*In the EU context, the idiom fundamental rights usually refers to the rights protected by EU law* […]. *EU law is very attached to the idiom "fundamental freedoms", which has traditionally alluded in EU law to the basic freedoms of the common market: the free movement of goods, persons, services and capital. EU law has never provided a general definition of fundamental rights. Their current recognition is profoundly indebted to their historical unearthing by the European Court of Justice*» (González Fuster, 2014, p. 166).

121 Sobre el art. 51 de la CDFUE, su aplicación por la jurisprudencia e interpretación de la misma, así como los efectos que este precepto ha supuesto en cuanto a la vinculación de los Estados miembros a los derechos fundamentales reconocidos en la CDFUE, vid. (Rodríguez-Izquierdo Serrano, 2020). La autora califica considera que la relación entre los Estados miembros y los derechos reconocidos en la CDFUE es un tanto ambigua, oscilando entre una mayor adhesión y el límite que supone el ámbito competencial europeo. Está siendo el TJUE quien, caso a caso, está perfilando la cuestión.

122 En cuanto al alcance del art. 53 de la CDFUE y sus implicaciones para la relación entre las tradiciones nacionales, coincido con Carmona Contreras en que la coexistencia de ambas anida en la razón de ser del precepto, que la relación no se debe encauzar por la vía del mayor estándar de protección, so pena de vaciar de contenido la primacía del derecho de la UE, así como la necesidad de distinguir entre aquellas situaciones en las que existe normativa europea vinculante, de aquellas otras en las que esto no es así, vid. (Carmona Contreras, 2020).

123 Las características de este precepto, de sus convergencias y divergencias con el art. 17 del CEDH y el 30 de la DUDH, sus limitaciones aplicativas, derivadas de la particular posición de la CDFUE, «que no tiene aplicación autónoma sino solo en la medida en que la UE ejerce una competencia atribuida» (Petit de Gabriel, 2020, p. 262), son tratadas de manera extensa por la citada autora. Sobre la jurisprudencia del TJUE respecto de este precepto, es muy recomendable el análisis de Azpitarte, en (Azpitarte, 2019).

apartado primero establece los requisitos que ha de cumplir cualquier limitación de los derechos de la Carta: previsión legal, respeto del contenido esencial y del principio de proporcionalidad[124].

El apartado segundo del artículo 52 CDFUE apunta la necesidad de acompasar el contenido de los derechos a los límites fijados por los Tratados. En el caso del derecho a la protección de datos, el parámetro de referencia se encuentra en el art. 16 del TFUE[125], aunque en dicho precepto no se establezca límite o condición alguna que altere lo ya previsto en la CDFUE. Del tenor literal de ambos preceptos se constata que existe un correlato absoluto entre el artículo del TFUE y la CDFUE. El art. 16.1 del TFUE reconoce, en los mismos términos que el 8.1 de la CDFUE, el derecho de toda persona a la protección de sus datos, e incorpora un apartado segundo en el que encomienda al Parlamento y al Consejo la conformación de un sistema normativo que garantice este derecho cuando el tratamiento sea llevado a cabo «por las instituciones, órganos y organismos de la Unión» (art. 16.2 TFUE).

Este encargo específico podría sugerir la eventual configuración del derecho a la protección como un mandato de optimización, sin embargo, el TFUE no incorpora aditamento alguno. Lo que sí hace es incidir en la exigencia de una garantía institucional para velar por el cumplimiento de las previsiones adoptadas.

El apartado tercero del art. 52 señala al CEDH como parámetro mínimo de protección[126]. Sin negar su importancia orientativa, amén de su evidente valor interpretativo, no puede soslayarse que, en la medida en que la UE no es parte del CEDH, «el mandato de interpretación conforme [es]

---

[124] El modo de articular el art. 52 de la CDFUE le diferencia del CEDH. En él, algunos artículos han incorporado cláusulas de restricción específicas(los arts. 8, 9, 10 y 11), incluido el art. referente al derecho a la vida privada. No obstante, como ha señalado Redondo Saceda, la presencia de este tipo de cláusulas no supone una jerarquización de los derechos del CEDH, ni implica que el resto de derechos no estén sometidos a limitaciones y condicionantes aplicativos (Redondo Saceda, 2021).

[125] El art. 16 del TFUE constituye, junto al art. 8 de la CDFUE, las bases constitucionales del derecho a la protección de datos en la UE.

[126] Art. 52.3 CDFUE: «En la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio.

Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa».

Aunque es parte interesada, el TEDH reconoció tempranamente que, «*the Charter recognises the Convention as establishing the minimum human rights standars*», en la STEDH, Bosphorus Airways c. Irlanda, de 30 de junio de 2005, apdo. 159.

un acto de voluntad en manos del TJUE» (Álvarez-Ossorio Micheo, 2020, p. 102). Este margen de actuación es consustancial a la particular relación del Tribunal de Luxemburgo con el CEDH[127], al menos hasta que se materialice la adhesión prevista en el 6.2 del TUE[128].

Por otra parte, en la medida en que la CDFUE establece un reconocimiento singularizado del derecho a la protección de datos, desligándolo –al menos desde un punto de vista sistemático– del derecho a la vida privada, resulta razonable plantear hasta qué punto es trasladable la doctrina del TEDH sobre el art. 8 del CEDH, al contenido del derecho a la protección de los datos del art. 8 de la CDFUE. En esta línea argumental, la relación de equivalencias de las Explicaciones sobre la Carta de los Derechos Fundamentales[129] solo incluye al art. 7 de la CDFUE como trasunto del artículo 8 del CEDH. Se refuerza, así, la particular condición del derecho a la protección de los datos personales previsto en el artículo 8 de la Carta[130]. El TJUE ha apostillado esta interpretación, pronunciándose en el mismo sentido[131].

En consecuencia, la traslación por equivalencia entre el CEDH –y la jurisprudencia del TEDH– y la CDFUE –y la jurisprudencia del TJUE– no debería ser automática, no al menos por defecto, pues la singularidad de la normativa europea justifica la existencia de divergencias interpretativas. Por otra parte, debido a su mayor especialización y concreción, es probable

---

[127] La posición adoptada por el TJUE en relación con el CEDH tiene en el Dictamen 2/2013 del Tribunal de Justicia (Pleno), de 18 de diciembre de 2014, su plasmación más directa. Puede consultarse en: https://curia.europa.eu/juris/document/document.jsf?docid=160882&doclang=ES. Sobre el Dictamen, sus consecuencias, vid. (Fernández Rozas, 2015) o (Martín y Pérez de Nanclares, 2015).

[128] Art. 6.2 TUE: «La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados».
Sobre las consecuencias de la unión al CEDH y la relación entre el TJUE y el TEDH, vid., entre otros, (Martín y Pérez de Nanclares, 2014); (Alonso García, 2015); (Martinón Quintero, 2016) o (Cortés Martín, 2018).

[129] Explicaciones sobre la Carta de los Derechos Fundamentales (2007/C 303/02) de 14 de diciembre de 2007.

[130] No obstante, en la interpretación del art. 8 de la CDFUE, las Explicaciones sí incluyen al art. 8 del CEDH como una referencia en la configuración de los postulados de la Carta. Sin embargo, en este caso, debe interpretarse como un antecedente que ha sido tomado en consideración, pues las Explicaciones señalan que el artículo 8 «se ha basado», entre otras disposiciones, en CEDH y en el Convenio 108. Es distinto ser una referencia para configurarse que tener una contenido equivalente. De ahí que después las Explicaciones no consideren el art. 8 de la CDFUE se corresponda con el 8 del CEDH.

[131] STJUE asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB, de 21 de diciembre de 2016, apdo. 129

que el derecho de la UE «conceda una protección más extensa» (art. 52.3 CDFUE), en cuyo caso el CEDH, y a la jurisprudencia del TEDH respecto del derecho a la protección de datos, operarían con un criterio de orientación hermenéutica de atención potestativa, en lugar de un estándar mínimo de obligado cumplimiento.

Por su parte, el apartado cuarto del art. 52 CDFUE sitúa a «las tradiciones constitucionales comunes» como una posible pauta interpretativa de la Carta. Su utilidad, una vez que la CDFUE ha alcanzado la misma posición jurídica que el Derecho originario, descansaría en su capacidad «para "puentear" las limitaciones a la aplicación de derechos fundamentales que incluye la propia Carta. […] [ya sea] para cubrir lagunas, actuar de bálsamo frente a las jurisdicciones nacionales ante la aplicación del principio de primacía o justificar el activismo del Tribunal cuanto éste lo necesite» (Gordillo Pérez, 2020, p. 144), por ejemplo, acudiendo a los desarrollos e innovaciones jurisprudenciales de los Estados miembros o, incluso, del TEDH.

En la misma línea, y con una función similar, se halla el apartado sexto del art. 52 CDFUE, en el que se apunta a «las legislaciones y prácticas nacionales» como elementos que también se han de considerar. El apartado quinto, por su parte, dispone que los principios contenidos en la Carta «solo podrán alegarse ante un órgano jurisdiccional en lo que se refiere a la interpretación y control de legalidad» de los actos legislativos y ejecutivos mediante los que se apliquen[132].

Por último, el apartado séptimo del artículo 52 establece que «las explicaciones elaboradas para guiar en la interpretación de la presente Carta serán tenidas debidamente en cuenta por los órganos jurisdiccionales de la Unión y de los Estados miembros». Aun siendo difícil establecer el exacto valor interpretativo de las Explicaciones sobre la Carta de los Derechos Fundamentales (en adelante, Explicaciones), es razonable considerar que «es superior al que usualmente se atribuye a los trabajos preparatorios de un tratado internacional, pero inferior al del Derecho originario» (Cruz Mantilla de los Ríos, 2020, p. 198).

[132] En el caso de las instituciones, órganos y organismos de la Unión serán actos legislativos y ejecutivos, en el caso de los Estados miembros, serán actos aplicativos del Derecho de la Unión (art. 52.5 CDFUE).

5.2.1. Las Explicaciones sobre la Carta de los Derechos Fundamentales

Las Explicaciones señalan que «la Directiva [Directiva 95/46/CE] y el Reglamento [Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y la libre circulación de esos datos] […] establecen condiciones y límites para el ejercicio del derecho a la protección de los datos de carácter personal»[133]. Según este enunciado, el contenido y límites del derecho fundamental será el previsto en el derecho derivado de la Unión, con el único condicionante de su compatibilidad con lo dispuesto en la CDFUE y los Tratados.

Sin embargo, la aportación más relevante de las Explicaciones es la aseveración de que la Directiva y el Reglamento sobre tratamiento de datos por las instituciones europeas, son el desarrollo, en exclusiva, de un único derecho, el de protección de datos del artículo 8 de la CDFUE[134]. Por lo tanto, no son la regulación normativa de diversos derechos, aunque tenga por objetivo la salvaguarda de los «derechos y libertades fundamentales» (art. 1.2 del RGPD).

En la actualidad, las disposiciones a las que aluden las Explicaciones se corresponden con el RGPD (que sustituye a la Directiva) y el Reglamento 2018/1725 (que deroga y reemplaza al Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE). En ambos casos, su Considerando 1 señala, como referencia *iusfundamental* y base normativa habilitante, al art. 16.1 del TFUE y al art. 8.1 de la CDFUE, refrendando el enfoque marcado por las Explicaciones.

Mientras el RGPD establece un marco normativo general para el tratamiento de la información personal, el Reglamento 2018/1725 diseña un sistema de protección específico para su ámbito de aplicación, el «tratamiento de datos personales por parte de todas las instituciones y organismos de la Unión» (art. 2.1), y entronca con lo dispuesto en el 16.2 del TFUE[135]. Ambos Reglamentos comparten el mismo objetivo: proteger

[133] Explicación relativa al artículo 8 – Protección de datos de carácter personal.

[134] En esa línea interpretativa parece apuntar el TJUE en el asunto Coty, al señalar que «el derecho a la protección de los datos personales […] forma parte del derecho fundamental de toda persona a la protección de los datos de carácter personal que le conciernan, como lo garantizan el artículo 8 de la Carta y la Directiva 95/46» STJUE asunto C-580/13, Coty Germany Gmbh y Stadtsparkasse Magdeburg, de 16 de julio de 2015, apdo. 30.

[135] Art. 16.2 TFUE: «El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas

«los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales» (art. 1.2 de ambos Reglamentos). Para lograrlo, establecen «normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales» (art. 1.1 de ambos Reglamentos).

Por lo tanto, cualquier análisis de la naturaleza del derecho a la protección de datos, en su configuración europea, requerirá, inexorablemente, la toma en consideración del Derecho derivado destinado a desarrollarlo y, en particular, por su mayor amplitud y alcance más general, el RGPD.

5.3. El objeto de los Reglamentos de protección de datos y la naturaleza del derecho

El objeto de los Reglamentos dedicados a disciplinar el tratamiento de datos es la protección «de los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales» (art. 1.2 del RGPD y del Reglamento 2018/1725). Si estos son la plasmación efectiva y exclusiva del derecho a la protección de datos regulado en la CDFUE, emerge una incógnita de difícil resolución: ¿cómo ha de interpretarse que el derecho a la protección de los datos personales tenga como cometido proteger el derecho a la protección de datos?

La posible existencia de un derecho del derecho plantea no pocas dudas y complejidades interpretativas. Si los Reglamentos son la plasmación exclusiva del derecho a la protección de datos, ¿por qué se enlista este como un derecho más a proteger o, acaso, se trata de dos realidades con una denominación similar y estrechamente conectadas, pero distintas?, ¿una engloba a la otra? Si la respuesta fuese afirmativa, ¿lo hace de manera completa o ese segundo derecho tiene un cierto grado de autonomía?, ¿acaso hay un único derecho a la protección de datos, incardinado en un sistema general de protección de la información

respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes».

personal?, de ser así, ¿ese sistema de protección es una consecuencia del derecho fundamental, o tiene un fundamento más amplio?

En este sentido, en el asunto Coty, el TJUE afirma que «el derecho a la protección de los datos personales, del que gozan las personas contempladas en el artículo 8, apartado 1, de la Directiva 2004/48, forma parte del derecho fundamental de toda persona a la protección de los datos de carácter personal que le conciernan, como lo garantizan el artículo 8 de la Carta y la Directiva 95/46»[136]. Con esta aserción, además de corroborar la condición de la Directiva 95/46/CE (en la actualidad el RGPD) como contenido directamente vinculado al derecho fundamental reconocido en la Carta, el Tribunal de Luxemburgo parece estar afirmando que el derecho fundamental a la protección de datos tiene, como una de sus manifestaciones, un derecho a la protección de datos. Es como si existiesen dos derechos con un mismo nombre, pero con características particularizadas.

Cabe, no obstante, una lectura diferente del pronunciamiento, conforme a la que el TJUE no estaría reconociendo la existencia de un derecho del derecho, sino realizando una afirmación acerca de la identidad entre el derecho a la protección de datos que se reconoce a las personas que actúen en el marco de la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual, y el derecho fundamental del art. 8 de la CDFUE. Es decir, estaríamos ante dos reconocimientos legales diferentes (la Directiva 2004/48/CE y la CDFUE) que, en lo relativo al tratamiento de la información personal, deben considerarse coincidentes a los solos efectos de la inclusión del primero en el mayor rango de protección del segundo.

Con todo, persisten las dudas acerca de las implicaciones jurídicas que tiene el particular objeto de las normativas que son plasmación exclusiva del derecho a la protección de datos. De una parte, parece que nos encontremos ante un derecho eminentemente instrumental, cuyo cometido es salvaguardar los bienes jurídicos del interesado frente al tratamiento de los datos personales (protección «de los derechos y

[136] STJUE asunto C-580/13, Coty Germany Gmbh y Stadtsparkasse Magdeburg, de 16 de julio de 2015, apdo. 30. La versión en inglés tampoco aclara nada respect de esta dualidad, al contrario, la reafirma: «*The right to protection of personal data, granted to the persons referred to in Article 8(1) of Directive 2004/48, is part of the fundamental right of every person to the protection of personal data concerning him, as guaranteed by Article 8 of the Charter and by Directive 95/46*».

libertades fundamentales de las personas físicas»). De otra, la exigencia de prestar una atención particularizada a la salvaguarda del «derecho a la protección de los datos personales» pudiera ser el reflejo de un derecho complejo, polidimensional. Las preguntas en torno a la naturaleza del derecho a la protección de datos se acumulan.

5.4. Interrogantes a solventar en torno a la naturaleza del art. 8 de la CDFUE

La evolución jurídica de la CDFUE, especialmente a partir del Tratado de Lisboa, refleja el peso que los derechos fundamentales han ido ganando en la UE. La regulación de la protección frente al tratamiento de la información personal también se ha transformado, al sustituir la fundamentación económica de su regulación normativa (en la Directiva), por el anclaje *iusfundamental* proporcionado por la CDFUE (art. 8) y el TFUE (art. 16) (en el RGPD).

Con este punto de partida, surgen una serie de interrogantes en torno a la condición normativa y contornos del derecho a la protección de datos, alentados por la confusa jurisprudencia del TJUE, tendente a aplicarlo en conjunción con el art. 7 CDFUE[137]. ¿Coincide el contenido del derecho a la protección de datos con el objeto de las normativas de protección de datos? o, por el contrario, la normativa tiene un objeto, en parte coincidente, pero más amplio y diverso. ¿Se ha producido una asimilación entre el contenido normativo y el *iusfundamental*, o el derecho a la protección de datos ha absorbido otras realidades que, siendo protegidas mediante la normativa encargada de disciplinar el tratamiento de datos personales, tendrían una sede de protección más apropiada en otros derechos (v. gr. intimidad/vida privada, libertad ideológica o religiosa, derecho a la salud…)?

En definitiva, ¿qué protege realmente el derecho a la protección de datos?, ¿cuál es el contenido jurídico del art. 8 de la CDFUE?, ¿es un derecho

[137] A lo largo de las diferentes opciones interpretativas de la naturaleza del derecho a la protección de datos se irá poniendo de manifiesto como la jurisprudencia del TJUE tiende a utilizar conjuntamente el art. 7 y el art. 8 de la CDUFE (v. gr. STJUE asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke GbR c. Land Hessen y Eifert v. Land Hessen y Bundesantalt fur Landwirtschaft un Ernahrung, de 9 de noviembre de 2010), pero, en ocasiones, lo aborda de manera singularizada (v. gr. ; asuntos C-293/12 y C-594/12, Digital Rights Ireland c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014). Para un estudio más detallado de esta cuestión, vid. (Lynskey, 2020, pp. 358-359).

negativo (prohibición del tratamiento como premisa) o positivo (disciplina las condiciones en que se ejerce)?, ¿el art. 8 de la CDFUE, realmente regula un derecho fundamental o, pese a la designación y ubicación sistemática[138], tiene una naturaleza jurídica diferente?

Responder a estas cuestiones resulta crucial para resolver las preguntas que motivan esta tesis, a saber: ¿es posible un concepto de dato personal diferente y más amplio que el actualmente previsto?, ¿puede prescindirse de las categorías especiales de datos, o el objeto del derecho a la protección de datos las hace imprescindibles?

6. El artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea

El artículo 8 de la CDFUE no define qué es el derecho a la protección de datos, no, al menos, en todos sus extremos. En su apartado primero, establece que «toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan». Es decir, el centro de imputación del derecho son los datos personales, y su satisfacción se lograría asegurando su salvaguarda.

Si la CDFUE (y el TFUE) se limitasen a realizar la proclamación contenida en el apartado 1 del art. 8 CDFUE, la naturaleza, sentido y alcance del derecho fundamental a la protección de datos en su concepción europea dependería, en gran medida, del desarrollo normativo que hubiese seguido el derecho, así como de las precisiones y delimitaciones que la jurisprudencia realizase. Sin embargo, la base constitucional del derecho a la protección de datos no se agota en el apartado primero. Los apartados 2 y 3 del artículo 8 vienen a concretar y precisar su contenido y alcance.

[138] El derecho a la protección de datos está ubicado en el Título II de la CDFUE, intitulado Libertades. Además, el art. 8 de la CDFUE consagra, expresamente, el «derecho», evitando otras fórmulas de expresión más ambiguas o amplias.

6.1. El apartado segundo del art. 8 CDFUE. Las vertientes objetiva[139] y subjetiva[140] del derecho

«Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación» (art. 8.2 CDFUE).

En el precepto que preside este apartado se aglutinan un conjunto variado de obligaciones y derechos que dan forma al contenido del derecho a la protección de datos. Si bien cada una de las actuaciones que en él se prevén goza de individualidad, desde un punto de vista funcional es posible clasificarlas en dos grupos. El primero, reflejo de su vertiente objetiva, estaría integrado por las exigencias de actuación previstas en la primera parte del enunciado (tratamiento leal, finalidad concreta y base de legitimación). Al segundo grupo pertenecerían los derechos enunciados en la parte final del apartado segundo del artículo 8 de la CDFUE (acceso y rectificación), dando forma a la vertiente subjetiva del derecho.

6.1.1. Las condiciones de ejercicio como contenido del derecho

Las medidas enunciadas en la primera parte del apartado 2 del artículo 8 de la CDFUE establecen las condiciones básicas para que el tratamiento de la información personal sea compatible con el derecho a la protección de datos. Ese conjunto de previsiones revela el carácter procedimental del derecho, pues no buscan prohibir o permitir una determinada acción, sino asegurar que esta se lleve a cabo de un modo determinado. Para ello, el precepto establece una serie de actuaciones de obligado acatamiento. No son pautas o guías para la actuación, sino

---

[139] Por contenido objetivo se entenderá, «el mandato de optimización de la libertad individual (o colectiva) protegida en cada concreto derecho fundamental mediante un permiso o una prohibición. […] [Este] mandato posee una doble faz. De un lado, impone a todo aquel que ejerza poder público el deber positivo de proteger los derechos fundamentales que puedan verse afectados […]. De otro lado, le impone el deber de abstenerse de todo acto contrario a ese deber positivo de protección» (Bastida Freijedo et al., 2004. p. 94).

[140] Por contenido subjetivo se entenderá, «el haz de facultades jurídicas atribuidas al titular del derecho para defender el objeto del derecho fundamental frente a terceros. […] a través de […] [ellas] exige la observancia de los deberes de abstención o de acción, según el caso, que pesan sobre el Estado o los particulares». (Bastida Freijedo et al., 2004, p. 94).

requisitos *sine qua non*, cuya ausencia o elusión comporta la vulneración del derecho.

Así, la CDFUE disciplina: cómo han de realizarse los tratamientos («de modo leal»), para qué («fines concretos») y con qué fundamento (consentimiento u otra base legalmente prevista).

Desde el punto de vista de su contenido, no puede dejar de constatarse la identidad entre las exigencias del art. 8.2 CDFUE y algunos de los principios relativos al tratamiento de datos reconocidos en el RGPD (art. 5)[141] y en el Reglamento 2018/1725 (art. 4)[142]. Nada hay de sorprendente en el hecho de que la normativa encargada de desarrollar el derecho a la protección de datos incluya y concrete las exigencias establecidas en la CDFUE.

Más llamativo resulta, sin embargo, la denominación que el derecho derivado ha dado a ese conjunto de obligaciones. Al referirse a ellas como principios podría pensarse que, jurídicamente, se ha rebajado su nivel de exigencia normativa. Nada más lejos de la realidad. Un análisis detenido del papel que los principios desempeñan en los Reglamentos sobre tratamiento de datos permite constatar que, pese a su *nomen iurirs*, no operan como meras orientaciones al legislador, sino que «son fórmulas de derecho fuertemente condensadas que[, al formar parte del contenido de un derecho fundamental,] albergan gérmenes de reglas. En todo caso, los principios relativos al tratamiento, por su conexión a un derecho fundamental, tienen un carácter dogmático-axiológico» (Troncoso Reigada, 2021b, p. 851)[143].

[141] Así, en el RGPD, el tratamiento leal se correspondería con el principio de igual nombre reconocido en el art. 5.1.a); el tratamiento para fines específicos se correspondería con el principio previsto en el art. 5.1.b) y el tratamiento sobre la base del consentimiento u otra legalmente prevista con el principio de licitud del 5.1.a) complementado y concretado con lo previsto en el art. 6.

[142] En el caso del Reglamento 2018/1725, el tratamiento leal se correspondería con el principio de igual nombre reconocido en el art. 4.1.a); el tratamiento para fines específicos se correspondería con el principio previsto en el art. 4.1.b) y el tratamiento sobre la base del consentimiento u otra legalmente prevista con el principio de licitud del 4.1.a) complementado y concretado con lo previsto en el art. 5.

[143] Prueba de ello es que la vulneración de los principios se califica en el RGPD como una conculcación muy grave del derecho y, por consiguiente, lleva aparejadas las sanciones con las multas de mayor cuantía. Las multas por incumplimiento de lo dispuesto en el art. 5 del RGPD serán «de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía» (83.5 RGPD).

Pese a tan equívoco nombre, son el alma del modelo de protección de datos europeo y constituyen un límite para los desarrollos legislativos posteriores. Razón por la que las eventuales restricciones o exenciones a las que pretendan someterse siempre han de estar expresamente previstas en la norma, ser proporcionadas, perseguir una finalidad legítima y ser necesarias en una sociedad democrática (Considerando 73 RGPD). Una afirmación concordante con lo dispuesto en el art. 52.1 de la CDFUE para la limitación en el ejercicio de los derechos. Nos encontramos, pues, ante obligaciones jurídicas que forman parte del contenido del derecho fundamental a la protección de datos.

Solo motivos históricos y la inercia del legislador explican que se sigan denominando "principios". Como se recordará, uno de los grandes hitos en la configuración originaria de la protección frente al tratamiento de la información personal son los *Fair Information Practices* estadounidenses, consolidados en Europa merced al Convenio 108 de 1981, en el que se adoptó, en cierto modo, ese modelo principialista[144]. Con el tiempo, los principios fueron ganando en sustantividad y obligatoriedad hasta alcanzar su actual posición jurídica. Sin embargo, aunque su realidad ha evolucionado en el modelo europeo, hasta convertirlos en piezas constitutivas de un derecho fundamental, la fuerza de la costumbre les mantuvo el nombre.

6.1.2. Lealtad, finalidad y licitud del tratamiento[145]

Los «datos se tratarán de modo leal». Así comienza el apartado 2 del art. 8 CDFUD. En su versión en inglés, se utiliza el término «*processed fairly*» lo que sugiere la idea de razonabilidad, claridad y ausencia de mala fe en el tratamiento. La lealtad a que se refiere el precepto tiene, por tanto, una semántica propia.

Las características del principio de lealtad («*fairness*»[146] en la versión en inglés) enunciado en los Reglamentos así lo corrobora. El principio exige que «*only handle personal data in ways that people would*

[144] Vid. Capítulo II del Convenio 108, en especial el art. 5.
[145] Se ha realizado un análisis más detallado de estos elementos en el Cap. III, al estudiar los principios del RGPD. Consecuentemente, en este apartado solo se identificarán los elementos que permiten caracterizar el derecho fundamental.
[146] Sobre el rol de este principio en la efectividad del derecho, vid. (Kasirzadeh y Clifford, 2021).

reasonably expect»[147], lo que significa que el «responsable solo trataría datos de forma que no pueda generar un efecto negativo o injustificado respecto de los titulares de dichos datos» (Palma Ortigosa, 2018b, p. 43).

La lealtad o razonabilidad en el tratamiento enmarca jurídicamente la relación entre las partes. Que los datos deban ser tratados de forma «leal» implica actuar con un nivel mínimo de rigor, esto es, con un estándar básico de confiabilidad en el que han de valorarse los posibles efectos negativos del tratamiento, evitándolos, o minorándolos, en aras de lograr la menor afectación posible.

Los «datos se tratarán […] para fines concretos» (art. 8.2 CDFUE), la limitación del tratamiento a finalidades específicas y previamente determinadas persigue la consecución de una serie de objetivos concurrentes: asegurar que el tratamiento obedezca a razones justificadas y legítimas; y hacerlo previsible.

La limitación a la finalidad es una condición necesaria para el despliegue efectivo del derecho: si los tratamientos no se acomodasen a las finalidades previstas y conocidas por el interesado, supondría, en última instancia, privarle de cualquier posible control sobre la información a él referida. Gracias a ese conocimiento previo, es factible determinar si la finalidad perseguida justifica las eventuales afectaciones de bienes jurídicos que pudieran producirse –este criterio también resulta útil a la hora de enjuiciar la viabilidad de los tratamientos–.

Los «datos se tratarán […] sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley» (art. 8.2 CDFUE).

Con este aserto, la CDFUE establece la premisa de partida de toda operación en la que se vayan a utilizar datos personales. Los tratamientos deben contar con un fundamento jurídico que los justifique, en caso contrario, se produciría una injerencia inasumible en el derecho a la protección de datos. De este modo, se vincula la naturaleza del derecho a las condiciones para su ejercicio, reforzando su condición procedimental.

[147] *Guide to the General Data Protection Regulation (GDPR)* elaborada por el ICO. Puede consultarse la sección referente a este principio en: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/.

Que la CDFUE mencione de manera expresa al consentimiento no es casualidad. Esta base de legitimación está en el origen mismo de la concepción del derecho a la protección de datos como manifestación de la autodeterminación informativa. Así, las primeras configuraciones jurisprudenciales del derecho a la protección de datos situaban al consentimiento como un elemento nuclear del derecho[148].

Que el consentimiento, esto es, «la manifestación de voluntad, expresa o tácita, por la que un sujeto se vincula jurídicamente»[149], se situase en el centro de un derecho que tiene en la autodeterminación personal su razón de ser resulta plenamente coherente, por ser la manifestación más elocuente de la voluntad y dominio del sujeto respecto de su proyección exterior.

No obstante, las evoluciones acaecidas en el procesamiento de la información, la multiplicidad de formas en que los datos personales son recabados y utilizados en el día a día, el modo en que las tecnologías basadas en su uso se han inserido, de manera inescindible, en la vida de las personas, han puesto en cuestión el valor del consentimiento como fundamento del tratamiento de la información (Schermer, Custers, y van der Hof, 2014)[150].

Como hemos visto en el Capítulo I, la tecnología basada en datos se ha integrado en el devenir diario de la ciudadanía, hoy se vive, en parte, en la Red y, en ella, los datos son moneda de cambio habitual. En consecuencia, el consumidor-usuario no siempre estará en la mejor condición para prestar un consentimiento informado y válido, bien porque la información

---

148 Sirva como ejemplo el FJ 7 de la STC 292/2000, FJ 7, en el que el TC establece que: los «poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos».

149 Diccionario panhispánico del español jurídico, segunda acepción de consentimiento. Vid. en: https://dpej.rae.es/lema/consentimiento

150 Para Bergemann el consentimiento no se ha debilitado, de hecho, considera que sigue siendo omnipresente. Frente a la ubicuidad del consentimiento, y tratando de paliar los problemas que presenta, apunta a la necesidad de ahondar en una configuración del derecho a la protección de datos «*as a critique of power necessitates us to make clear how power and data processing relate to each other, what are the risks associated with it, and consequently, what should be the ends and means of data protection*» (Bergemann, 2017, p. 128).

proporcionada sea inabarcable[151], bien porque ciertos servicios han convertido al consentimiento en un acto casi debido; y a su condición de manifestación de la autodeterminación personal, en un mito (Koops, 2014, pp. 251-253)[152].

Cuando, quien ha de consentir se encuentra en la disyuntiva de elegir entre vivir en sociedad o quedar excluido de una parte significativa de la misma, no puede decirse que exista una situación de igualdad entre las partes, o que el consentimiento sea una auténtica manifestación de voluntad (Bashir, Hayes, Lambert, y Kesan, 2015)[153]. En ocasiones, el

---

[151] La amplitud de las políticas de privacidad, el modo en que se presentan, dificultan una lectura comprensiva de las mismas, y abocan a evitar su lectura, pues los tiempos requeridos para su asimilación serían demasiado elevados (p. ej. las políticas de privacidad de Facebook o Google, sin contar la información en segundo plano [que también es relevante], superan las 5000 palabras. Multipliquemos el tiempo que se requeriría por el de cada web a la que se accede, cada servicio, cada app), debido a su inabarcable extensión, se ha generado un efecto desaliento evidente que ha llevado a que el tiempo medio que las personas dedican a la lectura de tales políticas gire en torno al minuto. Es decir, las políticas de privacidad no se leen y su aceptación es «*the biggest lie on the Internet*» (Obar y Oeldorf-Hirsch, 2020). Para un estudio sobre las razones por las que se tienden a ignorar las políticas de privacidad, vid. (Rudolph, Feth, y Polst, 2018).
A las barreras del tiempo habría que añadir el grado de dificultad de alguna de ellas, así, el New York Times, después de analizar 150 políticas de privacidad, puso de manifiesto que, a pesar de los esfuerzos del RGPD por fomentar la claridad y la accesibilidad de la información que se transmite, algunas seguían teniendo el mismo nivel de dificultad de comprensión de lectura que la *Crítica de la Razón Pura* de Inmanuel Kant. Puede consultarse el reportaje en: (Litman-Navarro, 2019).
Con todo, se ha comprobado que, el modo en que se presenta la información podría revertir esta situación, especialmente en aquellos casos que se distribuye por capas y, al menos los elementos básicos son fácilmente identificables (Steinfeld, 2016). También contribuiría a reforzar la posición del interesado a la hora de ejercitar el consentimiento, y de revocarlo, una mayor transparencia por parte de los responsables de los tratamientos (Drozd y Kirrane, 2020).

[152] A paliar este problema está dedicada, además del RGPD, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Con todo, el arsenal normativo destinado a hacer del entorno digital un medio más seguro para sus usuarios se verá notablemente incrementado y mejorado con el Reglamento del Parlamento y el Consejo sobre el Mercado Único de Servicios Digitales (Reglamento de Servicios Digitales) y enmienda da la Directiva 2000/31/EC (puede consultarse en: https://eur-lex.europa.eu/legal-content/es/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN). Así como con la sustitución de la Directiva 2002/58/CE por el Reglamento e-privacy, puede consultarse la propuesta en la que se está trabajando en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010.

[153] La prueba más evidente de la resignación de los usuarios a ver sus datos utilizados a cambio de poder utilizar determinados servicios es que, en cuanto se les ofreció la posibilidad de mantener los servicios sin tener que "pagar" con sus datos, el 96% optaron por dicha opción, esto es, allí donde realmente pudieron decidir acerca del destino y uso de su información personal, la apuesta por la reserva prevaleció. El 96% ese el porcentaje de

consentimiento no es una proyección de la autodeterminación personal, esto es, no siempre es «el momento e instrumento del gobierno de uno mismo» (Rodotà, 2014, p. 260).

Precisamente porque el consentimiento puede generar una falsa apariencia de dominio de la situación por parte del interesado, esta figura se ha ido devaluando. Las normativas actuales de protección de datos así lo reflejan. Para evitar que el consentimiento se convierta en «*a dystopian stick to control citizens*» (Morrow, 2019), se han implementado toda una serie de medidas destinadas a complementarlo y reforzarlo. Se han ido precisando las condiciones en que su manifestación se considera válida[154] (v. gr. art. 7 RGPD); se han detallado los deberes de información, reforzándolos con la obligación de transparencia (arts. 12 a 14 del RGPD); se han removido los obstáculos para su retirada, haciendo que sea igual de fácil que la prestación (art. 7.3 RGPD), amén de ajustar las exigencias en función de las circunstancias, ya sea por la naturaleza de los datos tratados (art. 9.2.a) RGPD)[155], por el sujeto que lo presta (art. 8 RGPD, referido al consentimiento de menores[156]) o por las particularidades del contexto en que se otorga (v. gr. el consentimiento prestado en el marco de una prestación de servicios (art. 7.4 RGPD)[157]). Además, en algunas legislaciones nacionales se ha excluido, para determinados casos, al consentimiento como condición habilitante válida. Por ejemplo, en España,

usuarios de IOS optaron por no permitir que las aplicaciones les rastreasen, vid. (Wituschek, 2021).

154 Sobre los modos de prestación del consentimiento, exigencias y tipos, resultan de especial utilidad las Directrices del EDPB, pueden consultarse en: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_es.

155 Si bien es cierto que en el caso del consentimiento explícito del 9.2.a) lo que se produce es un incremento de las exigencias de la base de una base de legitimación, debe advertirse, que en general, las exigencias del artículo 9.2, esto es, los supuestos que han de concurrir para poder enervar la prohibición de tratar datos especiales no excluyen la exigencia de una base de legitimación, sino que la complementan, son requisitos adicionales.

156 A efectos del RGPD se considera como menor a aquellos que tengan menos de 16 años. Con todo, esta edad puede verse minorada, pues se deja margen a los estados miembros para establecer la edad de los menores entre los 13 y los 16 (art. 8.1 RGPD). Puede consultarse la edad que cada Estado miembro ha fijado en: (Milkaite y Lievens, 2019).
Sobre el consentimiento de menores de edad, vid. (Presano, 2020), (Arenas Ramiro, 2019a), (Volosevici, 2019), (Brito Izquierdo, 2018) o (Rodríguez Ayuso, 2020, pp. 1004-1008). Para un análisis de las previsiones específicas previstas en la normativa española, vid. (Aba Catoira, 2020a) o (De las Heras Vives y De Verda y Beamonte, 2019).

157 Sobre las características de este consentimiento «sin condicionalidad», vid. (García Pérez, 2020, p. 894).

el consentimiento explícito no es condición suficiente para el tratamiento de ciertas tipologías de datos especiales[158].

Junto al conjunto de actuaciones llevadas a efecto sobre el consentimiento, se han establecido una serie de opciones alternativas al mismo, capaces de proporcionar licitud al tratamiento, con el mismo nivel de legitimidad. El art. 6 RGPD[159] es la materialización de las mismas, dando contenido a la previsión del 8.2 de la CDFUE[160].

El consentimiento no ha perdido toda su virtualidad, sigue jugando un papel relevante, pero ya no ocupa una posición singularizada. En este sentido, se puede decir que la autodeterminación personal se ha actualizado, ampliado y objetivado. Desde el punto de vista de la morfología del derecho, este cambio de paradigma ha supuesto que el consentimiento, otrora fundamento inexcusable, hoy sea solo una de las opciones posibles.

Señala la CDFUE que, junto al consentimiento, los datos podrán tratarse «en virtud otro fundamento legítimo previsto por la ley». La concreción de esas otras bases de legitimación del tratamiento obliga a fijar la vista en el RGPD. De manera específica, ha de atenderse al principio de licitud (art. 5.1 RGPD) y a las condiciones para la ejecución del tratamiento previstas en el art. 6 del RGPD.

El punto de partida es el principio de licitud, conforme al que se exigen que los datos personales sean «tratados de manera lícita». El RGPD regula el principio de licitud en el art. 5.1.a), junto a los principios de lealtad y transparencia[161]. Este principio implica que todo tratamiento de datos ha de estar sustentado jurídicamente por, al menos, una base de legitimación

---

[158] El art. 9.1 LOPDGDD establece que, «el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico». La Ley portuguesa de Protección de datos, *Lei* 58/2019, de 8 de agosto de 2019, establece, en su artículo 17, una previsión similar respecto del consentimiento prestado en el marco de una relación laboral, no obstante, apunta un par de situaciones en las que se consideraría válido el consentimiento:
«a) *Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador; ou*
b) *Se esse tratamento estiver abrangido pelo disposto na alínea b) do n.º 1 do artigo 6.º do RGPD*»

[159] Bases de licitud del tratamiento: consentimiento, ejecución de un contrato, cumplimiento de una obligación legal, protección de intereses vitales, misiones realizadas en interés público e interés legítimo (art. 6.1 RGPD)

[160] Además del consentimiento, el 8.2 de la CDFUE señala que se podrán tratar datos personales «en virtud de otro fundamento legítimo previsto por la ley».

[161] Para un análisis más detallado del principio de licitud, vid. (Puente Escobar, 2019, pp. 117-151) o (Berrocal Lanzarot, 2019, pp. 87-150).

(Considerando 40 RGPD)[162]. El RGPD establece, exclusivamente, seis (art. 6 RGPD)[163], a saber: consentimiento, contrato, obligación legal, protección de intereses vitales, misión realizada en interés público o ejercitando poderes públicos y, finalmente, la concurrencia de algún interés legítimo del responsable o de un tercero que prevalezca sobre los intereses del interesado[164].

Las bases de legitimación están vinculadas al contexto, a las circunstancias específicas del tratamiento y, en última instancia, al criterio del legislador que las fijó. Algunas varían su nivel de exigencia en atención a las condiciones, a los sujetos que intervengan en el tratamiento o a la naturaleza de los datos en concurso. Sería el caso del consentimiento, como ya se ha indicado, pero también otras, como la protección de intereses vitales, que se ve reforzada cuando los datos a tratar pertenecen a las categorías especiales[165].

Con todo, es en el interés legítimo[166] donde la importancia de tomar en consideración el contexto y la realidad concreta del tratamiento se manifiestan de manera más evidente. Las circunstancias del tratamiento, la ponderación de intereses en conflicto o la adecuación de las garantías son inherentes a esta base de legitimación[167]. No es que las condiciones del

[162] La concurrencia de una base de legitimación es una condición general de licitud de los tratamientos. Vid. SSTJUE asuntos acumulados C-465/00, C-138/01 y C-139/01, Rechnungshof contra Österreichischer Rundfunk y otros y Christa Neukomm y Joseph Lauermann contra Österreichischer Rundfunk, 20 de mayo de 2003, apdo. 65; STJUE asunto C-524/06, Heinz Huber contra Bundesrepublik Deutschland [GS], 16 de diciembre de 2008, apdo. 48; STJUE asuntos acumulados C-468/10 y C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado, 24 de noviembre de 2011, apdo. 26.

[163] Por su claridad y grado de detalle en el análisis del alcance, límites, casos más relevantes, implicaciones y problemáticas en la utilización de cada una de las bases de legitimación, son especialmente recomendables los trabajos de (Gil González y de Hert, 2019) y (Kotschy, 2020b).

[164] En el caso del Reglamento 2018/1725 se excluye el interés legítimo como base habilitante. Acaso por considerar que, al ser tratamientos llevados a cabo por parte de las instituciones, órganos y organismos de la Unión no es una base de legitimación adecuada o necesaria. Lo que resulta coherente, en la medida en que pueden canalizar sus actuaciones bien a través de la existencia de un interés público o de una potestad pública.

[165] En el caso de la protección de los intereses vitales, la diferencia es sustancial, pues solo será operativa para el tratamiento de datos especiales en aquellos casos en que «el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento» (art. 9.2.c) RGPD).

[166] Sobre esta base de legitimación, además de las referencias y elementos apuntados a lo largo de esta tesis, vid. (Niedermeier y Mpame, 2019).

[167] La guía más actualizada y, desde un punto de vista práctico, mejor pensada, es la que ofrece la autoridad británica de protección de datos, la Information Commisioner's Office (ICO), puede consultarse en: https://ico.org.uk/for-organisations/guide-to-data-

tratamiento modulen la posibilidad de llevarlo a cabo, es que son su premisa. Si no se realiza esa valoración previa, este título habilitante no es aplicable[168].

En su conceptualización europea, cualquiera que sea el tratamiento, ha de contar con una cláusula habilitante que lo justifique y asegure su licitud, además, merced a las exigencias de tratamiento leal y para fines concretos, la persona titular del derecho siempre tendrá la información disponible para saber el destino de las informaciones a ella referidas.

6.1.3. Acceso y rectificación. La vertiente subjetiva del derecho

Del conjunto de facultades que las normativas de protección de datos reconocen a los interesados, solo dos, los derechos de acceso y rectificación están expresamente reconocidos en la CDFUE[169]. ¿Qué caracteriza a estos derechos? ¿Qué nos dicen estos elementos concretos de la naturaleza del derecho a la protección de datos?

La CDFUE proclama que «toda persona tiene derecho a acceder a los datos recogidos que le conciernan» (art. 8.2). Este derecho resulta crucial en el tratamiento de la información personal al posibilitar que, en cualquier momento, se pueda conocer el destino y usos de la misma, además, de ser la puerta al ejercicio de otros derechos[170]. En efecto, para poder emprender acciones concretas sobre los datos personales que están siendo objeto de tratamiento, primero hay que saber, a ciencia cierta, qué datos específicos

protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/. Por otra parte, si bien con una aproximación más doctrina, resulta clarificador el análisis de (Fernández-Samaniego y Fernández-Longoria, 2019).

[168] Sirva como ejemplo de la importancia de realizar las valoraciones pertinentes el asunto resuelto por la AEPD en el procedimiento sancionador PS/00070/2020. En él, la autoridad española ha tenido ocasión de resolver un supuesto en el que el interés legítimo no se justificaba convenientemente por parte de un alcalde que publicó íntegramente en Facebook una sentencia referida a su ayuntamiento y a un empleado del mismo. Puede consultarse en: https://www.aepd.es/es/documento/ps-00070-2020.pdf.

[169] El RGPD reconoce los derechos de: acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y el derecho a no ser objeto de decisiones individuales automatizadas (artículos 15 a 18 y 20 a 22). Con todo, si atendemos a la Directiva, por ser la normativa en vigor en el momento de adoptarse la CDFUE, vemos que derechos como el de oposición (art. 14) o el no sometimiento a decisiones automatizadas (art. 15) no fueron incluidos en la CDFUE, lo que no deja de ser un elemento reseñable. Con esa decisión se pone en valor a los que están y, a la vez, al no estar todos, se está indicando que lo relevante es lo que subyace y tienen en común todos ellos, el poder de control y disposición.

[170] STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017, apdo. 57

están siendo tratados. Solo con esa información resultará viable ejecutar las actuaciones más acordes a los intereses que se pretendan salvaguardar.

Desde el punto de vista de su ejercicio, el derecho de acceso, resulta muy revelador de la naturaleza del derecho a la protección de datos. No precisa de ningún tipo de detonante o condición justificativa, no es un derecho reactivo, la mera voluntad del interesado de saber si los datos a él referidos están siendo objeto de tratamiento, por quién y en qué condiciones, es suficiente para activarlo. Es la actuación, junto al consentimiento, en la que mejor se refleja la función de autodeterminación informativa que caracteriza al derecho a la protección de datos.

La otra facultad de actuación reconocida en la CDFUE es el derecho de rectificación (art. 8.2). El ejercicio de este derecho posibilita al interesado «obtener sin dilación indebida del responsable la rectificación de los datos personales inexactos que le conciernan» (art. 16 RGPD)[171]. Este derecho habilita a instar la corrección aquellas informaciones erróneas o inexactas que estén siendo objeto de tratamiento.

Con él se pretenden evitar los efectos nocivos que pudiera tener el tratamiento de datos incorrectos. En congruencia con dicho objetivo, el derecho de rectificación posibilita tanto la corrección de lo erróneo, como la opción de completar el conjunto de informaciones necesarias para lograr los fines del tratamiento[172].

La posibilidad de rectificar conecta directamente con la idea de dominio sobre la proyección exterior del ser, así como con el vínculo dato-persona. En efecto, en tanto los datos son el reflejo de la realidad personal del individuo, resulta plenamente coherente que se disponga de un mecanismo jurídico mediante el que asegurar la coincidencia entre la representación simbólica (los datos) y el original (la persona). El derecho de rectificación se presenta como la herramienta mediante la que el individuo puede lograr la adecuación entre información y realidad.

[171] Para una exégesis más completa y detallada de este derecho, vid. (Pascual Huerta, 2021b) y (De Terwangne, 2020).
[172] El RGPD permite completar la información «inclusive mediante una declaración adicional» (art. 16 RGPD).

6.2. El apartado tercero del artículo 8 de la CDFUE. La garantía institucional

La concepción europea del derecho a la protección de datos exige la existencia de autoridades de control independientes (art. 8.3 CDFUE[173]) encargadas de velar por la protección de «los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento […] y libre circulación de datos personales» (art. 51.1 RGPD). Es la expresión técnica del contenido objetivo de este derecho fundamental[174], manifestada en la exigencia de establecer una garantía institucional.

Las autoridades de control son una exigencia directa del derecho a la protección de datos, forman parte del contenido legalmente indisponible[175]. No estamos, pues, ante un órgano cuya creación dependa de la voluntad política, ni ante un simple mecanismo adicional de garantía. Se trata de una pieza clave para la satisfacción del derecho a la protección de datos. A él corresponde, como expresión de la dimensión preventiva del derecho, controlar el «respeto de las normas» (art. 8.3 CDFUE) destinadas a disciplinar el tratamiento de la información personal.

El rol que las autoridades de control (que no meros órganos o unidades administrativas) desempeñan en el modelo de protección de datos[176] suministra algunas pistas acerca del proceso de europeización del derecho a la protección de datos[177], de su contenido y de su relación con otros derechos fundamentales. En efecto, la función de las autoridades de control[178] no se circunscribe a asegurar el cumplimiento del derecho a la

---

173 Artículo 8.3 CDFUE: «El respeto de estas normas quedará sujeto al control de una autoridad independiente».

174 Conforme a la conceptualización de las garantías institucionales establecida en (Bastida Freijedo et al., 2004, p. 94).

175 STJUE asunto C-518/07, Comisión v. Alemania, de 9 de marzo de 2010, apdo. 25 o STJUE asunto C-614/10, Comision Europea c. Austria, de 16 de octubre de 2012, apdo. 36.

176 Acerca del sistema de autoridades de control europeo, el rol del *European Data Protection Board*, su relación con el Supervisor Europeo y con las diferentes autoridades de protección de datos de los estados miembros, vid. (Lynskey, 2017, pp. 4-21).

177 Como apunta Lynskey, el papel que el RGPD otorga al *European Data Protection Board* (EDPB) es un reflejo de la europeización del derecho a la protección de datos. La capacidad del EDPB, merced a su potestad para emitir decisiones vinculantes, le ha convertido en la agencia de gobernanza en la protección frente al tratamiento de la información personal. Ha hecho que la estructura institucional de garantía se haya vuelto más vertical, reforzando la concepción europea del derecho, vid. (Lynskey, 2017).

178 Sobre las funciones de las autoridades de control, la importancia de su condición independiente, vid. (Aperribai Ulacia, 2021) y (Fernández Scagliusi, 2018). En el primer trabajo destaca la importancia de la cooperación y coordinación entre las diferentes autoridades de control europeas para lograr una interpretación armonizada de la normativa. En el segundo es de especial interés el análisis de las funciones que las autoridades de control

protección de datos, sino debe «proteger los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento y […] la libre circulación de datos personales» (art. 51.1 RGPD). «Para garantizar esa protección, las autoridades nacionales de control han de lograr un justo equilibrio entre el respeto del derecho fundamental a la vida privada y los intereses que exigen la libre circulación de datos personales»[179].

Como Rodotà ha puesto de manifiesto, el apartado tercero del artículo 8 es la culminación de la evolución en la protección del libre desarrollo personal y la dignidad frente al uso de la información personal. Con él se supera la protección estrictamente individual de los intereses personales, para convertirlos en una cuestión de responsabilidad social, en la que habrá una autoridad pública encargada de velar, permanentemente, por el respeto a los bienes jurídicos de la persona en relación con el tratamiento de sus datos (Rodotà, 2009, p. 80).

Por lo tanto, la garantía institucional que las autoridades de control representan es la manifestación más acabada derecho a la protección de datos; al imponer una vigilancia constante para el cumplimiento del conjunto de normas destinado a generar el caldo de cultivo necesario para asegurar la efectividad del derecho.

Por otra parte, si nos atenemos a los fines perseguidos, especialmente a la alusión al «respeto de estas normas» (art. 8.3 CDFUE), se constata la importancia del desarrollo normativo en la garantía del derecho de toda persona «a la protección de los datos de carácter personal que la conciernan» (art. 8.1 CDFUE). Parece evidente que, el derecho a la protección de datos, requiere de un alto nivel de colaboración del legislador para su efectiva realización.

tienen encomendadas, así como los poderes de que disponen para su materialización (pp. 235-240).

[179] STJUE asunto C-362/14, Maximillian Schrems y Data Protection Commissioner, 6 de octubre de 2015, apdo. 42.

7. Las posiciones negadoras de la fundamentalidad y autonomía del derecho a la protección de datos

7.1. La no fundamentalidad como punto de partida. Dos propuestas a considerar

El reconocimiento en la CDFUE del derecho a la protección de datos como derecho fundamental autónomo podría haber conjurado cualquier cuestionamiento acerca de su estatus jurídico, quedando solo por concretar su objeto y finalidad. Sin embargo, no faltan autores que ponen en duda la fundamentalidad y autonomía de este derecho.

Bart van der Sloot (Van der Sloot, 2017), considera que el derecho a la protección de datos encaja mejor con la condición de derecho del consumidor y que sus normativas de desarrollo «*are more akin to market regulation than to traditional human rights instruments*» (Van der Sloot, 2017, p. 28). Por su parte, Ralf Poscher (Poscher, 2017) considera que el derecho a la protección de datos es «*a mere modulation of other fundamental rights*» (Poscher, 2017, p. 136).

Estos planteamientos no persiguen reactivar el inveterado debate acerca de la condición del derecho a la protección de datos como una faceta más del derecho a la vida privada y/o la intimidad[180], sino que niegan su *iusfundamentalidad* a partir del análisis de las características del propio derecho.

Las dos propuestas "negacionistas" comparten un punto de partida similar, la puesta en cuestión del reconocimiento formal del derecho a la protección de datos como derecho fundamental. Además, ambas se centran en el objeto que el derecho a la protección de datos disciplina, sin los apriorismos de su configuración normativa. Con ese punto de partida común, emprenden caminos diferentes para alcanzar una misma conclusión, la condición de derecho fundamental autónomo no se compadece con la realidad material del derecho a la protección de datos.

[180] Sobre el proceso de diferenciación entre vida privada y protección de datos me remito al recorrido histórico presentado en el Capítulo II de esta tesis y las referencias allí citadas. Además de lo comentado en este mismo Capítulo acerca de la oscilante y poco clara jurisprudencia del TJUE respecto de la vida privada y la protección de datos.

7.2. No es un derecho fundamental, es una regulación de mercado

Bart van der Sloot se interroga acerca de las implicaciones de la calificación de un derecho como fundamental, y cuestiona el encaje en ella del derecho a la protección de datos. Con el *iter* seguido por este derecho como telón de fondo (su desvinculación del derecho a la intimidad, el constante aumento de atribuciones y el refuerzo en su estatus hasta su reconocimiento como derecho fundamental autónomo, amén del desarrollo mediante reglamentos directamente aplicables), el autor analiza si sus características se corresponden con la naturaleza que la CDFUE le atribuye.

A tal fin, realiza, en primer lugar, una exégesis de los posibles significados e implicaciones de la categoría derechos fundamentales en el marco normativo europeo[181], incidiendo en la ausencia de una definición clara de lo que implica esta condición en el derecho de la UE. Tras descartar la asimilación a los derechos constitucionales, concluye que bajo «*the term "fundamental rights" is used in European Union (EU) to express the concept of "human rights" within a specific EU internal context.* […] [*Its role would be to provide*] *protection to values that have a special moral status and protecting particularly weighty interests for individuals and society at large*» (Van der Sloot, 2017, p. 31). Por tanto, la entidad del bien jurídico protegido sería, para van der Sloot, el elemento determinante de la condición de derecho fundamental.

Al negar la *iusfundamentalidad* del derecho a la protección de datos, le otorga un valor menor a su objeto, situándolo en un estatus inferior en la escala de valores socio-jurídicos. Para él, es un interés digno de salvaguardar, pero no con la misma dimensión que otros derechos fundamentales, como la libertad de expresión, el secreto de las comunicaciones, la tutela judicial efectiva o el derecho a la vida.

---

[181] Van der Sloot se cuestiona acerca de las implicaciones del reconocimiento de esa condición fundamental a los derechos reconocidos en la Carta. No se trata, por tanto, de una consideración general de qué son los derechos fundamentales, sino de las implicaciones en el ámbito europeo.
Como es conocido, el término derechos fundamentales, «*droits fondamentaux*, aparece en Francia hacia el año 1770» (Pérez Luño, 2004, p. 29), y sería «el constitucionalismo *iusracionalista* norteamericano del siglo XVIII, al incluirlos primero en las Constituciones de los Estados recién independizados y, más tarde, en la Constitución de 1787 (tras su reforma en 1791)» (Bastida Freijedo et al., 2004, p. 21) el encargado de darles reconocimiento normativo.

Van der Sloot reconoce que existen ciertos ámbitos en los que, por la transcendencia de su objeto, la calificación *iusfundamental* podría llegar a ser adecuada para el derecho a la protección de datos. Sería el caso del tratamiento de los datos sensibles o de algunos de los casos resueltos por el TJUE, como serían los asuntos Digital Rights Ireland y Schrems, en los que se dilucidan ámbitos generales de protección y modos de entender la salvaguarda de los datos personales.

Pero, frente a esos supuestos posibles, existiría un conjunto amplio de normas y situaciones que no se avienen con la proyección típica de un derecho fundamental, «*because they protect more ordinary interests*» (Van der Sloot, 2017, p. 21). A estos efectos, plantea una serie de supuestos en los que la vulneración de la normativa de protección de datos no parece estar en condiciones de generar una afectación de los valores esenciales que anidan en la proclamación de un derecho fundamental (v. gr. utilizar el nombre y la dirección de una persona sin informarla debidamente, o no mantener una base de datos debidamente actualizada).

En definitiva, al no tener término medio y dar cobertura tanto a valores esenciales como a otros que no lo serían, el derecho a la protección de datos no justificaría suficientemente su condición *iusfundamental*. Atribuirle dicha naturaleza supondría un desvalorizar la categoría a la que se pretende incorporar, pues equipararía los bienes jurídicos de mayor transcendencia con cuestiones de menor calado y enjundia (Van der Sloot, 2017, p. 26).

Como refuerzo de su convicción, subraya la particular dualidad que caracteriza a las normativas de protección de datos, cuya finalidad sería «*to protect two quite opposite values, namely the interests of individuals to protect their personal data on the one hand and the interests of data controllers to process their data within the internal market of the EU on the other hand. Thus, data protection rules must be seen as already providing a compromise between the rights and interests of different parties*» (Van der Sloot, 2017, p. 21).

Vinculado con esa condición bifronte, estima que el artículo 8 de la CDFUE no se limita a reconocer un derecho, sino que lo regula con un nivel de detalle que lo diferencia del resto de bienes jurídicos salvaguardados por la CDFUE. Así, mientras al resto de derechos se les aplicarían las cláusulas de limitación e interpretación del art. 52 CDFUE, en el caso del derecho a la protección de datos, ya se «*specifies when and how personal*

data can be legitimately processed. Again, not only does a general limitation clause apply to Article 8 of the Charter, the fundamental right to data protection is in itself already a compromise between different legitimate interests».

Para van der Sloot, la clave para determinar la naturaleza del derecho radica en su finalidad y en la de las normativas que lo desarrollan. En concreto, considera que la protección de datos es «*a consumer right instead of a fundamental human right*» (Van der Sloot, 2017, p. 24). Los motivos que subyacen a esta afirmación son, en primer lugar, que la función principal del derecho a la protección de datos es establecer las condiciones y salvaguardas para el ejercicio de una actividad necesaria para el mercado (el tratamiento de la información y su aprovechamiento económico). En segundo lugar, las normativas que desarrollan al derecho se caracterizan por (1) una clara finalidad armonizadora, cuando «*the classic goal of human rights is not to harmonize national legislations, but to provide an absolute minimum level of protection*» (Van der Sloot, 2017, p. 24); (2) un elevado nivel de detalle de las regulaciones, de una extensión y minuciosidad no equiparables a las de ningún otro derecho fundamental; y (3) el conjunto de funciones asignadas a las autoridades de control, van mucho más allá de la mera garantía institucional de un derecho. Todos estos aspectos justificarían considerar a los reglamentos de desarrollo del derecho como una «*market regulation* […] [*and the right to*] *data protection as an ordinary consumer right*» (Van der Sloot, 2017, p. 28).

7.3. Un modulador de otros derechos

Ralf Poscher plantea la duda acerca de cuál es la libertad que se pretende salvaguardar con el derecho a la protección de datos para, desde ahí, tratar de establecer un marco relacional entre Europa y Estados Unidos en esta materia[182]. Su necesidad de respuestas obedece a una razón práctica: es necesario saber qué se invoca para poder conformar un punto de encuentro con una tradición jurídica tan diferente como la estadounidense. Si se quiere evitar un diálogo hacia lo absurdo, los

[182] El trabajo de Poscher se incardina en una obra destinada a analizar los problemas en el tratamiento de la información entre Europa y Estados Unidos, especialmente en materia de seguridad.

europeos deben estar en condiciones de explicar de qué hablan cuando hablan de la protección de datos como un derecho fundamental.

A esa duda, Poscher responde con rotundidad: «*the right to data protection is not a specific right at all. Rather, it is a systematic modal enhancement of potentially every other fundamental right*» (Poscher, 2017, p. 133). En concreto, el derecho a la protección de datos tendría como finalidad proveer «*a preemptive protection against abstract dangers that accompany the collection, storage, and processing of personal data*» (Poscher, 2017, p. 133). Expresado de otro modo, este derecho aportaría un plus de garantía, lo que Lynskey identificó como el «*added-value*» (Lynskey, 2014) de la protección de datos, frente a la protección dispensada por la conceptualización de la vida privada regulada en el CEDH[183].

Para Poscher, el derecho a la protección de datos no podría ser independiente (y por tanto no sería fundamental), pues su existencia estaría inexorablemente unida a la del derecho fundamental –cualquier derecho– que, en cada caso, modulase, potenciase o reforzase.

En apoyo de su teoría, el autor aduce una serie de evidencias que vendrían a confirmar la condición simbiótica del derecho a la protección de datos. En primer lugar, apunta la muy escasa comparecencia en solitario de este derecho en la jurisprudencia del TJUE[184], pues, en la amplísima mayoría de asuntos, concurre con otros derechos, singularmente con la vida privada[185], pero también otros[186]. En concreto, Poscher se remite a las

[183] No obstante, a diferencia de Poscher, Lynskey considera que el refuerzo de la autodeterminación informativa y la reducción de los riesgos de discriminación y asimetrías derivadas del mayor control que ofrece el derecho a la protección de datos justificarían su condición de derecho fundamental autónomo.

[184] Esta realidad no resulta extraña si se toma en consideración que la mayor parte de supuestos resueltos por el TJUE en el momento en que Poscher elabora su artículo están vinculados a la aplicación de la Directiva, que tenía por objeto «la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales» (art. 1 de la Directiva). No obstante, en las sentencias posteriores al RGPD, sigue observándose esa afectación conjunta del derecho a la protección de datos y otros derechos. Por ejemplo, en la STJUE asunto C-311/18, Facebook Ireland & Maximillian Schrems, de 16 de julio de 2020, el tratamiento de los datos personales no solo afecta al derecho a la vida privada del art. 7, sino, también a la tutela judicial efectiva.

[185] También resalta que esta particularidad ocurre en la jurisprudencia del TEDH y del TCFA. No obstante, a los efectos que aquí interesan, se trata de determinar la naturaleza del derecho fundamental en su configuración europea (de la UE).

[186] En el asunto Bavarian Lager la controversia giró en torno a los derechos a la protección de datos y la libertad de información, STJUE asunto C-28/08, Bavarian Lager, de 29 de junio de 2010.

diversas posibilidades de afectación derivadas del tratamiento de información personal que Solove ha identificado (autonomía personal, dignidad, libertad de expresión, intimidad, libertad de asociación, libertad ideológica o discriminación por afectación de las categorías sospechosas)[187].

Este enfoque también sirve a Poscher para explicar por qué suele asociarse al derecho a la protección de datos con el derecho a la vida privada o con una «*general freedom*». En la medida en que no todo tratamiento de datos implica un daño potencial directo sobre un derecho específico, la eventual afectación del derecho a la vida privada o del libre desarrollo de la personalidad serviría «[*as*] *a kind of subsidiary function in the context of data collection*» (Poscher, 2017, p. 136). Esto es, se ha tendido a vincular al derecho a la protección de datos con la vida privada o con el libre desarrollo de la personalidad[188] porque, en general, son los usualmente afectados y, además, en ciertos tratamientos, son las únicas realidades jurídicas que podrían verse vulneradas.

Una vez establecido que el derecho a la protección de datos opera como complemento al servicio de los demás derechos, Poscher se pregunta acerca de qué clase de refuerzo proporciona, esto es, cuál es el objetivo último de su existencia. Para el autor, la función del derecho a la protección de datos sería hacer frente a los «*concrete but also abstract dangers that are involved with the collection and storage of personal data*» (Poscher, 2017, p. 137). Así considerado, el derecho a la protección de datos sería un derecho preventivo, cuyo cumplimiento exige «*a justification for the collection of personal data even if such misuse is only an abstract danger*» (Poscher, 2017, p. 137).

En definitiva, la protección de datos implicaría la existencia de unas condiciones a partir de las cuales se consideraría aceptable el tratamiento de la información personal. Desde el punto de vista jurídico, esto supone la

---

En el asunto Digital Rights Ireland se llegó a plantear (sin llegar el TJUE a resolverlo) la eventual afectación del derecho a la libertad de expresión, a raíz del modo en que se operaba con la información, vid. STJUE, asuntos C-293/12 y C-594/12, asunto Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014.

[187] Poscher menciona en exclusiva el artículo de Solove «"I've Got Nothing to Hide" and Other Misunderstandings of Privacy» (Solove, 2007), no obstante, sobre el contenido y alcance de la *privacy* en relación con el tratamiento de datos, Solove se ha pronunciado en diversos artículos, siendo los dos más detallados en la descripción de la fisonomía de la *privacy*: (Solove, 2002) y (Solove, 2006).

[188] Rodotà señalaría que la protección de datos es «*an essential tool to freely develop one's personality*» (Rodotà, 2009, p. 80).

necesidad de establecer un sistema que permita evaluar el peligro abstracto derivado del tratamiento de datos, así como el contexto en que se produce. Poscher propone la creación de umbrales, tanto para identificar aquellos tratamientos que suponen un riesgo inasumible, como para valorar la efectividad de las actuaciones destinadas minorar el riesgo en aquellos que sí pueden llevarse a cabo (transparencia, el diseño de medidas de seguridad y su fiabilidad o la existencia de sistemas de supervisión independientes) (Poscher, 2017, pp. 138-139).

7.4. Enseñanzas e inconcreciones de las propuestas "negacionistas"

Las opciones interpretativas "negacionistas" abordan la posible naturaleza del derecho a la protección de datos partiendo del marco protector configurado por las normativas que lo desarrollan. Tanto la interpretación de Poscher, como la de van der Sloot, aportan argumentos que resultan acordes a las condiciones del sistema de salvaguarda frente al tratamiento de la información personal, y contribuyen a perfilar las singularidades del derecho a la protección de datos. Sin embargo, al no considerar su vertiente subjetiva, al no profundizar en la razón de ser de las facultades de actuación de los individuos ante al uso de los datos a ellos referidos (v. gr. acceso, rectificación, supresión, oposición, limitación o portabilidad), fallan en la determinación de la naturaleza real del derecho reconocido en el artículo 8 de la CDFUE.

Las tesis analizadas no consideran que la proyección personal, y los derechos de actuación de ella derivados, tengan la entidad (van der Sloot) o la autonomía (Poscher) suficientes como para hacer del derecho a la protección de datos un derecho fundamental. Sin embargo, el «poder de disposición y de control»[189] sobre la información a uno referida que esas facultades de actuación representan no es una condición baladí, por más que, por su finalidad, se aplique a asuntos de todo tipo, también a los de menor enjundia.

Cualquiera que sea la entidad del supuesto, esas facultades de actuación coinciden con la proyección de lo que el TCFA definió en 1983 como autodeterminación informativa («Jurisprudencia Constitucional Extranjera, Núm. 33, IV», 1984). Ese vínculo con la dignidad, la libertad y la

[189] Atinada descripción del TC español al caracterizar el derecho a la protección de datos, STC 292/2000, de 30 de noviembre de 2000, FJ 7.

autodeterminación personal justificaría la *iusfundamentalidad* de derecho reconocido en el art. 8 de la CDFUE. La condición de derecho fundamental implica que el bien jurídico protegido es la «proyección positiva, inmediata y vital» de la persona (Solozabal Echavarria, 2020, p. 26). En el caso del derecho a la protección de datos, esta realidad se materializa en el dominio la identidad, esto es, en el poder para «decidir […] sobre la difusión y la utilización de sus datos personales»[190].

En todo caso, la valoración de la transcendencia de los actos disciplinados, así como su afectación de los valores de la sociedad, no deja de ser una cuestión eminentemente subjetiva, respecto de la que el legislador europeo se ha posicionado de manera clara: en la UE, el derecho a la protección de datos es un bien jurídico fundamental. La importancia de esa decisión político-normativa no puede desconocerse y, ante la duda, ese debe ser el criterio decisivo.

Los negacionistas parten de una concepción material y, por tanto, subjetiva de lo que sea derecho fundamental, obviando que el proceso de juridificación es el que produce su carácter *iusfundamental*[191]. La protección de datos es fundamental porque así lo dice la Carta y porque el legislador no puede disponer enteramente de él, ni siquiera, como es el caso, cuando tenga una muy amplia capacidad de intervención.

El reconocimiento positivo de un determinado estatus jurídico no es una decisión inane. La condición *iusfundamental* les dota de «un sentido más preciso y estricto, ya que […] describen el conjunto de derechos y libertades jurídica e institucionalmente reconocidas y garantizadas por el Derecho positivo. Se trata, por tanto, de derechos delimitados espacial y temporalmente, cuya denominación responde a su carácter básico o fundamentador del sistema jurídico político» (Pérez Luño, 2004, p. 47).

Ítem más, la capacidad de actuación respecto de la información a uno referida no está inexorablemente unida a la afectación de otros derechos y libertades (como defiende Poscher), sino que puede aducirse de manera

[190] Puede consultarse la sentencia en, («Jurisprudencia Constitucional Extranjera, Núm. 33, IV», 1984). En cuanto al análisis e implicaciones de la misma, me remito a lo señalado en el Capítulo segundo y en los trabajos allí citados.

[191] Los derechos fundamentales no lo son en función de consideraciones histórico-éticas o ponderaciones subjetivas acerca de qué derechos son más o menos relevantes. Existen derechos muy relevantes en el seno de la UE o de los estados –como el de la libre competencia– que no son fundamentales y otros (como pudiera ser el derecho de petición) que paradójicamente siguen siendo fundamentales pese a su escasa transcendencia (al menos en España).

independiente, pues su condición de activación es la utilización de información personal. Por ejemplo, se puede ejercitar el derecho de acceso frente al responsable del tratamiento sin necesidad de que exista otro derecho fundamental afectado (o susceptible de serlo) al que apelar, basta con que se trate de datos a uno referidos. La vinculación entre sujeto e información es la que da fundamento al poder de control y disposición. Naturalmente, esa capacidad de actuación no es absoluta[192], pero su autonomía y fortaleza no pueden desconocerse o rebajarse.

En efecto, si el derecho a la protección de datos fuese un mero instrumento mediante el que responder ante la afectación cierta de los bienes de la personalidad, estaríamos en presencia de un derecho sin una finalidad propia, pues para esa función reactiva ya existen en el ordenamiento jurídico otros remedios más eficaces y directos: los derechos efectivamente vulnerados (v. gr. el derecho al honor, a la intimidad, la libertad ideológica, la igualdad o el derecho concretamente vulnerado) y su cuadro de garantías.

Por otra parte, por más que la regulación del tratamiento de los datos personales tenga un innegable impacto en el mercado, aunque en muchas ocasiones los interesados actúen como si fueran consumidores, ello no debería llevar a considerar que la normativa de protección de datos es una regulación de mercado más. Es cierto que, en ocasiones, las normativas de protección de los consumidores y las de protección de datos llegan a coincidir en sus postulados y objetivos, pero existen discrepancias en cuestiones tan relevantes como la finalidad perseguida, el modo de entender y configurar el consentimiento, o la importancia que se otorga a las obligaciones de los consumidores. En definitiva, las regulaciones del mercado y la normativa de protección de datos se complementan, pero no son lo mismo (Helberger y Reyna, 2017).

Finalmente, ninguno de los dos autores aborda las implicaciones derivadas del objeto de los dos Reglamentos que desarrollan el derecho (RGPD y Reglamento 2018/1725), a saber, proteger «los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales» (art. 1.2 de ambos

[192] STJUE asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke GbR c. Land Hessen y Eifert c. Land Hessen y Bundesantalt fur Landwirtschaft un Ernahrung, de 9 de noviembre de 2010, apdo. 48. En la línea ya apuntada, años antes por STJUE asunto C-112/00, Eugen Schmidberger, Internationale Transporte und Planzüge y Republik Österreich, de12 de junio de 2003, apdo. 80. El Considerando 4 del RGPD también se pronuncia en idénticos términos.

Reglamentos). No afrontan[193] que, el desarrollo regulatorio del derecho a la protección de datos, tiene entre sus cometidos proteger el derecho a la protección de datos. En efecto, no enfrentan las consecuencias de esa previsión auto-protectora, ni se plantean cual puede ser la razón por la que las normativas relativas al tratamiento de la información personal modularían y protegerían un derecho cuya fundamentalidad y autonomía niegan.

Suponiendo que la regulación general no tenga la condición de derecho fundamental, como ellos defienden, ¿podría tenerla ese derecho a la protección de datos mencionado en el art. 1.2 de los Reglamentos (especialmente cuando se enlista junto a «los derechos y libertades fundamentales», como uno más)? De ser así, ¿cuál sería el contenido de ese derecho? Los postulados "negacionistas" no dan respuesta a estas cuestiones, dando como resultado una explicación insatisfactoria respecto de la naturaleza real del derecho a la protección de datos y, consecuentemente, de las posibilidades de actuación y modificación que cabrían en su ámbito de protección.

Pese a las críticas planteadas, no pueden dejar de apreciarse las valiosas aportaciones que las tesis analizadas realizan a la caracterización del derecho. Así, dejan patente el vínculo existente entre el derecho a la protección de datos y el resto de derechos y libertades fundamentales, ya sea por proporcionarles un refuerzo anticipado, ya por asegurar su salvaguarda a la vez que se habilita el aprovechamiento económico de la información personal. Estrechamente vinculado con esto último, está la puesta en valor de la normativa de desarrollo, no solo por ser la proyección del derecho, sino por establecer el marco regulatorio que hace jurídicamente aceptable el tratamiento de los datos personales. Una actividad, por lo demás, esencial para la consolidación del mercado interior.

Con todo, sigue siendo preciso determinar el objeto del derecho regulado en el art. 8 de la CDFUE. ¿Es un derecho eminentemente subjetivo o es un derecho de configuración legal? ¿Es un derecho preventivo o reactivo? ¿El art. 8 de la CDFUE establece una prohibición del tratamiento,

[193] En el caso de van der Sloot, es una oportunidad perdida, pues llega a traer a colación la afirmación del TJUE en el asunto Coty, en la que el Tribunal de Luxemburgo señala «el derecho a la protección de los datos personales […] forma parte del derecho fundamental de toda persona a la protección de los datos de carácter personal que le conciernan, como lo garantizan el artículo 8 de la Carta y la Directiva 95/46». STJUE asunto C-580/13, Coty Germany Gmbh y Stadtsparkasse Magdeburg, de 16 de julio de 2015, apdo. 30.

con excepciones (apartados 2 y 3) o, desde la aceptación de la inevitabilidad del tratamiento, disciplina cómo debe ejercitarse? ¿Cuál sería la finalidad de ese derecho?

8. La caracterización del derecho a la protección de datos. La oscilante jurisprudencia del TJUE

8.1. El TJUE. Un clarificador de contenidos

El derecho a la protección de datos encontró en los tribunales la mejor vía de entrada en los ordenamientos jurídicos de algunos países[194]. No fue ese, sin embargo, el caso de la Unión Europea. Ahora bien, esta circunstancia no empaña el destacado rol desempeñado por el TJUE como agente dinamizador del derecho a la protección de datos. Sentencia a sentencia, el tribunal de Luxemburgo ha ido perfilando y (re)creando ese derecho, proyectándolo sobre nuevas realidades, definiendo sus límites y asentando los conceptos básicos que lo definen.

Desde los conocidos casos Osterreichischer Rundfunk y Lindqvist[195], el bagaje jurisprudencial del TJUE es abrumador, rico en matices y de volumen creciente[196]. Junto a sus pronunciamientos más mediáticos y relevantes[197] (Digital Rights Ireland[198], Google c. AEPD[199] o la saga

[194] Sobre esta cuestión, además de lo señalado en el Capítulo II, vid. (Ruiz Miguel, 2003, p. 40).

[195] SSTJUE asuntos acumulados C-465/00, C-138/01 y C-139/01, Rechnungshof c. Osterreichischer Rundfunk, de 20 de mayo de 2003 y asunto C-101/01, Lindqvist, 6 de noviembre de 2003. Como jurisprudencia precedente, podría mencionarse, por ser la primera en la que hay una resolución en la que se toma en consideración la vida privada, el asunto C-29/69, Erich Stauder v City of Ulm, de 12 de noviembre de 1969.

[196] Como queda patente en el proyecto GDPRhub, en el que se recopilan todos los pronunciamientos vinculados al RGPD llevados a cabo tanto por el TJUE, como por tribunales y autoridades de control nacionales. Puede consultarse esta completa recopilación, que se actualiza día a día, en: https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub.

[197] RALLO LOMBARTE realiza un análisis detallado de tres de esos pronunciamientos, sus precedentes y sus efectos en (Rallo Lombarte, 2017b).

[198] STJUE asuntos C-293/12 y C-594/12, Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014. Esta sentencia supuso la anulación de la Directiva 24/2006/CE. Sobre ella, vid. (Granger y Irion, 2014) y (López Aguilar, 2017).

[199] STJUE asunto C-131/12, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014. Por la que se reconoce definitivamente el derecho al olvido. Sobre esta sentencia, existe abundante bibliografía, a título meramente ejemplificativo, vid. (Rallo Lombarte y Díaz Díaz, 2014); (Minero Alejandre, 2014); (Rallo Lombarte, 2014) en el que, además de la sentencia del TJUE,

Schrems[200]), se encuentra todo un conjunto de resoluciones que complementan –y completan– las previsiones normativas. Sin ellas, sería imposible comprender la realidad del derecho a la protección de datos personales en el seno de la UE[201].

El TJUE ha precisado el alcance de conceptos tan nucleares como tratamiento[202], dato personal[203], interés legítimo[204], responsable del tratamiento[205] y corresponsable[206]; ha consagrado[207] y delimitado facultades de actuación[208]; remarcado el carácter ineludible de la exigencia de un nivel de protección equivalente[209] en las transferencias de datos a terceros países[210]; reafirmado el papel de las autoridades de control como

analiza todos los pronunciamientos previos de la AEPD que, desde 2007 venían generando la base doctrinal para el reconocimiento del derecho al olvido; en la misma línea de reconocimiento de las aportaciones de la AEPD a la conformación del derecho al olvido (Simón Castellano, 2015); (Azurmendi, 2015) o (Trinidad, 2018).

200 STJUE, Asunto C-362/14, Maximillian Schrems y Data Protection Commissioner, 6 de octubre de 2015 y STJUE asunto C-311/18, Facebook Ireland & Maximillian Schrems, de 16 de julio de 2020.

201 Como pone de manifiesto la detallada exégesis jurisprudencial realizada por Martínez Alarcón respecto de las múltiples resoluciones dictadas por el TJUE con relación al derecho a la protección de datos (Martínez Alarcón, 2019). También (Martínez López-Sáez, 2018, pp. 93-119) realiza una magnífica recopilación y análisis de los pronunciamientos del TJUE hasta 2017.

202 SSTJUE asunto C-101/01, asunto Lindqvist, 6 de noviembre de 2003; asunto C-212/13, František Ryneš c. Úřad pro ochranu osobních údajů, de 11 de diciembre de 2014 (también sobre la excepción doméstica); asunto C-230/14, Weltimmo s.r.o. c. Nemzeti Adatvedelmi es Informacioszabadsag Hatosag, de 1 octubre de 2015.

203 SSTJUE asunto C-582/14, Patrick Breyer contra Bundesrepublik Deutschland, de 19 de octubre de 2016; asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017.

204 STJUE asunto C-13/16, Rīgas Satiksme, de 4 de mayo de 2017.

205 STJUE asunto C-25/17, Tietosuojavaltuutettu, de 10 de julio de 2018.

206 STJUE asunto C-40/17, Fashion ID, de 29 de julio de 2019.

207 STJUE asunto C-131/12, Google Spain, S.L., c. AEPD y Mario Costeja Gonzalez, de 13 de mayo de 2014.

208 STJUE asunto C-507/17, Google LLC y CNIL, de 24 de septiembre de 2019, en la que delimita el alcance del derecho de supresión. STJUE C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce y Salvatore Manni, de 9 de marzo de 2017. Sobre la aplicación de derecho de acceso, aunque muy ligado a la conceptualización de dato personal, STJUE asuntos acumulados C-141/12 y C-372/12, YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie; Integratie en Asiel contra M y S, de 17 de julio de 2014.

209 El asunto Schrems supone una evolución en el criterio del nivel de protección aceptable, elevándose desde la adecuación a la equivalencia, vid. (Pollicino, 2016, pp. 229-238).

210 STJUE, asunto C-362/14, Maximillian Schrems y Data Protection Commissioner, de 6 de octubre de 2015. Este pronunciamiento supuso un cambio en las relaciones transatlánticas en materia de protección de datos, llevando a la firma de un nuevo acuerdo, el *Privacy Shield*. Entre los elementos reseñables del pronunciamiento, se incluye la necesidad de realizar el test de necesidad estricta cuando el tratamiento suponga una injerencia o una limitación en el ejercicio de los derechos fundamentales a la vida privada o a la protección de datos. Un

agentes fundamentales en la salvaguarda de los derechos que se pueden ver afectados con el tratamiento automatizado de datos[211]; ha tenido que solventar supuestos de aplicabilidad de la Directiva[212]; dirimir conflictos de derechos[213] y/o fijar los criterios que harían jurídicamente aceptable una injerencia en el mismo[214].

8.2. El «privacy thinking»[215] del TJUE y el derecho a la protección de datos como prohibición

Pese a su indudable labor de creación y concreción conceptual, la jurisprudencia del TJUE no termina de definir el contenido y naturaleza del derecho a la protección de datos. Como han puesto de manifiesto González Fuster y Gutwirth, la jurisprudencia del Tribunal de Luxemburgo está excesivamente condicionada por los pronunciamientos del TEDH. Ello ha provocado la ausencia de una conceptualización propia del derecho a la protección de datos, adaptada a las particularidades de la realidad comunitaria.

Así, pese a que la normativa europea desliga al derecho a la protección de datos de la noción vida privada, el TJUE no ha explicitado cuál es «*the idiosyncrasy of personal data protection*, [*but*] *it leads it through a*

análisis de la sentencia y sus efectos puede consultarse en, v. gr., (López Aguilar, 2017); (Ortega Giménez, 2016) o (Ni Loideain, 2016).
Doctrina, reforzada (y matizada) por la STJUE asunto C-311/18, Facebook Ireland & Maximillian Schrems, de 16 de julio de 2020. Sobre este pronunciamiento, vid. (Martínez Martínez, 2020), (Costello, 2020) o el sugerente análisis de (Ruiz Tarrías, 2020).

211 SSTJUE Comisión c. Alemania. Asunto C-518/07, Comisión c. Alemania, de 9 de marzo de 2010; Asunto C-614/10, Comisión Europea c. Austria, de 16 de octubre de 2012.

212 SSTJUE asuntos acumulados C-465/00, C-138/01 y C-139/01, Rechnungshof c. Osterreichischer Rundfunk, de 20 de mayo de 2003; asunto C-524/06, Huber c. Alemania, de 16 de diciembre de 2006.

213 STJUE asunto C-73/07, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy, Satamedia Oy, de 16 de diciembre de 2008. También posibles afectaciones a la libertad religiosa, STJUE asunto C-25/17, Tietosuojavaltuutettu, de 10 de julio de 2018.

214 SSTJUE asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke GbR c. Land Hessen y Eifert v. Land Hessen y Bundesantalt fur Landwirtschaft un Ernahrung, de 9 de noviembre de 2010; asuntos C-293/12 y C-594/12, Digital Rights Ireland c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014, que incluye el deber de los legisladores de realizar un test de proporcionalidad riguroso en aquellas previsiones legislativas que puedan suponer una injerencia en los derechos fundamentales previstos en la CDFUE.

215 La expresión ha sido tomada de (González Fuster y Gellert, 2012, p. 74), donde se apuntan las razones, características y consecuencias de analizar el derecho a la protección de datos como si fuese un trasunto de la vida privada.

complex roundabout to an indirect assimilation of data protection under the right to respect for private life, at best, and to an ill defined series of displaced criteria, most often» (González Fuster y Gutwirth, 2013, p. 538).

Tratar al derecho a la protección de datos como una de las facetas de la vida privada produce ciertas disonancias, al imponer un marco conceptual que no se acomoda a la realidad que el derecho disciplina. En la práctica, al tratar de acomodarlo al molde de la vida privada, se le está confiriendo una condición eminentemente reactiva/defensiva, en lugar de identificar su naturaleza real.

Esta aproximación a la naturaleza del derecho provoca que la proclamación «toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan» (art. 8.1 CDFUE) se entienda como una prohibición y, consecuentemente, se termine por considerar a todo tratamiento como una injerencia.

En la práctica, esto ha provocado que, «*instead of considering whether the processing complied with the concrete criteria of Articles 8(2) and Article 8(3), it basically merely examines whether the processing follows a weighing of interests* […]. *And its trend to focus on the existence of a balancing act further deviates the Court from considering any possibly applicable substantive criteria*» (González Fuster y Gutwirth, 2013, p. 539).

El asunto Digital Rights Ireland es un buen ejemplo de ello. En él, se señala que «la Directiva 2006/24 constituye una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta puesto que establece un tratamiento de datos de carácter personal»[216]. Tras esta aseveración, el TJUE analiza si, en el caso concreto, concurren circunstancias que justifiquen la afectación del derecho[217].

---

[216] STJUE asuntos C-293/12 y C-594/12, Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014, apdo. 36. En la misma línea se pronuncia en el Dictamen 1/15, donde señala que: las operaciones previstas en el Acuerdo PNR UE-Canadá son «constitutivas de una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta, puesto que constituyen tratamientos de datos de carácter personal», apdo. 126 del Dictamen 1/15 del TJUE, de 26 de julio de 2017. Puede consultarse en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&doclang=ES

[217] No solo el TJUE opera desde esta óptica, también el TC ha empleado el mismo modo de aproximarse y entender el derecho a la protección de datos, v. gr. STC 76/2019, de 22 de mayo, FJ 9.

Es decir, en lugar de valorar si se cumplen las condiciones de los apartados 2 y 3 del artículo 8 y aplicar después los criterios del 52.1 de la CDFUE (trasunto del 8.2 del CEDH), se aplican directamente las exigencias generales, prescindiendo de los elementos singulares que individualizan y dan autonomía al derecho a la protección de datos en su configuración europea. Siendo esa la forma habitual de aproximarse a la cuestión, en ocasiones, como en el asunto Rundfunk[218], el Tribunal ha empleado los criterios del apartado 3 como parámetro para determinar la afectación del derecho a la protección de datos (y de la vida privada)[219].

Además de esa indefinición, el TJUE también ha oscilado a la hora de configurar las interrelaciones entre el derecho a la protección de datos y el derecho a la vida privada. Pueden establecerse dos grupos de sentencias. De una parte, un pequeño conjunto de pronunciamientos en los que el derecho a la protección de datos se presenta como un derecho autónomo, con características propias[220]. Y, de otra, un gran conglomerado de pronunciamientos, en los que el derecho a la protección de datos aparece en conjunción con la vida privada.

Ese segundo bloque no es homogéneo. En él pueden encontrarse sentencias en las que la protección de datos es completamente absorbida por la vida privada[221], mientras que en otras aparecen como derechos

[218] SSTJUE asuntos acumulados C-465/00, C-138/01 y C-139/01, Rechnungshof c. Osterreichischer Rundfunk, de 20 de mayo de 2003, apdo. 91 y ss.

[219] STJUE asunto C-518/07, Comisión v. Alemania, de 9 de marzo de 2010 y STJUE asunto C-614/10, Comision Europea c. Austria, de 16 de octubre de 2012. En estos casos, pese a utilizar un criterio estrechamente vinculado a la protección de datos, este derecho se presenta estrechamente conectado con la vida privada, como una manifestación más del mismo.

[220] En este bloque se incardinaría la STJUE asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB, de 21 de diciembre de 2016, apdo. 129, en la que el TJUE señala con rotundidad el carácter autónomo del derecho a la protección de datos, al «recordar que las explicaciones relativas al artículo 52 de la Carta indican que el apartado 3 de ese artículo pretende garantizar la coherencia necesaria entre la Carta y el CEDH, "sin que ello afecte a la autonomía del Derecho de la Unión y del Tribunal de Justicia de la Unión Europea" […]. En particular, […] no impide que el Derecho de la Unión conceda una protección más amplia que el CEDH. A esto se añade, finalmente, el hecho de que el artículo 8 de la Carta se refiere a un derecho fundamental distinto del previsto en el artículo 7 de ésta y que no tiene equivalente en el CEDH». En la misma línea, pero con menor contundencia, se había pronunciado anteriormente el TJUE en el asunto C-28/08, Bavarian Lager, de 29 de junio de 2010, apdo. 59

[221] Es el caso de la STJUE asunto C-473/12, IPI, de 7 de noviembre de 2013, apdo. 39, en el que con rotundidad, el TJUE señala que: «la protección del derecho fundamental a la intimidad exige que las excepciones a la protección de los datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de lo estrictamente necesario». En la misma línea se manifestó en la STJUE asunto C-212/13, František Ryneš, de 11 de diciembre de 2014, apdo. 28 y 29.

concurrentes[222]. La oscilación es, en definitiva, un rasgo caracterizador de la jurisprudencia del TJUE referida a la condición jurídica del derecho a la protección de datos.

8.3. El derecho a la protección de datos no es una prohibición

8.3.1. Aires de cambio en la jurisprudencia del TJUE

La mirada del TJUE con las lentes de la vida privada puede estar, hasta cierto punto, justificada. En primer lugar, porque resulta perfectamente razonable, incluso obligado (art. 52.3 CDFUE), que se tome en consideración el CEDH y la jurisprudencia del TEDH, tanto por representar un mínimo a considerar[223] –que la UE puede rebasar–, como por el bagaje que suponen los más de 60 años de pronunciamientos[224] y su contribución a la forja de un sustrato común europeo en materia de derechos (Bustos Gisbert, 2017, pp. 345-346). En segundo lugar, si se toma en consideración el modo en que se ha construido el derecho a la protección de datos[225], resulta entendible esa imbricación protección de datos-vida privada. Ambos derechos están estrechamente vinculados a la salvaguarda de la esfera personal e íntima de los sujetos, lo que hace, en parte, natural la ascendencia de la vida privada a la hora de interpretar en qué consiste proteger los datos personales.

---

[222] En ciertos casos, el TJUE opera tomando en consideración ambos derechos, sin embargo, no termina de aclarar si se trata de una doble afectación de derechos o, si es un único derecho vulnerado de dos modos diferentes. Así ocurre en la STJUE asuntos C-293/12 y C-594/12, Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014, apdos. 32-37, en el que, pese a ofrecer una imagen autónoma del derecho a la protección de datos, no deja de resaltar el valor especial de la afectación de la vida privada. En el asunto Schrems I, también se citan conjuntamente ambos derechos, STJUE asunto C-311/18, Facebook Ireland & Maximillian Schrems, de 16 de julio de 2020, apdo. 91. En la STJUE asunto C-131/12, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014, el TJUE realiza una aproximación diferente, pues menciona a vida privada y a la protección de datos de manera separada (apdo. 80, 81, 97, 99), pero los trata como si la protección de datos estuviese subordinada a la garantía de la vida privada, apdos. 58, 66 o 74.

[223] Si bien es cierto que, como ha advertido el TJUE en el asunto Menci, el CEDH «no constituye, dado que la Unión no se ha adherido a él, un instrumento jurídico integrado formalmente en el ordenamiento jurídico de la Unión», STJUE asunto C-524/15, Menci, de 20 de marzo de 2018, apdo. 22.

[224] Los primeros miembros del TEDH fueron elegidos en enero de 1959. Teniendo su primera sesión en febrero del mismo año. Vid. *The Court in brief*, del TEDH. Puede consultarse en: https://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf.

[225] Vid. Capítulo II de esta tesis.

Por otra parte, la Directiva 95/46/CE contribuyó a ahondar en esta confusión, pues tenía como objetivo «mantener un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad»[226]. Esta conceptualización no es inane para el TJUE, pues condiciona su margen interpretativo (Brkan, 2017, p. 13). En efecto, si esa era la finalidad de la Directiva, resulta coherente que el Tribunal de Luxemburgo interpretase el derecho a la protección de datos como una manifestación de la vida privada.

Sin embargo, conforme el derecho a la protección de datos ha ido ganando sustantividad, la vida privada ha ido perdiendo espacio en su caracterización. Así, después del Tratado de Lisboa, se produce un *overruling* evidente en lo referente a la fundamentación de la Directiva 95/46/CE. Esta, deja de ser un mecanismo de equilibrio entre la intimidad y la libre circulación (asunto Linqvist) y pasa a tener un único fundamento: «garantizar, en los Estados miembros, la protección de los datos personales»[227]. Con todo, ese reconocimiento no deja de ser un primer paso, pues, en la interpretación del derecho derivado, la afectación de la vida privada ha seguido teniendo un peso significativo[228].

La consolidación de un espacio propio por parte del derecho a la protección de datos y su diferenciación de la vida privada ha continuado. Que el RGPD no mencione, ni una sola vez, el derecho a la intimidad, o que aluda, en una única ocasión, al derecho a la vida privada (y como uno más de los derechos fundamentales que ha de respetar en su articulación), da buena cuenta del cambio de paradigma que ha supuesto el estatus reforzado de la CDFUE, y la consecuente consolidación de un espacio propio para el derecho a la protección de datos.

---

[226] STJUE asunto C-101/01, asunto Lindqvist, 6 de noviembre de 2003, apdo. 97. En consonancia con lo dispuesto en el art. 1.1 de la Directiva que pone el acento en la protección de la intimidad.

[227] STJUE asunto C-543/09, Deutsche Telekom AG c. Bundesrepublik Deutschland, de 5 de mayo de 2011, apdo. 50. Esta interpretación, por lo demás, se compadece con lo indicado en las Explicaciones a la CDFUE.

[228] V. gr. STJUE STJUE asuntos C-293/12 y C-594/12, Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014, apdos 32-35; STJUE asunto C-131/12, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014, apdo. 58; STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017, apdos. 56-57; STJUE asunto C-311/18, Facebook Ireland & Maximillian Schrems, de 16 de julio de 2020, apdo. 171.

Resulta razonable augurar que, en atención al enfoque adoptado por el derecho derivado, el TJUE se vea liberado del condicionante de la vida privada a la hora de interpretar el derecho a la protección de datos y, con ello, ganen en nitidez sus pronunciamientos en torno al objeto y finalidades del derecho.

8.3.2. Condicionar no es prohibir

Como el Abogado General Siegbert Alber ha puesto de manifiesto, la consideración del derecho a la protección de datos como una prohibición no se ajusta a la realidad del derecho, de hecho, supone su negación, pues, «en el caso de existir una prohibición general de comunicación de los datos no sería en modo alguno necesaria su protección»[229].

Sin tratamiento no hay riesgo y, sin este, el derecho a la protección de datos pierde su fundamento. Ergo, un enfoque prohibitivo choca con la razón de ser del derecho, y contradice su condición, esencialmente preventiva.

Al argumento anterior, por sí solo suficiente, pueden añadirse otros dos. En primer lugar, que la prohibición del tratamiento sea la regla no resulta compatible con el otro elemento caracterizador del modelo europeo de protección de datos: la libre circulación de los mismos. Difícilmente se puede proclamar la libre circulación como premisa si, a la vez, se parte de un sistema de prohibición del uso de la información. Con lo que se refuerza la condición del derecho a la protección de datos como mecanismo para asegurar que lo inevitable (el tratamiento) sea jurídicamente aceptable.

El segundo de los argumentos pone de manifiesto una disonancia entre la concepción del TJUE y la del legislador europeo. Si se aceptase la concepción del derecho a la protección de datos como prohibición de su tratamiento (TJUE), la prohibición expresa de tratar las categorías especiales de datos (art. 9.1 del RGPD) no tendría sentido alguno, pues esa sería la regla general. No habría "especialidad".

[229] Conclusiones del Abogado General Alber presentadas el 10 de febrero de 2000, respecto del asunto C-369/98, The Queen c. Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher, apdo. 41. Puede consultarse en: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:61998CC0369

En este punto, procede preguntarse si existe una interpretación alternativa a la prohibición que se ajuste a la realidad jurídica del derecho proclamado en el artículo 8 de la CDFUE. La respuesta es afirmativa y tiene como basamento la asunción de la inevitabilidad del tratamiento de datos y la necesariedad de su regulación (González Fuster y Gellert, 2012, p. 80). El uso de los datos personales, su importancia en la sociedad actual[230], su valor estratégico para la UE[231], le han hecho transitar hacia un derecho eminentemente activo. En consecuencia, el tratamiento no es la excepción, es la regla. Su prohibición, lo excepcional; su regulación, lo imprescindible.

Desde el punto de vista jurídico, esta consideración del derecho tiene como consecuencia que, como González Fuster y Gutwirth han puesto de manifiesto, los apartados segundo y tercero del artículo 8 «*would not outline demands applicable to interferences with the right, but those of the very right itself, which is thus expressed and substantiated through them*» (González Fuster y Gutwirth, 2013, p. 533).

Dicho con otras palabras, no serían meras condiciones habilitantes, sino exigencias inherentes al derecho, componentes nucleares del mismo. De manera que, solo si se constata el cumplimiento de los límites y exigencias en ellos establecidos, se considerará que la afectación del derecho (consustancial a todo tratamiento de datos, conforme a la interpretación del TJUE) es jurídicamente aceptable. Por tanto, los apartados 2 y 3, en combinación con el art. 52, conformarían una especie de test de admisibilidad[232].

Conforme a esta concepción, cuando el legislador no hubiese contemplado alguno de los requerimientos dimanantes de esos dos apartados, se produciría una conculcación del derecho fundamental.

Allí donde la regulación del modelo no ofrezca un nivel de protección suficiente y/o el tratamiento no se lleve a cabo de un modo leal, con una

[230] Así se ha ido demostrando a lo largo de esta tesis, especialmente en los Capítulos 1 y 2, a los que me remito.

[231] La libre circulación de datos es una característica basilar del sistema de protección de datos europeo. La garantía de su flujo y utilización ocupa un papel preponderante en el RGPD, al punto de llegar a proclamar que, «el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales» (Considerando 13 RGPD).

[232] Vid. asunto Schrems II, en cuyos apartados 173 a 176 se enuncia tanto el deber de cumplir con las condiciones del 8.2 CDFUE (apdo. 173), como con el «requisito de proporcionalidad» (apdo. 176), pasando por el respeto al contenido esencial (apdo. 174) y la regulación legal de las limitaciones (apdo. 175).

finalidad específica y una base de legitimación adecuada; o cuando se impida el ejercicio de los derechos de acceso y rectificación y/o no se incluya una garantía institucional independiente, se estará vulnerando el derecho a la protección de datos. La injerencia no sería un a priori derivado del tratamiento, sino una consecuencia del contexto jurídico en el que se desarrolla. En mi criterio, esta interpretación es la que mejor refleja la idiosincrasia del derecho a la protección de datos en su configuración europea.

9. El derecho a la protección de datos: un derecho de configuración legal

«Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan a la protección de los datos de carácter personal que le conciernan» (art. 8.1 CDFUE). El enunciado normativo que proclama el derecho a la protección de datos parece contener en su seno una obligación de resultado.

Si esto es así, el derecho a la protección de datos comportaría un principio de optimización[233] consistente en la configuración de un sistema que asegurase la defensa frente al uso de la información personal. Sería, en suma, un derecho precisado de configuración legal[234].

Item más, el derecho en su conjunto precisaría, para su plena efectividad, del desarrollo de un marco normativo adecuado para su realización plena. Sin embargo, con la excepción de las características previstas en los apartados dos y tres del artículo, no impone un modelo determinado de protección. Esto es, el desarrollo legislativo sería la primera de las obligaciones/consecuencias de su proclamación como derecho fundamental.

---

[233] En el sentido alexiano de mandato de optimización, admitiendo, en consecuencia, cierta graduación en su nivel de materialización (Alexy, 1993. pp. 83-87).

[234] Entendiendo por derecho de configuración legal aquel que solo puede «existir y realizarse si media la colaboración del poder público pues requieren para su ejercicio prestaciones de bienes o servicios o [como es el caso en el derecho a la protección de datos] el establecimiento de normas de procedimiento y organización» (Bastida Freijedo et al., 2004, p. 162). De este modo, «la titularidad del derecho subjetivo fundamental surge sólo, como realidad práctica y actual, de la convergencia o conexión entre el enunciado abstracto de la Constitución y la ordenación legal de los procedimientos y condiciones que delimitan el derecho» (Jiménez Campo, 1999, p. 43).

Esta opción hermenéutica no niega la *iusfundamentalidad* del derecho, ni su fuerza vinculante o su aplicabilidad inmediata, solo describe el modo en que ha de materializarse, poniendo de manifiesto el grado de formalidad que exige su satisfacción plena.

El derecho a la protección de datos impone al legislador el desarrollo de las medidas necesarias para asegurar su salvaguarda. En tanto derecho reconocido en la CDFUE y en el TFUE, su no regulación comporta la vulneración de un derecho fundamental, no es, por tanto, un mero mandato al legislador. En este sentido, el derecho a la protección de datos, guarda cierta similitud con otros derechos de configuración legal, como la tutela judicial efectiva[235].

Conforme a esta línea argumental, el respeto a este derecho estaría inexorablemente unido al modelo de garantías jurídicamente establecido. Las normativas reguladoras del tratamiento de datos serían la plasmación positiva de ese deber de protección. Estamos ante un derecho que demanda un alto grado de formalidad, tal como reflejan las diferentes exigencias de los apartados segundo y tercero del artículo 8 que, ineludiblemente, conducen a la necesidad de una actuación positiva y proactiva por parte del legislador.

El tratamiento de la información personal solo sería aceptable mediante un entramado normativo capaz de asegurar un nivel de protección adecuado. La mayor o menor capacidad para garantizar su defensa determinaría el grado de cumplimiento real del derecho, así como su eventual vulneración. Esto convertiría a los Reglamentos (RGPD y Reglamento 2018/1725) en la proyección exclusiva del derecho reconocido en el art. 8 de la Carta. Lo que se compadece con lo previsto en las Explicaciones y el Considerando 1 de los dos Reglamentos.

Así, el sistema de protección, el conjunto de normativas previstas para disciplinar el tratamiento de la información personal, sería la consecuencia del diálogo internormativo: constitución (CDFUE+TFUE)/ley (Reglamentos europeos), refrendando la naturaleza del derecho del art. 8 de la CDFUE como derecho de configuración legal.

Con todo, el artículo 8 de la CDFUE no se reduce a establecer el derecho de toda persona a la protección de su información personal (apartado 1), sino que prevé, en los preceptos subsiguientes, ciertos

[235] V. gr. STC 99/1985, de 5 de noviembre, FJ 4.

elementos que habrán de concurrir para asegurar el cumplimiento efectivo del derecho. Así, el artículo 8 «*not only provides that the personal data of individuals should be protected, but also specifies when and how personal data can be legitimately processed*. […] *Article 8 of the Charter, the fundamental right to data protection is in itself already a compromise between different legitimate interests*» (Van der Sloot, 2017, p. 22).

Los apartados 2 y 3 desarrollan el mínimo esencial y definitorio del derecho, al establecer una serie de atribuciones que le dotan de sustantividad y exigibilidad directa, aun cuando el desarrollo legislativo no se hubiese producido. Es decir, el derecho fundamental a la protección de los datos personales no se colmaría con la mera salvaguarda de la información, sino que esta debe realizarse de un modo determinado.

Esta interpretación resulta, por lo demás, coherente con la idea de derecho de configuración legal. En la medida en que el riesgo es inherente a toda operación que involucre el uso de datos personales, todo tratamiento genera una situación de partida en la que la información deja de estar protegida. Esto es, los apartados segundo y tercero vendrían a establecer las condiciones mínimas que harían jurídicamente aceptables los tratamientos. Son presupuestos de obligado cumplimiento para el legislador y su inobservancia produce la vulneración del derecho fundamental. No basta con asegurar la indemnidad de la información mediante la articulación de un sistema de protección, sino que, además, el modelo implementado ha de reunir una serie de condiciones. Es decir, garantizar que los datos están protegidos, en el sentido de estar seguros por haber adoptado las medidas técnicas y organizativas necesarias, no es suficiente[236].

Al diseñar el sistema de tratamiento de la información el legislador ha de atender a esos contenidos que le son indisponibles: tendrá que implementar medidas que aseguren que el tratamiento sea «leal»; implementar condiciones que aseguren que solo se realizan tratamientos «para fines concretos»; considerar el fundamento de los tratamientos, esto es, deberá prever las condiciones que los habilitan, entre las que se habría de incluir como opción el consentimiento de la persona concernida, sin

[236] Para no vulnerar el derecho fundamental reconocido en la CDFUE ha de asegurarse que los datos se tratan «de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. […] [Reconocerse a] toda persona […] [el] derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación» (art. 8.2 CDFUE) y, además, cuentan con una garantía institucional: «una autoridad independiente» (art. 8.3 CDFUE).

perjuicio de cualquier otro instrumento que decidiese implementar, siempre que fuese congruente con el deber de protección que debe presidir sus actuaciones.

10. La protección de datos y el dominio de la proyección exterior. El derecho como poder de control y disposición

10.1. Un bagaje jurisprudencial a considerar. La jurisprudencia creadora de los Tribunales Constitucionales español y alemán

La sentencia sobre la ley del censo de 1983 del TCFA explicitó la existencia de un derecho fundamental con características propias, el derecho a la autodeterminación informativa[237]. Este sería un derecho, proyección directa de la dignidad, que otorgaría a los individuos el poder para «decidir básicamente por sí solo[s] sobre la difusión y la utilización de sus datos personales»[238].

Este modo de conceptualizar el derecho, entendiéndolo como una manifestación de la dignidad cuyo cometido es asegurar y hacer efectiva la autodeterminación personal mediante el dominio de las informaciones a uno referidas, constituye la base dogmática del derecho a la protección de datos como derecho fundamental y autónomo.

Sería otro tribunal constitucional, el español[239], el que elaboraría una de las más claras conceptualizaciones del derecho a la protección de datos, al definirlo, en la STC 292/2000, como: «un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al

[237] Para un análisis más detallado de este pronunciamiento me remito a lo señalado en el Capítulo II, respecto del TCFA y el derecho a la autodeterminación informativa, así como a la bibliografía allí referenciada.

[238] Original en alemán: «*grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*», en BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983- 1 BvR 209/83 -, Rn. 1-215, Grunde C, II-1a), apdo. 147. Puede consultarse en español en: («Jurisprudencia Constitucional Extranjera, Núm. 33, IV», 1984).

[239] Para un análisis más detallado del proceso evolutivo de conformación jurisprudencial del derecho a la protección de datos en España, me remito a lo señalado en el Capítulo II, respecto del Tribunal Constitucional español y el derecho a la protección de datos, y a la bibliografía allí referenciada.

individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso»[240].

Dicho pronunciamiento no solo determinó las características definitorias del derecho, sino que delimitó su objeto, al proporcionar las claves para distinguirlo de otros con los que pudiera concurrir en el tratamiento de la información personal, y con los que podría llegar a confundirse, esencialmente con la intimidad. Así, señaló que el derecho a la protección de datos, «no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato […], sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales»[241].

Es significativo que, contando con una argumentación doctrinal tan consolidada acerca de la naturaleza del derecho a la protección de datos, el TJUE mantenga su jurisprudencia oscilante, en lugar de apostar, de manera clara[242], por considerar al derecho a la protección de datos como un poder de disposición y control sobre la información personal.

Lo paradójico de la situación se agudiza aún más si se toma en consideración lo dispuesto en el art. 52.4 de la CDFUE, en el que se establece que, «en la medida en que la presente Carta reconozca derechos fundamentales resultantes de las tradiciones constitucionales comunes a los Estados miembros, dichos derechos se interpretarán en armonía con las citadas tradiciones». Se han apuntado ya las posibles razones que pueden explicar la jurisprudencia del TJUE, con todo, la postura etérea del Tribunal de Luxemburgo no deja de ser reveladora de la dificultad y dudas

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

[241] Ibídem, FJ 6.

[242] Es cierto que, en su interpretación del Considerado 25 de la Directiva 95/46/CE, el TJUE utiliza una aproximación similar a la de la jurisprudencia constitucional mencionada, sin embargo, reduce ese poder de control y disposición a una característica de los principios inspiradores del derecho a la protección de datos, no la aplica, por tanto, al derecho mismo. Sirva como ejemplo: «En efecto, del considerando 25 de la Directiva 95/46 se desprende que los principios de la protección que esta contempla tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas que efectúen tratamientos —obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento— y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias». STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017, apdo. 48. En los mismos términos se pronuncia en la STJUE asunto C-131/12, Google Spain, S.L., c. AEPD y Mario Costeja Gonzalez, de 13 de mayo de 2014, apdo. 67.

existentes en torno a la naturaleza del derecho a la protección de datos en su configuración europea.

10.2. El derecho a la protección de datos como poder de control y disposición

A lo largo de este apartado se examinará la verosimilitud de la opción hermenéutica que configura al derecho a la protección de datos como un poder de control y disposición destinado a gestionar la proyección exterior del ser. Esta perspectiva del derecho supone reconocer al individuo la capacidad para «decidir […] [qué] datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso»[243].

El derecho a la protección de datos como poder de disposición y control tendría como causa el vínculo dato-persona y como finalidades, asegurar la posición de dominio de la persona en relación con su información personal y prevenir los efectos que el uso de la misma pudiese generar, tanto en la proyección exterior de la persona, como en sus derechos y libertades fundamentales.

Así caracterizado, el derecho a la protección de datos supondría la imposición de un conjunto de obligaciones específicas para quienes pretendan operar con datos personales (tratamiento leal, adecuación a la finalidad y base de licitud); el reconocimiento de una serie de facultades de actuación destinadas a hacer efectivo ese poder (acceso y rectificación) y una garantía institucional que vincula a los poderes públicos en la protección activa del derecho. Es decir, hay deberes de actuación que precisan de activación por el interesado (acceso, rectificación) y otros que son estructurales, por haberse objetivado (las obligaciones en torno al modo de realizar el tratamiento de los datos o la exigencia de garantías institucionales).

En este sentido, el derecho de acceso se presenta como el reflejo más fiel derecho como poder de control y disposición, mientras que, el derecho de rectificación es la constatación más genuina del vínculo dato-persona como fundamento del derecho. En la fuerza de esa unión reside el alcance de las posibilidades de actuación que el derecho confiere, cuanto más

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

intensa sea, mayores serán. Esto es, cuanto mayor sea la capacidad del dato para reflejar a la persona, más fuerte será la posición jurídica del interesado frente a terceros que puedan tener algún interés en la información. De este modo, el poder de control y disposición tendría como causa, condición y límite la existencia de un vínculo entre la persona y la información.

En consecuencia, allí donde se acredite la existencia de esa relación, se generará ese poder, entre cuyas manifestaciones están el derecho de acceso y el de rectificación, pero también el conjunto de obligaciones previstos en la primera parte de apartado segundo del art. 8 (tratamiento leal, para un fin determinado y con una base de licitud que lo fundamente).

En efecto, una interpretación sistemático-funcional de la exigencia de licitud[244], poniéndola en conexión con las obligaciones de tratamiento leal y para fines concretos, proporciona una explicación ontológica de las exigencias relativas al modo de tratar los datos personales. Así, la vertiente objetiva del derecho, representada por las exigencias del tratamiento previstas en el apartado segundo del art. 8 de la CDFUE se correspondería con la obligación de proteger la efectividad del poder de disposición que el derecho representa.

De no establecerse esa serie de exigencias, se vaciaría de contenido la capacidad para controlar el destino de las informaciones a uno referidas. En efecto, la regulación de las condiciones de partida del tratamiento impide el uso indiscriminado de la información personal y posibilita al interesado mantener cierto dominio/control sobre los datos que le atañen. Vistas de este modo, las bases de legitimación propician que el interesado, o bien habilite directamente el tratamiento (consintiendo, firmando un contrato o para la protección de sus intereses vitales) o, en los casos en que no sea el causante directo, mantenga un control sobre la información a él referida.

Del mismo modo, la obligación de definir previamente para qué van a tratarse los datos o la exigencia de lealtad en el tratamiento resultan cruciales para asegurar el ejercicio del poder de control y disposición.

[244] Un análisis individualizado de cada una de las bases de legitimación podría generar más dudas que respuestas. En efecto, mientras el consentimiento encaja muy bien con el poder de control y disposición (Polo Roca, 2020); otras bases de licitud, como puede ser el interés legítimo, parecen inclinar la balanza hacia la concepción del derecho como mandato tendente a hacer jurídicamente aceptable el tratamiento.

Pudiera aducirse, que la finalidad de las autoridades de control (asegurar el respeto de «los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento […] y libre circulación de datos personales» (art. 51.1 RGPD)) plantea un contenido del derecho a la protección de datos más amplio que el representado por el poder de control y disposición.

Sin embargo, en la medida en que el derecho a la protección de datos precisa del desarrollo normativo para asegurar su despliegue efectivo, no resulta extraño que se establezca una autoridad independiente destinada a velar por el cumplimiento de ese marco jurídico-legislativo, asegurando, de ese modo, el pleno ejercicio del poder de control y disposición.

Dicho de otro modo, el derecho a la protección de datos impondría a los terceros y, sobre todo, al legislador, el deber de generar las condiciones adecuadas para el despliegue efectivo del poder de control y disposición[245]. En definitiva, la formulación del art. 8 de la CDFUE no contradice, *prima facie*, la interpretación del derecho a la protección de datos como poder de control y disposición.

10.3. Derechos fundamentales, poder de control y protección instrumental

10.3.1. La protección de los derechos y el derecho a la protección de datos

La relación del derecho a la protección de datos y el deber de salvaguarda de los derechos fundamentales es otra de las cuestiones candentes en la conceptualización del derecho[246]. Recordemos que la protección frente al tratamiento de datos personales nace como una

[245] En estos términos lo definió el TC español: «el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer» STC 292/2000, de 30 de noviembre, FJ 6.
Hasta cierto punto, ese conjunto de atribuciones conferidas al interesado se han ido objetivando, convirtiéndose en obligaciones estructurales precisadas de concreción legislativa.

[246] No nos estamos refiriendo, como se puede intuir, a la habitual conflictividad entre derechos (tema que, por lo demás, no es ajeno al derecho a la protección de datos, cuyas fricciones con derechos como la libertad de información (Cotino Hueso, 2011), la transparencia (Llaneza González, 2018) u otros, son habituales y lógicas en un derecho que –como todos– no es absoluto.

respuesta jurídico-técnica frente a las amenazas que, para los derechos de la ciudadanía, supone la capacidad de procesar, de manera rápida y eficiente, grandes cantidades de información. Por eso la intimidad fue el derecho protagónico en las primeras regulaciones, al punto de considerarla el fundamento de las normativas relativas al tratamiento de datos. No era el único derecho afectado o en peligro, pero sí el más evidente[247].

Siguiendo esa estela, las normativas sobre tratamiento de la información personal, singularmente los Reglamentos, tienen como cometido la protección de los derechos y libertades fundamentales de las personas físicas (art. 1.2 de los Reglamentos). Esta finalidad podría simplemente considerarse como una proyección del deber general de respeto a los derechos fundamentales que ha de presidir toda regulación, sin embargo, en el derecho a la protección de datos, se sitúa en un plano jurídico diferente.

La salvaguarda de los derechos fundamentales establecida en las normativas es un objetivo a lograr y no un desiderátum o un principio inspirador. Los Reglamentos son proyección directa y exclusiva del art. 8 de la CDFUE y del 16 del TFUE. Son normativas que ocupan una posición preeminente en la configuración del derecho, debido a la dependencia de la formulación legal para su despliegue y efectividad (v. gr. gran parte de las facultades de actuación y de las condiciones para el ejercicio del tratamiento de la información son de creación legislativa)[248].

Los derechos y libertades –todos ellos– se presentan como parámetro y límite para el legislador[249] (p. ej. determinando el grado de protección que se debe establecer y las medidas a implementar). La protección de los derechos fundamentales es una obligación inherente al derecho a la protección de datos. Por lo tanto, ese deber de protección activa se integra en el contenido y naturaleza del derecho fundamental.

---

[247] Así lo ha apuntado también el TJUE, v. gr. en el asunto Schrems, al señalar que «el tratamiento de datos personales […] puede vulnerar las libertades fundamentales y, en particular, el derecho al respeto de la vida privada», STJUE asunto C-362/14, Maximillian Schrems y Data Protection Commissioner, 6 de octubre de 2015, apdo. 38.

[248] La concreción de las condiciones aplicativas resulta esencial para asegurar la efectividad del derecho, al punto de dotarlo «de un alto nivel de formalidad, lo que se refleja en la exigencia […] de una actuación positiva y proactiva por parte del legislador» (Jove Villares, 2021, p. 325).

[249] En esa línea apunta el Considerando 2 del RGPD cuando señala que «los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales».

Pudiera pensarse que esa función instrumental del derecho a la protección de datos como protector de otros derechos confirma la teoría de Poscher, negadora de la *iusfundamentalidad* del derecho. Pero no es así.

No cabe duda que existe un vínculo entre la protección de la información personal y la salvaguarda de los derechos y libertades, ni que aquel refuerza la protección de estos, ahora bien, ello no tiene porqué implicar una condición subordinada de uno sobre los otros.

Consecuentemente, las previsiones normativas sobre protección de datos no son una proyección de los diferentes derechos y libertades, sino que obedecen a un único derecho, el proclamado en el artículo 8 de la CDFUE, cuyo contenido es indisponible para un legislador, que, sin embargo, para dar cumplimiento pleno a los deberes de protección en él establecidos, habrá de articular un sistema de garantías.

La configuración de ese sistema de protección, el respeto de sus presupuestos y el diseño de los tratamientos, ha de asegurar que la utilización de la información personal transcurre por unos cauces en los que no se vean vulnerados los demás derechos fundamentales. Sin embargo, al contrario de lo postulado por Poscher, el refuerzo en la protección de los derechos y libertades no sería la única razón de ser del derecho a la protección de datos, sino una de sus manifestaciones.

10.3.2. La relación entre el poder de control y la protección de los derechos. Las dos opciones del modelo europeo

En la caracterización del derecho a la protección de datos como un poder de control y disposición se tiende a poner el acento en su fundamento jurídico, en la dignidad, en el libre desarrollo de la personalidad y en la garantía de la autodeterminación informativa. Se da respuesta al porqué de ese poder. Sin embargo, tiende a obviarse para qué se confiere, su finalidad. La contestación, seguramente por obvia poco valorada, sería el dominio de la proyección exterior de la persona. Esto es, el poder serviría «*to anticipate how orders will anticipate us*» (Morozov, 2013, p. 348). En definitiva, serviría para conformar nuestra identidad[250] y

[250] Entendida la identidad no solo como aquello que nos caracteriza frente a los demás y frente a nosotros mismos. Coincidente, por tanto, con las acepciones 2 y 3 de la RAE, («2. Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás.

prevenir los efectos que sobre ella pudieran derivarse de la utilización de información personal por terceros.

La consecución de dicho objetivo tiene en el control directo de la información, en cómo se usa, por quién y para qué, su manifestación más palmaria. La protección de la proyección exterior requiere del reconocimiento de ciertas facultades de actuación respecto de la información personal, así como de la implementación de mecanismos jurídicos destinados a asegurar las condiciones para que esa capacidad pueda desarrollarse, imponiendo obligaciones a terceros y articulando un marco normativo adecuado.

El reconocimiento de un poder de control y disposición cuya finalidad es la protección de la identidad de la persona mediante el dominio de la información a ella referida engendra una realidad jurídico-normativa en la que el conjunto de los bienes de la personalidad terminan siendo protegidos. Curiosamente, el *corpus* normativo del derecho a la protección de datos permite obtener este resultado de dos modos diferentes. Cada una de las vías, sin embargo, representa una concepción distinta del derecho y dota de un alcance diferente al poder de control y disposición.

10.3.2.1. La protección incidental

La primera de las opciones plantea la salvaguarda de los derechos como una protección incidental. El razonamiento que en ella subyace es el siguiente: la capacidad del interesado para intervenir en el modo en que se opera con los datos personales, para controlar su uso e imponer que se adopten medidas tendentes a asegurar la ejecución efectiva de ese dominio (p. ej. mediante las facultades de actuación) y la preservación de las condiciones que hicieron jurídicamente aceptable el tratamiento (protección técnica y medidas de seguridad), además de asegurar la efectividad del derecho a la protección de datos como poder de control, genera las condiciones adecuadas para salvaguardar al resto de derechos y libertades de los riesgos derivados del tratamiento de la información personal.

3. f. Conciencia que una persona o colectividad tiene de ser ella misma y distinta a las demás»).

Esto es, la protección de datos operaría como un mecanismo indirecto de defensa del resto de derechos fundamentales. El éxito de la protección derivaría del acierto de las medidas articuladas para garantizar el ejercicio del poder de control y disposición. Esto es, al controlar las condiciones en que se produce el tratamiento, se puede "asegurar" el resultado. Sería, por tanto, la consecuencia incidental, esperada pero no obligada, de conferir a los interesados capacidad para intervenir en el tratamiento de la información.

10.3.2.2. La instrumentalidad inherente y la prevención del riesgo

Por otra parte, si el poder de control y disposición se confiere para prevenir los efectos derivados del uso de datos personales, en ese caso, la salvaguarda de los derechos y libertades estaría en la esencia misma del derecho. No sería la consecuencia de utilizar dicho poder, sino una manifestación del mismo. Es decir, a diferencia de la primera vía, en la que se trataría de un efecto secundario –positivo, eso sí–, en este caso la protección de los derechos y libertades sería una obligación de partida, un objetivo a perseguir.

Esta opción resulta la más coherente con el objetivo de los Reglamentos, así como con el bagaje histórico del derecho a la protección de datos. Como se ha señalado a lo largo de esta tesis, la necesidad de protección de los derechos y libertades fundamentales frente al tratamiento de la información personal está estrechamente vinculada al surgimiento del derecho a la protección de datos. Por lo tanto, nada hay de extraño en que se integre en su contenido.

Al existir un deber de protección frente a los peligros derivados del tratamiento de la información personal, y ser la afectación de los derechos fundamentales el principal riesgo[251], resulta lógico que, al establecer las medidas de protección, se tome en consideración las posibles afectaciones de derechos. El resultado es un sistema condicionado por los derechos fundamentales, pero su razón de ser no está en ellos, sino en el derecho a la protección de datos.

[251] Hay otros, como la producción de una brecha de seguridad que lleve a chantajes para recuperar el dominio de la información. En ese caso, de afectarse algún derecho, sería el correspondiente al dominio de la información personal, esto es, de afectarse un derecho, sería el de la protección de datos.

Conforme a esta interpretación, el poder de control consiste en la imposición, tanto al legislador como a los terceros que tratasen con datos personales, del deber de implementar las medidas adecuadas para preservar los bienes jurídicos del interesado. Es decir, alcanza la obligación de establecer un modelo de protección en el que, con carácter preventivo, se velase por la no afectación de los derechos y libertades, amén de permitir el ejercicio de las facultades de actuación inherentes al poder de control y disposición.

Diversos preceptos del RGPD contribuyen a reforzar esta interpretación, y a ratificar la condición del derecho reconocido en el art. 8 como un derecho dotado de una relevante dimensión objetiva, cuya configuración corresponde al legislador, y en la que se ha de priorizar la defensa de ciertos derechos y valores constitucionales[252]. Esta línea argumental se compadece con diversos Considerandos que señalan la protección de los derechos y libertades como un objetivo ineludible del RGPD[253], las exigencias de realizar evaluaciones de impacto (arts. 35 y 36 RGPD), la obligatoriedad de llevanza de un registro de actividades (art. 30.5 RGPD) o la existencia de categorías especiales de datos (art. 9 RGPD).

Las evaluaciones de impacto tienen como fundamento de su obligatoriedad el que los tratamientos en cuestión puedan entrañar «un alto riesgo para los derechos y libertades de las personas físicas» (art. 35.1 RGPD). La llevanza de un registro de actividades tiene como una de sus causas justificativas que el tratamiento llevado a efecto por el responsable «pueda entrañar un riesgo para los derechos y libertades de los interesados» (art. 30.2 RGPD). Finalmente, el reconocimiento de una protección reforzada para las categorías especiales de datos obedece a «que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su

[252] El derecho a la tutela judicial efectiva, es un derecho al servicio de otros derechos y no por ello se confunde con ellos. En cierto modo algo parecido ocurre con el derecho a la protección de datos. Ambos son derechos de configuración legal, que permiten la protección de otros derechos sin perder su identidad.

[253] Sirva, como ejemplo ilustrativo de esta afirmación el Considerando 4, en el que se establece que, el RGPD, «respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta […], en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística». Además del Considerando 4, apuntan en esta línea condicional los Considerandos 2, 47, 52, 53, 102 (donde se exige para terceros países un «nivel adecuado de protección»), 111 o 113.

tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales» (Considerando 51 RGPD).

En todos los casos, la necesidad y obligatoriedad de las medidas son contenidos inherentes al derecho a la protección de datos personales. Este, debe procurar ofrecer un mayor nivel de garantía frente a los tratamientos más peligrosos para los demás derechos fundamentales de la ciudadanía. Esto es, a mayor peligro para los derechos, menor margen para el tratamiento de la información personal y mayores exigencias en la regulación.

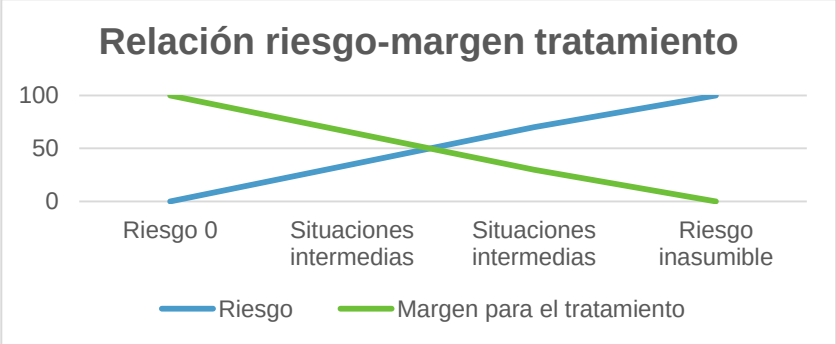

Figura 3. Fuente: elaboración propia

La Figura 3 ilustra esa relación inversa entre el nivel de riesgo para los derechos fundamentales y las posibilidades de llevar a efecto el tratamiento. Si, en la práctica, la relación no es tan proporcional como se muestra en la tabla, ello se debe a que en los tratamientos confluyen otros factores (intereses en concurso, finalidades perseguidas) que pueden hacer variar el nivel de riesgo que se está dispuesto a asumir.

En todo caso, queda patente la existencia de una relación entre el riesgo y el margen de actuación en el tratamiento de datos. El derecho a la protección de datos requiere una necesaria colaboración normativa del legislador, mediante la que establecer un conjunto de medidas que mantengan al riesgo de afectación de los derechos en unos parámetros aceptables para el tratamiento de la información personal.

Ahora bien, que el derecho a la protección de datos sea un derecho de configuración legal con una significada vertiente objetiva, no es óbice para que también incluya la necesaria dimensión subjetiva que lo configura

como un derecho individual. En efecto, la configuración legal del derecho debe incluir ciertas facultades de actuación, destinadas a posibilitar que el tratamiento se desarrolle por los cauces adecuados (art. 8.2 CDFUE)[254]. Las exigencias del apartado 2 del art. 8 se presentan como la ratificación definitiva de la singularidad y autonomía del derecho, (y la constatación de la inadecuación de la tesis de Poscher).

En definitiva, esta vía interpretativa, que amplía la vertiente obligacional del derecho, es la que mejor encaja con su conceptualización europea, al configurar la salvaguarda de los derechos y libertades como uno de los contenidos del derecho, y no como una mera consecuencia[255]. Además, hace plenamente compatible la atribución de un poder de control y disposición con la condición de derecho de configuración legal.

10.3.3. Una variante a considerar. La particularidad española

En la relación entre la protección de la información personal y la salvaguarda de los derechos fundamentales existe una tercera vía, la española. Las particularidades de la misma justifican esta digresión, pues puede resultar una referencia interesante en la determinación de la naturaleza del derecho a la protección de datos en su configuración europea.

En su configuración constitucional, el derecho a la protección de datos tiene una naturaleza bifronte[256] representada, de una parte, por el poder de disposición y control –en su doble vertiente activa y obligacional– y, de otra, por su condición de «derecho instrumental ordenado a la protección de otros derechos fundamentales»[257].

---

[254] Art. 8.2 CDFUE señala que los datos personales serán tratados «de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación».

[255] Además de la exigencia legislativa, a las autoridades de control se les encomienda la protección de los derechos fundamentales afectados por el tratamiento de la información personal (art. 51.1 RGPD) y STJUE asunto C-362/14, Maximillian Schrems y Data Protection Commissioner, 6 de octubre de 2015, apdo. 42.

[256] El TC se refiere a esta condición del derecho del artículo 18.4 CE como «la doble perspectiva, [representada por su condición] como derecho fundamental autónomo dirigido a controlar el flujo de informaciones que concierne a cada persona, y como derecho fundamental instrumental ordenado a la protección del también derecho fundamental a la libertad ideológica» STC 76/2019, de 22 de mayo de 2019, FJ 5.

[257] STC 76/2019, de 22 de mayo de 2019, FJ 5.

En este caso, la condición de «instituto de garantía»[258] del derecho a la protección de datos no surge del poder de control, ni directa ni indirectamente, sino que convive con él en una relación simbiótica de retroalimentación. El derecho a la protección de datos, en su versión española, es un poder de control y es un instituto de garantía. Esta dualidad obedece al particular modo en que se configuró el derecho a la protección de datos en España y, sobre todo, a la condicionalidad que genera la literalidad de la CE. En efecto, el art. 18.4 CE establece un mandato de protección de los derechos[259] que no podía ser eludido por el TC al identificar, en dicho precepto, el derecho a la protección de datos, por lo que tuvo que integrar ambos contenidos.

Esa dualidad llevó a Nicolás Jiménez a señalar que, en el caso de España, «habría que hablar de tutela jurídica de datos personales, operada a través del derecho a la autodeterminación informativa[260] y del derecho a la intimidad» (Nicolás Jiménez, 2006). Si bien esta apreciación no está desencaminada, considero que sería más acorde a la realidad constitucionalmente reconocida que hubiese extendido el ámbito de la tutela jurídica al conjunto de los derechos fundamentales, en lugar de focalizarlo, en exclusiva, en el derecho a la intimidad. Es decir, la fórmula adecuada sería: tutela jurídica de los datos personales=autodeterminación informativa + protección de los derechos fundamentales.

Desde un punto de vista material, la variante española ha generado los mismos resultados que la europea: la protección de los derechos y libertades cuando se tratan informaciones personales está jurídicamente vinculada al derecho a la protección de datos.

10.4. El poder de control y disposición y el resto de facultades y derechos no previstos en la CDFUE

Cabe preguntarse cómo encajan en la interpretación del derecho a la protección de datos como poder de control y disposición el conjunto de facultades y principios no previstos en la CDFUE, pero sí establecidos en la

[258] STC 254/1993, de 20 de julio, FJ 6

[259] Art. 18.4 CE: «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».

[260] La autora considera que la denominación autodeterminación informativa es más adecuada que derecho a la protección de datos, precisamente «para diferenciarlo de la tutela más amplia de la que gozan los datos personales»

normativa que disciplina el tratamiento de la información personal. Pues bien, como advirtiera de Otto, al tratar de determinar el contenido de un derecho fundamental ha de partirse «de una concepción del derecho y de su función» (De Otto y Pardo, 1988, p. 163), en este caso, la del derecho a la protección de datos como poder de control y disposición.

Conforme a esta aproximación hermenéutica, el conjunto de derechos, medidas de protección y exigencias de comportamiento reguladas en el derecho derivado europeo (singularmente en los Reglamentos) son los mecanismos mediante los que preservar los bienes jurídicos del interesado frente a los riesgos que, para su identidad e indemnidad, pudiese generar el tratamiento de su información personal.

Las características específicas del marco regulatorio, más allá de las ineludibles exigencias de la CDFUE, son la plasmación positiva de uno de los modos posibles de hacer efectiva la finalidad que fundamenta al derecho a la protección de datos, a saber, garantizar el poder de control y disposición respecto de los datos a uno referidos. Como, de Otto ha señalado, «la determinación de las concretas facultades reaccionales de un derecho, la opción por esta o aquella fórmula de protección […] está condicionada en buena medida […] por el peso que se dé al elemento libertad o al elemento institución» (De Otto y Pardo, 1988, p. 163). En el caso del derecho a la protección de datos, su actual configuración normativa es el reflejo de un modo concreto de entenderlo, el europeo.

Naturalmente, las facultades que el derecho derivado reconoce son una manifestación del poder de control y disposición, pues, en caso contrario, no podrían formar parte de la normativa que desarrolla el derecho a la protección de datos. Entendido de este modo, los derechos de supresión, limitación, oposición, portabilidad, intervención humana en decisiones automatizadas serían las facetas que se han decidido pulir de ese diamante en bruto que el derecho a la protección de datos. Pero podrían no haberse revelado todas ellas o, incluso, haberse incorporado otras, como el derecho a unas inferencias justas[261].

[261] Derecho destinado a hacer frente a las decisiones algorítmicas que busca evitar situaciones de discriminación, así como otorgar una posición de dominio a la persona frente a este tipo de operaciones al permitirle actuar sobre el modo en que los datos son tratados. Wachter y Mittelstadt realizan la propuesta que, en mi opinión, mejor perfila las características de ese posible derecho a incorporar al arsenal de la protección de datos, vid. (Wachter y Mittelstadt, 2019).

Por consiguiente, el elemento identificador del derecho a la protección de datos no son las actuaciones concretas, sino el fundamento que las justifica, el poder de control y disposición. Cómo se desarrolle el derecho, las caras del diamante que se quieran mostrar, será el producto de decisiones político-jurídicas, que la se limitará normativa reflejar. Adicionalmente, la jurisprudencia también puede llegar a operar como orfebre y "descubrir" alguna nueva faceta del derecho[262].

Conforme a esta opción hermenéutica, el derecho a la protección de datos no es una mera manifestación de voluntad, sino que entraña, también, un conjunto jurídico de obligaciones de comportamiento, garantías institucionales y mecanismos de actuación destinados a generar las condiciones propicias para la defensa de los intereses jurídicos del interesado frente al tratamiento de sus datos personales. Esta fisonomía compleja y poliédrica pone de manifiesto su carácter finalista y formalizado.

Aunque la vertiente activa del derecho como poder de disposición y control refleja, de un modo directo, esa capacidad de dominio sobre la información personal; es la vertiente objetiva plasmada, por ejemplo, en la obligación de salvaguarda de los derechos y libertades o la necesidad de establecer las condiciones para el ejercicio del derecho (v. gr. mediante la articulación de bases de licitud del tratamiento distintas de consentimiento), la que condiciona de un modo más intenso el desarrollo del tratamiento, garantizando el despliegue efectivo del poder de disposición y control. El desarrollo normativo del derecho, la articulación y ejecución de las medidas necesarias para su ejercicio, son esenciales para comprender la fisonomía del derecho a la protección de datos.

De este modo, el derecho a la protección de datos como poder de control y disposición y como derecho de configuración legal convergen, dando como resultado la obligación de articular un marco regulatorio adecuado para disciplinar el tratamiento de la información personal.

[262] Como ocurrió con la formulación del derecho al olvido en la STJUE asunto C-131/12, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014.

10.5. El problema del derecho del derecho

La eventual existencia de un derecho a la protección de datos, que el derecho fundamental a la protección de datos debe salvaguardar (art. 1.2 *in fine* de los Reglamentos[263]) es una realidad jurídico-normativa de difícil explicación desde la conceptualización unívoca del derecho a la protección de datos como poder de control y disposición.

No resulta posible plantear, ni siquiera a título de hipótesis, cuál sería el contenido de ese segundo derecho a la protección de datos. Si el derecho fundamental tiene como finalidad asegurar un poder de disposición y control al interesado, ¿cuál sería la función, el objeto, de ese segundo derecho? La respuesta se antoja imposible. El derecho a la protección de datos como poder de control surge desde lo concreto, está estrechamente vinculado a las actuaciones directas del interesado, no quedando espacio disponible para ese segundo derecho.

En definitiva, a pesar de servir para explicar las diferentes manifestaciones del derecho a la protección de datos, su condición como poder de control no parece conciliable con la existencia de dos derechos a la protección de datos diversos, por más que puedan ser convergentes o estar relacionados.

11. La tutela jurídica de los datos personales. El derecho a la protección de datos en sentido amplio y en sentido estricto

11.1. Un escenario diabólico

El estudio de las posibles naturalezas del derecho a la protección de datos arroja un panorama desconcertante. En efecto, aunque todas la opciones interpretativas, incluso las negadoras del carácter *iusfundamental* y autónomo del derecho, son capaces de explicar alguna de las manifestaciones del mismo; especialmente el derecho como poder de control y disposición que, en una concepción amplia de su vertiente objetiva es capaz de justificar, de un modo coherente, la mayor parte de los contenidos y actuaciones caracterizadores del derecho fundamental. Sin embargo, ninguna de las opciones planteadas parece ser capaz de ofrecer

[263] V. gr. art. 1.2 RGPD: «El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales».

una respuesta completa y satisfactoria a la existencia de ese derecho a la protección de datos cuya salvaguarda deben asegurar las normativas de protección de datos (art. 1.2 de los Reglamentos).

Por otra parte, el objeto de las normativas, además de sembrar la duda acerca de cuál es ese derecho a la protección de datos cuyo cometido se ha de salvaguardar, pone de manifiesto la condición de instituto de garantía de los derechos y libertades del derecho fundamental a la protección de datos. Una condición que no puede considerarse accesoria al derecho, sino que forma parte de él, pues, como hemos visto, los Reglamentos son el desarrollo y manifestación del derecho reconocido en el art. 8 de la CDFUE y 16 del TFUE.

Esas dos variables (el derecho del derecho y la relación entre la protección de datos y los demás derechos), junto a las actuaciones específicas que el derecho a la protección de datos posibilita con relación al tratamiento de los datos personales, descartan cualquier propuesta que plantee una concepción unívoca del derecho. Consecuentemente, la pregunta persiste ¿cuál es el fundamento del derecho a la protección de datos? La respuesta parece residir en la aceptación de que, el derecho a la protección de datos, se funda sobre más de una base jurídica. En definitiva, aceptando que no hay una única alma residiendo en la configuración europea del derecho a la protección de datos.

11.2. Las finalidades como factor delimitador y definidor de la naturaleza del derecho a la protección de datos

Las diferentes opciones interpretativas vistas hasta el momento proporcionan una respuesta jurídicamente consistente con la fisonomía del derecho. Por consiguiente, esas opciones hermenéuticas no deben ser completamente desechadas, hay en ellas un reflejo de la realidad jurídica del derecho a la protección de datos.

Su problema radica en que buscan amoldar una naturaleza jurídica compleja y diversa en una única horma, siendo incapaces de reflejar todos los matices de la pieza original. Con todo, las interpretaciones vistas hasta el momento nos han permitido conocer las características del derecho y sus finalidades. Con ellas como referencia, se puede llegar a determinar la naturaleza real del derecho.

Si las propuestas "negacionistas" ponían de manifiesto la vinculación entre el derecho a la protección de datos y la protección de los derechos fundamentales, e incidían en la importancia del desarrollo normativo como elemento caracterizador del derecho; la interpretación del derecho como derecho de configuración legal sublimó dichos aspectos hasta convertirlos en el fundamento mismo del derecho, situando a los riesgos como agente de cambio. Es decir, los datos no se protegerían tanto por lo que son (reflejo de la persona), sino por los efectos que su uso pudiera causar.

Esa condición conectaría con las razones históricas que laten en el surgimiento del derecho a la protección de datos: la defensa de las personas frente a las amenazas derivadas de la emergencia del tratamiento automatizado de datos personales y la consiguiente desaparición de las barreras de protección que el tiempo, el esfuerzo y los costes proporcionaban. En definitiva, la configuración legal es el reflejo de un derecho centrado en el tratamiento del dato y la prevención de sus consecuencias, y menos condicionado por la naturaleza de la información.

Sin embargo, el derecho como poder de control y disposición se funda en el vínculo dato-persona. Es ese nexo el que determina la existencia, intensidad y alcance del dominio sobre la información personal. La posición de dominio que el derecho confiere tiene como objetivo velar por la preservación de la identidad personal del sujeto lo que, en una interpretación extensiva, permite a esta opción hermenéutica explicar tanto las facultades atribuidas a los interesados, como las obligaciones generales de protección de los derechos y libertades fundamentales, condicionando, por esa vía, el desarrollo legislativo del derecho.

Sin embargo, en la medida en que dicha opción no termina de explicar el objeto del RGPD (art. 1.2), parece oportuno acotar el alcance de dicho poder de control y disposición, y no atribuirle finalidades generales de salvaguarda. Conforme a esta reconsideración, la atribución de una posición de dominio sobre los datos personales no tendría una función finalista. Esto es, no se reconocería un poder de disposición para lograr objetivos predefinidos, sino que las facultades de actuación obedecerían, únicamente, a la existencia del vínculo dato-persona. Consecuentemente, sus finalidades serían exclusivamente subjetivas, pudiendo atribuírseles, solamente, la función de reflejar la voluntad del sujeto y el dominio de este sobre su proyección exterior, sin importar para qué haga uso de dicho poder.

Entendido de este modo, solo aquellas previsiones destinadas a asegurar que el individuo pueda controlar el uso de la información tendrían cabida en el concepto de derecho a la protección de datos como poder de control y disposición. Esto es, sería la manifestación exclusiva de la autodeterminación informativa, en su sentido más estricto.

Como puede comprenderse, esta interpretación restrictiva del alcance de la posición de dominio supone excluir de su contenido la salvaguarda de los derechos y libertades fundamentales. En la medida en que se trataría de un objetivo que, si bien se podría lograr mediante el ejercicio de ese poder de control y disposición, no sería una finalidad consustancial a dicho poder, sino una de las posibles consecuencias.

Desde un punto de vista práctico, esto supondría que, cuando se reconoce el derecho de acceso a los datos personales se hace, sencillamente, porque dichos datos están referidos a la persona que solicita el acceso, sin importar cuál sea la finalidad que lleva al interesado a querer acceder a ellos. Esta posición, por lo demás, resulta coherente con el hecho de que el interesado no tiene porqué motivar las razones que subyacen al consentimiento prestado o al ejercicio de las facultades de actuación, excepto, naturalmente, en aquellos casos en que su ejercicio entre en conflicto con otros intereses en concurso y, en todo caso, será una justificación a posteriori, no un requisito para su ejercicio (p. ej. cuando se pretenda acceder a una información personal sujeta a secreto profesional, por estar siendo tratada por un abogado).

Por lo tanto, es razonable concluir que, en la tutela jurídica de los datos personales, concurren dos finalidades diferentes (la salvaguarda de los derechos y el dominio sobre la proyección externa del ser).

Entendido de este modo, y aceptando que, en el derecho a la protección de datos conviven dos almas. La primera, se correspondería con el deber de protección destinado a salvaguardar los derechos y libertades fundamentales mediante la regulación, ejecución y fiscalización del tratamiento de la información personal. A esta realidad jurídica podemos denominarla como derecho a la protección de datos en sentido amplio, pues se focalizaría en proporcionar una protección de carácter general y preventivo, destinada a disciplinar los usos y tratar de impedir los abusos y consecuencias que la utilización de la información personal pudiera deparar. En este sentido, se trataría de un derecho que tendría en el

tratamiento su objeto de regulación y en los legisladores, responsables del tratamiento y autoridades de control a sus destinatarios.

La segunda de las almas del derecho, a la que podemos denominar como derecho a la protección de datos en sentido estricto, se compadecería con el derecho como poder de control y disposición. En este caso, su ámbito de actuación estaría circunscrito a asegurar la autodeterminación informativa mediante la atribución de facultades de actuación directa sobre los datos a uno referidos (desde consentir su uso hasta instar su supresión, pasando por el resto de posibilidades que normativamente se establezcan, si bien los derechos de acceso y rectificación estarían necesariamente incluidos). Esa vertiente activa iría acompañada de una vertiente obligacional, destinada a garantizar las condiciones necesarias para hacerla efectiva (p. ej. regulando los modos de ejercicio o imponiendo deberes de información que permitan un uso más eficaz de las posibilidades de actuación).

11.3. El derecho fundamental a la protección de datos en su configuración europea

11.3.1. La unidad de lo dual

Una vez se han identificado los dos elementos que concurren en la tutela jurídica de los datos personales, la siguiente incógnita a despejar es la relativa a la existencia de un único derecho fundamental a la protección de datos (el reconocido en el art. 8 de la CDFUE), esto es, ¿cómo encaja la dualidad de almas con el reconocimiento de un único derecho fundamental?

La respuesta a esa cuestión radica en el objeto, pues, tanto el derecho a la protección de datos en sentido amplio, como el derecho a la protección de datos en sentido estricto se proyectan sobre los datos personales y su tratamiento. Es decir, en la tutela jurídica del tratamiento de la información personal concurren dos realidades jurídicas.

Por lo tanto, para asegurar el derecho que «toda persona tiene […] a la protección de los datos de carácter personal que la conciernan» (art. 8.1 CDFUE), es necesario garantizar las finalidades que fundamentan a ambas realidades. En términos matemáticos, el derecho fundamental a la protección de datos en su configuración europea sería igual a la suma del

derecho a la protección de datos en sentido amplio más el derecho a la protección de datos en sentido estricto. Ambos conforman una entidad única, a la que dotan de sustantividad y contenido. El derecho fundamental a la protección de datos es un derecho de derechos.

11.3.2. Contenido autónomo y convergencia de los derechos del derecho fundamental a la protección de datos

Entendido el derecho a la protección de datos como un derecho bifronte, en el que confluyen dos vertientes destinadas a conformar un marco normativo completo[264], las interrelaciones entre ellas contribuyen a establecer cuál es el contenido y naturaleza real del derecho fundamental a la protección de datos, en su configuración europea.

11.3.2.1. El derecho a la protección de datos en sentido amplio

El derecho a la protección de datos en sentido amplio exigiría la toma en consideración de los posibles efectos que un determinado tratamiento pudiera tener sobre los derechos del interesado. Estaríamos ante una obligación cuyos principales destinatarios son: el legislador y los responsables del tratamiento (en tanto son quienes determinan los fines y los medios del tratamiento)[265].

El legislador debe diseñar un marco normativo en el que se establezcan las medidas adecuadas para evitar la afectación de los derechos de los interesados, so pena de incurrir en la vulneración del derecho fundamental. En el diseño de la regulación destinada a disciplinar el tratamiento de información personal habrá de asegurarse que las medidas adoptadas y los tratamientos habilitados cumplan con las

[264] Van der Sloot (Van der Sloot, 2017, p. 24) señalaba como una de las razones para negar la *iusfundamentalidad* del derecho a la protección de datos la extensión y grado de detalle de la regulación sobre la materia, remarcando que excede al habitual desarrollo legislativo de un derecho fundamental. Como puede constatarse, el nivel de detalle de la regulación viene exigido por el propio contenido del derecho, merced, sobre todo, al derecho a la protección de datos en sentido amplio.

[265] Art. 4.7 RGPD: «"responsable del tratamiento" o "responsable": la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento»

exigencias del artículo 52.1 de la CDFUE (respeto al contenido esencial y al principio de proporcional, amén de regulación legal).

Esta exigencia cobra plena vigencia en el desarrollo de la regulación sectorial, esto es, en la articulación de medidas específicas para tratamientos concretos en ámbitos determinados. En estos casos, la nueva legislación (pues ha de establecerse mediante ley) habrá de cumplir con las condiciones del 52.1 de la CDFUE, además de respetar las exigencias del marco general de protección (los principios del tratamiento y el reconocimiento de facultades de actuación).

En lo referente a los responsables, estos habrán de cumplir con las exigencias que normativamente se les impongan para asegurar que el tratamiento transcurre por cauces jurídicamente aceptables. En el caso del modelo europeo de protección de datos, ese conjunto de obligaciones incluiría el respeto a los principios del tratamiento (art. 5 del RGPD); la protección de datos desde el diseño y por defecto (art. 25 RGPD), con la consecuente adopción de las medidas técnicas y organizativas necesarias para asegurar la seguridad del tratamiento; la llevanza de un registro de actividades (art. 30 RGPD); la realización de evaluaciones de impacto (arts. 35 y 36 RGPD) y, en general, la adopción de las medidas apropiadas para reducir los riesgos inherentes a cualquier tratamiento.

11.3.2.2. El derecho a la protección de datos en sentido estricto

El derecho a la protección de datos en sentido estricto puede operar sin otro fundamento que la activación de sus propias atribuciones. Como se ha apuntado, el ejercicio de las facultades de actuación no se funda en las concretas medidas que regulen el tratamiento, sino en la mera voluntad del sujeto.

Cuestión diferente es que las condiciones en que se opere con los datos, o los riesgos que el tratamiento concreto pueda implicar, sirvan de acicate al interesado para ejercitar los derechos de acceso, rectificación o aquellos otros que normativamente se hayan reconocido en desarrollo del poder de control y disposición. Pero, en todo caso, las circunstancias, el contexto del tratamiento, no serían el fundamento, sino un detonante para la activación de las facultades de actuación.

En este punto, se pone de manifiesto una diferencia sustancial entre el derecho a la protección de datos en sentido amplio y en sentido estricto. Mientras en el primero el contexto, el riesgo y la realidad del tratamiento son determinantes para su materialización, en el segundo es indiferente, pues su razón de ser es el vínculo dato-persona, no los eventuales efectos y peligros que el tratamiento pudiera deparar.

Por otra parte, no deja de ser reseñable que el derecho a la protección de datos en sentido estricto, a su vez, contenga un conjunto de derechos que le dotan de contenido. En efecto, los derechos de acceso, rectificación, y los demás reconocidos por la normativa europea (oposición, limitación del tratamiento, supresión, portabilidad, intervención humana en las decisiones automatizadas) tienen su cometido y finalidad específicos, pero, a su vez, integran el derecho a la protección de datos en sentido estricto. Es, por tanto, un derecho complejo[266], un «derecho racimo», como elocuentemente lo definió Jiménez Asensio (Jiménez Asensio, 2019, p. 31).

Un razonamiento similar al de las facultades puede realizarse con relación al consentimiento, su prestación es, en exclusiva, una manifestación de voluntad del interesado. Las condiciones en que se van a tratar los datos, los riesgos que pueda suponer, son factores que tiene derecho a conocer y valorar para conformar su voluntad. Pero la capacidad para decidir acerca del destino de la información a él referida no trae causa de esas circunstancias, sino de su derecho a la autodeterminación informativa.

En definitiva, cada una de las dos almas del derecho fundamental a la protección de datos tiene un espacio propio, vinculado a la finalidad que le caracteriza.

[266] Al igual que ocurre, por ejemplo, con el derecho a la tutela judicial efectiva, que es «un derecho fuente del que emanan a su vez derechos específicos» (González Alonso, 2012, p. 149).

11.3.2.3. Convergencias entre el derecho a la protección de datos en sentido amplio y el derecho a la protección de datos en sentido estricto

Pese a sus contenidos particulares, el derecho a la protección de datos en sentido amplio y el derecho a la protección de datos en sentido estricto conforman un único derecho fundamental. En este sentido, y aunque se trate de realidades con finalidades diferentes, lo cierto es que comparten muchos de sus elementos, más allá del común objeto sobre el que se proyectan.

El derecho fundamental a la protección de datos en su configuración europea es el reflejo de una relación simbiótica entre las dos almas que le dan vida. Señalábamos en páginas precedentes que, si hubiera que expresar matemáticamente la naturaleza del derecho fundamental, este sería la suma de las dos realidades jurídicas que lo integran. Lo cierto es que, para ser precisos, un diagrama de Venn (ver Figura 4) representaría mejor la multiplicidad de interrelaciones, sumas, multiplicaciones y simplificaciones que se producen entre los dos derechos que conforman el derecho fundamental. Por así decirlo, la fórmula derecho a la protección de datos en sentido amplio + derecho a la protección de datos en sentido estricto = derecho fundamental a la protección de datos sería la versión simplificada de una relación compleja y con contornos difusos.

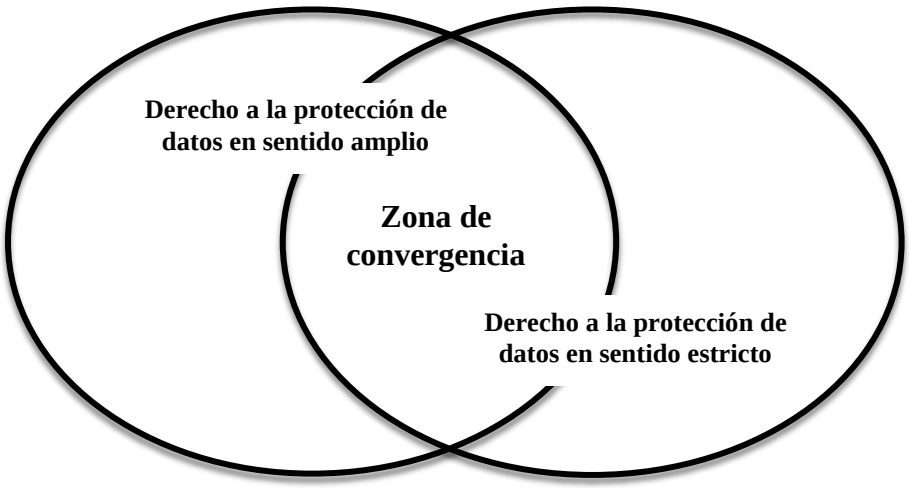

Figura 4: Representación del derecho fundamental a la protección de datos. Elaboración propia

A efectos puramente ilustrativos, en las próximas páginas se dará cuenta de algunos ámbitos en los que se refleja la convergencia entre las dos almas del derecho fundamental a la protección de datos.

A. La regulación como nexo de unión

Las normativas de protección frente al tratamiento de la información personal protegen «los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales» (art. 1.2 de los Reglamentos). La dificultad para encontrar una explicación jurídicamente satisfactoria a esta previsión ha sido uno de los detonantes que han llevado a descartar las opciones interpretativas del derecho como poder de control y disposición. Sin embargo, a la luz de la conceptualización dual del derecho fundamental, cobra pleno sentido.

Si la salvaguarda de los derechos fundamentales mediante la articulación de un modelo de protección capaz de hacer jurídicamente aceptable el tratamiento de la información personal coincide con lo que se ha denominado derecho a la protección de datos en sentido amplio, el mandato general que el art. 1.2 de los Reglamentos tiene pleno sentido. Pero, ¿cómo encaja la mención expresa al derecho a la protección de datos? La respuesta es ahora automática, ese derecho al que ha de prestarse particular atención es el derecho a la protección de datos en sentido estricto. Esto es, la faceta del derecho fundamental centrada en asegurar un espacio de libertad para el sujeto, en el que pueda desplegar su poder de control y disposición respecto de la información a él referida.

Por consiguiente, en aquellos casos en que la jurisprudencia o la normativa hagan referencia al derecho a la protección de datos como parte de un todo más amplio, están refiriéndose al derecho a la protección de datos en sentido estricto.

Pudiera plantearse que el derecho a la protección de datos en sentido estricto está subordinado al derecho a la protección de datos en sentido amplio, esto es, que dentro del derecho fundamental habría

jerarquías. No es así. En primer lugar, porque cada uno de ellos tiene su cometido propio y, en segundo lugar, en aquellos aspectos que confluyen, la relación entre las dos almas del derecho fundamental es de retroalimentación e influencia mutua.

Los derechos y libertades y, consecuentemente, también el derecho a la protección de datos en sentido estricto, son los que delimitan el modo en que se ha de desarrollar ese deber de protección frente al tratamiento de la información personal. Son los parámetros que permiten determinar qué modo de tratar los datos personales es jurídicamente aceptable. Por lo tanto, el derecho a la protección de datos en sentido estricto no está subordinado al derecho a la protección de datos en sentido amplio, más bien al contrario, lo condiciona.

Sin embargo, mientras la mayoría de los derechos y libertades fundamentales tienen una condicionalidad abstracta y focalizada en la implementación de medidas de seguridad destinadas a prevenir su afectación, en el caso del derecho a la protección de datos en sentido estricto, el cumplimiento del deber de protección requiere la inclusión de sus contenidos en la normativa destinada a disciplinar el tratamiento de la información personal. Es decir, para cumplir con el deber de protección que caracteriza al derecho a la protección de datos en sentido amplio, han de incorporarse, a la regulación general, los contenidos del derecho a la protección de datos en sentido estricto.

Esta particularidad se debe, en primer lugar, a que el derecho a la protección de datos en sentido estricto incide directamente sobre la materia objeto de regulación (los datos personales) y, en segundo lugar, a su particular morfología: un derecho eminentemente activo, focalizado en proporcionar a los interesados facultades de actuación frente al uso de sus datos).

De este modo, el derecho a la protección de datos en sentido amplio se cumple al considerar las exigencias respecto del tratamiento de los datos que el derecho a la protección de datos en sentido estricto demanda. A su vez, el derecho a la protección de datos en sentido estricto encuentra, en el derecho a la protección de datos en sentido amplio, el marco normativo en que desplegar sus contenidos del modo más adecuado posible.

El derecho a la protección de datos en sentido amplio, al tener que considerar los diferentes intereses en concurso, termina dando lugar a un producto normativo que es, en sí mismo, un sistema de resolución de

conflictos entre derechos. Efectivamente, el marco normativo en que se materializa el derecho a la protección de datos en sentido amplio, al considerar los derechos que, de algún modo, pueden concurrir en el tratamiento de la información, se constituye en un sistema que ha de incorporar las reglas necesarias para asegurar un equilibrio entre el uso de datos personales y el respeto a los derechos y libertades, también al derecho a la protección de datos en sentido estricto.

En definitiva, la regulación del tratamiento de la información es la manifestación del derecho fundamental a la protección de datos como un todo. El marco jurídico en que se desarrolla es el agregado de los componentes que lo integran. Más allá de la común regulación de los elementos que conforman el derecho fundamental a la protección de datos, sus dos almas también convergen en ámbitos específicos, como son los principios del tratamiento y las autoridades de control.

B. Los principios de tratamiento y la garantía del derecho

La operatividad común en las condiciones de tratamiento de la información personal no deja de ser una consecuencia lógica de que ambas manifestaciones del derecho fundamental tengan el mismo sustrato (los datos y su tratamiento). Tanto las obligaciones previstas en el art. 8.2 de la CDFUE (tratamiento leal, para fines concretos y con un base de licitud adecuada), como el resto de principios que normativamente se establezcan para disciplinar el tratamiento de la información personal (transparencia, minimización de datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva[267]; así como la obligación de aplicar la protección de datos desde el diseño y por defecto[268]) ponen en conexión a las dos facetas del derecho fundamental.

Las obligaciones de actuación tienen conexión directa con la finalidad que fundamenta el derecho a la protección de datos en sentido amplio (la salvaguarda de los derechos y libertades fundamentales mediante la regulación, ejecución y fiscalización del tratamiento de la información personal). Sin embargo, su cumplimiento contribuye a

[267] Art. 5 del RGPD y 4 del Reglamento 2018/1725.

[268] Art. 25 del RGPD y art. 27 del Reglamento 2018/1725. Aunque la protección de datos desde el diseño y por defecto no está catalogada como principio, lo cierto es que impone una serie de obligaciones de actuación a la hora de llevar a efecto cualquier operación de tratamiento de datos que, en la práctica, opera de un modo similar a los principios.

construir el escenario más adecuado para que los interesados puedan hacer efectivo su poder de control y disposición. Es decir, los principios, bien de modo directo (reconocimiento del consentimiento como base habilitante), bien indirectamente, facilitan el despliegue del derecho a la protección de datos en sentido estricto.

Entre las influencias indirectas se encontrarían, a título puramente ilustrativo, el principio de transparencia[269], en tanto que facilita el conocimiento de las condiciones del tratamiento y permite una mayor efectividad en el ejercicio del poder de control y disposición (ya sea por conocer mejor las condiciones para consentir, ya para ejercitar las facultades de actuación con mayor precisión)[270]. El principio de minimización[271], además de reducir los riesgos del tratamiento, también acota la materia prima sobre la que se ha de proyectar el dominio de la proyección exterior del ser, facilitando su control.

Por su parte, la protección de datos desde el diseño y por defecto[272], al exigir la implementación de las «medidas técnicas y organizativas apropiadas»[273] para que el tratamiento de la información se lleve a cabo de un modo seguro y con todas las garantías, no solo reduce riesgos, también contribuye a hacer más efectivo el poder de control y disposición, al generar las condiciones adecuadas para el seguimiento y fiscalización del uso de la información y, consecuentemente, el ejercicio de las facultades de actuación.

En el caso del principio de exactitud, la relación es mucho más directa, pues se presenta como la contraparte obligacional y constante del derecho de rectificación. En efecto, al imponer al responsable que opere con datos exactos y actualizados, se están reduciendo los casos en que el interesado ha de acudir al derecho de rectificación, pues la finalidad que persiguen es la misma: que los datos reflejen la realidad y, consecuentemente, proporcionen una imagen fiel de la persona a la que se

[269] Sobre el principio de transparencia, su contenido y exigencias, vid. (Muñoz, 2018) y (Palma Ortigosa, 2018b).
[270] Recuérdese que, aunque no había condiciones previas para el ejercicio de los derechos de actuación, en ocasiones había límites y trabas a su uso reiterado. Por lo tanto, a mayor información y claridad en los tratamientos, más sencillo será evitar tener que acudir reiteradamente a los instrumentos jurídicos de actuación directa que el derecho a la protección de datos en sentido estricto reconoce.
[271] Sobre el principio de minimización, su contenido y aplicación, vid. (IT, 2019, pp. 42-43), (Binns y Gallo, 2019), (Biega, Potash, Daumé, Diaz, y Finck, 2020).
[272] Sobre la protección de datos desde el diseño y por defecto, su contenido y exigencias, vid. (R. Miralles López, 2021) y (Duaso Calés, 2016).
[273] Arts. 25.1 y 25.2 del RGPD y 27.1 y 27.2 del Reglamento 2018/1725.

refieren. Este principio es, en esencia, una objetivación del derecho de rectificación.

Los principios generan un ecosistema operacional en que el derecho a la protección de datos en sentido amplio y el derecho a la protección de datos en sentido estricto operan en perfecta simbiosis, beneficiándose mutuamente o, lo que es lo mismo, contribuyendo a la plena satisfacción del derecho fundamental a la protección de datos.

No obstante, en el principio de licitud[274], más que una simbiosis entre las dos almas del derecho fundamental, se produce una mera agregación de opciones. Esto es, a la manifestación de voluntad que el consentimiento representa se han incorporado, en pie de igualdad, otras opciones habilitantes del tratamiento de la información personal[275].

Tanto las nuevas posibilidades, no dependientes de la actuación del interesado, como la imposición de obligaciones de comportamiento a quienes vayan a operar con los datos, refuerzan la vertiente obligacional del derecho. Esa objetivación constante del derecho, la implementación de contrapesos y medidas jurídico-técnicas, tendría como finalidad prevenir una afectación incontrolada de la esfera personal (Kranenborg, 2014, pp. 228-229) y, a su vez, ratifica el carácter procedimental del derecho fundamental a la protección de datos.

Al formalizar y objetivar los usos de la información personal, no solo se logra que los datos sean tratados de un modo más previsible, estructurado y seguro, sino que se colectiviza la defensa de los bienes jurídicos del interesado. Ya no será el sujeto afectado, mediante el ejercicio de su derecho a la autodeterminación personal, el único que vele por la salvaguarda de su proyección exterior, sino que el resto de operadores que intervienen en el tratamiento tendrán su cuota de responsabilidad en la garantía del derecho fundamental a la protección de datos.

C. La garantía institucional común. Las autoridades de control

[274] Este principio supone, como se recordará, la obligación de contar con una base de legitimación adecuada para el tratamiento de la información personal.

[275] Son bases de licitud, el consentimiento, contrato, obligación legal, protección de intereses vitales, misión realizada en interés público o ejercitando poderes públicos y, finalmente, la concurrencia de algún interés legítimo del responsable o de un tercero que prevalezca sobre los intereses del interesado (art. 6 del RGPD).

El deber de «proteger los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento y […] la libre circulación de datos personales» (art. 51.1 RGPD), que caracteriza a las autoridades de control, es fiel reflejo –como ocurría con la regulación normativa– de la convergencia de las dos caras del derecho fundamental o, lo que es lo mismo, del porqué de su unidad pese a las diferencias.

Esa encomienda de protección de los derechos fundamentales que pudieran verse afectados por el tratamiento de la información personal coincide con el contenido del derecho a la protección de datos en sentido amplio. Esto es, la función de las autoridades de control es velar porque se den las condiciones adecuadas para que el tratamiento de la información sea jurídicamente aceptable, lo que incluye, como hemos visto, la garantía del derecho a la protección de datos en sentido estricto. Sin embargo, no debería extenderse a la reparación de los daños efectivamente producidos en los demás derechos fundamentales, pues cada uno de ellos tiene las medidas de respuesta frente a la vulneración que el ordenamiento jurídico reconozca.

En este sentido, la función de las autoridades de control es velar por que se implementen las medias adecuadas para el tratamiento de la información personal, así como asegurar que no se impida, de manera injustificada, el ejercicio del poder de control y disposición sobre los datos personales. Esto es, realiza tanto un control general del marco de actuación, como una atención particularizada a supuestos concretos donde se pueda obstaculizar el dominio sobre la proyección exterior.

El conjunto de atribuciones que tienen encomendadas, desde las destinadas a orientar y promover buenas prácticas en la materia, hasta las de inspección y sanción, dan buena cuenta de su importancia en el sistema de protección. Algo que, por otra parte, se compadece con su inclusión en el 8.3 de la CDFUE y el 16.2 del TFUE como uno de los elementos definitorios del derecho fundamental.

12. Elementos definitorios del derecho fundamental a la protección de datos

12.1. Un simbionte

El derecho fundamental a la protección de datos, en su configuración europea, es un simbionte. En él conviven dos realidades jurídicas, el derecho a la protección de datos en sentido amplio y el derecho a la protección de datos en sentido estricto. Cada una de ellas persigue una finalidad diferente, sin embargo, ambas concurren sobre el mismo objeto: los datos y su tratamiento; además, se retroalimentan y benefician mutuamente, conformando ese simbionte que es el derecho fundamental.

Si se quiere conocer la naturaleza del derecho fundamental, han de comprenderse los elementos que lo conforman, aunque en la práctica no sea posible distinguir con claridad dónde comienza uno y dónde termina el otro, como gráficamente se ha representado con el diagrama de Venn (Figura 4). En este sentido, el elemento a considerar son las finalidades que dan vida a cada una de las dos almas del derecho fundamental: la salvaguarda de los derechos y libertades frente a los riesgos derivados del tratamiento de la información personal (derecho a la protección de datos en sentido amplio) y la protección de la proyección exterior del ser mediante el ejercicio de un poder de control y disposición sobre la información a uno referida, destinada a asegurar que somos percibidos por lo demás conforme a nuestra realidad (derecho a la protección de datos en sentido estricto).

El derecho fundamental a la protección de datos se asemeja notablemente a la concepción dual de la *privacy* planteada por Fried. Este considera que la privacy supone «*the control we have over information about ourselves*» (Fried, 1968, p. 482) y, además, es un instituto de garantía de la libertad personal[276].

12.2. La faceta eminentemente subjetiva: el poder de control y disposición

El control sobre la información a uno referida se funda en el vínculo dato-persona y constituye la proyección de la voluntad personal sobre el destino de los datos personales. Desde el punto de vista de la

[276] «*Besides giving us control over the context in which we act, privacy has a more defensive role in protecting our liberty*» (Fried, 1968, p. 483).

caracterización del derecho fundamental, implica que, cualquiera que sea el modelo de tratamiento que se implemente, para garantizar la protección del derecho fundamental, se ha de asegurar al interesado la posibilidad de ejercitar las actuaciones necesarias para preservar su control sobre los datos atinentes a su persona.

En cuanto a su materialización, se concreta tanto en la posibilidad de consentir –sin perjuicio del establecimiento de otras opciones o, incluso, la reducción del abanico de tratamientos para los que el consentimiento puede operar como condición habilitante–, como en el reconocimiento de facultades de actuación directa sobre los datos, singularmente las posibilidades de acceder y rectificar reconocidas en la CDFUE.

Naturalmente, el poder de control y disposición no se agota en los derechos de acceso y rectificación, sino que puede manifestarse de otros modos. Las facultades de actuación que la normativa europea reconoce son prueba de ello[277]. En todo caso, el elemento definitorio del derecho radica en que el interesado cuente con las herramientas adecuadas para asegurar su posición de dominio.

El constante desarrollo técnico, y el consecuente incremento de la complejidad y magnitud de los tratamientos, requiere una actualización y ampliación constante de los instrumentos jurídicos destinados a hacer efectivo el poder de control y disposición. Ello implica que, de una parte, no hay un *numerus clausus* de facultades de actuación que identifiquen al derecho y, de otra parte, que difícilmente se podrá prescindir de aquellos derechos actualmente reconocidos, salvo que se quedasen obsoletos o fuesen reemplazados por una versión más adecuada a las exigencias de cada momento (como en parte ha ocurrido con el derecho de cancelación y el derecho de supresión que viene a ser como una versión 2.0 de aquel).

Es decir, las facultades que actualmente caracterizan el derecho a la protección de datos, al ser necesarias para asegurar el poder de disposición y control, no son prescindibles, han pasado a integrar el contenido definitorio del derecho y, por lo tanto, cualquier limitación de las mismas habría de cumplir con las exigencias del art. 52.1 de la CDFUE.

Por otra parte, la vigencia del poder de control y disposición requiere de una evaluación constante de los instrumentos jurídicos

[277] Sería el caso de los derechos de supresión, limitación, oposición, portabilidad, intervención humana en decisiones automatizadas.

disponibles para asegurar su efectividad. Solo de ese modo se podrá determinar su vigencia y, de ser necesario, reconocer nuevas atribuciones, como podría ser el derecho a unas inferencias justas.

De este modo, puede afirmarse que la constante en el derecho fundamental a la protección de datos es el poder de control y disposición, pero sus manifestaciones concretas se han de ir acomodando a las exigencias de un entorno en permanente transformación.

El contexto y la realidad de los tratamientos son factores evolutivos para el derecho a la protección de datos, ya sea ampliando sus capacidades de actuación, ya condicionando el modo en que se manifiesta la voluntad del interesado, como ocurre con el consentimiento.

12.3. La faceta normativo-preventiva y la salvaguarda de los derechos y libertades

La importancia del contexto, la necesidad de adaptarse a la constante evolución de las posibilidades de tratamiento y defenderse de los riesgos y consecuencias que ello supone es una nota común entre las dos vertientes del derecho fundamental a la protección de datos, pues también es un factor a considerar para alcanzar la finalidad del derecho a la protección de datos en sentido amplio.

Esta vertiente del derecho fundamental exige que cualquier actuación que implique el tratamiento de la información personal transcurra por cauces jurídicamente aceptables. Además, ha de estar encaminada a la protección de los derechos y libertades de la persona frente a los posibles efectos adversos que el uso de datos a ella referidos pueda generar. Al presentarse como un derecho finalista y preventivo, será necesario una actualización y revisión constante para asegurar su alineación con los objetivos perseguidos.

En esta faceta del derecho fundamental, los derechos y libertades fundamentales cumplen un papel crucial, al operar como límites de actuación. No solo sirven como parámetro a la hora de determinar las medidas a implementar, sino que su defensa frente a los avatares que el tratamiento de la información pudiera deparar está en el núcleo del derecho. Sin embargo, no es una función del derecho a la protección de datos reparar los daños en dichos bienes jurídicos en caso de que estos,

finalmente, se produzcan. Esto es, la función y finalidad del derecho fundamental a la protección de datos es eminentemente preventiva. Pero, si falla, los mecanismos de reparación que se han de activar son los que cada derecho afectado tenga.

Por ejemplo, cuando se produce una brecha de seguridad y se revela una información, se puede producir una afectación del derecho a la protección de datos, (habrá que dirimir si se implementaron las medidas adecuadas, incluso si se actuó con diligencia a posteriori). Pero, si a raíz de tal quiebra en la seguridad, terceros han tenido acceso a información íntima y la usan, esa afectación del derecho a la intimidad no debería quedar colmada porque se imponga una sanción por el incumplimiento de la normativa de protección de datos, porque, entonces, el derecho a la intimidad quedaría minusvalorado.

Cuando, a raíz de un tratamiento, alguien determina la tendencia ideológica de una persona y, en función de esta, la discrimina, podrá haber una vulneración del derecho a la protección de datos en la medida en que se tratan los datos para una finalidad no legítima (pues no es posible tratar datos para discriminar), pero ello no debe opacar que se ha producido una discriminación que debe ser reparada. El reconocimiento y sanción por la vulneración del derecho a la protección de datos no puede hacer esa función, pues no es su cometido. De lo contrario, además de producirse una absorción de todos los derechos por el derecho a la protección de datos, se estaría negando a los individuos la posibilidad de ver resarcidas las injerencias y afectaciones de sus otros bienes jurídicos.

El carácter preventivo del derecho a la protección de datos no puede llevar a negar los resultados negativos realmente producidos. Sería como si una aseguradora no pagase el resultado lesivo de un accidente porque ella misma no cumplió con sus obligaciones (v. gr. por no indemnizar o no cumplir los plazos) y ya la hubieran sancionado por ello. No hay aquí *non vis in idem*, ni redundancia alguna, son desvalores distintos con consecuencias diferentes. El incumplimiento de una obligación previa no debe absorber el desvalor de un resultado lesivo posterior. Del mismo modo que, en materia de derechos, el cumplimiento de las exigencias relativas a uno –el derecho a la protección de datos– no exime de respetar a los demás.

Por más que los derechos y libertades jueguen un papel determinante en la tutela del derecho a la protección de datos, la

protección de datos no alcanza a absorberlos, sino que su función es tratar de protegerlos. El derecho a la protección de datos no es la póliza de seguros de los demás derechos, su cometido se asemeja más al de una política de prevención de riesgos.

Para proteger a los datos personales mediante una actuación autónoma y capaz de aportar una funcionalidad diferenciada, se necesita un tipo distinto de herramienta jurídica, a cuyo través se puedan imponer obligaciones jurídicas a quienes operen con ellos. Solo así es factible evitar la materialización de los riesgos y temores y, con ello, la ulterior producción de efectos lesivos para los derechos de las personas. Así entendido, el derecho del art. 8 de la CDFUE es la respuesta jurídica a una ineludible necesidad de protección anticipada, además de una materialización de la autodeterminación informacional de la persona.

Esa condición preventiva y finalista del derecho fundamental a la protección de datos le dota de una fisonomía funcionalmente variable, debiendo adecuar las medidas a implementar a las particularidades de cada tratamiento –solo de ese modo se mantendrían unos niveles de protección jurídicamente aceptables–. En este cometido se verán involucrados tanto el legislador, en la medida en que ha de propiciar marcos normativos apropiados[278], como los responsables de los tratamientos, al tener que diseñar y aplicar las medidas técnicas y organizativas más convenientes para evitar la afectación de los derechos y libertades.

12.4. Un factor limitante característico del modelo europeo. La libre circulación de datos

Los derechos y libertades no son el único condicionante, modificador y límite del derecho fundamental a la protección de datos. La correcta delimitación de este derecho exige la toma en consideración de otro factor: la libre circulación de la información personal.

[278] La condición adaptativa de los derechos de configuración legal no es nueva, así lo expresó el TC en relación con el derecho a la tutela judicial efectiva, al afirmar que «como derecho de configuración legal, puede tener y, de hecho tiene, un contenido distinto en los distintos momentos históricos, al compás de los cambios en la legalidad que lo configura», STC 108/1999, de 14 de junio, FJ 2.

La importancia estratégica de la libre circulación de datos en el espacio común europeo hace de ella un elemento determinante en la conformación de la tutela jurídica del derecho fundamental a la protección de datos, pues «no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales» (art. 1.3 RGPD)[279].

No obstante, esta exigencia se enmarca dentro de un sistema de protección que asegura un mínimo de garantías a los derechos, por lo que no es un juego de suma cero. Es una condición limitante de las posibilidades de actuación, pero no niega el contenido del derecho, solo introduce otro factor a considerar en su desarrollo normativo y aplicativo.

Así, cuando se quiera operar con datos personales, el derecho fundamental a la protección de datos exige que se establezca un marco de actuación jurídicamente aceptable en el que se salvaguarden los derechos y libertades y se garantice el ejercicio del poder de control y disposición de los interesados respecto de las informaciones a ellos referidas. Todo ello, sin suponer un obstáculo insalvable para la libre circulación de la información.

12.5. El derecho fundamental

El conjunto de factores concurrentes en el tratamiento de la información personal conforman un modelo de protección extraordinariamente complejo. Para lograr un equilibrio entre los diferentes intereses en conflicto es imprescindible un marco normativo flexible, capaz de adecuarse a las particularidades de cada tratamiento. Un sistema de «*check and balances*» (Kranenborg, 2014, p. 229)[280].

Ese conjunto de elementos permite definir las características del derecho fundamental a la protección de datos como un derecho anfibológico, de configuración legal, con un marcado carácter

[279] En la misma línea apunta el Considerando 13 del RGPD al señalar que «el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales» (Considerando 13 RGPD).

[280] Kranenborg utilizó este apelativo para definir al modelo europeo de protección de datos.

procedimental, finalista y preventivo[281], pero que, a la vez, posibilita el control personal de la información a uno referida mediante la atribución de facultades de actuación directa sobre los datos. Un derecho con dos almas, destinado a proporcionar una tutela jurídica completa frente al tratamiento de la información personal.

[281] Martínez Martínez lo define como un «derecho de naturaleza instrumental, relacional, contextual, esencialmente adjetivo» (Martínez Martínez, 2021b).

CAPÍTULO V. LAS CATEGORÍAS ESPECIALES. DEL DATO AL TRATAMIENTO

«*Hazards are ever-present, [...] they must be identified, analyzed, evaluated and controlled or rationally accepted*»
J. F. Lederer

1. Las categorías especiales de datos[1]

Dato, tratamiento y derecho a la protección de datos conforman un ecosistema interdependiente. Cada uno de ellos afecta y condiciona a los demás. Sin dato no hay tratamiento y este puede llegar a determinar la existencia de un dato personal. Finalmente, si no hay un dato personal que esté siendo tratado, no se activan los mecanismos de protección del derecho. Además, corresponde al legislador establecer las condiciones y características que ha de reunir una información para ser considerada dato personal, amén de determinar los requisitos y exigencias que el tratamiento debe cumplir para considerarse lícito.

En esa imbricada realidad que es el tratamiento de la información personal, existen un conjunto de interrelaciones que se distinguen de las demás porque, en ellas, los datos tienen una condición particularizada: son sensibles. Como consecuencia de ello, se establecen, en el plano legislativo, unas condiciones distintas que se plasman en un conjunto singularizado de obligaciones de tratamiento. Me refiero, claro está, a las denominadas categorías especiales de datos.

El modelo europeo reconoce como especiales un conjunto cerrado de tipologías de datos. Para ellas, establece un régimen jurídico en el que, la regla general, es la prohibición del tratamiento (art. 9.1 del RGPD), de tal modo que solo bajo determinadas condiciones se puede llegar a operar con este tipo de informaciones (art. 9.2 RGPD).

En consecuencia, obligado es preguntarse a cerca de la razón de ser de las categorías especiales ¿Qué motivos justifican su existencia? ¿Qué consecuencias tiene el reconocimiento de una condición singular a determinados tipos de datos personales? ¿Cómo se refleja en el sistema normativo europeo esta particular concepción de la naturaleza de la

[1] Desde un punto de vista terminológico, se utilizarán como sinónimos: datos especiales, datos sensibles, categorías particulares de datos, categorías especiales y tipologías especiales o sensibles.

información? ¿Qué ventajas e inconvenientes encierra esa opción? ¿Existen otras alternativas más acordes a la idiosincrasia del modelo vigente? ¿De las particularidades de las categorías especiales, puede extraerse alguna enseñanza en relación con el concepto de dato personal? ¿Hay margen de mejora en ese ámbito?

A dar respuesta a estas cuestiones se dedicará este Capítulo, para ello, se analizará el fundamento de las categorías especiales, tratando de determinar la razón de su existencia. A continuación, se expondrán los diferentes modelos de protección de jurídica de lo sensible, se examinarán las particularidades del sistema adoptado por la UE y se abordarán sus posibilidades de mejora. Finalmente, con las propuestas en relación con las categorías especiales como referencia, se planteará las posibilidades de perfeccionar el concepto de dato y el modelo de protección europeo.

2. El fundamento de las categorías especiales

2.1. No todos los datos son iguales

La existencia de un conjunto de informaciones necesitadas de una protección reforzada implica reconocer que no todos los datos personales son iguales[2]. ¿Qué razones son las que fundamentan esta distinción tipológica? El Considerando 51 del RGPD ofrece un primer argumento cuando afirma que «especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales».

Conforme a la normativa europea, no todas las informaciones, por más que estén referidas a una persona física concreta, tienen el mismo impacto, ni implican el mismo nivel de riesgo para los bienes jurídicos del sujeto afectado. El factor determinante de esa mayor peligrosidad radicaría

[2] La distinción entre tipologías de datos personales es una constante en el análisis de los regímenes de tratamiento de la información personal. «*The concept that some kinds of information are more sensitive than others has been often articulated by privacy scholars and operationalized by lawmakers, albeit using a variety of terms. Additional terms that have been applied include "intimate information" or "revealing information," and some scholars have defined them in terms of the level of risk to one's privacy or the extent of harm to one's privacy. Still others refer to some searches as "highly intrusive"*» (Etzioni, 2015, p. 1277).

en la «naturaleza» de la información. El punto de partida es meridiano: no todos los datos son iguales, algunos, por su contenido, tienen un potencial de injerencia en los derechos mayor que otros.

La sensibilidad de la información, su vinculación con los aspectos más personales y delicados de la persona, el riesgo que su uso por terceros pueda comportar para los derechos y libertades, serían los factores mediante los que identificar, dentro del conjunto de datos personales existentes, aquellos que merecen la consideración de especiales.

El principal problema de este modelo de protección radica en que «*the notion of sensitivity is a particularly difficult concept*» (Al-Fedaghi, 2007, p. 165). Además, está muy vinculada a la percepción personal de cada individuo (Fukuta, Murata y Orito, 2020), lo que introduce un factor de subjetividad en el sistema, que dificulta su objetivación.

Más allá de si es por naturaleza o por contexto –cuestión que se analizará posteriormente–, en lo que ahora importa, el fundamento de las categorías especiales reside en su potencial para generar un riesgo de afectación mayor para los derechos y libertades fundamentales. Por tanto, se puede considerar que son datos sensibles aquellos «*whose unauthorised access would make the subject of the data feel uncomfortable or could imply negative consequences for the subject*» (Christen, Ranbaduge, y Schnell, 2020, p. 9).

La existencia de categorías especiales es una prueba inequívoca de la importancia del riesgo como elemento conformador del derecho a la protección de datos. La implementación de un régimen de protección más severo para este tipo de informaciones no deja de ser una forma de prevención y respuesta frente al mayor peligro que se presupone en su utilización.

2.2. El difícil consenso sobre lo sensible

Identificar qué tipologías de datos son merecedoras de ser consideradas como sensibles no es una tarea meramente aplicativa. De hecho, no existe un consenso global acerca de qué informaciones son susceptibles de esa calificación.

Como Wang y Jiang han puesto de manifiesto, después de analizar la regulaciones de protección de datos de 92 países y regiones, si bien «*the*

majority of countries and regions in the world have defined or classified sensitive data in their data protection laws» (Wang y Jiang, 2017, p. 3299), la variabilidad de los datos que reciben tal consideración es muy elevada, existiendo hasta 33 categorías diferentes de información considerada como sensible. Entre ellas, se constata la existencia de ciertas tipologías comunes o con una presencia recurrente, a saber: los datos relativos a «*physical or mental health*, *religious beliefs or affiliations*, *political opinions or membership*, *sexual life*, *race or ethnicity*, *trade union*, *philosophical or moral beliefs*, *and criminal records or proceedings or administrative proceedings*» (Wang y Jiang, 2017, p. 3293).

La dificultad para establecer un conjunto común de informaciones a las que revestir con una protección reforzada no es nueva. La cultura de cada país, su particular experiencia histórica, su forma de entender y considerar lo sensible, dificultan alcanzar un consenso global acerca de aquella información que debe ser objeto de una especial protección. A medida en que se incrementan los países intervinientes en la ecuación y las culturas jurídicas concurrentes, más complejo resulta encontrar un punto de acuerdo. «*Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive*»[3]. Que tanto el Convenio 108, como el modelo europeo de protección de datos, hayan logrado consensuar, para un conjunto amplio de Estados, las informaciones que merecen el apelativo de sensibles constituye un logro de indudable valor[4].

Las tipologías de datos consideradas especiales en el sistema europeo aparecen recogidas en el artículo 9 del RGPD: los «datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física».

---

[3] Párrafo 19, letra a) de la Memoria Explicativa de las Directrices del Consejo de la Organización para la Cooperación y el Desarrollo Económico, sobre protección de la privacidad y el flujo transfronterizo de datos personales, de 23 de septiembre de 1980. Puede consultarse el conjunto de previsiones de la OCDE sobre protección de datos, incluida la Memoria Explicativa Original (pp. 39-64), en: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[4] No obstante, el Convenio 108, tal como acredita su Informe Explicativo, consciente de que «*the degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned*», no establece una lista cerrada y deja abierta la posibilidad a los estados a que incluyan en sus regulaciones nacionales otras informaciones sensibles, párrafo 48 del Informe Explicativo del Convenio 108. Puede consultarse en: https://rm.coe.int/16800ca434.

Se trata de un catálogo sustancialmente coincidente con el del Convenio 108, en su versión actualizada[5]. No obstante, el listado del Convenio y el del RGPD difieren respecto de la inclusión de los datos relativos a condenas e infracciones penales. Una divergencia menor, si se analiza con detalle la regulación de esta materia en el sistema europeo y los particulares condicionantes que la rodean.

2.2.1. Los datos sobre condenas e infracciones penales. La particular regulación europea

La regulación europea sobre condenas e infracciones penales se encuentra dispersa. El RGPD no es la única fuente normativa en la que se disciplina su tratamiento. También debe considerarse lo dispuesto en la Directiva (UE) 2016/680 del Parlamento y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[6].

La «prevención, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales» es una materia especialmente compleja en la UE, pues entronca con la política europea en materia de

---

[5] El art. 6 del Convenio 108, en su versión actualizada señala que, «1. *The processing of:*
- genetic data;
- personal data relating to offences, criminal proceedings and convictions, and related security measures;
- biometric data uniquely identifying a person;
- personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention
2. *Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination*».

[6] En consonancia con esta previsión, el RGPD excluye expresamente de su ámbito de aplicación el 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 de protección frente a amenazas a la seguridad pública y su prevención» (art. 2.d) RGPD).

cooperación judicial y policial[7] y la realización de un espacio de libertad, seguridad y justicia (arts. 67 a 89 TFUE)[8].

Lo delicado de la materia y su importancia estratégica, justifica detraer del régimen general la regulación de ciertos usos, los más relevantes, de los datos referidos a infracciones y sanciones penales (Considerandos 9 a 12 de la Directiva (UE) 2016/680).

Al sustraerse uno de sus usos más significativos del ámbito de aplicación del RGPD, resulta, hasta cierto punto, coherente que los datos referidos a condenas e infracciones penales no se incluyesen entre las categorías del art. 9 del RGPD. En ese precepto se enuncia el sistema general de protección de las tipologías sensibles, por lo que no podía aplicarse a los datos relativos a condenas e infracciones penales, dado que parte de su regulación se encontraba en una norma específica y distinta.

Sin embargo, tanto desde una perspectiva sistemática (están regulados en el artículo siguiente, el 10), como atendiendo al contenido y modo de regular su tratamiento, puede afirmarse que, para el legislador europeo, esa tipología de información también es especial[9] o, al menos, «algo muy similar o anejo» (Gudín Rodríguez-Magariños, 2018, p. 212)[10].

El art. 10 del RGPD establece que, «el tratamiento de datos personales relativos a condenas e infracciones penales o medidas de

---

[7] La política de la UE en materia de cooperación judicial se vio reforzada con la adopción del Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por la que se sustituye y deroga la Decisión 2002/187/JAI del Consejo (Reglamento Eurojust). En él se ratifica que la Directiva 2016/680 será la norma de referencia en la materia. En todo caso, las prácticas de la Agencia Eurojust y de las autoridades de los Estados miembros, habrán de ser coherentes, también, con el RGPD (Considerando 28 del Reglamento Eurojust). Sobre el conjunto de interrelaciones entre normativas y su encaje en el sistema *constitucional* de protección de los datos personales, vid. (López Aguilar, 2019, pp. 38-43). Acerca de los mecanismos destinados a asegurar una transmisión segura de los datos personales, vid. (Galán Muñoz, 2015).

[8] Sobre el espacio de libertad, seguridad y justicia de la Unión Europea, vid. p. ej. (AA. VV., 2020b); (AA. VV., 2020c) o (Alzina Lozano, 2020).

[9] Así lo entiende, también, Medina Guerrero, quien incluye su exégesis en el análisis de las categorías especiales de datos (Medina Guerrero, 2019, pp. 265-269). La condición sensible de los datos penales también es reconocida, por ejemplo, por el legislador británico (arts. 10 y 11), pertenecientes la Sección 10: *Special categories of personal data*, en los que se regulan las condiciones adicionales, tanto de las categorías especiales del art. 9 del RGPD, como los datos relativos a condenas e infracciones penales del art. 10 del RGPD. Puede consultarse la Data Protection Act de 23 de mayo de 2018 en, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

[10] Si bien es cierto que, para el autor, «no cabe incluir *strictu sensu* entre los datos sensibles, los tratamientos relativos a las condenas penales» (Gudín Rodríguez-Magariños, 2018, p. 214).

seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas». Por tanto, únicamente cuando concurran las circunstancias previstas de manera expresa en el RGPD se podrán tratar los datos de esta naturaleza. Fuera de ese supuesto, su tratamiento está prohibido.

La regulación de esta tipología de datos consigue los mismos resultados que el resto de los datos especiales, pero articulando su protección de un modo inverso. En los datos especiales se parte de la prohibición, y luego se establecen los supuestos y condiciones en los que, de producirse, será viable su tratamiento. En el caso de los datos relativos a condenas e infracciones penales, se prevén expresamente los únicos supuestos en que será jurídicamente aceptable el tratamiento, entendiéndose que todos los demás quedan vedados. El resultado final es el mismo. Solo difieren en el modo de alcanzarlo.

Al contenido del precepto, como indicador de la condición especial de los datos relativos a condenas e infracciones penales, se suma, como argumento adicional, que tanto en la Directiva 95/46/CE[11], como en la Propuesta de la Comisión[12], se incluía a esta tipología de datos en el listado de datos especiales.

Por tanto, es razonable pensar que su regulación en un precepto distinto obedece más a razones de organización sistemática y de diferenciación regulatoria, exigida por las necesidades políticas de construcción del espacio de libertad, seguridad y justicia, que a una voluntad de negarle su condición de especial pues, de facto, la regulación del artículo 10 le proporciona una protección equivalente.

---

[11] Art. 8.5 de la Directiva: «El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos».

[12] La Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) incluía en su art. 9 a «las condenas penales o medidas de seguridad afines». Puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52012PC0011.

El hecho de que el Convenio 108 sí haya incluido esta tipología de datos entre los especiales reafirma esa apreciación. No se debe olvidar que la adopción del RGPD y la modernización del Convenio 108, «se llevaron a cabo en paralelo […] [y que] los reguladores de ambos sistemas jurídicos han hecho todo lo posible por asegurar la coherencia y la compatibilidad entre los dos marcos jurídicos» (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2019, p. 14). Como el Convenio no está condicionado por la necesidad de respetar las competencias de los Estados, ni por el deber de adecuación al marco de cooperación en materia de cooperación policial y judicial, resulta plausible entender que la diferencia regulatoria introducida por el legislador europeo se debe a la necesidad técnica de adecuar el modelo de protección a su singular realidad jurídica.

2.3. ¿Qué subyace a las categorías especiales?

2.3.1. Representación de los elementos más identificativos y sensibles de la persona

La existencia de categorías especiales de datos parte de una doble convicción. En primer lugar, concibe al dato personal como una manifestación del ser, como un reflejo de cierto aspecto de la persona a la que se refiere. Es decir, utiliza un concepto de dato centrado en el contenido de la información. En segundo término, en tanto los datos son proyecciones de la persona, no todos los datos tienen la misma importancia, ni idéntica capacidad para incidir en sus derechos. En definitiva, ni todos los datos son igual de valiosos, ni su uso es igual de peligroso.

El Informe Explicativo del Convenio 108 resulta elocuente: «*while the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests*»[13]. Esto es, existen ciertos datos que, por sí solos, por lo que representan, entrañan un mayor riesgo. El RGPD ahonda en esta idea, al señalar que merecen «especial protección […] los datos personales que, por su naturaleza, son

[13] Párrafo 43 del Informe Explicativo del Convenio 108. Puede consultarse en: https://rm.coe.int/16800ca434.

particularmente sensibles en relación con los derechos y las libertades fundamentales» (Considerando 51).

La condición identificativa se torna evidente: aquellas informaciones que reflejen los aspectos más íntimos de la persona o que, por su contenido, tengan un potencial discriminatorio mayor, han de gozar de protección especial. Establecida la premisa, solo resta identificar qué datos se acomodan a ella. Ahora bien, la juridificación de esa pretensión, es un proceso marcado por la cultura de cada sociedad y la voluntad del legislador.

El diseño de las categorías especiales es fruto de una abstracción selectiva del conjunto de informaciones relativas a una persona, en la que confluyen elementos culturales y políticos. De la pluralidad de datos, se identifican aquellos que, en el sentir mayoritario, tienen un mayor nivel de riesgo y, posteriormente, son ordenados en categorías más o menos homogéneas en función de su conexión temática. Así, los datos de salud, o la información genética (por poner dos ejemplos) conforman categorías completas, pese a que, no parece, a priori, que todas las informaciones que se incluyen en ellas tengan el mismo nivel de riesgo (v. gr. no tiene el mismo nivel de "sensibilidad" un resfriado común que una enfermedad degenerativa y, sin embargo, ambas serían datos relativos a la salud).

El mapa de riesgos de los datos especiales adolece, en consecuencia, de cierta distorsión, pues, la agrupación por temática o por asociación desvirtúa la intensidad del riesgo como criterio de clasificación. Un efecto que, paradójicamente, pone en cuestión la principal razón de ser de la categoría de los datos especiales.

No se pretende, con ello, negar la condición especial de los datos así reconocidos. Tan solo se busca poner de manifiesto que, tanto en la selección de las categorías especiales, como en su configuración jurídica, anida una metodología procedimental (general y abstracta) no exenta de contradicciones, ya sea por no incluir informaciones que pudieran considerarse delicadas (v. gr. datos financieros[14]), o por extender la

[14] La información crediticia tiene un importante potencial discriminatorio, especialmente mediante los sistemas de *credit score*. Sobre este tema, vid. (Aridor, Che, y Salz, 2020); (Gillis y Spiess, 2019); (Henderson, Herring, Horton, y Thomas, 2015) o (Zeidan, Boechat, y Fleury, 2015).

condición de especial a tipologías de datos heterogéneas y que, desde el enfoque del riesgo, admitirían diversos niveles de protección[15].

Sin cuestionar aquí las preferencias de cada legislador (¿Por qué estas categorías y no otras? ¿Son todos los datos especiales igual de sensibles? ¿Por qué no escalar los niveles de protección?), no puede desconocerse la apuntada distorsión de fondo, pues existe acuerdo al entender que las categorías especiales de datos tienen como finalidad establecer una protección reforzada para aquellos tratamientos que representan un alto nivel de riesgo y, a lo que parece, esto no es siempre así.

2.3.2. Las bases de lo sensible: intimidad, alto riesgo y discriminación

El carácter especial de los datos personales entronca con su condición de proyección exterior del ser. La sensibilidad de la información se incrementa de manera proporcional al nivel de profundidad que alcance en la esfera íntima de la persona. Junto a ese presupuesto, los Estándares Internacionales sobre Protección de Datos Personales y Privacidad[16] identifican, en su apartado 13.1, otros dos factores determinantes de la condición especial del dato: su potencial discriminatorio (p. ej. datos sobre origen racial u orientación sexual) y que el tratamiento de esa información conlleve un riesgo elevado (p. ej. biométricos).

2.3.2.1. Cuanto más privado[17], más sensible

Otorgar una protección reforzada a aquella información que se considera más reservada, conecta el derecho a la protección de datos con la protección de la intimidad y la vida privada, con la que tendió a

[15] La previsión del 9.4 del RGPD, relativa a la inclusión de «condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud», parece apuntar en esta idea. Sobre este precepto y sus posibilidades interpretativas he tenido ocasión de pronunciarme en (Jove, 2017).

[16] Pueden consultarse los Estándares Internacionales sobre Protección de Datos Personales y Privacidad de 2009 (Resolución de Madrid) en: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf.

[17] Entendido aquí como sinónimo de íntimo, y que estaría representado por la «esfera de actividad personal protegida contra la injerencia de todo poder externo» (Bobbio, 1991, p. 44).

confundirse en sus orígenes. Pero, a su vez, lo diferencia de ellas, al constatar que la finalidad del derecho a la protección de datos no es, en sí misma, la protección de la intimidad; por más que pueda ser un factor modulador, al punto de motivar la configuración de las categorías especiales de datos[18].

La finalidad del derecho a la protección de datos es la protección frente a los riesgos derivados del tratamiento de información referida a una persona. Si la información es reservada o íntima, los peligros se incrementan, pues cualquier quiebra en la seguridad, o pérdida de control sobre ella, supondría la, más que probable, afectación del derecho a la vida privada. Este es el elemento detonante de la condición especial de, por ejemplo, los datos sobre la vida sexual, la información genética o la relativa a la salud[19].

2.3.2.2. Categorías sospechosas y derecho antidiscriminatorio

La inclusión, entre las categorías especiales, de los «datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical […] o datos relativos a […] la orientación sexual de una persona física» no es casual. La condición sensible de estas informaciones está estrechamente vinculada con la protección frente a la discriminación. Así, la prohibición del tratamiento de las categorías especiales, su regulación más exigente, operaría como un mecanismo mediante el que evitar la «*possibility for direct discrimination*» (Žliobaite y Custers, 2016, p. 185).

Este factor identificativo de lo sensible está estrechamente vinculado con el contenido de los datos, con su condición de proyección personal. Consecuentemente, los datos que proporcionen información sobre el individuo, conectada con las categorías tradicionalmente consideradas como sospechosas de generar discriminación, reciben una

[18] Sobre el valor de la intimidad como modulador del derecho a la protección de datos, no solo como condicionante de las categorías especiales, sino como mecanismo específico a considerar a la hora de resolver conflictos, he tenido ocasión de pronunciarme en, (Jove, 2020).

[19] El vínculo dato relativo a la salud e intimidad ha sido reconocido reiteradas veces, tanto en la jurisprudencia del TEDH (STEDH, Z. c. Finlandia, de 25 de febrero de 1997, apdo. 95; STEDH, asunto L.L. c. Francia, apdos. 32 y 44), del TJUE (STJUE asunto C-101/01, asunto Lindqvist, 6 de noviembre de 2003, apdos. 50-51 para salud y 86-88 para datos relativos a información religiosa) o del TC español (STC 70/2009, de 23 de marzo, FJ 2).

protección adicional. Su inclusión resulta coherente e incardina al derecho a la protección de datos entre los mecanismos jurídicos de lucha contra la discriminación[20].

Los datos sensibles se refieren a informaciones personales respecto de las que, la experiencia histórica, ha evidenciado su capacidad «para configurar una diferencia peyorativa entre las personas, basada en perjuicios gravemente odiosos para la dignidad de la persona, capaces de generar una situación de subordinación social de ciertos grupos. […] La discriminación opera a partir de una generalización o estereotipo negativo, es decir, un prejuicio, ligado a un grupo, que se adjudica a una persona tan solo por pertenecer a él» (Rey Martínez, 2019, p. 48).

Resulta evidente que existe una conexión entre las categorías sospechosas, la lucha contra la discriminación y las categorías especiales. Sin embargo, en el caso del RGPD, esa conexión solo opera como fundamento originario para la determinación de las tipologías de informaciones sensibles. En efecto, la discriminación no consta como criterio identificativo de los datos especiales, sino, exclusivamente, como factor condicionante de las medidas de seguridad a adoptar e, incluso, como criterio para determinar la lealtad del tratamiento[21].

El RGPD prevé un conjunto tasado y cerrado de informaciones consideradas especiales (art. 9 y, con las matizaciones apuntadas, art. 10). El legislador europeo ha prescindido de la posibilidad de incorporar, como mecanismos identificadores de datos especiales, la esfera reservada, el riesgo alto y la lucha contra la discriminación. Estos, sirven para conocer el origen y razón de ser de los datos sensibles jurídicamente reconocidos, pero carecen de capacidad para extender la condición especial a otras tipologías de datos.

---

[20] En esta línea apunta la Resolución 45/95 de Naciones Unidas, de 14 de diciembre de 1990, en la que se establecen los Principios Rectores para la reglamentación de los ficheros computarizados de Datos Personales. Entre ellos se incluye el «principio de no discriminación» (apdo. 5), conforme al cual, «no deberían registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación a un sindicato». Puede consultarse la Resolución de la ONU en:
http://ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf.

[21] Sobre la conexión entre el principio de tratamiento leal y la no discriminación, vid. Considerando 71. Sobre el efecto modulador de las medidas frente a la discriminación, vid. p. ej. Considerandos 75 y 85 o la exigencia de evaluación del impacto del art. 35 RGPD, especialmente los apartados 1 y 3, en los que se constata que el riesgo de discriminación puede operar como factor justificativo de su obligatoriedad.

El factor discriminación es, de los tres, aquel en que resulta más evidente el efecto cristalizador que supone la positivación de un conjunto cerrado de tipologías de datos. Como se ha señalado, algunas de las categorías de datos sensibles coinciden con categorías sospechosas de discriminación; sin embargo, las formas de discriminación son más variadas que las tipologías previstas en el RGPD. Sin ir más lejos, la UE, con la referencia ineludible que, en esta materia, representa el CEDH[22], reconoce como formas de discriminación posibles, además de las coincidentes con las categorías especiales de datos, las siguientes: discriminación por motivos sociales, lengua, patrimonio, pertenencia a una minoría nacional, nacimiento, discapacidad o edad (art. 21.1 CDFUE)[23]. Si bien alguno de los supuestos previstos en el art. 21 de la CDFUE, como puede ser la discriminación por discapacidad, podrían llegar a canalizarse mediante la protección de los datos relativos a la salud, otros, como la discriminación por patrimonio, no tienen correlato alguno en las categorías especiales.

Si en la configuración legal de las categorías especiales reside, entre otras, la voluntad de combatir las diversas formas de discriminación derivadas del tratamiento de la información personal, la opción del legislador europeo de reconocer un conjunto cerrado de categorías prediseñadas no parece que sea la más adecuada para alcanzar ese

[22] El papel referencial del CEDH es reconocido por la Agencia de los Derechos Fundamentales de la Unión Europea en el Manual de legislación europea contra la discriminación (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2019).
El art. 14 del Convenio Europeo para la Protección de los Derechos Humanos es el punto de referencia del derecho antidiscriminatorio en Europa. La jurisprudencia del TEDH ha concretado, precisado y ampliado el concepto. En la actualidad, la discriminación se entendería como la actuación consistente en «tratar de manera diferente sin justificación objetiva y razonable a personas que se encuentran en situaciones parecidas y que un trato diferenciado está desprovisto de "justificación objetiva y razonable" cuando no persigue un "fin legítimo" o no existe "una relación razonable de proporcionalidad entre los medios empleados y el fin perseguido"» (STEDH, asunto G.L. c. Italia, de 10 de septiembre de 2020, apdo. 52, así como la jurisprudencia en él mencionada). El TEDH también ha remarcado que la prohibición de discriminación incluye, también, una faceta positiva de actuación, conforme a la cual, los Estados, deben realizar «los ajustes razonables» necesarios para corregir desigualdades efectivas, no justificadas (STEDH, asunto Çam c. Turquía, de 23 de febrero de 2016 (versión final de 23 de mayo de 2016), apdo. 65). Sobre la evolución de la jurisprudencia del TEDH en la protección contra la discriminación, vid. (Hernández Llinás, 2020).

[23] Art. 21 CDFUE. No discriminación
«1. Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual.
2. Se prohíbe toda discriminación por razón de nacionalidad en el ámbito de aplicación de los Tratados y sin perjuicio de sus disposiciones particulares».

objetivo; sobre todo, cuando tampoco existe una cláusula subsidiaria de apertura; por ejemplo, incorporando un aditamento en el que se indicase que también tendrá la condición de especial, "cualquier dato que pueda dar lugar a un supuesto discriminatorio".

2.3.2.3. El alto riesgo: el factor con mayor alcance

El alto riesgo, como factor identificativo de la condición especial de una información, es elusivo en exceso. En primer lugar, porque el riesgo es inherente al tratamiento de la información y no al dato en sí. El dato, sin tratamiento, no genera riesgo, solo el tratamiento permite evaluar los peligros. Su inclusión como identificador implica que ha de tratarse de informaciones que, por su naturaleza, entrañen un riesgo adicional. Deben ser datos que, por su contenido, elevan el riesgo del tratamiento, cualesquiera que sean las condiciones en que este se desarrolle.

Este factor, en virtud de su alcance, bien podría embeber a los otros dos (riesgo de discriminación y datos relativos a la esfera reservada), pues, tanto la posible discriminación, como la eventual afectación de la vida privada conllevan, *per se*, un alto riesgo.

La elasticidad del factor riesgo resulta particularmente útil en un ámbito tan dinámico como el de la protección de datos. El alto riesgo bien puede convertirse en la cláusula de apertura del sistema, a modo de comodín mediante el que extender la protección de las categorías especiales a datos que, teniendo capacidad potencial para afectar a los derechos y libertades fundamentales, no encajen, sin embargo, en alguno de los otros dos factores.

Este podría ser el caso de los datos biométricos[24], cuya particular naturaleza[25] no siempre se compadece ni con la no discriminación, ni con

[24] Como acreditan los análisis acerca de los riesgos derivados del uso de este tipo de informaciones, en las que se constata que su capacidad de identificación unívoca y permanente entraña un riesgo elevado de afectación de los derechos y libertades, en este sentido, vid., p. ej., (Moraes, Almeida, y de Pereira, 2020); (Binder, Iannone, y Leibner, 2020) o (Quintanilla Mendoza, 2020).

[25] Los datos biométricos son una tipología de información singular, en la medida en que requieren de la mediación de algún tipo de técnica u operación previa para su existencia. El RGPD los define como aquellos «datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos» (art. 4.14 del RGPD). Sobre las técnicas de

la protección de la esfera íntima. Así, el reconocimiento facial, del iris o las huellas dactilares, por citar los ejemplos más conocidos de datos biométricos, no encuentran su fundamento en el riesgo de discriminación. Podría plantearse su vinculación con la intimidad o la propia imagen, sin embargo, al menos en el reconocimiento facial, resulta difícilmente encuadrable en la condición de información especialmente reservada. Otros tipos de información biométrica, como la identificación unívoca a partir del ADN, sí podrían tener encaje en esos ámbitos e, incluso, obtener la protección de categorías ya reconocidas (datos genéticos, en el caso del ADN).

En definitiva, una inteligente utilización del alto riesgo puede servir para cubrir la falta de una cláusula residual de apertura.

No obstante, en el RGPD, el alto riesgo, al igual que ocurría con la discriminación, es un factor cuya funcionalidad para identificar datos especiales está muy acotada, por no decir agotada. Solo puede utilizarse para incardinar, en alguna de las tipologías jurídicamente reconocidas, informaciones que se presentasen como dudosas. Nada más. Su potencialidad como cauce de ampliación de la protección especial a otras informaciones colisiona con la taxatividad del art. 9 (y el 10) del RGPD. Para el legislador europeo, solo son especiales las tipologías normativamente previstas, ni más, ni menos.

3. El reconocimiento jurídico de lo sensible. Modelos de protección

El contenido más reservado, el potencial discriminatorio o el riesgo alto son los fundamentos justificativos de las categorías especiales de datos, y la razón por la que no todos los datos personales son igualmente

---

reconocimiento biométrico, los distintos tipos de biometrías (estáticas o dinámicas) y sus funcionalidades y posibilidades de uso, los retos y riesgos que representan, vid. la completa monografía de Escajedo San-Epifanio, (Escajedo San-Epifanio, 2017).

Son datos heterogéneos, que en determinados casos permiten conocer otras informaciones sensibles (datos genéticos u origen racial), así lo ha refrendado el GT29, en su Dictamen 3/2012, de 27 de abril de 2012, sobre la evolución de las tecnologías biométricas, p. 16. Puede consultarse en: https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf. Además, se ha demostrado su potencial para llegar a conocer otras informaciones del individuo, como su estado emocional o el consumo de estupefacientes, tal como apunta la AEPD en el documento: 14 equívocos con relación a la identificación y autenticación biométrica, puede consultarse en: https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf.

considerados. Sin embargo, el reconocimiento de una información como especial dista de ser fácil.

Existen diversas formas de configurar la protección jurídica de los datos especiales. En términos generales, los modelos pueden agruparse en dos grandes bloques: En uno se presta atención al contenido de la información y se identifican un conjunto de tipologías de datos sensibles. En el otro, se toma en consideración la realidad del tratamiento (su contexto y finalidad) para determinar la naturaleza de la información.

Al igual que ocurría con la identificación de una información como dato personal, donde la finalidad y los efectos eran variables diferentes, algunos autores dividen este segundo bloque en dos, estableciendo el contexto y la finalidad como formas de clasificación diferenciadas, v. gr. (McCullagh, 2007) o (Wong, 2007). En el caso de los datos especiales, y a efectos meramente expositivos, se ha optado por agrupar contexto y finalidad, debido a que ambos concurren en la conformación de la realidad del tratamiento. Como apunta Von Grafenstein, el contexto incluye a la finalidad y ésta es uno de los elementos que definen el contexto (von Grafenstein, 2018, pp. 101-105). La imbricación entre ambos hace que su diferenciación resulte poco operativa, cuando no engañosa, pues ambos conforman un todo.

3.1. El contenido y las categorías de datos predefinidas. La seguridad aplicativa como valor

El contenido de la información es un elemento determinante de la condición de dato personal (STJUE Nowak)[26]. Un dato es personal, entre otras razones, por ser el reflejo de la realidad del individuo. En consecuencia, no resulta extraño que, aquellas informaciones que revelen los ámbitos más reservados del ser, tengan la consideración de datos sensibles. Este modo de configurar las categorías especiales es, sin duda, el más intuitivo. La especial protección se justifica en la naturaleza del dato, y su contenido es el elemento que determina su naturaleza.

Así entendida, la configuración del modelo de protección presentaría dos niveles: primero se reconocerían, de manera apriorística, un conjunto

[26] STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017.

de datos sensibles y, después, se establecería una fórmula de validación para corroborar la pertenencia del dato personal concreto a alguna de las tipologías predefinidas. Este método obliga a la positivación del conjunto de categorías que se van a considerar especiales.

La apuesta por el contenido como instrumento de catalogación proporciona importantes ventajas. En primer lugar, su sencillez aplicativa, pues bastaría con comprobar si una determinada información encaja con algunas de las categorías que previamente se han tipificado como sensibles. Así, si se consideran como sensibles los datos relativos a la salud, el modo de identificar que un dato tiene tal condición será analizando si su contenido ofrece información relacionada con ese ámbito. Abundando en esa dirección, la declaración general podría complementarse con una definición específica de qué se entiende por dato relativo a la salud, acotando, de este modo, el conjunto de datos personales susceptibles de ser subsumidos en esa tipología.

La segunda de las ventajas radica en el hecho de que la determinación en abstracto de la naturaleza de una información facilita el diseño del tratamiento, ofreciendo seguridad a quienes vayan a operar con datos personales. Bastará con constatar si la información dada es subsumible en alguna de las tipologías predefinidas, sin tener que preocuparse por los efectos o por las consecuencias derivadas del tratamiento. De este modo se dota de previsibilidad y confiabilidad al modelo establecido.

Como Simitis ha puesto de manifiesto, la existencia de un conjunto acotado y definido de informaciones sensibles desempeña «*a strategic function* […] *guarantees a maximum of transparency and stability and therefore also protects them* [the individuals] *against too quick and too many changes. The legislative intervention has however also another equally important side. It demonstrates that there is no definitive list of sensitive data. The still widespread assumption that the lists contain no more than a few once and for all fixed data is a pure fiction. The best that one can expect is that at least some of these data will be included in most enumerations. The legislative intervention illustrates and embodies the variability of the list*» (Simitis, 1999, p. 3).

Esto implica sacrificar la posibilidad de ofrecer la respuesta más adecuada a cada caso concreto, en aras de un sistema previsible, que ofrezca certezas a quienes se ven involucrados en operaciones de

tratamiento de datos. Por lo tanto, la principal ventaja de este sistema es la seguridad que ofrece a los aplicadores, frente a las dudas propias de un sistema centrado en la realidad del tratamiento[27].

Las categorías de datos especiales son la imagen provisional de aquello que se considera sensible en un momento dado y en un espacio concreto. No son una constante atemporal, sino una solución que nace bajo un preciso eje de coordenadas. Al configurar las categorías especiales de datos, el legislador dispone el marco que considera más adecuado para arrostrar a la realidad de ese momento y, a la vez, ofrece seguridad frente a los cambios acelerados que se pueden producir en un modelo estrictamente contextual.

Su principal inconveniente, su mayor debilidad, reside en los efectos negativos que se derivan de esa estructura de seguridad, así como de la extrema rigidez que introduce en el modelo. Los problemas de delimitación de los contornos de las tipologías parecen no existir, como si todos quedasen solventados por su carácter performativo. Lo mismo puede decirse de la inexistencia de fórmulas que permitan la graduación interna del riesgo. El resultado de todo ello es que, en la medida en que la información tratada no encaje en alguna de las categorías previstas, aun cuando entrañe un riesgo cierto para los derechos y libertades, no podrá extenderse a ella el régimen de protección más garantista, que queda formal y jurídicamente reservado a las categorías especiales de datos indicadas por el legislador.

Una regulación tan taxativa propicia, además, una aplicación cuasi-automática de las medidas de protección, dando lugar a situaciones en las que no existe adecuación entre el nivel del riesgo y las medidas adoptadas. La objetivación de lo especial blinda tipologías completas, sin atender a la percepción personal y, por exclusión, convierte en no sensibles a datos que, para individuos concretos, bien pudieran serlo.

El ICO[28], a partir de dos ejemplos ciertamente ilustrativos, puso de manifiesto los problemas que ocasionan la objetivación y la no

[27] Sobre las ventajas y desventajas de uno y otro enfoque se ha pronunciado, en extenso, el GT29 en Advice paper on special categories of data ("sensitive data") de 20 de abril de 2011, especialmente, pp. 13-15. Puede consultarse en: https://www.pdpjournals.com/docs/88417.pdf.

[28] El ICO es el acrónimo Information Commissioner's Office (United Kingdom), esto es, de la autoridad de protección de datos del Reino Unido. Puede accederse a su web a través de: https://ico.org.uk/

consideración de la afectación individual y de la realidad social en que el tratamiento se produce[29]. Así, advirtió acerca de que la categorización de los datos relativos a la afiliación sindical, razonable en épocas pretéritas, pero que, en la actualidad, en sociedades democráticas, podría no ser considerada, por muchos miembros de las organizaciones sindicales, como una información sensible. En contraposición, señaló que la información financiera[30], no catalogada como especial, podría, sin embargo, ser considerada sensible por muchos individuos.

3.2. La realidad del tratamiento determina la naturaleza del dato. El contexto como identificador

Reconocer categorías especiales de datos, atendiendo al contenido de los datos y a su naturaleza intrínseca, no es el único modo de identificar una información como sensible. El contexto y la finalidad[31] del tratamiento son factores que permiten determinar, en cada caso concreto, las características de la información y los riesgos que representa para las personas a las que se refiere.

El método es sustancialmente diferente. La aproximación a partir del contenido concibe al dato como un reflejo de la persona y, consecuentemente, es la información que en él se transmite la que representa un peligro para el individuo. En la concepción contextual-finalista, la realidad del tratamiento, el conjunto de interacciones,

[29] ICO, The Information Commissioner's (United Kingdom) response to A comprehensive approach on personal data protection in the European Union. A Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on 4 November 2010, de 14 de enero de 2011, pp. 6-8. Puede consultarse en:
https://amberhawk.typepad.com/files/ico-response.pdf

[30] En sentido contrario se manifestó el Gobierno austriaco en los asuntos acumulados Rechnungshof c. Osterreichischer Rundfunk, cuando señaló, apoyándose, además en la jurisprudencia del TEDH, que, «en el marco del control de proporcionalidad, se ha de tener en cuenta la medida en la que los datos afectan a la intimidad. Así, los datos relativos a la intimidad de la persona, a la salud, a la vida familiar o a la sexualidad deben protegerse más que los datos relativos a los ingresos y a los impuestos que, si bien revisten también un carácter personal, afectan en menor medida la identidad de la persona y son, por tanto, menos sensibles (véase, a este respecto, STEDH, asunto Fressoz y Roire c. Francia de 21 de enero de 1999, *Recueil des arrêts et décisions* 1999-I, § 65», en STJUE asuntos acumulados C-465/00, C-138/01 y C-139/01, Rechnungshof c. Osterreichischer Rundfunk, de 20 de mayo de 2003, apdo. 52.

[31] Como se ha apuntado, en este caso se analizarán contexto y finalidad como un único elemento, por lo que, especialmente cuando se utilice la palabra contexto, referida al tratamiento, se estará incluyendo la finalidad del mismo.

ramificaciones, efectos y objetivos perseguidos son los elementos que, junto a la naturaleza de la información, permiten averiguar si, en un tratamiento específico, el dato tratado es especialmente sensible para los intereses de la persona afectada.

La determinación normativa de un conjunto tasado de tipologías especiales de datos supone la configuración de una protección en abstracto, despersonalizada y objetiva[32]. Por el contrario, la opción contextual-finalista, facilita la adecuación normativa de las medidas de protección a los supuestos fácticos. Representa, por así decir, la personalización de las medidas de protección. «Conforme a un enfoque contextual, cualquier dato personal puede, dependiendo de las circunstancias de su tratamiento, adquirir el carácter sensible» (Huerta Anguiano, 2020, p. 17). Esa capacidad de adecuación es, a la vez, la mayor ventaja y la principal debilidad de este tipo de aproximación.

Las ventajas de la perspectiva contextual nacen de su adaptabilidad. Permiten aplicar la protección especial a aquellos tratamientos en los que se aprecie la presencia de las causas que subyacen al reconocimiento de un dato como sensible (esfera íntima, riesgo alto y discriminación). De este modo, al no estar condicionado más que por la realidad específica del tratamiento y la concurrencia, en el caso concreto, de alguno, o varios, de los factores identificadores de la condición especial, resulta posible prestar una protección más adecuada y personalizada, graduando su intensidad en función de los efectos y riesgos del tratamiento concreto.

Cuanto mayor sea el número de variables a considerar, mayor será el grado de especialización en la protección de los datos. No puede equipararse un sistema que solo tenga en consideración la naturaleza del dato, con uno en el que, junto a ese elemento, se consideren otros, como los efectos, las finalidades del tratamiento, los riesgos, las medidas de protección o, incluso, la situación personal del sujeto afectado.

No obstante, como apunta Huerta Anguiano, la incorporación de la escala de valores personales en la determinación de lo sensible «trae consigo el problema de convertir la valoración y determinación del carácter especialmente protegido de cierta información en una decisión altamente subjetiva» (Huerta Anguiano, 2020, p. 26). Para evitar ese efecto

[32] La objetividad de la categorización parte de un acto subjetivo previo, la selección de las tipologías por el legislador.

no deseado, resulta obligado establecer límites y condiciones que proporcionen cierta seguridad aplicativa.

La ausencia de previsibilidad es el principal inconveniente de un modelo basado preferentemente en la adecuación de las medidas de protección a la realidad de cada concreto tratamiento. Esta indefinición de origen dificulta la consecución de un marco regulatorio homogéneo y, por tanto, entorpece la libre circulación de la información. Un aspecto que resulta especialmente importante para el legislador europeo, que tiene en la construcción constante del mercado interior un condicionante ineludible. Esta circunstancia, convierte al sistema contextual en una opción, a priori, poco adecuada para el logro de los objetivos e intereses de la UE.

Un modelo absoluto de atención al contexto prescindiría de las categorías especiales de datos como condicionante abstracto y atendería, en exclusiva, a la realidad del tratamiento para determinar el grado de sensibilidad.

En el año 2011, el ICO se pronunció a favor de esta forma de protección y sugirió adoptar, en el ámbito europeo, «*a definition based on the concept that information is sensitive if its processing could have an especially adverse or discriminatory effect on particular individuals, groups of individuals or on society more widely. Any future definition might state that information is sensitive if the processing of that information would have the potential to cause individuals significant damage or distress.* […] *the distinctions between special categories and ordinary data could be removed from the new framework, with emphasis instead on the risk that particular processing poses in particular circumstances*»[33]. Si bien es cierto que, como opción menos radical, apuntó la posibilidad de mantener las categorías previstas, pero permitiendo una aproximación más flexible que posibilitase ampliar la protección a otras tipologías de datos[34].

---

[33] ICO, The Information Commissioner's (United Kingdom) response to A comprehensive approach on personal data protection in the European Union. A Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on 4 November 2010, de 14 de enero de 2011, p. 8. Puede consultarse en:
https://amberhawk.typepad.com/files/ico-response.pdf

[34] La apuesta por un enfoque que combinase la identificación conceptual y la contextual volvió a ser reiterada por el ICO, en 2013, en su análisis de la Propuesta de Reglamento General de Protección de Datos. No obstante, esa opción intermedia es planteada después de constatar que el modelo europeo de protección mediante categorías abstractas forma parte de la idiosincrasia de la UE y, por tanto, se improbable que sea abandonado y sustituido por

Al margen de la propuesta del ICO, importa señalar que, el enfoque contextual, no es ajeno a la realidad jurídica europea. Fue el modelo de protección utilizado en Austria y Alemania hasta que la Directiva 95/46/CE, cuya trasposición les obligó a incorporar las tipologías especiales de datos. Hasta ese momento, estos países venían «*consistently rejected all abstract categorisations of personal data and instead focussed on a context-orientated appreciation of the data*» (Wong, 2007, p. 13)[35]. De tal manera que, en el caso del sistema de protección datos alemán, datos como el nombre o la dirección, generalmente carentes de riesgo, si eran tratados en relación con una lista pacientes de un hospital psiquiátrico eran considerados sensibles[36]. Es decir, el contexto operacional en que el dato se insería era lo que determinaba su sensibilidad real.

3.3. La protección jurídica de los supuestos dudosos. La combinación contexto-naturaleza

3.3.1. El valor del contexto

Entre un sistema de categorías predefinidas y uno que determine el grado de sensibilidad/peligrosidad en atención a la realidad de cada tratamiento, es posible establecer modelos intermedios de protección en los que las dos vías para la identificación de lo especial confluyan en la configuración del régimen de protección de lo sensible. Las combinaciones posibles variarán en función del peso relativo que quiera darse a cada una de ellas.

La mayoría de regulaciones reconocen la existencia de datos que, por su naturaleza, son sensibles (Wang y Jiang, 2017, p. 3299), es decir, acogen

una aproximación contextual. Vid. ICO, Proposed new EU General Data Protection Regulation: Article-by-article analysis paper, 12 de febrero de 2013, pp.11-12. Puede consultarse en:
https://ico.org.uk/media/about-the-ico/documents/1042564/ico-proposed-dp-regulation-analysis-paper-20130212.pdf

[35] En la misma línea apunta Simitis, al señalar, respecto de la Directiva, que «*the prohibition against processing a series of highly sensitive data, such as information concerning an individual's racial or ethnic origin, political opinions, religious beiefs, trade-union membership, health, or sexual life* (art. 8), *affirms a standpoint shared, for example, by the Belgian, French, Spanish, and Portuguese laws. The prohibition is inconsistent, however, with legislation embodying the German view that "sensitivity" depends on the particular processing context rather than on an abstract classification of the data*» (Simitis, 1995, p. 450).

[36] Este y otros ejemplos de la regulación alemana previa a la Directiva, así como las características de la misma, pueden consultarse en (Simitis, 1990).

el modelo abstracto de protección, con categorías de datos predefinidas. Es la base regulatoria preferente a nivel global.

El reconocimiento de categorías especiales acota el marco de aplicación a un conjunto cerrado de informaciones, para las que se reservan medidas de protección reforzada. Al establecer un listado predefinido de informaciones, se veda la posibilidad de extensión de las salvaguardas a situaciones de riesgo análogo, limitando la esfera de actuación. La previsión expresa de determinados requisitos fácticos introduce una rigidez en el sistema que no se corresponde con la variabilidad y flexibilidad que la práctica demanda.

Si bien es cierto que hay datos que, por contenido, siempre encajarán en las conceptualizaciones legales y son, por así, decir, naturalmente especiales[37]; hay otras informaciones que no tienen una naturaleza predeterminada, sino que, en función del tratamiento en que se utilicen, pueden operar como dato sensible, o no.

Así, por ejemplo, el código postal no parece, per se, una información relativa a la salud, sin embargo, se ha constatado que el lugar de residencia es un factor determinante de la esperanza de vida de una persona (Sarkodie, Strezov, Jiang, y Evans, 2019)[38]. En la misma línea, la crisis sanitaria derivada de la Covid-19 ha puesto de manifiesto el valor de la ubicación, y su capacidad para inferir informaciones sensibles. Sin embargo, los datos sobre ubicación no encajan, al menos en abstracto, ni en la definición de dato relativo la salud, ni en el de dato relativo a la orientación sexual, aunque, a veces, operen como tales[39]. La ubicación[40], al igual que otros datos personales, ofrece una información que, según como se utilice, por quién y para qué, permitirá inferir otras informaciones, más o menos sensibles, en función del contexto del tratamiento.

---

[37] Así lo considera (Al-Fedaghi, 2007), para quien es posible identificar un conjunto de datos naturalmente sensibles.

[38] Del mismo modo, el nivel educativo no es incardinable en ninguna categoría especial, sin embargo, es un factor a considerar en la esperanza de vida de las personas (Requena, 2017).

[39] Las apps de rastreo de contactos, especialmente los modelos implementados en países como Corea, permitieron combatir la pandemia de la Covid-19, la ubicación de las personas se convirtió en un valioso activo para la salud pública. Sin embargo, también provocó que se revelase la orientación sexual de ciertas personas, al rastrear sus visitas a determinados distritos de las ciudades (Pratamasari, 2020) o (Jung, Lee, Kim, y Lee, 2020).

[40] El potencial informativo de la ubicación es enorme, pues también podría servir para conocer las convicciones religiosas de una persona (por las visitas a centros religiosas), su ideología (por revelar si asiste a determinadas manifestaciones, por ejemplo) o su pertenencia a un sindicato.

Ante lo evidente de este hecho fáctico, la inclusión de soluciones jurídicas capaces de complementar, o sustituir, la protección dispensada por las categorías especiales resulta más que necesaria. El contexto del tratamiento sería el factor destinado a responder, con mayor o menor intensidad, a los supuestos dudosos. Se trataría, por tanto, de articular un sistema en el que, sin cuestionar la condición central de las categorías especiales, se posibilitase tomar en consideración la realidad específica del tratamiento.

La importancia que se otorgue al contexto, el margen identificador que se le conceda, propicia modelos de lo más variado. Estos, pueden ir desde una relevancia mínima, en la que el contexto solo operaría como factor de resolución de supuestos dudosos, hasta conceder a la variable contextual-finalista el mismo valor identificativo de lo sensible que tendría el contenido de la información.

3.3.2. Una aportación de mínimos. El contexto como clarificador de supuestos difusos

Existen datos que no resultan fáciles de clasificar apriorísticamente. Una fotografía ¿es un dato relativo al origen racial?, ¿puede ser un dato biométrico? En casos en los que el dato, por sí mismo, podría encajar en más de una tipología, solo el contexto permite resolver la duda surgida en el supuesto concreto. Así, si la fotografía se analiza mediante sistemas biométricos, será, en ese tratamiento concreto, un dato biométrico. En este tipo de situaciones, la adjetivación del dato como perteneciente a una tipología no supone una asignación general a la misma. Se trata de supuestos fronterizos, en los que el contexto sirve para resolver las dudas interpretativas respecto de datos con compatibilidad múltiple o difusa con las categorías especiales legalmente previstas.

3.3.3. El equilibrio entre contexto y contenido

Frente a esa propuesta de mínimos, cabe la posibilidad de un modelo en el que el contexto tenga una capacidad identificadora equivalente a la del contenido del dato. En estos casos, en lugar de resolver supuestos dudosos de datos compatibles, el contexto operaría como factor

determinante de la naturaleza de la información tratada, cualquiera que fuese su contenido.

En este escenario, serán las características del tratamiento las que ayuden a clasificar la información como especial. Así, si en un tratamiento en el que se está valorando algún aspecto vinculado con la salud (v. gr. calcular su esperanza de vida para hacer un seguro) se utilizan datos como la edad, el lugar de residencia o el salario, estos, pese a no encajar estrictamente en la definición de dato relativo a la salud, serían considerados como tales en ese tratamiento concreto.

Romeo Casabona propone esta solución para los datos relativos a la salud (Romeo Casabona, 2019, pp. 93-94), aunque es una opción interpretativa que perfectamente se puede aplicar al resto de tipologías de datos, pues el problema al que hace frente es común a todas ellas. De este modo, sería posible clasificar cualquier tipo de dato en función de la finalidad y realidad del tratamiento. Por ejemplo, una fotografía, si es tratada para determinar la raza de una persona, podría ser clasificada como dato de origen racial.

En biología, el fenotipo es la «manifestación del genotipo de un organismo en un determinado ambiente»[41], y abarca tanto elementos físicos como conductuales (Zerón, 2011). Pues bien, el modelo de protección que se comenta sería similar: las categorías especiales constituyen el genotipo[42], la caracterización funcional básica o, en términos informáticos, la configuración por defecto de la persona, mientras que el tratamiento sería fenotipo.

El resultado es un modelo mucho más flexible, que permite extender la protección de lo sensible tanto a las tipologías de datos dudosas, como a cualquier otro dato utilizado para una finalidad o en un contexto especial. Ahora bien, el tratamiento solo tendrá esa condición singular si puede conectarse con las categorías previamente definidas como sensibles.

Cualquiera que fuese la modalidad elegida, en todos los casos, el contexto solo podría operar como un cauce identificador de la información perteneciente a alguna de las categorías especiales. No podría introducir nuevas formas de protección de lo sensible. La fuerza condicionante del reconocimiento positivo de un conjunto de tipologías especiales seguiría

[41] Diccionario de la Real Academia Española.

[42] Genotipo: «conjunto de los genes de un individuo» en Diccionario de la Real Academia Española.

impidiendo una determinación de lo sensible basada en los elementos subyacentes: la capacidad para revelar la información más reservada, el potencial discriminatorio o el riesgo alto.

4. El modelo europeo de protección de los datos especiales

4.1. La naturaleza del dato como premisa, el contexto como factor clarificador de supuestos dudosos

El RGPD[43] enuncia un conjunto de datos que son los únicos que, en el ámbito europeo, tienen la condición de especiales[44]. A su vez, para algunas de esas informaciones, ofrece una definición específica y acotada de las características que han de reunir, en concreto para tres tipologías: los datos genéticos[45], los datos biométricos[46] y los datos relativos a la salud[47].

[43] A estos efectos se tomará el RGPD como referencia normativa en el análisis de las categorías especiales, por ser la regulación europea más completa.

[44] «Datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física» (art. 9.1 RGPD).

[45] Conforme al art. 4.13 del RGPD, serán datos genéticos, los «datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona». El Considerando 34 abunda en la misma idea, señalando que tendrán esta condición, los datos obtenidos «a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente». Este listado no debe interpretarse con carácter taxativo, sino como meramente ejemplificativo de los mecanismos más habituales de generación de información genética tratable como dato personal. Sobre el carácter del Considerando 34 y sus posibilidades interpretativas he tenido ocasión de pronunciarme, junto al profesor De Miguel Beriain, en (De Miguel Beriain y Jove Villares, 2021).

[46] Conforme al art. 4.14 del RGPD, serán datos biométricos, los «datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos».

[47] Conforme al art. 4.14 del RGPD, serán datos relativos a la salud, los «datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud». El Considerando 35 detalla un conjunto de datos que, por su contenido, tendrán la condición de dato relativo a la salud, ahondando en la consideración del objeto como elemento determinante a la hora de determinar la naturaleza del dato.

Del resto de datos especiales no proporciona una conceptualización específica[48], acaso porque se trata de aquellos datos cuya naturaleza coincide con las clásicas categorías sospechosas[49], lo que hace menos necesario delimitar de forma expresa su contenido ya que su objeto es más conocido[50], aunque no por ello más claro[51]. Con todo, la lógica subyacente a las tipologías especiales no expresamente definidas es la misma: si una información es susceptible de ser etiquetada como perteneciente a alguna de las categorías enunciadas, será un dato sensible.

A la hora de etiquetar las informaciones pueden producirse dos tipos de error. Que no se considere como sensible un dato que debiera serlo. O, al revés, que se otorgue la condición especial a una información que no lo es. Al imponerse legalmente un régimen más exigente de protección, se produciría una suerte de congelación del rango para ese tratamiento concreto, lo que puede afectar a la libre circulación de datos[52].

---

[48] Más allá de alguna aclaración puntual, como la referida al origen racial y la no «aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas» Considerando 51 RGPD.

[49] La *suspect classification* tiene su origen en el reconocimiento jurisprudencial por el Tribunal Supremo de una serie de situaciones y supuestos en los que, por las características del caso y la temática de los mismos, podría generar discriminación y, consecuentemente, es necesario, realizar un *strict scrutiny* a las acciones gubernativas que tengan conexión con dichos temas. Entre las categorías se encontrarían, la raza, el origen nacional, la religión (vid. Sentencias del Tribunal Supremo Hirabayashi v. United States, 320 U.S. 81 (1943); Korematsu v. United States, 323 U.S. 214 (1944); Graham v. Richardson, 403 U.S. 365 (1971)) o la orientación sexual, incorporada en la serie de casos agrupados en Hollingsworth v. Perry, 570 U.S. 693 (2013) (nombre completo: Dennis Hollingsworth, et al., Petitioners v. Kristin M. Perry, et al.).

[50] No resulta viable enunciar todas las previsiones que, bien con carácter general, bien respecto de alguna de las categorías sospechosas específicas, prohíben la discriminación y establecen medidas en favor de la igualdad. Sirvan como ejemplo de previsiones generales: la Declaración Universal de Derechos Humanos de 1948 (art. 2); el CEDH (art. 14), así como sus Protocolos, especialmente el nº 12; Pacto Internacional de Derechos Civiles y Políticos. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966 (art. 2); CDFUE (art. 21). En cuanto a las previsiones específicas para cada categorías sospechosa, las regulaciones son numerosas y variadas, vid. la magnífica monografía de Rey Martínez (Rey Martínez, 2019).

[51] El trabajo de Tussman y tenBroek (Tussman y TenBroek, 1949), de finales de la década de los cuarenta es, quizá, el mejor punto de partida para comprender las dificultades para implementar políticas de igualdad, así como una referencia obligada en este ámbito.

[52] La libre circulación de datos es una de las razones por las que se aprueba el RGPD y un elemento esencial del sistema europeo. Como establece el Considerando 13 del RGPD, «el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales». Por lo tanto, la clasificación errónea en un nivel de protección diferente es un obstáculo no aceptable en el sistema europeo.

«Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales» (Considerando 51). Vista la dicción del Considerando, pudiera pensarse que, al hacer referencia al «contexto de su tratamiento», el RGPD apuesta por un modelo en el que, junto a la naturaleza de la información, también se consideran las circunstancias en que se opera con ella. Así lo entiende, por ejemplo, Huerta Anguiano, para quien «el legislador europeo matizó el alcance a la expresión "naturaleza", al referir expresamente al contexto del tratamiento que puede dar surgimiento a diversos riesgos para los derechos y las libertades fundamentales de los individuos» (Huerta Anguiano, 2020, p. 17).

Compartiendo la idea de que el contexto modula al factor naturaleza, no considero que la previsión del RGPD tenga un alcance interpretativo tan amplio. La mención al contexto no lo convierte en un mecanismo identificador de la naturaleza del dato. El Considerando 51 no reconoce dos factores en concurrencia, pues el contexto nunca podría invocarse para negar la naturaleza sensible a un dato que lo fuese por definición aunque, en un específico contexto, no generase riesgo alguno.

Antes bien, la referencia al contexto no es un más que la ratificación de que los datos especiales lo son por su naturaleza. En efecto, lo que se está señalando es que el tratamiento de datos especiales genera un riesgo mayor. Como antes se ha dicho, sin tratamiento no hay peligro. Por tanto, lo que el RGPD está indicando es que, de producirse el tratamiento, ha de considerarse que, determinados datos, por su contenido, son susceptibles de generar un daño mayor en los derechos de las personas a las que se refieren.

La mención al contexto no se puede desconectar del resto del enunciado en que se inserta, ni del contenido del art. 9 del RGPD. Si se analiza el Considerando, se comprueba, en primer lugar, que, para el legislador europeo, los datos especiales lo son «por su naturaleza» y, por eso, reconoce un conjunto cerrado de tipologías sensibles. En segundo lugar, esa naturelaza los hace «particularmente sensibles en relación con los derechos y las libertades fundamentales». La especialidad se justifica en la condición sensible de la información tratada, y la sensibilidad solo se pregona de aquellos datos cuya naturaleza los hace más propensos a afectar a los derechos y libertades. Finalmente, el tratamiento sería el modo

en que ese peligro potencial, consustancial a la información, se manifestaría. Es decir, cuando en un tratamiento concurrieran datos especiales, esa operación comportaría un mayor riesgo.

Esa condición de la sensibilidad (el riesgo para los derechos y libertades) acota el espectro de datos susceptibles de ser considerados especiales, aunque se trata de una premisa bastante amplia. Prueba de ello es que, en el Considerando 75 del RGPD, se ofrece un listado mucho más extenso de datos y circunstancias en las que puede materializarse ese riesgo[53]. Que, de la pleyade de informaciones capaces de engendrar un peligro alto, el legislador europeo haya seleccionado un conjunto, específico y limitado, al que ha conferido una condición especial, ratifica la posición central de la naturaleza como factor identificativo de lo sensible.

Para el RGPD, al menos conforme al Considerando 51, el dato genera el contexto peligroso, no es el contexto peligroso el que determina la condición especial del dato. No obstante, al analizar en detalle la regulación de los datos especiales, se constata que, en ocasiones, el contexto del tratamiento sirve para confirmar la condición especial de determinadas informaciones, sobre las que pudieran existir dudas acerca de su condición.

Esto significa que el contexto opera, en esencia, como clarificador de supuestos inciertos y fronterizos. Ejemplo de ello sería la clasificación de las fotografías como dato biométrico, en la medida en que tal condición depende de la utilización de medios adecuados para asegurar la

[53] Considerando 75 RGPD:
«Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados».

identificación inequívoca de la persona[54], o la condición de datos relativos a las convicciones religiosas cuando consten en los ficheros y registros de iglesias y asociaciones religiosas[55].

En definitiva, el RGPD adopta un modelo de predeterminación expresa de lo especial. Reconoce un conjunto tasado de tipologías de datos, seleccionados en atención a su condición «intrínsecamente sensible» (Huerta Anguiano, 2020). La identificación de los datos que pertenecen a ese conjunto cerrado de categorías tiene, en el contenido de la información, el principal medio de subsunción.

El sistema europeo aboca a un ejercicio de identificación de lo sensible necesariamente abstracto, pues, solo los datos que a priori encajen con las características de las tipologías especiales jurídicamente reconocidas tendrán tal condición. Ahora bien, debido a la multiplicidad de datos personales existentes, y de tratamientos posibles, hay informaciones cuya naturaleza resulta dudosa y no puede establecerse su condición sin tomarse en consideración la realidad del tratamiento en que se insertan. Para esos supuestos, el factor contextual opera como criterio identificador.

4.2. El régimen jurídico de los datos especiales en el RGPD. La prohibición como premisa

Con independencia de la idiosincrasia que inspira la configuración de las categorías especiales, es importante conocer, siquiera someramente, la plasmación normativa del sistema de protección de lo sensible positivizado en el RGPD. Recordemos que su elemento más característico es la prohibición del tratamiento como regla (art. 9.1 RGPD).

Esta prohibición condiciona todo el sistema de protección, pues veda cualquier intento de modulación en función de las circunstancias del tratamiento, si bien la interdicción del tratamiento de categorías especiales no es absoluta. El legislador europeo reconoce un conjunto tasado de

[54] «El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física» (Considerando 51 RGPD).

[55] El art. 91 RGPD ayuda a clarificar cuando los archivos de las entidades religiosas tienen la condición de dato relativo a las convicciones religiosas. Para una exégesis más detallada de la interpretación de este precepto, vid. (Medina Guerrero, 2019, pp. 270-273).

circunstancias que, de producirse, y existiendo alguna de las bases de licitud para el tratamiento del art. 6.1 RGPD[56], posibilitarían operar con estas tipologías de datos. Por tanto, la prohibición solo podrá enervarse en las situaciones legalmente previstas.

Cuando se analizan las condiciones en las que es factible el tratamiento de datos especiales (art. 9.2 del RGPD)[57], se constata que obedecen a razones vinculadas a elementos contextuales, ya sean personales (p. ej. consentimiento explícito), circunstanciales (como puede ser el hecho de que los datos se hayan hecho públicos), por la finalidad perseguida (v. gr. protección frente a amenazas transfronterizas graves para la salud o garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria) o por quien opera con la información (p. ej. tratamiento por parte de asociaciones para la realización de sus actividades legítimas).

Así, en el caso del consentimiento explícito (art. 9.2.a)[58], este no deja de ser la manifestación de la voluntad personal de permitir la utilización de información a uno referida. Esa decisión afirmativa por parte del

---

[56] Art. 6.1 RGPD:
«El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones».

[57] El apartado 3 del art. 9 del RGPD específica, aún más las condiciones del habilitantes previstas en la letra h) del apartado 2. A efectos interpretativos, también resultan de interés los Considerandos 52 y 54, especialmente el primero de ellos. Sobre el alcance de las circunstancias habilitantes del tratamiento de datos especiales, vid. (López Calvo, 2017, pp. 186-187).

[58] La prohibición de tratar datos especiales no será de aplicación cuando «el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado» (art. 9.2.a). Sobre el consentimiento explícito, sus requisitos, excepciones o modo de expresión, vid. (De Miguel Beriain y De Lorenzo y Aparici, 2020, pp. 83-90).

interesado obedecerá, en última instancia, a las circunstancias del tratamiento. Será el contexto del mismo, las finalidades que persiga y los réditos que le pueda generar, lo que fundamente la decisión. No obstante, debe advertirse que, el RGPD, habilita a los Estados miembros para desactivar o limitar las posibilidades del consentimiento como mecanismo enervante de la prohibición de tratar categorías especiales[59].

Por lo que respecta al supuesto habilitante relativo a la necesidad de tratar la información «para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social» (art. 9.2.b RGPD), será preciso que medie algún tipo de previsión normativa sectorial, ya sea previsión legal o convenio colectivo, en la que se disciplinen las garantías específicas para la protección «de los derechos fundamentales y de los intereses del interesado» (art. 9.2.b RGPD).

Este supuesto, como otros previstos en este apartado segundo del art. 9 RGPD, se fundamenta en la necesidad de operar con datos especiales para asegurar el normal funcionamiento de un determinado sector. Sin embargo, son las circunstancias subyacentes a las categorías especiales (riesgo alto, afectación de la esfera reservada y riesgo de discriminación) las que han de orientar la utilización de la información sensible.

La protección de los «intereses vitales del interesado o de otra persona física» (art. 9.2.c RGPD), es un supuesto paradigmático en el que la situación del interesado determina las posibilidades de llevar a cabo el tratamiento. Solo será jurídicamente aceptable utilizar datos especiales por esta causa cuando «el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento» (art. 9.2.c RGPD).

También se permiten los tratamientos necesarios para la realización de las finalidades legítimas de asociaciones y fundaciones cuyo objeto y «finalidad sea política, filosófica, religiosa o sindical» (9.2.d RGPD). Al igual que en 9.2.b RGPD, se asume que el tratamiento de datos sensibles es consustancial a la actividad que da sentido a la existencia de esas entidades. Ante un escenario semejante, el legislador europeo optó por admitir el tratamiento de datos especiales, pero condicionando el marco de actuaciones posibles y el modo en que han desarrollarse (el tratamiento ha de circunscribirse, «exclusivamente [,] a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con

[59] Habilitación de la que ha hecho uso el legislador en el art. 9.1 LOPDGDD.

ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesado» (9.2.d RGPD)).

En el caso de los datos hechos manifiestamente públicos (art. 9.2.e RGPD), la premisa habilitante conecta directamente con la razón de ser de las categorías especiales. Si la información ya es conocida, el riesgo adicional que supondría el uso por terceros de esos datos especiales estaría amortizado, pues ya son conocidos. No quiere decirse con esto que los riesgos hayan desaparecido, pero esa información ha perdido uno de los elementos que la hace sensible, su carácter reservado. Adicionalmente, imponer una prohibición de tratamiento, sobre datos susceptibles de ser conocidos por cualquiera, supondría, teniendo en cuenta las circunstancias, imponer al responsable que pretenda utilizarlos una limitación desproporcionada.

La posibilidad de tratar datos sensibles en los casos en que sean necesarios «para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial» (9.2.f RGPD) tiene una vinculación contextual evidente. El objetivo perseguido es lo suficientemente valioso como para asumir el riesgo que pueda generar el tratamiento de los datos.

Este supuesto ejemplifica bien la realidad de las excepciones del 9.2 RGPD. Estas son, en esencia, el fruto de un ejercicio de ponderación de intereses en concurso. Solo que, esa valoración, no la realiza un tribunal para un caso concreto, sino el legislador europeo en abstracto.

La misma lógica justifica el tratamiento por razones de interés público[60] (art. 9.2.g RGPD)[61]. Para este supuesto, se establecen una serie de condiciones que, de cumplirse, harían viable el tratamiento. En concreto, que el interés público sea «esencial»[62], que haya proporcionalidad entre el tratamiento y la finalidad perseguida y, como no podía ser de otro modo,

[60] Sobre la complejidad del concepto interés público y las diferentes interpretaciones posibles del mismo, vid. (Salas Carceller, 2014).

[61] El art. 9.2.g RGPD habilita operar con datos especiales cuando «el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado».

[62] Que deba ser un interés público esencial supone elevar el nivel de exigencia y exige un mayor nivel de concreción. Acerca del término esencial y sus implicaciones, vid. (R. M. García Sanz, 2019).

que se establezcan las garantías adecuadas para asegurar la integridad de la información.

Los supuestos previstos en las letras h)[63] (complementado con lo dispuesto en el 9.3 RGPD)[64] e i)[65] del art. 9.2 RGPD prevén diversos escenarios, estrechamente relacionados con contextos sanitarios[66], en los que se considera que los fines del tratamiento, y el contexto en que se produce, permiten enervar la prohibición prevista en el 9.1 RGPD[67]. En estos casos, la utilización de la información sensible redundaría en un beneficio directo para el interesado (v. gr. diagnóstico médico o asistencia sanitaria) o para la sociedad en su conjunto –razones de interés público– (p. ej. gestión de los sistemas salud o seguridad de los productos sanitarios). En estos tratamientos, el cálculo riesgo-beneficio tiende a inclinarse a favor del uso de los datos personales, no solo porque *salus populi suprema lex est*, sino, también, porque las medidas técnicas, y de seguridad, que pudieran implementarse se verían reforzadas con la

[63] Art. 9.3.h RGPD señala que podrán tratarse datos sensibles cuando «el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3».

[64] El art. 9.3 RGPD precia lo dispuesto en el 9.2.h) al señalar que, «los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes».

[65] Conforme a lo dispuesto en el 9.2.i), podrán utilizarse datos especiales cuando «el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional». Ejemplo de situaciones susceptibles de ser incardinadas en este supuesto se contaría la respuesta a las pandemias, como ha ocurrido durante con la del Covid-19 (Abellán-garcía Sánchez, 2021).

[66] Con carácter general los datos utilizados en los tratamientos permitidos serán informaciones relativas a la salud de las personas, sin embargo, nada impide que se traten otro tipo de informaciones sensibles (por ejemplo datos genéticos), siempre que sean necesarias para la consecución de los fines que se habilitan.

[67] Sobre los tratamientos habilitados por la normativa europea en materia de Salud pública, asistencia sanitaria e investigación, vid. el detallado análisis de Troncoso Reigada en (Troncoso Reigada, 2018).

obligación de secreto médico, y de secreto profesional, de quienes manejasen la información.

Finalmente, el legislador europeo considera que, los tratamientos «con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos» (art. 9.2.j RGPD) persiguen finalidades lo suficientemente valiosas como para permitir la utilización de datos especiales. Los objetivos que inspiran la investigación, o el preservar un archivo de interés general, pudieran parecer motivo suficiente, pero no es así. Además, han de implementarse importantes medidas de seguridad (proporcionalidad, respeto a los derechos y adecuación de los mecanismos de protección), que se suman a la obligación de secreto profesional o estadístico inherente a la mayoría de los tratamientos habilitados.

Si el tratamiento que se pretende llevar a efecto requiere de datos especiales, pero no es subsumible en alguna de las previsiones del RGPD, no será posible llevarlo a efecto. Con todo, los Estados miembros están facultados para establecer regulaciones particularizadas respecto de estas categorías de datos, lo que ha hecho variar las condiciones de tratamiento de la información especial[68]. No obstante, no es una capacidad incondicionada, sino que ha de ejercitarse con una finalidad determinada: proteger datos personales u otros derechos fundamentales, siempre que se funde en razones de interés público y se implementen las garantías adecuadas[69].

Además de esas habilitaciones generales previstas en los Considerandos, el apartado cuarto del artículo 9 RGPD establece, expresamente, que «los Estados miembros podrán mantener o introducir

[68] El Considerando 10 del RGPD reconoce «un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el [...] Reglamento no excluye el Derecho de los Estados miembros a determinar las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito». Adicionalmente, el Considerando 52, viene a reforzar las opciones

[69] El Considerando 52 del RGPD estipula que «deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud»

condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud».

Como he apuntado en un trabajo previo, «esta habilitación supone que cada una de esas tres tipologías de datos […] podría tener un régimen particularizado en atención a las peculiares características que las singularizan. La materialización de un escenario semejante implicaría el establecimiento de unas condiciones más severas para el tratamiento de ese tipo de datos» (Jove, 2017, p. 63). La articulación de ese modelo más restrictivo supondría la materialización del escenario apuntado Toniatti décadas antes de que el RGPD existiese (de hecho, antes incluso de la Directiva 95/46/CE), la emergencia de una nueva categoría datos: los «supersensibles» o «sensibilísimos» (Toniatti, 1991, p. 159).

Finalmente, ha de consignarse que, el contenido del RGPD, no se agota en la regulación de las condiciones en que se puede operar con datos pertenecientes a las categorías especiales. En congruencia con su condición de normativa omnicomprensiva, establece un conjunto de previsiones que, sin tener en el tratamiento de las tipologías sensibles su único fundamento, contribuyen a refrendar la condición reforzada de su marco de protección.

Entre las medidas previstas con relación al tratamiento de categorías especiales de datos estarían: la prohibición de adoptar decisiones automatizadas a partir de ellas (art. 22.4 RGPD); la designación de representante (art. 27.2.a RGPD); la exigencia de llevar un registro de actividades (art. 30.5 RGPD); la realización de una evaluación de impacto (art. 35.3.b RGPD) o la designación de un delegado de protección de datos (art. 37.1.c RGPD). La presencia de datos especiales es un factor a considerar en cada una de esas características del tratamiento, y supone un incremento de las exigencias normativas; ya sea por solicitar la implementación de actuaciones adicionales, ya por requerir la presencia de ciertos sujetos que refuercen la protección de los derechos en conflicto.

4.3. Dos modos de afrontar la habilitación del RGPD. El modelo español y el alemán

Los Estados miembros han hecho uso de las posibilidades de regulación que el RGPD les brinda. A título puramente ilustrativo se presentarán algunas particularidades de las regulaciones de España y Alemania con relación a las categorías especiales de datos. No se pretende

describir con detalle las previsiones implementadas en estos Estados. Tan solo reflejar las posibilidades normativas abiertas por el RGPD en lo referente al tratamiento de las categorías especiales de datos.

4.3.1. España

El legislador español ha hecho uso de esta habilitación[70], y ha incorporado ciertas limitaciones y exigencias adicionales. De una parte, ha considerado que el consentimiento, aunque sea explícito, no es suficiente por sí solo «para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico» (art. 9.1 LOPDGDD).

La selección de tipologías no es casual (no se incluyen los datos relativos a la salud, ni los genéticos, ni los biométricos; tampoco se incluye la vida sexual, solo la orientación sexual); se corresponde con las categorías de datos coincidentes con las categorías sospechosas. Así lo reconoce el propio precepto cuando señala que su finalidad es «evitar situaciones discriminatorias» (art. 9.1 LOPDGDD).

Por otra parte, el apartado segundo del art. 9 de la LOPDGDD, impone la regulación «en una norma con rango de ley» de cualquier previsión complementaria relativa a la «seguridad y confidencialidad» de los tratamientos habilitados en los apartados g), h) e i) del 9.2 del RGPD. El párrafo segundo del 9.2 LOPDGDD incide en la importancia de aplicar esas exigencias a los supuestos en que se opere con datos relativos a la salud, y demanda que el tratamiento tenga como finalidad «la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte». La mención expresa de los datos relativos a la salud no supone una exclusión aplicativa de esta previsión al resto de tipologías de datos[71]. Antes bien, solo refleja el papel preponderante que, en los supuestos habilitantes de las letras g), h) e i), tiene esa tipología de datos.

Junto a estas previsiones generales, la LOPDGDD establece otras mucho más específicas en relación con el tratamiento de los datos relativos a la salud (Disposición adicional decimoséptima). Ese precepto es el correlato de la obligación del 9.2 LOPDGDD. El apartado primero de la

[70] Para un análisis general del art. 9 de la LOPDGDD, vid. (Aba Catoira, 2020b).
[71] Cano Ruiz, considera que las previsiones del 9.2 LOPDGDD también serían aplicables a los datos genéticos y biométricos, además de a los datos relativos a la salud (Cano Ruiz, 2019, p. 82).

Disposición adicional decimoséptima se limita a proporcionar una relación pormenorizada de las normativas en las que se disciplinan los tratamientos «amparados en las letras g), h), i) y j) del artículo 9.2 del» RGPD. Su finalidad es eminentemente clarificadora y descriptiva.

Más detallado y preciso es el apartado segundo de la Disposición adicional decimoséptima, que regula el régimen de protección y el uso de los datos personales en la investigación en salud. Se trata de una auténtica regulación sectorial, en la que el legislador ha disciplinado y precisado cada una de las fases y usos admitidos en un ámbito tan delicado y, a la vez, tan crucial[72].

Menos cuidadoso estuvo el legislador español al hacer uso de la habilitación del Considerando 56 del RGPD[73] en relación con el uso de datos relativos a las opiniones políticas. La Disposición final tercera de la LOPDGDD, modificó la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, e incorporó un apartado bis al artículo 58. El primero de los apartados de este precepto fue declarado inconstitucional en la sentencia 76/2019, de 22 de mayo de 2019. El vicio de inconstitucionalidad era triple, pues no se definía la finalidad justificadora de la injerencia en el derecho a la protección de datos, ni se establecían límites claros, ni se articulaba un marco de garantías apropiado[74].

A los efectos que aquí interesan, baste con señalar que, en el caso de España, se ha hecho un uso moderado y, esencialmente, clarificador de las posibilidades que ofrece el RGPD en relación con la regulación del tratamiento de datos especiales, con la excepción, ya corregida por el TC, del uso de datos relativos a opiniones políticas.

El aspecto en el que el legislador español más ha innovado es el referente a la inviabilidad del consentimiento explícito como base

---

[72] Sobre la regulación de la investigación en salud, tanto desde el punto de vista del RGPD, como en un enfoque transversal en el que se incluyen los efectos y matices de la Disposición adicional decimoséptima, me remito a los excelentes análisis de (Recuero Linares, 2019a); (De Miguel Beriain y De Lorenzo y Aparici, 2020, pp. 129-148); (Ferrer Martín de Vidales, 2020) y (Nicolás Jiménez, 2021).

[73] Considerando 56 RGPD, «Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas».

[74] Sobre la inconstitucionalidad del art. 58bis de la LOREG he tenido ocasión de pronunciarme en (Jove Villares, 2021). Sobre la STC 76/2019, de 22 de mayo se han realizado detallados y atinados comentarios, por todos, vid. (Arenas Ramiro, 2019b); (Adsuara Varela, 2019) y (Pascua Mateo, 2019).

habilitante para el tratamiento. Esta limitación refuerza la posición del dato personal como elemento nuclear de la regulación, reafirma la condición natural de estos, y prescinde del riesgo real de discriminación del tratamiento, como criterio fundante del modelo de protección.

4.3.2. Alemania

En Alemania se ha adoptado una regulación expansiva (Arora, 2020, p. 60), y se reconocen otros supuestos adicionales[75] en los que es posible tratar los datos reconocidos en el 9.1 del RGPD. Con ello, parece rebajarse el nivel de protección de las tipologías sensibles (Weichert, 2017). Sin embargo, más que un menor nivel de garantías, la normativa alemana trata de acomodar las exigencias del RGPD con el sistema de protección que, tradicionalmente, han utilizado –mucho más apegado al contexto–.

Una de las particularidades de la regulación alemana es el modo en que regula los supuestos en los que es posible tratar datos especiales. Para ello, distingue entre los tratamientos llevados a cabo por los entes públicos (§ 22 (1).1 y § 23) y los realizados por particulares y entidades privadas (§ 22 (1).1 y § 24). Esta diferenciación entre responsables le permite adecuar las medidas específicas a desarrollar a las particularidades de los tratamientos, pues cada sujeto opera con los datos para unas finalidades específicas. De este modo, el legislador alemán incorpora un criterio de especialización en la regulación de los tratamientos que posibilita una mayor precisión de las medidas de protección.

Ese primer perfilado de los tratamientos se complementa con una mayor exigencia en la atención al riesgo del tratamiento y a las condiciones en que tiene lugar. Muestra de ello es el apartado 2 del § 22, en el que, para los supuestos adicionales de tratamiento, vinculados a la defensa del interés público –condición ineludible del RGPD–, se exige tomar en consideración «el estado de la técnica, el costo de implementación y la naturaleza, alcance, contexto y propósitos del procesamiento, así como los

[75] Además de una mayor concreción de los supuestos habilitantes del 9.2 del RGPD, los §§ 22 (1), 23 y 24 incluyen opciones específicas de tratamiento de categorías especiales en ámbitos como la protección social, la preservación del bien común, cuestiones de seguridad nacional o la imposición de sanciones administrativas. Puede consultarse en: https://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf. Una versión oficial en inglés de la Ley alemana de protección de datos puede consultarse en: https://www.gesetze-im-internet.de/englisch_bdsg/.

riesgos de variabilidad y severidad de los derechos y libertades de las personas físicas que plantea el tratamiento»[76].

Por último, el sistema de garantías se refuerza con la inclusión de un marco de actuación específico, con garantías adecuadas, para el tratamiento de las categorías especiales de datos. Ante la eventualidad de un tratamiento de datos especiales, el responsable, además de cumplir con las exigencias previstas en el apartado 2 del § 22, cuenta con un conjunto de garantías legalmente previstas que, en ausencia de regulación sectorial específica, permiten llevar a efecto el tratamiento sin que ello suponga una injerencia en el derecho fundamental. Es una especie de modelo supletorio de garantías que resulta especialmente útil, porque el RGPD no «fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles»[77].

En definitiva, el modelo alemán apuesta por una regulación contextual y de adecuación a las particularidades del tratamiento, como lo acreditan las exigencias en materia de riesgos, la incorporación de un marco general específico para los tratamientos especiales o la distinción en atención a los sujetos que los llevan a efecto. Esa combinación de medidas culmina con el establecimiento, en la propia *Bundesdatenschutzgesetz*, de un marco de garantías básico para el tratamiento de cualquier dato perteneciente a las categorías especiales. De este modo, se reduce notablemente la dependencia de una normativa sectorial detallada para los tratamientos de datos de categorías especiales, algo que no ocurre en el modelo español.

4.4. Valoración conjunta de las condiciones de tratamiento de los datos especiales en el RGPD

Ya sabemos que la prohibición del tratamiento es el factor diferencial de las categorías especiales y que no son las características del tratamiento, sino la condición del dato, lo que determina las posibilidades de actuación.

---

[76] § 22.2 (2) de la *Bundesdatenschutzgesetz*, de 30 de junio de 2017, (BGBl. I S. 2097). Texto Original: «*Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen*».
[77] STC 76/2019, de 22 de mayo, FJ 8.

Con todo, se han reconocido ciertas circunstancias en las que se estima que el uso de los datos especiales es necesario para el buen funcionamiento de la sociedad o, incluso, para el beneficio de la persona (p. ej. el tratamiento de información relativa a la salud en la atención sanitaria). Esto significa que, el contexto, limitado como agente identificador, se torna en factor justificativo del tratamiento de las categorías especiales, abriendo una senda para su adecuación a la particular idiosincrasia de cada Estado miembro. Siempre, claro está, con ciertos límites.

El conjunto de causas habilitantes del tratamiento de datos especiales refleja la existencia de un monopolio legislativo en la interpretación de lo posible. La apreciación de qué contexto y tratamientos de datos especiales son jurídicamente admisibles no es un ejercicio hermenéutico que pueda hacerse descansar en el riesgo real, ni en sus posibilidades discriminatorias. Antes bien, es una decisión apriorística de los legisladores, especialmente del europeo. Al igual que se ha seleccionado un conjunto tasado de tipologías de datos sensibles, también se han predeterminado el abanico de tratamientos jurídicamente aceptables, excluyendo, por omisión, a todos los demás.

Esta opción legislativa proporciona las mismas ventajas de seguridad y certeza que la previsión taxativa de las categorías especiales, pero adolece de sus mismos defectos. En cuanto que ejercicio predictivo de lo posible, puede dar lugar a desajustes que, por exceso o por defecto, terminen por privar de la debida protección a datos personales relevantes.

El contexto –finalidad incluida–, las medidas de seguridad y las consecuencias del tratamiento son la tríada de elementos que subyacen a todas las habilitaciones previstas para los datos especiales en el 9.2 RGPD. En consecuencia, no parece descabellado plantearse la posibilidad de convertirlos en los criterios de valoración sobre los que pautar la viabilidad de un tratamiento de datos especiales, en lugar de enlistar un conjunto apriorístico de tratamientos posibles. Es cierto que un planteamiento de este cariz obliga a replantear el sistema vigente, pero, ¿qué sentido tiene mantener una prohibición apriorística si después se reconocen un número indeterminado y abierto de excepciones?

5. ¿Es posible mejorar el modelo europeo de protección en lo relativo a las categorías especiales? Una propuesta moderada

5.1. Ajustar el modelo sin alterarlo en exceso. Una ampliación con el contexto como protagonista

El modelo europeo de protección de datos parte de la premisa de que hay tipologías de datos que exigen un régimen especial de protección. Sin embargo, el reconocimiento de categorías especiales condiciona el sistema.

En el caso del RGPD, esta situación se agrava como consecuencia del reconocimiento de un conjunto de tipologías legalmente definidas (datos relativos a la salud, datos genéticos y datos biométricos) y que dificultan la extensión de su mayor nivel de garantía a supuestos próximos y asimilables. Naturalmente, como apunta Romeo Casabona, es posible extender el ámbito de aplicación de estas tipologías «por vía interpretativa, siempre que no se llegue a rebasar el marco legal» (Romeo Casabona, 2019, p. 93).

El problema de los datos relativos a la salud, los datos genéticos y los datos biométricos, reside en aquellas informaciones que, pese a no coincidir con lo jurídicamente conceptualizado, operan, en determinados tratamientos, como si fuesen sensibles. Es decir, son datos que, «funcionalmente» (Romeo Casabona, 2019, p. 94), operan como especiales, pero que, jurídicamente, carecen de esa condición. Este problema no es exclusivo de los datos expresamente definidos en el RGPD, pues, en general, no es descartable que cualquier dato, en el contexto apropiado, pueda llegar a operar como un dato sensible y, por tanto, directamente relacionado con alguna de las categorías especiales, aunque no encaje en la definición de estas tipologías.

En la era de la inteligencia artificial, del *big data* y la combinación e interrelación de los datos, es perfectamente posible obtener informaciones de una determinada naturaleza, a partir de otras que no gozan de esa condición. Potencialmente, cualquier dato puede llegar a ser considerado especial. El sistema legal de protección de datos no puede seguir ignorando esa situación fáctica que, el paso del tiempo, solo va a consolidar y complicar.

5.2. De los datos especiales a los tratamientos especiales

Para afrontar estos retos, podría apostarse por un enfoque en el que se combinase la determinación de la condición especial en atención al contenido, con un enfoque contextual que permitiese extender la protección reforzada a aquellos supuestos en los que las categorías especiales pudieran verse afectadas.

Esta alternativa tendría que construirse a partir de una concepción extensiva del Considerando 51, aprovechando la decidida apuesta por la proactividad que ha realizado el RGPD[78]. Su finalidad última, sería extender la protección especial a supuestos en que el tratamiento pudiera «parecer neutral e inocuo […][y], sin embargo, atenta contra la dignidad y los derechos de la persona afectada, si se pretende revelar determinada información de ella» (Tomás Mallén, 2019, p. 74). Con una condición: esa información que se pretende revelar debe estar referida a alguna de las categorías especiales legalmente reconocidas.

Es decir, la calificación como sensible no vendría dada por los datos utilizados, sino por la voluntad de utilizar una información determinada (no necesariamente "especial") para conocer algún aspecto calificado normativamente como sensible[79]. Con todo, como advierten Georgieva y Kuner, «*this view has not yet been affirmed by courts or regulators*» (Georgieva y Kuner, 2020, p. 374).

De compartirse esta hipótesis, y aceptarse una interpretación expansiva de la función del contexto en la determinación de lo especial, lo más adecuado sería trasladarla al RGPD. La reforma tendría como finalidad clarificar los instrumentos que permiten determinar la condición especial de una concreta información y, consecuentemente, otorgarle una protección reforzada.

La forma más expedita y eficaz mediante la que alcanzar ese objetivo, pasa por cambiar el centro de imputación del dato especial al tratamiento. El mejor modo de incorporar el contexto del tratamiento como elemento de tipificación sería convertirlo en el elemento referencial. La base argumental resulta evidente. En un enfoque con los datos como núcleo, la

[78] Sobre la importancia de la proactividad y su condición de elemento basilar del sistema europeo de protección me remito a lo señalado en el Capítulo 3 de esta tesis.
[79] En esta línea se manifestaron, hace más de una década, Gola, Schomerus y Klug, en (Gola, Schomerus, y Klug, 2007).

incorporación de los matices que conlleva la realidad de cada concreto tratamiento resulta poco satisfactoria.

Sin embargo, al situar el tratamiento como referente principal, la inclusión de los matices se convierte en un acto obligado, natural, sin que, por otra parte, se impida la protección de los supuestos que, por el contenido de los datos, fuesen especiales. En aquellos tratamientos que, por contenido, los datos fuesen sensibles, automáticamente, convertirían al tratamiento en especial. Pero, además, también tendrían la condición de especial los tratamientos que, por finalidad o contexto, se pudiesen vincular a esas tipologías.

Este enfoque evita la necesidad de etiquetar a los datos como pertenecientes a una determinada tipología, pues sería la realidad específica de cada tratamiento la que desempeñase esa función de adjetivación. Es cierto que se perderían los apriorismos y la previsibilidad, pero esa pérdida de robustez en la certeza se compensa con la mayor seguridad aplicativa en los supuestos dudosos.

En todo caso, la dificultad para el cambio no se encuentra tanto en la literalidad de los artículos del RGPD, como en el modelo de protección que propician. Prueba de ello es que el articulado del RGPD no sufriría cambios bruscos. El precepto más afectado sería el art. 9.1 del RGPD, cuya nueva redacción podría asemejarse a la siguiente:

Quedan prohibidos los tratamientos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los que estén dirigidos a identificar de manera unívoca a una persona física, los vinculados a conocer la información genética de un persona física, así como los relativos a su salud, su vida sexual u orientación sexual[80].

En cuanto a los efectos de este cambio en los supuestos contemplados por el art. 9.2 del RGPD, cabrían dos aproximaciones. Una conservadora, en la que se mantendrían las circunstancias habilitantes previstas, con los ajustes imprescindibles para implantar el cambio en el

[80] La redacción propuesta trata de ser lo más fiel posible a la del art. 9.1 RGPD para permitir un mejor contraste entre los modelos. La actual redacción del 9.1 es: «Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física».

centro de imputación. De seguirse esta vía, tendría que revisarse el resto del articulado para reflejar el nuevo paradigma. Así, por ejemplo, cuando en el 9.2.a) se señala como circunstancia habilitante del tratamiento que «el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales», bastaría con reformular la redacción y señalar que el interesado dio su consentimiento explícito para efectuar un tratamiento de esta naturaleza.

La segunda posibilidad, más radical, supondría la eliminación de los supuestos habilitantes del art. 9.2 del RGPD y la adopción del contexto, las medidas de seguridad y las consecuencias del tratamiento, como criterios decisorios para realizar tratamientos especiales.

Naturalmente, además del artículo 9 del RGPD, los ajustes deberían extenderse al resto de preceptos que, de algún modo, afectan al tratamiento de los datos especiales[81]. Las definiciones de los datos relativos a la salud, los datos genéticos y los biométricos podrían mantenerse, pues no se prescinde del contenido como elemento identificador, sino que se complementa con el contexto. Por lo tanto, la conceptualización de las categorías seguiría siendo útil por su valor referencial, pero quedarían privadas de su efecto excluyente.

Con una redacción como la propuesta, la realidad del tratamiento y su conexión con las categorías especiales sería el elemento determinante de la aplicación de la protección reforzada. El marco operacional así formulado produciría un cambio de paradigma en la protección de las categorías especiales, superando las complicaciones derivadas de un modelo, el vigente, que tiene en la sensibilidad del dato personal su elemento referencial. A mi juicio, esta concepción omnicomprensiva comportaría una notable mejora del sistema de protección de las categorías especiales configurado en el RGPD.

El sacrificio que este cambio pudiese suponer en cuanto a certeza y previsibilidad se vería a todas luces compensado. De una parte, permite extender la protección reforzada a tratamientos en los que se afronten cuestiones relativas a las categorías especiales pero que, jurídicamente, no encajan en la definición legal. De otra parte, sirve como remedio frente a la obsolescencia programada de una normativa en constante amenaza por las futuras innovaciones tecnológicas. En definitiva, al incorporarse al sistema una perspectiva más teleológica que ontológica, su sustento normativo

[81] Sería el caso de los artículos 22.4; 27.2; 30.5; 35.3.b o 37.1.c del RGPD.

adquiere una mayor adaptabilidad para hacer frente a los desafíos de la era digital.

El principal riesgo de esta aproximación radica en la variabilidad que puede generar la recepción de este margen de apreciación en los distintos Estados miembros. Sin embargo, la entidad de las discrepancias no sería inasumible, pues las categorías especiales están previstas en el RGPD y son comunes a todos los países de la UE. Las divergencias, de producirse, se circunscribirían a la aplicación en casos concretos, algo que, el modelo actual, tampoco solventa. En dirección opuesta, también pudiese ocurrir que el contexto y la finalidad llegasen a convertirse en elementos de homogeneización dando pie a una jurisprudencia común respecto de los supuestos dudosos.

5.3. Carencias de la propuesta

La ampliación identificativa de las categorías especiales, como consecuencia de la inclusión del contexto y la finalidad de los tratamientos, resulta muy adecuada para solventar la condición variable de los datos personales, aunque presenta algunas carencias. En primer lugar, se pierde la seguridad que ofrece tener un conjunto cerrado de informaciones sensibles. Con la propuesta que se acaba de exponer, un mismo dato, en función del tratamiento, podría ser asignado a diversas tipologías e, incluso, podría variar en su nivel de sensibilidad. Tendría, por así decir, una condición especial de carácter variable.

En segundo lugar, la aproximación contextual sigue condicionada por la existencia de categorías especiales. La protección reforzada solo se podría extender a datos que, en un determinado tratamiento, operasen como alguna de las tipologías consideradas sensibles. Por lo tanto, seguirían quedando excluidas de esa condición aquellas situaciones en las que, sin pretender conocer informaciones sobre algunas de esas categorías, se generase un alto riesgo para el ciudadano, o se propiciase un acto discriminatorio, como, por ejemplo, a través de la utilización de información financiera o de edad.

Finalmente, tampoco ofrece una fórmula para graduar la protección. En el RGPD, si una información es considerada especial, se le aplica el régimen específico para este tipo de datos y, si acaso, algunas limitaciones

o condiciones adicionales (v. gr. 9.4 RGPD[82]). Sin embargo, no es posible establecer una protección menor cuando se constate que, en un caso concreto, no hay un peligro tan elevado, pues la condición especial impone un mínimo ineludible. A no ser que se apostase por una reforma ambiciosa del 9.2 RGPD, y se adoptase el contexto, la seguridad de las medidas y las consecuencias del tratamiento como parámetros para enervar la prohibición de tratar datos especiales.

Como puede comprobarse, la propuesta de incluir el contexto como factor de identificación de las categorías especiales mejoraría el modelo, pero seguirían existiendo ciertas disonancias e ineficiencias que han de ser consideradas antes de proceder a cualquier modificación del marco regulatorio e interpretativo del derecho a la protección de datos.

6. ¿Es posible mejorar el modelo europeo de protección en lo relativo a las categorías especiales? Una propuesta más rupturista

6.1. La sustitución de las categorías especiales por un modelo de protección riesgos racionalizado

Si, en el contexto apropiado, cualquier información puede ser personal (aunque no absolutamente todas), no es menos cierto que, bajo las circunstancias apropiadas, cualquier dato personal puede llegar a revelar información de la esfera más reservada del individuo, representar un riesgo alto o tener potencial discriminatorio.

Que haya una información sensible implica que habrá otra que no lo es. La existencia de estas categorías tiene un valor simbólico innegable y el mensaje que envían es nítido, «*specific forms of data can generate substantial harm and therefore must be treated with greater care*» (Zarsky, 2017, p. 1014). Pero, en la era digital, esa fortaleza se quiebra. El reconocimiento de tipologías sensibles ya no asegura que se alcancen los objetivos subyacentes a su existencia: la protección de la esfera reservada, evitar la discriminación y ofrecer mayor protección en los tratamientos que conllevan un riesgo alto.

[82] Art. 9.4 RGPD: «Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud».

La tipificación de ciertas categorías como especiales y merecedoras de una protección reforzada provoca, en el subconsciente colectivo, la sensación de que aquellos tratamientos que no empleen datos sensibles son menos peligrosos, o que no tienen capacidad suficiente para discriminar a las personas o afectar a su esfera privada. Pero no es así. Puede discriminarse sin utilizar las categorías especiales (p. ej. por edad o por capacidad económica); es posible conocer datos de la esfera privada y reservada a partir de otros que no lo son, mediante procesos inferenciales basados en datos no sensibles (v. gr. conocer el estado de salud y esperanza de vida a partir del lugar en que se vive o del salario que se cobra); y, el riesgo alto, como ha puesto de manifiesto el propio RGPD (art. 35.1 RGPD[83]), puede tener más causas que el tipo de datos utilizados.

En definitiva, si todo es susceptible de llegar a ser especial –aunque unos datos tengan muchas más aptitudes y posibilidades que otros–, en el fondo, nada lo es. Por lo tanto, si una medida, cuya principal valía es ofrecer seguridad y certeza, genera incógnitas y distorsiona el modelo dificultando la consecución de los objetivos que le subyacen (la protección frente a los riesgos altos, evitar la discriminación y salvaguardar lo reservado), procede preguntarse si existen alternativas que ofrezcan mejores resultados y mayor eficiencia.

Los modelos intermedios que conservan las categorías especiales como referencia, por más que puedan modularse y ampliarse mediante interpretaciones amplias, siguen presentando carencias significativas, al estar constreñidos por las categorías previamente establecidas. Amén de dificultar la graduación intratipologías. Por ejemplo, haber padecido un gripe o tener una enfermedad degenerativa incurable, siendo los dos datos relativos a la salud y, por tanto, especiales, no tienen el mismo potencial para producir efectos nocivos en las personas.

Por este motivo, antes de introducir factores de incertidumbre que hibriden –más– el modelo de protección, parece más adecuado adoptar un mecanismo de protección diferente. Por ello, se propone un modelo alternativo, que prescinda de las categorías especiales como parámetro de referencia, reemplazándolas por unos criterios más apropiados, mediante los que alcanzar los objetivos que subyacen a su existencia.

[83] En el art. 35.1 RGPD se señala que será probable que un tratamiento entrañe un riesgo alto «cuando […] utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines». Es decir, no solo por la naturaleza del dato.

Ese modelo transita de la naturaleza de los datos a la realidad del tratamiento. El (nuevo) sistema de protección de los datos personales tendría como principal factor de caracterización el reconocimiento de unos umbrales de afectación de los derechos y de riesgo de discriminación, a partir de los cuáles el uso de la información personal no sería aceptable. En él, las evaluaciones de impacto operarían como condición de viabilidad del tratamiento. Las categorías especiales, o no existirían en absoluto o se convertirían en una herramienta de ordenación, pero nunca serían condicionantes jurídicos previos.

Con arreglo a esta formulación, en la que el criterio determinante sería el nivel de peligro en cada caso concreto y no la naturaleza del dato, podría prescindirse de cualquier reconocimiento de tipologías especiales, sin bien puede ser útil, para escalar los riesgos, contar con un listado orientativo de tipologías sensibles. Esto es, podrían operar como indicios, como una variable más en la determinación del riesgo real, incidiendo en su carácter abierto, no exhaustivo y meramente orientativo. En todo caso, el criterio determinante sería el nivel de peligro del tratamiento, no la naturaleza de los datos utilizados.

Realizar una evaluación general de la realidad del tratamiento, permite apreciar el riesgo real de afectación de la esfera más reservada, o de discriminación. Constatando que, aunque no se utilice alguna de las tipologías consideradas como sensibles, otros factores, como la información utilizada, el modo de usarla, la finalidad perseguida, los sujetos intervinientes o el contexto operacional en el que se inserta (p. ej. en sistemas de *big data* y perfilado algorítmico) pueden producir los mismos efectos no deseados.

De tal manera, la razón justificativa de la prohibición de llevar a cabo un tratamiento concreto pasaría a ser la superación de determinados umbrales de riesgo.

Del mismo modo, eliminar el carácter jurídicamente insoslayable de las categorías especiales permite valorar la concurrencia de circunstancias que atenúen los peligros inherentes a la utilización de esas informaciones y que hacen el tratamiento jurídicamente aceptable, por no exceder los umbrales de riesgo. Así, en lugar de un listado, igualmente tasado, de supuestos en los que se enerva la prohibición de tratar los datos calificados como especiales, habrían de ponderarse, para cada tratamiento, factores

como: las medidas adoptadas, finalidad del tratamiento, o la importancia de la información para el interesado concreto.

En suma, la naturaleza del dato y su contenido serían aspectos a considerar, pero la determinación final de la viabilidad del tratamiento, y el régimen jurídico de protección, serían el resultado de una valoración de conjunto.

6.2. Viabilidad de la propuesta

6.2.1. Una propuesta acorde con el modelo europeo de proactividad y riesgo

Pudiera aducirse que esta propuesta choca con la cultura jurídica europea, esto es, que no es compatible con la idiosincrasia que preside el tratamiento de la información personal en la Unión Europea. Este argumento fue esgrimido por el ICO en el año 2013 cuando señaló que, pese a que ellos «*have always had reservations about the general concept of non-contextual sensitive data categories. However, this approach is a part of the European mainstream and is unlikely to be dropped*»[84].

Al establecer las categorías especiales como elemento determinante de la posibilidad de tratar los datos (art. 9.1 RGPD y la prohibición como premisa) y no como un factor más de valoración, el RGPD se aleja del modelo contextual y se aproxima a los sistemas de protección en abstracto. En el RGPD, las categorías especiales y la posibilidad de llevar a cabo el tratamiento son una condición previa, y la realidad del tratamiento y sus riesgos, factores que se han de apreciar a posteriori.

Sin embargo, la visión pesimista del ICO (en 2013) no se compadece del todo con la realidad actual. La idiosincrasia del modelo europeo de protección frente al tratamiento de la información personal no es tan refractaria a una aproximación contextual como para hacer impracticable la propuesta planteada.

[84] ICO, Proposed new EU General Data Protection Regulation: Article-by-article analysis paper, 12 de febrero de 2013, pp.11-12. Puede consultarse en: https://ico.org.uk/media/about-the-ico/documents/1042564/ico-proposed-dp-regulation-analysis-paper-20130212.pdf. (Última consulta: 20/10/2021).

La opción de articular un modelo de protección como el que aquí se ha planteado se sitúa dentro de los márgenes de configuración normativa que corresponden al legislador.

En este sentido, el RGPD contiene ciertos elementos, como la evaluación de impacto (arts. 35-36) o el enfoque proactivo y la atención al caso concreto, que constituyen bases jurídicas sólidas sobre las que transitar hacia un modo diferente de concebir la protección de lo sensible.

Ítem más, el conjunto de principios que vertebran el tratamiento de datos conjura los temores e inseguridades que pudiera generar un enfoque menos tasado normativamente, pues configuran un marco de actuación en el que la atención a las particularidades de cada caso concreto y el diseño previo del tratamiento son la regla general de actuación.

Adicionalmente, la tendencia del conjunto de normativas que conforman el ecosistema europeo del dato, demuestra que la protección contextual, centrada en la finalidad y la atención a las particularidades del caso concreto, forma parte de la idiosincrasia del modelo europeo actual. La adopción de un modelo diferente de protección de los datos especiales no es, por tanto, incompatible con la cultura jurídica europea en la materia.

6.2.2. Compatibilidad con el derecho fundamental a la protección de datos

¿Hay en la opción propuesta algún elemento que pudiera suponer una limitación del derecho fundamental a la protección de datos? ¿Son las categorías especiales una exigencia del derecho fundamental? ¿Son imprescindibles para la consecución de las finalidades que caracterizan el derecho fundamental?

Desde el punto de vista del derecho a la protección de datos en sentido estricto, no se produce afectación alguna. Ello es así porque, con la propuesta realizada, las posibilidades de actuación de la persona respecto de sus datos se mantienen incólumes.

Más dudas genera la viabilidad de la propuesta en relación con el derecho a la protección de datos en sentido amplio, pues las categorías especiales se fundan en su estrecha vinculación con los aspectos más sensibles de la persona. Las tipologías especiales de datos lo son por su conexión directa con los aspectos más íntimos de la persona (Troncoso

Reigada, 2021a, p. 4650), por los mayores riesgos que entraña su tratamiento y por el potencial discriminatorio de su contenido.

En la media en que el derecho a la protección de datos exige el establecimiento de las medidas adecuadas para salvaguardar los derechos y libertades, parece razonable concluir que el reconocimiento de unas tipologías especiales de datos es un instrumento adecuado para hacer frente a esa amenaza. Los datos especiales son la respuesta intuitiva a la protección de los derechos fundamentales frente al tratamiento de datos en contextos no inferenciales. Son un medio de asegurar la salvaguarda del derecho fundamental.

Que el reconocimiento de categorías especiales de datos sea una opción adecuada para cumplir con las exigencias de protección instrumental de los derechos y libertades, no quiere decir que sea el único posible, ni el más efectivo.

El derecho a la protección de datos no exige la existencia de las categorías especiales, sino que se salvaguarden los derechos y libertades que les subyacen. El derecho a la protección de datos es un derecho finalista, no impone un modo determinado de lograr su fines (más allá de las previsiones de los apartados 2 y 3 del art. 8 de la CDFUE).

Consecuentemente, el parámetro de viabilidad de la propuesta es si esta es adecuada para lograr la finalidad de protección que el derecho impone. La sustitución de las categorías especiales por un modelo omnicomprensivo en el que los riesgos del tratamiento sean la clave de bóveda, se presenta como una decisión entre dos opciones jurídicamente posibles.

6.2.3. No entraña un menor nivel de protección

Prescindir de las categorías especiales y transitar hacia un modelo de protección gradual, con el riesgo y las características del tratamiento como parámetros a considerar, sirve para dar cobertura a los derechos y libertades y, además, es una fórmula más adecuada para lograrlo con éxito.

Es una respuesta jurídica más flexible, adaptada a las particularidades de cada tratamiento y al nivel de amenaza real para los derechos y libertades; con la que, además, se conjuran los riesgos de aplicación mecanizada a los que las categorías especiales conducen.

Finalmente, esta propuesta no afecta al sistema de garantías de la normativa europea, sino al modo de activarlas. Los instrumentos jurídicos que dotan al modelo europeo de un elevado nivel de protección (los principios, los derechos y las políticas de prevención de riesgos) permanecen indemnes.

En definitiva, se logra una mayor precisión en la protección, sin restar garantías y sin imponer un esfuerzo adicional desproporcionado, pues las exigencias de protección anticipada (proactividad, evaluación de impacto y protección de datos desde el diseño y por defecto) ya forman parte del sistema.

7. La deseable ampliación del concepto de dato personal. El contexto como factor a considerar

7.1. El concepto de dato personal ante el espejo de su realidad

Las reflexiones en torno a las categorías especiales obligan a mirar, por elevación, a la categoría general: los datos personales. ¿Es su actual configuración la mejor respuesta que, desde el modelo europeo, se puede dar a los riesgos derivados del tratamiento de la información personal?

En el dato personal se produce la conexión información-persona que dota de subjetividad al tratamiento de la información y justifica su condición de bien jurídico protegible mediante un derecho personal. Si la información tratada no es subsumible en la categoría datos personales, ya sea por su naturaleza (datos industriales o datos de personas jurídicas), ya por la imposibilidad de conectar información y persona en unas condiciones de tiempo, costes y esfuerzo, razonables, no habrá posibilidad de aplicar a esa información el manto protector del derecho fundamental.

En este sentido, contar con pautas hermenéuticas firmes, mediante las que determinar metodológicamente la existencia de un dato personal es un factor que proporciona seguridad jurídica y previsibilidad al modelo de garantías legalmente establecido.

Con todo, la definición con la que se opera en el sistema europeo, «toda información sobre una persona física identificada o identificable (“el interesado”)» no ofrece tantas certezas como, en principio, pudiera parecer. Como se ha señalado, la proporcionalidad de los esfuerzos

necesarios para lograr identificar a una persona a partir de una determinada información impregna de incertidumbre al concepto.

De una parte, la razonabilidad de la capacidad, los costes o el tiempo requeridos varían según el sujeto, obligando a relativizar la decisión acerca de cuándo se descarta que un dato sea personal (Zwenne, 2013, p. 4). De otra, la constante evolución de las capacidades técnicas provoca que, tanto en las informaciones anonimizadas, como en aquellas en las que las barreras naturales[85] sirven para negar la condición de dato personal (con el matiz de la relatividad apuntado), hacen imprescindible la contextualización del tratamiento. Así, un dato puede no ser personal en un momento dado, pero pasar a serlo en un futuro, no necesariamente lejano.

La mejora de las capacidades tecnológicas y de las posibilidades de interrelación de la información, hace de la existencia de datos anónimos una realidad con fecha de caducidad muy próxima. Como ya advirtiera Ohm hace más de una década, «*easy reidentification represents a sea change not only in technology but in our understanding of privacy. It undermines decades of assumptions about robust anonymization, assumptions that have charted the course for business relationships, individual choices, and government regulations. Regulators must respond rapidly and forcefully to this disruptive technological shift, to restore balance to the law and protect all of us from imminent, significant harm. They must do this without leaning on the easy-to-apply, appealingly nondisruptive, but hopelessly flawed crutch of personally identifiable information*» (Ohm, 2010, p. 1776).

Aunque, potencialmente, cualquier información puede llegar a ser considerada dato personal, la anonimización y la imposibilidad "natural" por costes, tiempo y esfuerzo de conectar a ese dato con una persona, son barreras jurídicamente insuperables.

7.2. ¿Hacia una ampliación del concepto de dato personal?

Cada vez existen más posibilidades de afectar a una persona determinada a través del uso de la información. El riesgo de reidentificación, el perfilado algorítmico, la interrelación de datos y las posibilidades de conocimiento inferencial, combinado con el ingente

[85] Barreras naturales por los factores que las constituyen (tiempo, esfuerzo y costes), pero pueden ser erigidas artificialmente, por ejemplo, mediante sistemas de encriptado seguros.

volumen de información que se genera cada segundo, y sus posibilidades de uso, obligan a evaluar las resistencias y adecuación de los modelos de protección para responder a estos desafíos. Como advirtió el TCFA en su sentencia de 1983, «ya no existe, bajo las condiciones del tratamiento automático de datos, ningún dato "sin interés"»[86].

En este sentido, cabe preguntarse si el concepto de dato personal refleja convenientemente los modos en que una información puede llegar a vincular y afectar a una persona.

El sistema europeo de protección frente al tratamiento de la información personal parece transitar, desde el asunto Nowak, hacia una ampliación del concepto de dato personal. Junto al contenido informacional –reflejo de la realidad de la persona–, habrían de considerarse otras dos variables: la finalidad y los efectos. La aplicación incondicionada de esos dos elementos amplía, notablemente, el abanico de situaciones a las que puede aplicarse la normativa de protección de datos.

Si la condición personal del dato deja de depender, exclusivamente, de su conexión directa con la persona a la que identifica, y si el vínculo se puede originar por la finalidad que se persiga con su tratamiento, o merced a los efectos derivados de su uso, el radio de acción de la normativa de protección de datos se incrementa sustancialmente. La conexión ya no habrá de buscarse, exclusivamente, entre el dato y la persona, sino, también, entre el tratamiento y el sujeto afectado. El contexto en que la información se utilice se convierte, de este modo, en un elemento identificador más.

Curiosamente, esta ampliación conceptual podría ser la respuesta que Ohm reclamaba frente al debilitamiento de la anonimización como mecanismo de garantía. En efecto, al incluir la finalidad y los efectos del tratamiento, se abre la posibilidad de que cualquier información, incluso anonimizada, pueda llegar a considerarse dato personal si, en el tratamiento concreto, se demuestra que produce efectos sobre una persona determinada. Pese a todo, a día de hoy, esta posibilidad debe considerarse descartada. El RGPD excluye de su ámbito de aplicación los

[86] «*insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr*» En BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983- 1 BvR 209/83 -, Rn. 1-215, Grunde C, II-2, apdo. 150. Puede consultarse la versión en español en: («Jurisprudencia Constitucional Extranjera, Núm. 33, IV», 1984).

datos anónimos (Considerando 26), por lo que, el criterio interpretativo amplificado siempre tendría por límite a ese tipo de informaciones.

La condición personal de la información dejaría de ser un *a priori* y el conjunto de informaciones susceptibles de ser vinculadas a una persona física se amplía y difumina. La realidad específica de cada tratamiento será la que determine si se está operando con datos personales y la que permita identificar los sujetos afectados y definir las medidas de protección más adecuadas.

No cabe duda que, esta opción interpretativa, dota de mayor flexibilidad al concepto dato personal y ofrece protección jurídica específica a un número más amplio de informaciones. Sin embargo, también introduce un importante factor de indeterminación, pues la condición de dato personal pasa a ser una realidad modulable, necesitada de identificación efectiva en cada caso concreto.

Una ampliación de esa magnitud, y con esos fundamentos, no es un mero ajuste de los límites del concepto, sino que encierra un auténtico cambio de modelo y de cultura jurídica. Ese cambio de paradigma no se ha producido, ni la jurisprudencia de Nowak está consolidada, ni el legislador europeo ha reconocido formalmente a la finalidad y los efectos como criterios identificativos de los datos personales.

7.3. Un concepto de dato personal para la era digital

La era digital y las posibilidades que los ingenios tecnológicos propician han hecho eclosionar problemas que, hasta el momento, permanecían larvados. Las inferencias o el perfilado algorítmico han exacerbado las discordancias del modelo de protección de datos europeo.

Históricamente, el legislador europeo ha apostado por sistemas de protección en los que, mediante la inclusión de definiciones y categorías taxativas, proporcionaba cierta seguridad aplicativa. Evidentemente, siempre podían darse supuestos dudosos, pero eran los menos, y la certeza que generaba la objetivación de los tratamientos compensaba, con creces, las eventuales disonancias. Conforme los tratamientos se han ido haciendo más complejos, y las posibilidades de interrelación de la información se han incrementado, haciendo posible obtener nuevas informaciones o inferir

aquellas que se desconocen, las seguridades y certezas se han resquebrajado.

Ante un panorama como el actual, y con la intuición de que la situación no mejorará en el futuro inmediato, parece recomendable renunciar a una concepción formal de dato personal y, en su lugar, aplicar un enfoque en el que toda la información es personal, salvo que se demuestre lo contrario. En última instancia, se propone transitar hacia un modelo de protección más contextual y singularizado.

En esa dirección apunta la propuesta de Purtova. Para ella, es factible un sistema en el que, «*all automated information processing should trigger at least an obligation to assess what impact it is likely to have. In this sense, to abandon the formal use of the notion "personal data" amounts to accepting that all data is personal. Some might argue that it is already a matter of good practice to perform such impact assessment prior to data processing. In fact,* […] *to meaningfully apply the definition of personal data and establish whether or not a planned instance of data processing is within the GDPR's material scope, one effectively has to assess both likely and factual intended and incidental impacts of data processing on people. However, the fact of the matter remains that there is no such legal obligation. The only way to change this is to shift the default setting to "all data is personal" and use this departing point to build a system of scalable data protection rules*» (Purtova, 2018, p. 80).

En lo esencial, considero que la propuesta de Purtova, con la afectación (finalidad y efectos) y el nivel de riesgo del tratamiento como criterios para determinar el grado de protección necesario, en sustitución del modelo *in-out* al que la distinción dato personal-dato no personal conduce, es la más adecuada para afrontar la realidad actual del tratamiento de datos.

Con todo, estimo necesario introducir una breve aclaración. El derecho a la protección de datos no puede extenderse a cualquier información. Necesariamente ha de darse la conexión personal, y esta no existiría, por ejemplo, en los datos sobre consumo de abonos de un país. Purtova es plenamente consciente de ello y cuando señala que «*all data is personal*», parece evidente que se está refiriendo a un tipo específico de datos no personales, los anonimizados. Pero, como hemos visto, la categoría de los datos no personales es más amplia, y abarca ciertas informaciones para las que no resulta posible establecer vínculo alguno

con las personas físicas. Conviene tener en cuenta este matiz, pues el elemento personal es esencial, al ser el detonante aplicativo del derecho. Si no se puede conectar con algún elemento del individuo, no procede aplicarlo.

Los datos se protegen porque son la materialización de la subjetividad de las personas, la proyección externa de su ser. Al ampliar el concepto, al incorporar la realidad del tratamiento (su finalidad y efectos) se busca dar cabida a otras posibles formas de conexión que, hasta el momento, no están convenientemente reconocidas.

La condición personal de la información no puede ser un a priori excluyente, sino que ha de determinarse a partir de la realidad de cada tratamiento concreto y sus consecuencias para la realidad de la persona. Conforme a la propuesta de Purtova, afectación y nivel de riesgo serían los mecanismos que permitirían determinar tal condición. A mayor intensidad en la afectación, medias más restrictivas para el tratamiento de la información.

Por su parte, la condición previa de la información, esto es, el grado de conexión con el individuo y su capacidad para reflejar su realidad, no sería un aspecto irrelevante. Al contrario, sería uno de los factores a considerar para la selección de las medidas de protección a implementar, así como un elemento a ponderar en la resolución de eventuales conflictos de intereses (ya sea entre el interesado y el responsable, ya entre diversos interesados).

7.4. Una propuesta en consonancia con el modelo europeo de protección de datos

La noción de dato personal ha ido evolucionando y ampliándose a lo largo del tiempo, no es, por tanto, una realidad inmutable. La función del concepto dato personal es servir como referencia aplicativa del marco de protección en que se materializa el derecho fundamental a la protección de datos. Qué es y qué no es un dato personal es una decisión legislativa cuyo único requisito condicionante es que establezca las condiciones en que se produce la conexión dato-persona que sirve de base al derecho fundamental.

Prescindir de la condición previa del dato y, consecuentemente, de la categoría dato no personal para apostar por los efectos y los riesgos como criterios identificativos impacta, sin ninguna duda, en el modo de entender la protección. Sin embargo, una ampliación de las condiciones habilitantes para la identificación de qué es un dato personal no sería, en *prima facie*, contraria al modelo europeo de protección de datos. Al contrario, considerar el impacto que el uso de una información puede tener en una persona es plenamente congruente con el carácter proactivo y contextual al que parece tender.

En este sentido, el elemento más delicado de la propuesta son los efectos que la misma pudiera generar sobre la libre circulación de la información. Como se ha puesto de manifiesto, el flujo de datos personales es un elemento basilar del modelo europeo de protección. La eventual ampliación de los conceptos y la posible difuminación de los límites pudieran llegar a considerarse un obstáculo para el fluir de la información en la esfera comunitaria. Sin embargo, no parece razón suficiente como para descartar de plano la propuesta realizada.

Ello es así, porque, en primer lugar, lo que se exige del marco regulatorio es que no restrinja ni prohíba (art. 1.3 RGPD) y la propuesta que se realiza no tiene el nivel de intensidad y condicionalidad suficiente como para cercenar el flujo de información. Sí puede suponer un mayor esfuerzo para quienes pretendan operar con información personal, pues en el diseño del tratamiento habrán de considerar más variables, pero no parece una dificultad insuperable o inhabilitante.

Además, esa complejidad adicional inicial se vería compensada con un sistema de protección más preventivo, con menos riesgo de afectación de los derechos, lo que no dejan de ser valores imponderables a considerar ¿Cuánto beneficia a la circulación de la información una reducción de los problemas durante el tratamiento? ¿Qué impacto tiene que el sistema de protección sea seguro y eficaz en la predisposición a compartir información?

Primar la adecuación a la realidad del tratamiento o apostar por la seguridad aplicativa de un modelo más tasado para tratar de lograr un mejor flujo de la información son opciones que están en el ámbito de lo jurídicamente posible, siempre que se articulen correctamente y se asegure la consecución de las finalidades que informan el derecho fundamental a la protección de datos.

La propuesta planteada, además de concordar con la idiosincrasia del RGPD, mejora la capacidad de respuesta del ordenamiento jurídico frente al enorme desafío de las inferencias algorítmicas y los efectos derivados de su utilización. Este tipo de procesos impactan notablemente sobre el libre desarrollo de la personalidad y la autodeterminación personal. «*Inferential analytics methods are used to infer user preferences, sensitive attributes (e.g., race, gender, sexual orientation), and opinions (e.g., political stances), or to predict behaviors (e.g., to serve advertisements). These methods can be used to nudge or manipulate us, or to make important decisions (e.g., loan or employment decisions) about us. The intuitive link between actions and perceptions is being eroded, leading to a loss of control over identity and how individuals are perceived by others*» (Wachter y Mittelstadt, 2019, p. 497).

Ante un reto de estas dimensiones, una concepción amplia de dato personal resulta más apropiada, pues abre una ventana a la eventual extensión de las garantías jurídicas de actuación y protección a un mayor número de informaciones y, al hacerlo, minora los efectos nocivos que pudieran derivarse de la utilización de procesos inferenciales que revisten meras probabilidades con el halo de verdades[87].

El éxito de los mecanismos de garantía que priman la personalización y la atención a las circunstancias del tratamiento (el sector en que se produce, sus finalidades, sus riesgos y particularidades) en las transferencias internacionales y el rol protagónico que en ellas desempeñan los responsables (evaluando los riesgos, determinando el nivel de seguridad de la operación y la valoración sobre la adecuación del nivel de protección) ponen de manifiesto que el contexto no es, solamente, un elemento a considerar –como también lo es la naturaleza del dato–, sino

[87] La inclusión del art. 22 en el RGPD, esto es, el reconocimiento de un derecho a intervención humana en la adopción de decisiones automatizadas, es una medida que apunta, precisamente, a la minoración de efectos indeseables del decisionismo algorítmico. Sin embargo, es necesario dar un paso más, y sin negar el valor y utilidad de las soluciones algorítmicas y el *machine learning*, si debe «*rejecting the assumption that its output defines us*» (Hildebrandt, 2019, p. 121) e implementar mecanismos que permitan asegurar que somos valorados y percibidos por lo que realmente somos, no por lo que un algoritmo determina, por ejemplo, mediante el reconocimiento de un derecho a las inferencias justas como el propuesto por Wachter y Mittelstadt (Wachter y Mittelstadt, 2019).
En todo caso, como apunta, Soriano Arnanz, para hacer frente a los desafíos del decisionismo algorítmico no basta con el derecho a la protección de datos, sino que este debe ser complementado con enfoques que tomen en consideración la afectación de otros derechos, y las aportaciones de otras disciplinas, tanto técnicas como formativa (p. ej. mediante cursos de ética algorítmica para programadores), destinadas a generar un bagaje más adecuado para afrontar los riesgos derivados del uso de algoritmos (Soriano Arnanz, 2021b).

que, en la práctica, constituye un factor decisivo a la hora de asegurar el éxito de las medidas y, por consiguiente, la protección de los derechos de los interesados.

7.5. Compatibilidad de la propuesta con el derecho fundamental a la protección de datos

¿Es la proposición planteada compatible con la naturaleza del derecho fundamental a la protección de datos? ¿Supone una afectación o limitación del mismo? La respuesta a ambas cuestiones debe ser negativa, pues no anida en el ánimo de la propuesta afectar o debilitar al derecho fundamental, sino extender su campo de actuación, para lograr un marco de protección más adecuado frente a los retos y riesgos que el tratamiento de la información depara. Sin embargo, no es la voluntad que en ella anida, sino sus consecuencias jurídicas lo que ha de determinar la viabilidad de la ampliación del concepto dato personal.

En este sentido, un modelo escalable, con el riesgo como modulador, no tiene por qué suponer una ablación del derecho fundamental. Con todo, como no puede ser de otro modo, la viabilidad de la propuesta dependerá del modo en que se articule, pero, en abstracto, no parece haber ningún elemento caracterizador de la misma incompatible con las exigencias del derecho a la protección de datos.

La renuncia a la seguridad que proporciona un concepto más acotado, para apostar por un sistema de protección más preciso y personalizado es una elección del legislador, no una cuestión de afectación del derecho fundamental. El debate no debería girar en torno a la compatibilidad de la propuesta con el derecho fundamental, sino respecto de la oportunidad, pertinencia, eficacia y adecuación de cada uno de los modelos a los objetivos jurídico-políticos que se pretendan.

Personalmente, considero que la propuesta de ampliación del concepto de dato personal proporcionaría un marco de actuación más adecuado para hacer frente a los desafíos que la era digital plantea en relación con el tratamiento de la información personal. No solo por responder mejor a problemas específicos actuales, como pueden ser el decisionismo algorítmico y el *big data*, sino porque propicia la creación de un sistema de protección más flexible y, por lo tanto, más capacitado para

adaptarse a los retos que el constante desarrollo tecnológico pueda plantear en el futuro.

Ítem más, este modo de configurar la protección de la información personal se ajusta mejor a la naturaleza compleja del derecho a la protección de datos, pues el dato se protegería por ser un medio a través del que afectar a los bienes jurídicos de la ciudadanía, y no solo por constituir una proyección materializada del ser.

La definición "clásica" de dato, esto es, la que se ajusta a una interpretación literal del RGPD, está vinculada a la existencia de una proyección de la persona en la información tratada. Conforme a ella, el dato sería un reflejo de la realidad personal del sujeto. Sería un concepto "natural", en la medida en que el contenido de la información determina su condición.

Sin embargo, la inclusión de la finalidad o los efectos, supone que la relación dato-persona no es algo predefinido y estático, sino un vínculo que puede aparecer en cualquier momento. En esos casos, la condición personal del dato tendría un componente funcional y/o circunstancial muy marcado. La protección del dato ya no estaría vinculada, en exclusiva, a su condición de representación de la persona, también dependería de las consecuencias que el tratamiento pudiera ocasionarle.

El dato personal no es la mera materialización informacional de la persona, sino el centro de imputación sobre el que se articularía la defensa de los intereses de la persona frente al tratamiento de la información que pudiera afectarle.

Si solo se considera dato personal a las informaciones que se relacionan directamente con la persona, en última instancia, implica que el derecho fundamental solo debería alcanzar a proteger aquellos datos que conforman proyección exterior del ser. Ahora bien, al ampliar su concepto mediante la inclusión de la finalidad y los efectos[88], el tratamiento y sus consecuencias pasan a ser el objeto de protección.

De este modo, a las informaciones consideradas personales porque su contenido está ligado a una persona –bien por identificarla, bien por posibilitar su identificación–, se añadirían todos aquellos datos que, no estando directamente conectados con un individuo determinado,

[88] Una inclusión que no hace desaparecer el criterio de la identificabilidad, pero que añade otros concomitantes: finalidad y efectos.

adquieren tal condición para un tratamiento específico. La vinculación personal se lograría por una doble vía: por el contenido del dato y por los efectos que su uso pudiera tener para una persona determinada.

La consecuencia de esta conceptualización es clara, los datos no se protegen, en exclusiva, por ser la proyección externa del ser, sino como medio para asegurar la autodeterminación personal y la indemnidad de la persona frente a la utilización de informaciones que le afectan.

La ampliación del concepto de dato personal se ajusta mejor al carácter anfibológico del derecho a la protección de datos (poder de control y disposición + derecho instrumental). En efecto, la activación de los mecanismos de protección en función de las posibles consecuencias del tratamiento acrecienta la funcionalidad del derecho a la protección de datos personales como garante del libre desarrollo de la personalidad[89], pues también protege frente a los potenciales efectos nocivos y condicionantes generados por el tratamiento de la información, con independencia de su naturaleza y origen.

Finalmente, no puede dejar de reseñarse que, si la condición de dato personal puede derivar de los efectos o las finalidades del tratamiento, resulta jurídicamente innecesaria la predeterminación normativa de un catálogo exhaustivo de informaciones susceptibles de ser clasificadas como tales. Será el modo en que son tratados los datos lo que permita considerar si son, o no, el dato personal de alguien. De este modo, al supuesto dato-persona, se uniría la opción tratamiento-persona. En esta última, el dato operaría como elemento conector, y adquiriría la condición de dato personal merced al tratamiento.

El dato personal es solo una premisa aplicativa que habilita la utilización de los instrumentos de protección de la información personal. Por ello, se hace perentorio el prescindir de concepciones estrictas acerca de lo que se considera dato personal e incluir a las circunstancias de cada tratamiento como criterios mediante los que determinar en qué grado, y hasta qué punto, se podrán ejercitar las facultades inherentes al derecho fundamental a la protección de datos.

[89] Como apunta Martínez López-Sáez, el derecho a la protección de datos, en su configuración europea, es una proyección de la dignidad de la persona y de su derecho al libre desarrollo de la personalidad (Martínez López-Sáez, 2018b).

CONCLUSIONES

I. La era digital genera un ecosistema lleno de posibilidades y esperanzas de mejora en la calidad de vida de la ciudadanía. Sin embargo, también constituye un desafío para la protección de los derechos y libertades.

II. Los datos se han convertido en una moneda de cambio, son un producto destinado al mercado, una pieza vital en el engranaje que da vida a las sociedades contemporáneas. En la era de la información, el dominio sobre la proyección exterior del ser está gravemente amenazado.

III. El derecho a la protección de datos incide en el modo en que se utiliza la información personal y proporciona las herramientas jurídicas mediante las que garantizar su control. Su capacidad para desplegarse de manera efectiva en entornos digitales, le ha convertido en el modelo de referencia para el conjunto de medidas jurídico-normativas destinadas a disciplinar la vida en la Red.

IV. Aunque aplicable a todo tipo de datos personales, el derecho a la protección de datos surge como respuesta a la automatización del procesamiento de información, y a la consecuente ruptura de las barreras que, el tiempo, el espacio y los costes proporcionan. Sin embargo, su constitucionalización ha sido un proceso de decantación. Primero se protegieron los derechos frente a las consecuencias que el uso de la información pudiera deparar y, posteriormente, se reconoció la sustantividad y autonomía del derecho a la protección de datos.

V. La necesidad de asegurar el dominio sobre la proyección exterior de la identidad propició el reconocimiento del derecho a la autodeterminación informativa. La atribución de un poder de control y disposición sobre los datos personales consolidó su autonomía respecto de la *privacy* y la vida privada, además de reforzar la garantía de la dignidad y el libre desarrollo de la personalidad.

VI. La densidad de la regulación de la Unión Europea, su esfuerzo constante por configurar un sistema de facultades, principios, garantías y sanciones comunes, la han convertido en una referencia global. Su éxito obedece a dos razones concurrentes. De una parte, la cultura jurídica europea, vinculada a la idea de estado social y a una concepción más comunitaria de los derechos, resulta más adecuada para responder

a los desafíos que el tratamiento de datos personales plantea. De otra, la habilidad con que la Unión Europea ha convertido en fortaleza la necesidad de articular un modelo de protección que compagine la garantía de los derechos, con el aprovechamiento de las oportunidades económicas que el tratamiento masivo de la información propicia.

VII. Las condiciones básicas de ejercicio de este derecho fundamental vienen determinadas por el derecho de la Unión Europea. La construcción del mercado interior y la armonización normativa entre los Estados miembros son el fundamento del proceso de europeización del derecho a la protección de datos, del que el Reglamento General de Protección de Datos es el reflejo más elocuente.

VIII. El Reglamento General de Protección de Datos, como buque insignia del marco normativo europeo de tratamiento de la información personal, es un reflejo de la idiosincrasia europea. Del análisis de sus elementos caracterizadores se infiere que, el modelo europeo de protección de datos es proactivo, preventivo y dinámico, pues propicia cierta adaptación de la respuesta jurídica a la realidad del tratamiento. A su vez, el reconocimiento de un conjunto amplio de derechos, garantiza la respuesta subjetiva frente al tratamiento de los datos personales.

Sin embargo, junto a esos elementos proactivos y flexibles, confluyen otros, más propios de un modelo rígido y reactivo (v. gr. la regulación de las categorías especiales de datos). En este sentido, el Reglamento General de Protección de Datos es un híbrido.

IX. El resto de normativas que conforman, o conformarán en un futuro próximo, el ecosistema europeo de protección de datos, revelan una tendencia hacia la regulación contextual, centrada en la anticipación de los riesgos y en la personalización de las respuestas jurídicas. Ese enfoque preventivo y proactivo tiene, en la Propuesta de Reglamento IA, su manifestación más representativa.

X. Los deberes de protección a que obliga el derecho a la protección de datos personales se construyen en torno al vínculo dato-persona. Qué se entienda por dato personal determina la morfología y alcance del derecho fundamental. El concepto europeo de dato personal tiene como elemento clave la identificabilidad de la persona física.

XI. El Tribunal de Justicia de la Unión Europea, en el asunto Nowak, utilizó el contenido, la finalidad y los efectos como criterios identificativos de

la existencia de datos personales. Esa tríada de opciones es compatible con el modelo de protección europeo. Su utilización como parámetros identificadores es jurídicamente posible y, en opinión de quien escribe, deseable. Con ellos, se amplía el concepto de dato personal y, consecuentemente, el ámbito de aplicación del sistema de protección.

XII. El vínculo dato-persona no es suficiente para accionar los mecanismos jurídicos del derecho a la protección de datos. Es preciso que la información personal sea objeto de tratamiento. El modo en que se utilizan los datos, los riesgos que ello comporta, son la realidad objeto de regulación. El derecho a la protección de datos no protege los datos personales por el hecho de serlo, sino por las consecuencias que su tratamiento pudiera tener en los bienes jurídicos de las personas.

XIII. La compleja conciliación de una concepción unívoca del derecho a la protección de datos con las diversas finalidades que le caracterizan, unido al modo en que surge (desde la legislación y la jurisprudencia y estrechamente vinculado al derecho a la vida privada), ha generado importantes dudas acerca de la naturaleza de este derecho. La oscilante jurisprudencia del Tribunal de Justicia de la Unión Europea es fiel reflejo de ello. Como también lo son las propuestas doctrinales negadoras de la *iusfundamentalidad* del derecho a la protección de datos.

XIV. El análisis hermenéutico del artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, pone de manifiesto la complejidad de un derecho fundamental que exige la colaboración del legislador para su realización plena. La garantía del derecho a la protección de datos demanda la articulación de un marco de actuación que haga jurídicamente aceptable el tratamiento de la información personal, sin poner en peligro la libre circulación de la información. En definitiva, el derecho a la protección de datos es un derecho de configuración legal.

XV. El derecho fundamental a la protección de datos, en su configuración europea, es un simbionte con dos almas: El derecho a la protección de datos en sentido amplio, que se corresponde con la función instrumental de salvaguarda de los derechos y libertades. Y el derecho a la protección de datos en sentido estricto, que se compadece con las manifestaciones más vinculadas al ejercicio del poder de disposición y control sobre los datos personales (sería el caso de las facultades de actuación o de las obligaciones de información del responsable). Solo

combinando ambas facetas resulta posible la cognición del derecho fundamental en toda su extensión.

XVI. La existencia de categorías especiales de datos se funda en una doble convicción: ni todos los datos son igual de valiosos, ni su uso entraña el mismo nivel de riesgo.

El modelo europeo de protección de datos ha vinculado la condición especial a la naturaleza del dato. De este modo, el mayor riesgo de discriminación y la capacidad más acuciada para revelar los aspectos más sensibles de la persona quedan inexorablemente unidos al contenido de la información.

XVII. En el plano normativo, el legislador europeo ha establecido un conjunto, cerrado, de tipologías de datos merecedoras de ser calificadas como especiales (los «datos personales que el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física» (art. 9.1 RGPD)).

El tratamiento de esas tipologías de datos está, como premisa, prohibido. Admitiéndose su utilización, exclusivamente, cuando se produzca alguna de las circunstancias normativamente previstas en el apartado segundo del art. 9.2 del Reglamento General de Protección de datos.

XVIII. El principal valor del sistema de protección de las categorías especiales es su certeza aplicativa. Sin embargo, adolece de flexibilidad para proporcionar una respuesta jurídica adecuada a aquellos tratamientos que, sin utilizar datos sensibles, pueden entrañar un riesgo elevado de discriminación (por ejemplo, por razones económicas o de edad). Además, al facilitar la aplicación mecanizada de las medidas previstas, genera dinámicas contrarias a la proactividad y a la atención a la realidad del tratamiento.

XIX. Frente a los problemas que plantea un conjunto tasado de tipologías sensibles, caben diferentes soluciones jurídicas. Es posible incorporar, por vía interpretativa, los supuestos dudosos a las categorías especiales. Sin embargo, la existencia de un conjunto tasado de datos especiales, alguno de los cuáles tiene, además, un contenido

jurídicamente definido (datos de salud, datos genéticos y datos biométricos), limita, considerablemente, el alcance de esta opción.

XX. La segunda de las posibilidades, pasaría por hacer del tratamiento el centro de imputación del derecho, en lugar de los datos especiales. Para ello, bastaría una reforma del Reglamento General de Protección de Datos, que pusiese de manifiesto ese cambio de enfoque. Esta propuesta, moderada, permitiría incorporar al contexto como elemento identificador de lo sensible.

De este modo, aquellos tratamientos en que, por contenido, los datos fuesen sensibles, automáticamente, convertirían al tratamiento en especial. Pero, además, también tendrían condición especial los tratamientos que, por finalidad o contexto, revelasen informaciones sensibles. Con ello, se evita la necesidad de etiquetar a los datos como pertenecientes a una determinada tipología, pues será la realidad específica de cada tratamiento la que desempeñará esa función de adjetivación.

La mayor adecuación de esta proposición, comporta, como contrapartida, una reducción en la seguridad aplicativa. Un mismo dato, en función del tratamiento, podría ser asignado a diversas tipologías e, incluso, podría variar en su nivel de sensibilidad. Además, esta aproximación contextual sigue condicionada por la existencia de las categorías especiales. No resuelve el problema que plantean los tratamientos en los que, sin pretender conocer informaciones sobre alguna de las categorías especiales, se genera un alto riesgo para el ciudadano, o se propicia algún tipo de discriminación.

XXI. La tercera posibilidad, más rupturista, aboga por la sustitución de las categorías especiales por un modelo de protección riesgos racionalizado. Esta propuesta, que considero la más adecuada, tendría a los riesgos de discriminación y de afectación de los derechos como parámetros de referencia. Serían los peligros concretos los que determinarían las medidas de protección más adecuadas para cada caso concreto y, a partir de determinados umbrales, el tratamiento dejaría de ser aceptable. La naturaleza de los datos tratados sería uno de los criterios a considerar, pero no sería el único, ni condicionaría, apriorísticamente, las medidas a adoptar.

XXII. El concepto de dato personal debería ser objeto de revisión. El riesgo de reidentificación de los datos anonimizados, unido a las posibilidades

de interrelación, combinación y análisis de la información, hacen que, en el contexto adecuado, prácticamente cualquier información pueda ser considerada dato personal.

XXIII. La adopción de un modelo que refleje convenientemente los modos en que la información puede vincular a una persona exige, de una parte, incorporar, expresamente, los criterios de contenido, finalidad y efectos al concepto de dato personal. De otra, debería transitarse hacia un modelo en el que toda información se considere personal, salvo que se demuestre lo contrario. En ese escenario, el grado de vinculación con el individuo y su capacidad para afectar o revelar ciertos aspectos de las personas determinaría las medidas de protección a implementar.

XXIV. No hay, en la naturaleza del derecho fundamental a la protección de datos, razón jurídica alguna que impida la adopción de un modelo de protección de los datos personales centrado en el riesgo y los efectos del tratamiento. La articulación de un sistema de protección caracterizado por un concepto de dato personal más amplio y sin la condicionalidad taxativa de las categorías especiales es jurídicamente posible y, en opinión de quien escribe, deseable.

CONCLUSIONS

I. The Information Age generates an ecosystem full of possibilities and hopes for improving citizens' quality of life. However, it also challenging for the protection of rights and freedoms.

II. Data has become a bargaining chip, a product destined for the market, a keystone in contemporary societies. In the Information Age, the dominion over the external projection of the self is seriously threatened.

III. The right to data protection affects the way in which personal information is used and provides the legal tools to ensure its control. The ability of the right to data protection to be deployed effectively in digital environments has made it the reference model for the set of legal-normative measures aimed at disciplining life on the Net.

IV. Although it is applicable to all types of personal data, the right to data protection arises as a response to the automatic personal data processing, breaking down in the process the barriers that time, space and costs implies. However, the constitutionalisation of the right to data protection has been a process of decantation. In an early stage, the protection focused on the negative consequences that the use of information could have and, subsequently, it was recognised the substantivity and autonomy of the right to data protection.

V. The need to ensure control over the external projection of identity led to the recognition of the right to informational self-determination. Control and disposition power over personal data consolidate its autonomy concerning *privacy* and private life, in addition to reinforcing the guarantee of dignity and the free development of personality.

VI. The density of the European Union's regulation, its constant effort to configure a system of common powers, principles, guarantees and sanctions, has made it a global reference. Its success is due to two concurrent reasons. On the one hand, the European legal culture, linked to the idea of the social state and to a more communitarian conception of rights, is better suited to respond to the challenges posed by the processing of personal data. On the other hand, the ability with which the European Union has turned into a strength the need to articulate a model of protection that combines the guarantee of rights with the

exploitation of the economic opportunities that the massive processing of information provides.

VII. The basic conditions for the exercise of this fundamental right are determined by European Union law. The construction of the internal market and the harmonisation of regulations between Member States are the basis of the process of Europeanisation of the right to data protection, of which the General Data Protection Regulation is the most eloquent reflection.

VIII. The General Data Protection Regulation, as the flagship of the European regulatory framework for the processing of personal information, is a reflection of the European idiosyncrasy. From the analysis of its characteristic elements, it can be inferred that the European data protection model is proactive, preventive and dynamic. In turn, the recognition of a broad set of rights guarantees the subjective response to the processing of personal data.

However, alongside these proactive and flexible elements, there are others, typical of a rigid and reactive model (e.g. the regulation of special categories of data). In this sense, the General Data Protection Regulation is a hybrid.

IX. The rest of the regulations that make up, or will make up in the near future, the European data protection ecosystem, reveal a trend towards contextual regulation, focused on the anticipation of risks and the personalization of legal responses. This preventive and proactive approach has, in the IA Regulation Proposal, its most representative manifestation.

X. The duties of protection to which the right to the protection of personal data obliges are built around the data-person link. What is understood by personal data determines the morphology and scope of the fundamental right. The European concept of personal data has as a key element the identifiability of the natural person.

XI. The Court of Justice of the European Union, in the Nowak case, used content, purpose and effects as identifiers of the existence of personal data. This triad of options is compatible with the European protection model. Their use as identifying parameters is legally possible and, in the opinion of this author, desirable. They broaden the concept of

personal data and, consequently, the scope of application of the protection system.

XII. The data-person link is not enough to trigger the legal mechanisms of the right to data protection. Personal information must be processed. The way in which data are used, the risks involved, are the reality to be regulated. The right to data protection does not protect personal data just because they are personal data, but because of the consequences of their processing for the rights and freedoms.

XIII. The complex reconciliation of a univocal conception of the right to data protection with the various purposes that characterize it, together with the way in which it arises (from legislation and case law and closely linked to the right to privacy), has generated significant doubts about the nature of this right. The oscillating case-law of the Court of Justice of the European Union is a faithful reflection of this. As are the doctrinal proposals denying the *iusfundamental* nature of the right to data protection.

XIV. The hermeneutic analysis of Article 8 of the Charter of Fundamental Rights of the European Union reveals the complexity of a fundamental right that requires the collaboration of the legislator for its full realization. The guarantee of the right to data protection requires the articulation of a framework of action that makes the processing of personal information legally acceptable, without endangering the free circulation of information. In short, the right to data protection is a right of legal configuration.

XV. The fundamental right to data protection, in its European configuration, is a symbiont with two souls: The right to data protection in the broad sense, which corresponds to the instrumental function of safeguarding rights and freedoms. And the right to data protection in the strict sense, which corresponds to the manifestations more closely linked to the exercise of the power of disposal and control over personal data (this would be the case of the powers of action or the obligations of information of the controller). Only by combining both facets is it possible to cognize the fundamental right in its full extent.

XVI. The existence of special categories of data is based on a twofold conviction: not all data are equally valuable, nor does their use carry the same level of risk.

The European data protection model has linked the special status to the nature of the personal data. Thus, the greater risk of discrimination and the greater ability to reveal the most sensitive aspects of the individual are inextricably linked to the content of the information.

XVII. At regulatory level, the European legislator has established a closed set of typologies of data worthy of being qualified as special (the «personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation» [art. 9.1 RGPD]).

The processing of these types of data is, as a premise, prohibited. Processing is only possible when a circumstance included in the art. 9.2 of the General Data Protection Regulation occurs.

XVIII. The main value of the system of protection of special categories is its certainty of application. However, it lacks the flexibility to provide an adequate legal response to processing operations which, without using sensitive data, may entail a high risk of discrimination (for example, for economic reasons or on grounds of age). Moreover, by facilitating the mechanised application of the envisaged measures, it generates dynamics contrary to accountability and attention to the reality of the processing.

XIX. There are different legal remedies for the above problems. It is possible to incorporate, by way of interpretation, doubtful cases into the special categories. However, the existence of a set of special categories of data, some of which also have a legally defined content (health data, genetic data and biometric data), considerably limits the scope of this option.

XX. The second remedy would be to make the processing the centre of imputation of the right, instead of the special data. For this, a reform of the General Data Protection Regulation would suffice, which would highlight this change of approach. This moderate proposal would make it possible to incorporate the context as an identifier of the sensitive.

In this way, those processing operations in which, due to their content, data are sensitive, would automatically turn the processing into special processing. But, in addition, processing operations that, due to their purpose or context, reveal sensitive information would also have a

special status. This avoids the need to label data as belonging to a certain typology, as it will be the specific reality of each processing that will perform this adjectival function.

The greater adequacy of this proposition entails, on the other hand, a reduction in application security. The same data, depending on the processing, could be assigned to different typologies and could even vary in its level of sensitivity. Moreover, this contextual approach is still conditioned by the existence of the special categories. It does not solve the problem posed by processing operations in which, without intending to know information on any of the special categories, a high risk is generated for the citizen, or some type of discrimination is encouraged.

XXI. The third possibility, more ground-breaking, advocates the replacement of the special categories by a model of rationalized risk protection. This proposal, which I consider to be the most appropriate, would have the risks of discrimination and the affectation of rights as reference parameters. It would be the specific dangers that would determine the most appropriate protection measures for each specific case and, above certain thresholds, the processing would no longer be acceptable. The nature of the personal data processed would be one of the criteria to be considered, but it would not be the only one, nor would it condition, a priori, the measures to be adopted.

XXII. The concept of personal data should be reviewed. The risk of re-identification of anonymised data, together with the possibilities of interrelation, combination and analysis of information, mean that, in the right context, practically any information can be considered personal data.

XXIII. The adoption of a model that adequately reflects the ways in which information can be linked to an individual requires, on the one hand, the criteria of content, purpose and effects to be expressly incorporated into the concept of personal data. On the other hand, there should be a move towards a model in which all information is considered personal. In this scenario, the degree of linkage with the individual and its capacity to affect or reveal certain aspects of individuals would determine the protection measures to be implemented.

XXIV. There is no legal reason in the nature of the fundamental right to data protection that prevents the adoption of a model of protection of

personal data focused on the risk and effects of the processing. The articulation of a system of protection characterised by a broader concept of personal data and without the restrictive conditionality of special categories is legally possible and desirable.

BIBLIOGRAFÍA

AA. VV. (2005). *The United States Supreme Court: The Pursuit of Justice*. (Christopher Tomlins, Ed.). Nueva york: Houghton Mifflin Company.

AA. VV. (2015). *Hacia un nuevo derecho europeo de protección de datos. Towards a new european data protection*. (Artemi Rallo Lombarte & Rosario García Mahamut, Eds.). Valencia: Tirant Lo Blanch.

AA. VV. (2016). *Multinationals and the Constitutionalization of the World Power System*. (Jean-Philippe Robé, Antoine Lyon-Caen, & Stéphane Vernac, Eds.). Nueva York: Routledge.

AA. VV. (2020a). *Administración electrónica, transparencia y contratación pública*. (Isaac Martín Delgado & José Antonio Moreno Molina, Eds.). Madrid: Iustel.

AA. VV. (2020b). *Garantías del proceso debido y Unión Europea. Implicaciones para los ordenamientos internos*. (Teresa Freixes Sanjuán, Ed.). Madrid: Centro de Estudios Políticos y Constitucionales.

AA. VV. (2020c). *Retos actuales de la cooperación penal en la Unión Europea*. (José Manuel Cortés Martín & Florentino-Gregorio Ruiz Yamuza, Eds.). Madrid: Dykinson.

Aba Catoira, Ana. (2020a). Artículo 7. Consentimiento de los menores de edad. En Alejandro (coord. .. Villanueva Turnes (Ed.), *Comentarios a la Nueva Ley de Protección de Datos. Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 33-38). Madrid: Dilex.

Aba Catoira, Ana. (2020b). IV Tratamiento de categorías especiales de Datos (Datos especialmente protegidos). En *Comentarios a la Nueva Ley de Protección de Datos. Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 41-45). Madrid: Dilex.

Aba Catoira, Ana. (2021). Libertades de expresión e información en la sociedad digital como garantías de la democracia. *Revista Doctrina Distrital*, *2*(2), 62-78.

Abella García, Alberto. (2020). Gobernanza inteligente a través de los datos. Modelo de Gobernanza y Arquitectura de los Datos. *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, (Extra 3), 167-194.

Abellán-garcía Sánchez, Fernando. (2021). El tratamiento por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los me. En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y*

Garantía de los Derechos Digitales (pp. 1201-1218). Cizur Menor (Navarra): Civitas Thomson Reuters.

Adsuara Varela, Borja. (2018). El ciudadano frente al Reglamento. En José López Calvo (Ed.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos: adaptado al Proyecto de Ley orgánica de Protección de Datos de 10 de noviembre de 2017* (pp. 163-172). Madrid: Wolters Kluwer-Bosch.

Adsuara Varela, Borja. (2019). El «perfilado ideológico» de los ciudadanos por los partidos políticos. *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, (Extra 3), 77-89.

Agencia de los Derechos Fundamentales de la Union Europea. (2018). *Manual de legislación europea en materia de la protección de datos*. Luxemburgo: Oficina de publicaciones de la Unión Europea. doi:10.2811/53770

Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa. (2019). *Manual de legislación europea contra la discriminación. Edición de 2018*. (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, Ed.). Luxemburgo: Oficina de Publicaciones de la Unión Europea.

Aguado Renedo, César. (2010). La protección de los datos personales ante el Tribunal Constitucional español. *Cuestiones constitucionales: revista mexicana de derecho constitucional*, (23), 3-25.

Al-Ameen, Abdalla y Talab, Samani A. (2013). The technical feasibility and security of e-voting. *Int. Arab J. Inf. Technol.*, *10*(4), 397-404.

Al-Fedaghi, Sabah. (2007). How Sensitive is Your Personal Information? En *Proceedings of the 2007 ACM Symposium on Applied Computing* (pp. 165–169). New York, NY, USA: Association for Computing Machinery. doi:10.1145/1244002.1244046

Alcaraz, Enrique y Hughes, Brian. (2002). *El español jurídico*. Barcelona: Ariel.

Alcaraz, Hubert. (2007). El derecho a la intimidad en Francia en la época de la Sociedad de la Información «Quand je vous ameray Ma foi, je ne le sais pas... peut-être jamais, peut être demain!» *Araucaria: Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, *9*(18), 6-28.

Alexy, Robert. (1993). *Teoría de los derechos fundamentales*. Madrid: Centro de Estudios Políticos y Constitucionales.

Alonso Blas, Diana. (1997). La aplicación de la directiva europea de protección de datos en España reformas necesarias en la Lortad. En Miguel Ángel Davara Rodríguez (Ed.), *X años de encuentros sobre informática y derecho, 1996-1997* (pp. 141-150). Cizur Menor (Navarra): Aranzadi.

Alonso García, Ricardo. (2015). Sobre la adhesión de la UE al CEDH:(o sobre cómo del dicho al hecho, hay un gran trecho). *Revista Española de Derecho Europeo*, (53), 11-16.

Álvarez-Ossorio Micheo, Fernando. (2020). Acto y potencia de la cláusula de apertura del artículo 52.3 de la Carta. En Ana Carmona Contreras (Ed.), *Las cláusulas horizontales de la Carta de Derechos Fundamentales de la Unión Europea: Manual de Uso* (pp. 99-119). Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Álvarez Robles, Tamara. (2018). Derechos digitales. Especial interés en los derechos de acceso a Internet y a la ciberseguridad como derechos constitucionales sustantivos. En Andrés Iván Dueñas Castrillo, Daniel Fernández Cañueto, & Gabriel Moreno González (Eds.), *Juventud y Constitución. Un estudio de la Constitución española por los jóvenes en su cuarenta aniversario* (pp. 135-158). Zaragoza: Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico.

Álvarez Robles, Tamara. (2021). El derecho de acceso a internet en el constitucionalismo español. Desde la influencia supranacional a la LO 3/2018, de protección de datos personales y garantía de los derechos digitales. En Federico Bueno de Mata & Irene González Pulido (Eds.), *Fodertics 9.0: Estudios sobre tecnologías disruptivas y justicia* (pp. 3-15). Granada: Comares.

Alzina Lozano, Alvaro. (2020). Los avances del espacio de libertad, seguridad y justicia en la protección de los ciudadanos europeos. En Julio Guinea Bonillo, José Enrique Anguita Osuna, & Vlad Florin Jurje (Eds.), *La Europa Ciudadana* (pp. 117-128). Madrid: Dykinson.

Amérigo Alonso, José. (2019). Objeto y ámbito de aplicación. En Artemi Rallo Lombarte (Ed.), *Tratado de Protección de Datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales* (pp. 79-113). Valencia: Tirant Lo Blanch.

Ananny, Mike, y Crawford, Kate. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *new media & society*, *20*(3), 973-989.

Aparicio Salom, Javier y Vidal Laso, María. (2019). *Estudio sobre la Protección de Datos*. Cizur Menor (Navarra): Aranzadi.

Aperribai Ulacia, Ana. (2021). Las autoridades de control independiente. Nuevo escenario normativo para la cooperación (Comentario al artículo 51 RGPD y al artículo 58 LOPDGDD. En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 2557-2572). Cizur Menor (Navarra): Civitas Thomson Reuters.

Arano Uría, Francisco. (2020). Las redes sociales en la formación de opiniones políticas. *Actas de Periodismo y Comunicación*, *6*(1).

Arenas Ramiro, Mónica. (2006). *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Tirant Lo Blanch.

Arenas Ramiro, Mónica. (2014). Unforgettable: a propósito de la STJUE de 13 de mayo de 2014. Caso Conseteja (Google v. AEPD). *Teoría y realidad constitucional*, (34), 537-558.

Arenas Ramiro, Mónica. (2019a). El impacto del Reglamento General de Protección de Datos Personales en el tratamiento de los datos personales de los menores de edad. En Rosario García Mahamut & Beatriz Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales* (pp. 237-263). Valencia: Tirant Lo Blanch.

Arenas Ramiro, Mónica. (2019b). Los políticos, opiniones políticas e Internet: la lesión del derecho a la protección de datos personales. *Teoria y Realidad Constitucional*, (44), 341-372.

Arenas Ramiro, Mónica. (2021a). El derecho de acceso y las condiciones generales de ejercicio de los derechos (Comentario al artículo 15 RGPD y a los artículos 12 y 13 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1437-1490). Cizur Menor (Navarra): Civitas Thomson Reuters.

Arenas Ramiro, Mónica. (2021b). El derecho de oposición (Comentario al artículo 21 RGPD y al artículo 18 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1701-1723). Cizur Menor (Navarra): Civitas Thomson Reuters.

Arias Pou, María. (2016). Definiciones a efectos del Reglamento General de Protección de Datos. En José Luis Piñar Mañas, María Álvarez Caro, & Miguel Recio Gayo (Eds.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (pp. 115-134). Madrid: Reus.

Aridor, Guy, Che, Yeon-Koo y Salz, Tobias. (2020). *The economic consequences of data privacy regulation: Empirical evidence from gdpr* (No. w26900). Nueva york: National Bureau of Economic Research.

Arjona Sebastià, César. (2006). *Los votos discrepantes del juez O. W. Holmes*. Madrid: Iustel.

Arora, Kim. (2020). *Privacy and data protection in India and Germany: A comparative analysis*. Berlin: WZB.

Arzoz Santisteban, Xabier. (2015). Artículo 8. Derecho al respeto de la vida privada y familiar. En Iñaki Lasagabaster Herrarte (Ed.), *Convenio europeo de derechos humanos: comentario sistemático* (3ª., pp. 338-438). Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Azpitarte, Miguel. (2019). Artículo 54. Prohibición del abuso de derecho. En Antonio (dir. .. López Castillo (Ed.), *La Carta de Derechos Fundamentales de la Unión Europea. Diez años de jurisprudencia* (pp. 1709-1717). Valencia: Tirant Lo Blanch.

Azurmendi, Ana. (2015). Por un "derecho al olvido" para los europeos aportaciones jurisprudenciales de la Sentencia del TJUE del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional de 29.12.2014. *Revista de Derecho Político*, (92), 273-310.

Balaguer Callejón, Francisco. (2019). Redes sociales, compañías tecnológicas y democracia. *Revista de Derecho Constitucional Europeo*, (32).

Ballantyne, Angela. (2020). How should we think about clinical data ownership? *Journal of Medical Ethics*, *46*(5), 289-294. doi:10.1136/medethics-2018-105340

Barbará i Fondevila, María Ángels. (2014). El principio de limitación de la finalidad a debate. Los usos secundarios. *I+S: Revista de la Sociedad Española de Informática y Salud*, (105), 9-10.

Baricco, Alessandro. (2019). *The Game*. Barcelona: Anagrama.

Barrio Andrés, Moisés. (2020). *Internet de las Cosas* (2ª.). Madrid: Reus.

Barrio Andrés, Moisés. (2021). Génesis y desarrollo de los derechos digitales. *Revista de Derecho de las Cortes Generales*, *Primer sem*(110), 197-233.

Bashir, Masooda, Hayes, Carol, Lambert, April D. y Kesan, Jay P. (2015). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1-10.

Bastida Freijedo, Francisco J. (1998). La soberanía borrosa: la democracia. *Fundamentos: Cuadernos monográficos de teoría del estado, derecho público e historia constitucional*, (1), 381-460.

Bastida Freijedo, Francisco J., Villaverde Menéndez, Ignacio, Requejo Rodríguez, Paloma, Presno Linera, Miguel Ángel, Aláez Corral, Benito, y Fernández Sarasola, Ignacio. (2004). *Teoría General de los Derechos Fundamentales en la Constitución Española de 1978*. Madrid: Tecnos.

Bauman, Zygmunt. (2006). *Vida líquida*. Barcelona: Paidós.

Baura, Eduardo. (1987). El "contenido esencial" del derecho constitucional al matrimonio. *Ius canonicum*, *27*(54), 697-739.

Bauzá Martorell, Felio J. (2019). El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura. *Ars Boni et Aequi*, *15*(1), 121-148.

Bayamlıoğlu, Emre. (2021). The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation". *Regulation & Governance*, 1-21.

Beck, Ulrich. (2000). Risk Society Revisited: Theory, Politics and Research Programmes. En Barbara Adam, Ulrich Beck, & Joostvan Loon (Eds.), *The Risk Society and Beyond. Critical Issues for Social Theory* (pp. 211-229). Londres: SAGE Publications.

Becker, David, King, Trish Dunn y McMullen, Bill. (2015). Big data, big data quality problem. En *2015 IEEE International Conference on Big Data (Big Data)* (pp. 2644-2653). doi:10.1109/BigData.2015.7364064

Benjamin, Patrick R. (2020). *An Analysis of the Adequacy of the Canadian Privacy Framework Under the General Data Protection Regulation*. University of Manitoba.

Benndorf, Volker y Normann, Hans-Theo. (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics*, *120*(4), 1260-1278.

Bennet, Colin J. y Bayley, Robin M. (2016). Privacy Protection in the Era of «Big Data»: Regulatory Challenges and Social Assessments. En Bart van der Sloot, Dennis Broeders, & Erik Schrijvers (Eds.), *Exploring the Boundaries of Big Data* (pp. 205-227). Amsterdam: Amsterdam University Press.

Bergelson, Vera. (2003). It's Personal but Is It Mine? Toward Property Rights in Personal Information. *U.C. Davis Law Review*, *37*(2), 379-452.

Bergemann, Benjamin. (2017). The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection. En *IFIP International Summer School on Privacy and Identity Management* (pp. 111-131). Springer.

Bergfeld, J. P. (1996). The impact of the EC Data Protection Directive on Dutch Data Protection Law. *The Journal of Information, Law and Technology (JILT)*, (1).

Berners-Lee, Tim. (2000). *Tejiendo la Red*. Madrid: Siglo Veintiuno.

Berrocal Lanzarot, Ana Isabel. (2019). *Estudio Jurídico-Crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Análisis conjunto del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y* . Madrid: Reus.

Bestué Salinas, Carmen. (2009). La traducción de términos jurídicos en el ámbito internacional. *Babel*, *55*(3), 244-262.

Biega, Asia J., Potash, Peter, Daumé, Hal, Diaz, Fernando y Finck, Michèle. (2020). Operationalizing the Legal Principle of Data Minimization for Personalization. En *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval* (pp. 399-408). Association for Computing Machinery. doi:https://doi.org/10.1145/3397271.3401034. (Última consulta: 20/10/2021).

Bieker, Felix, Martin, Nicholas, Friedewald, Michael y Hansen, Marit. (2017). Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool. En *IFIP International Summer School on Privacy and Identity Management* (pp. 207-220). Ispra, Italy: Springer.

Bilbao Ubillos, Juan María. (1997). *La eficacia de los derechos fundamentales frente a particulares. Análisis de la jurisprudencia del Tribunal Constitucional*. Madrid: Centro de Estudios Políticos y Constitucionales.

Binder, Susanne, Iannone, Andrea y Leibner, Chad. (2020). Correction to: Biometric technology in "no-gate border crossing solutions" under consideration of privacy, ethical, regulatory and social acceptance. *Multimedia Tools and Applications*, (pre-print), 1-14. doi:10.1007/s11042-021-10595-8

Binns, Reuben y Gallo, Valeria. (2019). Data minimisation and privacy-preserving techniques in AI systems. *AI blog. ICO*. Recuperado de: https://ico.org.uk/about-the-ico/news-and-events/ai-blog-data-minimisation-and-privacy-preserving-techniques-in-ai-systems/. (Última consulta: 20/10/2021).

Bioinformatics, EcSeq. (s. f.). Privacy implications of genetic data sharing. *https://www.ecseq.com/blog/2019/privacy-implications-of-genetic-information-sharing*. (última consulta: 20/10/2021).

Black, Forrest Revere. (1930). Ill-starred prohibition case: Olmstead vs. united states. *Georgetown Law Journal*, *18*(2), 120-129.

Bloustein, Edward J. (1964). Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, *39*(6), 962-1007.

Blume, Peter. (2010). Data Protection and Privacy–Basic Concepts in a Changing World. *Scandinavian Studies in Law. ICT Legal Issues*, *56*, 151-164.

Bobbio, Norberto. (1991). *El tiempo de los derechos*. Madrid: Sistema.

Bohannon, John. (2015, enero). Privacy. Credit card study blows holes in anonymity. *Science (New York, N.Y.)*. United States. doi:10.1126/science.347.6221.468

Bonet, Jordi. (2008). Los actores privados de carácter económico y su incidencia en la formación y aplicación del DIP: especial referencia a las empresas

transnacionales. En Victoria Abellán & Jordi Bonet (Eds.), *La incidencia de la mundialización en la formación y aplicación del Derecho Internacional Público* (pp. 135-176). Barcelona: Bosch.

Borra, Surekha. (2020). COVID-19 apps: Privacy and security concerns. En *Intelligent Systems and Methods to Combat Covid-19* (pp. 11-17). Springer.

Botella Pamies, Esther. (2019). Designación de un delegado de protección de datos. En Mónica Arenas Ramiro & Alfonso Ortega Giménez (Eds.), *Protección de datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)* (pp. 186-190). Madrid: Sepín.

Brito Izquierdo, Noemí. (2018). Tratamiento de los datos personales de menores de edad en la nueva normativa europea protectora de datos personales. *Actualidad Civil*, (5), 1-19.

Brkan, Maja. (2017). The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection. En Maja Brkan & Evangelia Psychogiopoulou (Eds.), *Courts, Privacy and Data Protection in Digital Enviroment* (pp. 10-31). Cheltenham, UK-Northampton, Massachusetts: Edward Elgar.

Brkan, Maja. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, *27*(2), 91-121.

Brouwer, Evelien y Zuiderveen Borgesius, Frederik. (2015). Access to Personal Data and the Right to Good Governance during Asylum Procedures after the CJEU's YS. and M. and S. Judgment (C-141/12 and C-372/12). *European Journal of Migration and Law*, *17*(2-3), 259-286.

Burkert, Herbert. (2000). Privacy - Data Protection. A German/European Perspective. En Christoph Engel & Kenneth H. Heller (Eds.), *Governance of global networks in the light of differing local values* (pp. 43-69). Baden-Baden: Nomos.

Bustos Gisbert, Rafael. (2017). La aplicación judicial de la CDFUE; Un decálogo a partir de la jurisprudencia del Triunal de Justicia de la Unión Europea. *Teoria y Realidad Constitucional*, (39), 333-359.

Butler, Judith. (2004). *Lenguaje, poder e identidad*. Editorial Síntesis.

Bygrave, Lee A. (2010). Privacy and data protection in an international perspective. *Scandinavian studies in law*, *56*(8), 165-200.

Bygrave, Lee A. (2020). Article 22. Automated individual decision-making, including profiling. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 522-542). Oxford: Oxford University Press.

Bygrave, Lee A. y Tosoni, Luca. (2020). Article 4(8). Processor. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 157-162). Oxford: Oxford University Press.

Caamaño Domínguez, Francisco y Jove Villares, Daniel. (2021). Corresponsables del tratamiento y supuestos de corresponsabilidad en el tratamiento (Comentario al artículo 26 RGPD y al artículo 29 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1819-1834). Cizur Menor (Navarra): Civitas Thomson Reuters.

Cai, Li, y Zhu, Yangyong. (2015). The challenges of data quality and data quality assessment in the big data era. *Data science journal*, *14*, 1-10.

Cano Ruiz, Isabel. (2019). Artículo 9. Categorías especiales de datos. En Mónica Arenas Ramiro & Alfonso Ortega Giménez (Eds.), *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)* (pp. 81-84). Madrid: Sepín.

Carmona Contreras, Ana. (2016). El espacio europeo de los derechos fundamentales de la Carta a las constituciones nacionales. *Revista Española de Derecho Constitucional*, *Año 36*(107), 13-40.

Carmona Contreras, Ana. (2020). ¿El nivel o los niveles de protección de los derechos fundamentales en el espacio europeo?: A vueltas con el artículo 53 de la Carta. En Ana Carmona Contreras (Ed.), *Las cláusulas horizontales de la Carta de Derechos Fundamentales de la Unión Europea: Manual de Uso* (pp. 202-222). Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Carrillo, Marc. (1993). *La Claúsula de conciencia y el secreto profesional de los periodistas : Una aproximación al estatuto jurídico de los profesionales de la información*. Madrid-Barcelona: Civitas-Centre d'investigació de la Comunicació.

Carrillo, Marc. (2016). Los ámbitos del derecho a la intimidad en la sociedad de la comunicación. En *Tribunal Constitucional-Centro de Estudios Políticos y Constitucionales. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional* (pp. 11-70). Madrid: Centro de Estudios Políticos y Constitucionales.

Casado Robledo, María Jesús. (2020). Proteger la información ha sido una constante a lo largo de la Historia. *Revista española de control externo*, *22*(Extra 64), 88-101.

Cavoukian, Ann. (2009). *Privacy by design. The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*. Ontario. Recuperado de: https://www.privacysecurityacademy.com/wp-

content/uploads/2020/08/PbD-Principles-and-Mapping.pdf. (última consulta: 20/10/2021).

Cavoukian, Ann y Castro, Daniel. (2014). *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*.

Cavoukian, Ann, Dix, Alexander y El Emam, Khaled. (2014). *The Unintended Consequences of Privacy Paternalism*. Information and Privacy Commisioner of Ontario, Canada. Recuperado de: https://www.ipc.on.ca/wp-content/uploads/2016/08/The-Unintended-Consequences-of-Privacy-Paternalism.pdf (última consulta: 20/10/2021).

Cerrillo i Martínez, Agustí. (2021). El tratamiento de los datos y la gestión de la huella digital de las personas fallecidas (Comentario a los artículos 2.2.b) y 3 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 529-550). Cizur Menor (Navarra): Civitas Thomson Reuters.

Chander, Anupam. (2017). The racist algorithm? *Michigan Law Review*, *115*(6), 1023-1045.

Chen, Jihong, Han, Lu y Kipker, Dennis-Kenji. (2020). An Introduction into the New Chinese Data Protection Legal Framework. *Datenschutz Datensich*, (44), 52-57.

Chopra, Aneesh. (2014). *Innovative state: How new technologies can transform government*. Nueva York: Open Road+ Grove/Atlantic.

Christen, Peter, Ranbaduge, Thilina y Schnell, Rainer. (2020). *Linking Sensitive Data. Methods and Techniques for Practical Privacy-Preserving Information Sharing*. Cham: Springer.

Comité Europeo de Protección de Datos. (s. f.). Grupo de Trabajo del artículo 29. Recuperado de: https://edpb.europa.eu/our-work-tools/article-29-working-party_es. (última consulta: 20/10/2021).

Connelly, A. M. (1986). Problems of Interpretation of Article 8 of the European Convention on Human Rights. *International & Comparative Law Quarterly*, *35*(3), 567-593.

Contreras Vásquez, Pablo y Trigo Kramcsák, Pablo. (2019). Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile. *Revista chilena de derecho y tecnología*, *8*(1), 69-106.

Copeland, Jack. (2006). *Colossus, The Secrets of Bletchley Park's Codebreaking Computers*. Oxford: Oxford University Press.

Córdoba Castroverde, Diego y Díez-Picazo Giménez, Ignacio. (2016). Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico.

En *El derecho a la privacidad en un nuevo entorno tecnológico. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional* (pp. 99-122). Madrid: Centro de Estudios Políticos y Constitucionales.

Cortés Martín, José Manuel. (2018). *Avatares del proceso de adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos*. Madrid: Reus.

Costa, Graça, Peris Brines, Nerea y Cervera Navas, Leonardo. (2020). El nuevo capítulo del Supervisor Europeo de Protección de Datos y las novedades del Comité Europeo de Protección de Datos. *La Ley privacidad*, (3), 13.

Costello, Róisín Áine. (2020). Schrems II: Everything is Illuminated? *European Papers-A Journal on Law and Integration*, *2020*(2), 1045-1059.

Cotino Hueso, Lorenzo. (2011). La colisión del derecho a la protección de datos personales y las libertades informativas en la red: pautas generales y particulares de solución. En Lorenzo Cotino Hueso (Ed.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (pp. 386-401). Valencia: Universidad de Valencia.

Cotino Hueso, Lorenzo. (2020). «SyRI, ¿a quién sanciono?» Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020. *La Ley privacidad*, *Abril-juni*(4).

Creemers, Rogier. (2018). China's social credit system: an evolving practice of control. *SSRN papers*, (22 mayo), 1-32. Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792. (última consulta: 20/10/2021).

Criado, Natalia, y Such, Jose M. (2019). Digital discrimination. En *Algorithmic Regulation* (pp. 1-13). OUP.

Cruz Mantilla de los Ríos, Pablo. (2020). Análisis de la configuración jurídica de las Explicaciones de la Carta: Su eficacia interpretativa de los derechos fundamentales. En *Las cláusulas horizontales de la Carta de Derechos Fundamentales de la Unión Europea: Manual de Uso* (pp. 187-199).

da Costa Carballo, Carlos Manuel. (1998). Los orígenes de la informática. *Revista general de información y documentación*, *8*(1), 215-262.

Dalla Corte, Lorenzo. (2020). A right to a rule: On the substance and essence of the fundamental right to personal data protection. En Dara Hallinan, Ronald Leenes, Serge Gutwirth, & Paul De Hert (Eds.), *Data protection and privacy* (pp. 27-58). Oxford: Hart.

Davara Fernández de Marcos, Elena. (2021). La violación de seguridad de datos personales en el Reglamento Europeo de Protección de Datos y en la LOPDGDD: aspectos de interés (Comentario a los arts. 33 y 34 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y*

Garantía de los Derechos Digitales. Vol. 1 (pp. 2115-2136). Cizur Menor (Navarra): Civitas Thomson Reuters.

Davara Rodríguez, Miguel Ángel. (2021). Tratamiento (Comentario al artículo 4.2. RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 591-599). Cizur Menor (Navarra): Civitas Thomson Reuters.

De Gregorio, Giovanni. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*. *19*(1), 41-70.

De las Heras Vives, Luis y De Verda y Beamonte, José Ramón. (2019). Consentimiento de los menores de edad. En Mónica Arenas Ramiro & Alfonso Ortega Giménez (Eds.), *Protección de datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD* (pp. 73-77). Madrid: Sepín.

De Miguel Asensio, Pedro Alberto. (2020). Implicaciones de la declaración de invalidez del Escudo de Privacidad. *La Ley Unión Europea*, (84), 1-5.

De Miguel Beriain, Iñigo y De Lorenzo y Aparici, Ricardo. (2020). *Datos genéticos y relativos a la salud*. Madrid: Francis Lefebvre.

De Miguel Beriain, Iñigo y Diéguez Lucena, Antonio. (2021). ¿Explicar o predecir? *Investigación y Ciencia*, *julio*(538).

De Miguel Beriain, Iñigo y Jove Villares, Daniel. (2021). Is it possible to place limits on the self-determination of your own genetic data? Certainly, and there is an urgent need for it! *Biolaw Journal-Rivista di BioDiritto*, (Special Issue), 209-222.

De Otto y Pardo, Ignacio. (1988). La regulación de los derechos y libertades. La garantía de su contenido esencial en el artículo 53.1 de la Constitución. En Lorenzo Martín-Retortillo & Ignacio de Otto y Pardo (Eds.), *Derechos fundamentales y Constitución* (pp. 95-171). Madrid: Civitas.

De Terwangne, Cécile. (2020). Article 16. Right to rectification. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 469-474). Oviedo: Oxford University Press.

de Tocqueville, Alexis. (s. f.). *La democracia en América*. epublibre.

Delgado Caravilla, Enrique y Puyol Montero, Javier. (2018). *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea*. Valencia: Tirant Lo Blanch.

Determann, Lothar y Gupta, Chetan. (2019). India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the

California Consumer Privacy Act of 2018. *Berkely Journal of International Law*, *37*(3), 481-515.

Dhar, Tripti. (2021). The California Consumer Privacy Act: The ethos, similarities and differences vis-a-vis the General Data Protection Regulation and the road ahead in light of California Privacy Rights Act. *Journal of Data Protection & Privacy*, *4*(2), 170-192.

Dias Venancio, Pedro. (2007). A previsão constitucional da utilização da Informática. *Tékhne - Revista de Estudos Politécnicos*, *V*(8), 243-264.

Díaz-Romeral Gómez, Alberto. (2016). Los códigos de conducta en el reglamento general de protección de datos. En José Luis (dir. .. Piñar Mañas, María Álvarez Caro, & Miguel (coords. .. Recio Gayo (Eds.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 389-412). Madrid: Reus.

Díaz Crego, María. (2005). Los derechos fundamentales en la Unión Europea: de la Carta a la Constitución. *Revista Española de Derecho Constitucional*, *mayo-agost*(74), 139-176.

Díaz Díaz, Efrén. (2016). El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones. *Revista Aranzadi Doctrinal*, (6), 155-190.

Díaz Díaz, Efrén. (2021). El derecho de supresión. El derecho al olvido (Comentario al artículo 17 RGPD y artículo 15 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1561-1604). Cizur Menor (Navarra): Civitas Thomson Reuters.

Domínguez, Pedro. (1996). Acerca del Juramento Hipocrático. *Anales de la Facultad de Medicina*, *57*(1), 65-66.

Dresner, Stewart H. (1994). Panorama de la legislación europea sobre protección de datos personales. *Informática y derecho: Revista iberoamericana de derecho informático*, (6-7), 385-396.

Drozd, Olha y Kirrane, Sabrina. (2020). Privacy CURE: Consent Comprehension Made Easy. En *IFIP International Conference on ICT Systems Security and Privacy Protection* (pp. 124-139). Cham: Springer.

Duaso Calés, Rosario. (2016). Los principios de protección de datos desde el diseño y protección de datos por defecto. En José Luis (dir. .. Piñar Mañas, María Álvarez Caro, & Miguel (coords. .. Recio Gayo (Eds.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 295-320). Madrid: Reus.

Durán Cardo, Belén. (2016). *La figura del responsable en el derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel*. Madrid: Wolters Kluwer.

Durán Cardo, Belén. (2021). Responsable del tratamiento (Comentario al artículo 4.7 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 637-665). Cizur Menor (Navarra): Civitas Thomson Reuters.

Durán Rivacoba, Ramón. (2020). Herencia y Testamento digitales. En Asociación de Profesores de Derecho Civil & Isabel (coord. .. González Pacanowska (Eds.), *Protección de Datos Personales* (pp. 239-305). Valencia: Tirant Lo Blanch.

Echevarría Ezponda, Javier. (1994). *Telépolis*. Barcelona: Destino.

Echevarría Ezponda, Javier. (2000). Democracia y sociedad de la información. *Isegoría: Revista de filosofía moral y política*, (22), 37-58.

Ehrlich, Eugen y Isaacs, Nathan. (1922). The Sociology of Law. *Harvard Law Review*, *36*(2), 130-145. doi:10.2307/1329737

Eliot, Thomas S. (2003). *La unidad de la cultura europea: Notas para una definición de la cultura*. Madrid: Encuentro.

Encabo Vera, Miguel Ángel. (2012). *Derechos de la personalidad*. Madrid: Marcial Pons.

Escajedo San-Epifanio, Leire. (2017). *Tecnologías biométricas, identidad y derechos fundamentales*. Cizur Menor (Navarra): Thomson Reuters-Aranzadi.

Etzioni, Amitai. (2015). A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational. *Brooklyn Law Review*, *80*(4), 1263-1308.

Fabbrini, Federico y Celeste, Edoardo. (2020). EU Data Protection Law between Extraterritoriality and Sovereignty. En Federico Fabbrini, Edoardo Celeste, & John Quinn (Eds.), *Data Protection Beyond Borders : Transatlantic Perspectives on Extraterritoriality and Sovereignty* (1.ª ed., pp. 9-26). Oxford: Hart Publishing. Recuperado de: http://www.bloomsburycollections.com/book/data-protection-beyond-borders-transatlantic-perspectives-on-extraterritoriality-and-sovereignty/ch2-eu-data-protection-law-between-extraterritoriality-and-sovereignty/. (última consulta: 20/10/2021).

Fairen Guillen, Víctor. (1981). Normas y notas sobre el « Ombudsman» de Suecia",. *Revista de Estudios Políticos*, (21), 127-152.

Farkas, Johan, y Schou, Jannick. (2019). *Post-truth, fake news and democracy: Mapping the politics of falsehood*. Nueva york: Routledge.

Farré Tous, Santiago. (2021). El encargado del tratamiento y los contratos de encargado del tratamiento (Comentario al art. 28 RGPD, al art. 33 LOPDGDD y a la Disposición transitoria quinta LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1845-1873). Cizur Menor (Navarra): Civitas Thomson Reuters.

Favaretto, Maddalena, De Clercq, Eva y Elger, Bernice Simone. (2019). Big Data and discrimination: perils, promises and solutions. A systematic review. *Journal of Big Data*, *6*(1), 1-27. doi:10.1186/s40537-019-0177-4

Federman, Heather. (2020). Exploring the California Privacy Rights Act, *67*(11), 10.

Fernández-Samaniego, Javier y Fernández-Longoria, Paula. (2019). El interés legítimo como principio para legitimar el tratamiento de datos. En Artemi Rallo Lombarte (Ed.), *Tratado de Protección de Datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales* (pp. 169-196). Valencia: Tirant Lo Blanch.

Fernández-Samaniego, Javier y Fernández-Longoria, Paula. (2021). Transferencias internacionales de datos mediante garantías adecuadas y excepciones (Comentario a los artículos 46-49 RGPD y a los artículos 41-43, Disposición adicional quinta y Disposición final sexta Cuatro LOPDGDD. En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 2497-2529). Cizur Menor (Navarra): Civitas Thomson Reuters.

Fernández, Carlos B. (2020). Primera sentencia europea que declara ilegal un algoritmo de evaluación de características personales de los ciudadanos. *Ciberderecho. Diario la ley*, (37).

Fernández, Carlos B. (2021). El Comité Europeo de Protección de Datos destaca la necesidad de que el proyecto de Data Governance Act esté alineado con el RGPD. *Ciberderecho. Diario la ley*, (51), online.

Fernández Rozas, José Carlos. (2015). La compleja adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos y las secuelas del Dictamen 2/2013 del Tribunal de Justicia. *La Ley Unión Europea*, (23), 40-56.

Fernández Scagliusi, María de los Angeles. (2018). Las autoridades de control. En Juan Pablo Murga Fernández, María de los Angeles Fernández Scagliusi, & Manuel Espejo Lerdo de Tejada (Eds.), *Protección de datos, responsabilidad activa técnicas de garantía. Curso de «Delegado de Protección de Datos»,*

adaptado a la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (pp. 229-264). Madrid: Reus.

Ferrer Martín de Vidales, Covadonga. (2020). Disposición adicional decimoséptima. Tratamientos de datos de salud. En *Comentarios a la Nueva Ley de Protección de Datos. Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 418-428). Madrid: Dilex.

Ferrer, X., Nuenen, T. v., Such, J. M., Coté, M. y Criado, N. (2021). Bias and Discrimination in AI: A Cross-Disciplinary Perspective. *IEEE Technology and Society Magazine*, *40*(2), 72-80. doi:10.1109/MTS.2021.3056293

Finck, Michèle, y Pallas, Frank. (2020). They who must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

Fiodorova, Anna. (2021). Directiva 2016/680: Hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal. En Víctor Manuel (dir. .. Moreno Catena, María Isabel (dir. .. Romero Pradas, & María Elena (ed. .. Laro González (Eds.), *Nuevos postulados de la cooperación judicial en la Unión Europea: Libro homenaje a la Prof.ª Isabel González Cano* (pp. 709-736). Valencia: Tirant Lo Blanch.

Flaherty, David H. (1989). *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: The University of North Carolina Press.

Foer, Franklin. (2017). *Un mundo sin ideas. La amenaza de las grandes empresas tecnológicsa a nuestra identidad*. Barcelona: Paidós.

Freixes Sanjuán, Teresa. (2007). Protección de datos y globalización. La convención de Prüm. *Revista de derecho constitucional europeo*, (7), 11-20.

Fried, Charles. (1968). Privacy. *The Yale Law Journal*, *77*(3), 475-493.

Fritz, W. Barkley. (1996). The Women of ENIAC. *IEEE Annals of the History of Computing*, *18*(3), 13-28.

Frosini, Tommaso Edoardo. (2018). Internet y Democracia. *Revista de Derecho Constitucional Europeo*, (30).

Fukuta, Yasunori, Murata, Kiyoshi y Orito, Yohko. (2020). Perceived Risk and Desired Protection: Toward a comprehensive understanding of data sensitivity. En Jorge Pelegrín-Borondo, Mario Arias-Oliva, Kiyoshi Murata, & Ana María Lara Palma (Eds.), *Paradigm Shifts in ICT Ethics. Proceedings of the Ethicomp 2020* (pp. 375-378). Logroño: Universidad de la Rioja y Universidad Rovira i Virgili.

Gacitúa Espósito, Alejandro Luis. (2014). *El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea. (En busca del equilibrio entre la libertad y la seguridad)*. Universidad Autónoma de Barcelona.

Galán Muñoz, Alfonso. (2015). La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos : hacia una nueva orientación de la política criminal de la Unión Europea. En Ignacio (dir. .. Colomer Hernández & Sabela (coord. .. Oubiña Barbolla (Eds.), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea* (pp. 37-70). Cizur Menor (Navarra): Aranzadi.

García-Pelayo, Manuel. (1984). *Derecho constitucional comparado*. Madrid: Alianza Editorial.

García del Poyo Vizcaya, Rafael. (2021). Las obligaciones generales del encargado del tratamiento (Comentario al artículo 28 RGPD y al artículo 28 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1875-1898). Cizur Menor (Navarra): Civitas Thomson Reuters.

García González, Antonio. (2020). Computación cuántica y aplicaciones. *Revista general de marina*, *278*(4), 635-640.

García Mexía, Pablo. (2016). La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre portección de datos. En José Luis Piñar Mañas, María Álvarez Caro, & Miguel Recio Gayo (Eds.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (pp. 23-34). Madrid: Reus.

García Mexía, Pablo y Perete Ramírez, Carmen. (2018). Internet y el Reglamento General de Protección de Datos. En José López Calvo (Ed.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos: adaptado al Proyecto de Ley orgánica de Protección de Datos de 10 de noviembre de 2017* (pp. 173-193). Madrid: Wolters Kluwer-Bosch.

García Pérez, Rosa María. (2020). Bases jurídicas relevantes del tratamiento de datos personales en la contratación de contenidos y servicios digitales. *Cuadernos de derecho transnacional*, *12*(1), 875-907.

García Sanz, Judit. (2005). El secreto profesional. *Anales de la Facultad de Derecho*, (22), 187-212.

García Sanz, Rosa María. (2019). Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público. *Revista de Estudios Políticos*, *enero-marz*(183), 129-159.

Garriga Domínguez, Ana. (2019). Exactitud de los datos. En Mónica Arenas Ramiro & Alfonso Ortega Giménez (Eds.), *Protección de datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)* (pp. 63-65). Madrid: Sepín.

Garzón Clariana, Gregorio. (1981). La protección de datos y la función normativa del Consejo de Europa. *Revista de Instituciones Europeas*, *8*(1), 9-25.

Gascón Marcén, Ana. (2021). El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea. *Cuadernos de Derecho Transnacional*. *13*(2), 209-232.

Gazizov, Andrey, Gazizov, Evgeny y Gazizova, Svetlana. (2020). Theoretical aspects of the protection of personal data of employees of the enterprise by the method of pseudonymization. *E3S Web of Conferences*, *210*(11001), 1-8.

Gellman, Robert. (2019). Fair Information Practices: A Basic History, 1-51. Recuperado de: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf. (última consulta: 20/10/2021).

Georgieva, Ludmila. (2020). Article 11. Proccesing which does not require identification. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 391-397). Oxford: Oxford University Press.

Georgieva, Ludmila y Kuner, Christopher. (2020). Article 9. Processing of special categories of personal data. En Christopher Kuner, Lee A. Bygrave, Christopher Docksey, & Laura Dreschler (Eds.), *The EU General Data Protection Regulation: A Commentary* (pp. 365-384). Oxford: Oxford University Press.

Gidney, Craig y Ekerå, Martin. (2019). *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits* (No. arXiv:1905.09749v2). Nueva york. Recuperado de: https://arxiv.org/abs/1905.09749. (última consulta: 20/10/2021).

Gil de Zúñiga, Homero, Veenstra, Aaron, Vraga, Emily y Shah, Dhavan. (2010). Digital Democracy: Reimagining Pathways to Political Participation. *Journal of Information Technology & Politics*, *7*(1), 36-51. doi:10.1080/19331680903316742

Gil González, Elena. (2016). *Big data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos.

Gil González, Elena y De Hert, Paul Papakonstantinou, Vagelis. (2020). The Proposed ePrivacy Regulation: The Commission's and the Parliament's Draft s at a Crossroads? En Dara Hallinan, Ronald Leenes, Serge Gutwirth, & Paul De Hert (Eds.), *Data Protection and Privacy. Data Protection and*

Democracy (pp. 267-298). Oxford-Londres-New York-New Delhi-Sydney: Hart Publishing.

Gil González, Elena y de Hert, Paul. (2019). Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. *Era Forum*, *19*(4), 597-621.

Gill-Pedro, Eduardo. (2019). *EU Law, Fundamental Rights and National Democracy*. Londres-Nueva York: Routledge.

Gillis, Talia B. y Spiess, Jann L. (2019). Big Data and Discrimination. *The University of Chicago Law Review*, *86*(2), 459-488.

Ginebra Molins, María Esperança. (2021). La [des]protección de los datos personales de las personas fallecidas. En Joaquín Ataz López & José Antonio Cobacho Gómez (Eds.), *Cuestiones clásicas y actuales del Derecho de daños: Estudios en Homenaje al Profesor Dr. Roca Guillamón. Vol. 2* (pp. 1111-1134). Cizur Menor (Navarra): Aranzadi Thomson Reuters.

Girka, Anastasiia, Terziyan, Vagan, Gavriushenko, Mariia y Gontarenko, Andrii. Anonymization as homeomorphic data space transformation for privacy-preserving deep learning. *Procedia Computer Science*, *180*, 867-876.

Glancy, Dorothy J. (1979). The Invention of the Right to Privacy. *Arizona Law Review*, *21*(1), 1-41. Recuperado de: http://digitalcommons.law.scu.edu/facpubs. (Última consulta: 20/10/2021).

Gobeo, Antoni, Fowler, Connor, y Buchanan, William J. (2018). GDPR and Cyber Security for Business Information Systems. En Antoni Gobeo, Connor Fowler, & William J. Buchanan (Eds.), *GDPR and Cyber Security for Business Information Systems* (pp. i-xix). Gistrup, Dinamarca: River Publishers.

Gobierno, Presidencia del. (1983). *Informática. Leyes de Protección de Datos (II)*. Madrid: Servicio Central de Publicaciones.

Goggin, Gerard, Vromen, Ariadne, Weatherall, Kimberlee, Martin, Fiona, y Sunman, Lucy. (2019). Data and digital rights: recent Australian developments. *Internet Policy Review*, *8*(1), 1-20.

Gola, Peter, Schomerus, Rudolf, y Klug, Christoph. (2007). *BDSG: Bundesdatenschutzgesetz*. München: CH Beck.

Goldstine, Herman Heine y Goldstine, Adele. (1946). The Electronic Numerical Integrator and Computer (ENIAC). *Mathematical Tables and Other Aids to Computation*, *2*(15), 97-110.

Gómez Sánchez, Yolanda. (2011). Derecho a no saber (jurídico). En Carlos María Romeo Casabona (Ed.), *Enciclopedia de Bioderecho y Bioética. Tomo I, a-h* (pp. 593-601). Granada: Comares.

González Alonso, Alicia. (2012). *La tutela jurisdiccional de los derechos del artículo 24.1 de la Constitución española*. Universidad Autónoma de Madrid. Recuperado de https://repositorio.uam.es/handle/10486/9207. (Última consulta: 20/10/2021).

González Fuster, Gloria. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1.ª ed.). Springer International Publishing. doi:10.1007/978-3-319-05023-2

González Fuster, Gloria. (2020a). Article 18. Right to restriction of processing. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 484-491). Oxford: Oxford University Press.

González Fuster, Gloria. (2020b). Article 19. Notification oblitgation regarding rectification or erasure of personal data or restriction of processing. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 492-495). Oxford: Oxford University Press.

González Fuster, Gloria y Gellert, Raphaël. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers & Technology*, *26*(1), 73-82. doi:10.1080/13600869.2012.646798

González Fuster, Gloria y Gutwirth, Serge. (2013). Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review*, *29*(5), 531-539.

González, Roberto J. (2017). Hacking the citizenry?: Personality profiling, 'big data' and the election of Donald Trump. *Anthropology Today*, *33*(3), 9-12. doi:https://doi.org/10.1111/1467-8322.12348. (Última consulta: 20/10/2021).

Gonzalo Domenech, Juan José. (2019). Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros. *Cuadernos de derecho transnacional*, *11*(1), 350-371.

Gordillo Pérez, Luis Ignacio. (2020). Las tradiciones constitucionales comunes como principios generales del derecho: evolución y perspectivas tras la constitucionalización de la Carta. En Ana Carmona Contreras (Ed.), *Las cláusulas horizontales de la Carta de Derechos Fundamentales de la Unión Europea: Manual de Uso* (pp. 121-149). Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Gormley, Ken. (1992). One Hundred Years of Privacy. *Wisconsin Law Review*, *1992*(5), 1335-1442.

Granger, Marie Pierre y Irion, Kristina. (2014). The Court of Justice and the data retention directive in Digital Rights Ireland: Telling off the EU legislator and teaching a lesson in privacy and data protection. *European Law Review*, (6), 835-850.

Groves, Austin y Schulte, Paul. (2020). *THE RACE FOR 5G SUPREMACY: Why China Is Surging, Where Millennials Struggle, & How America Can Prevail*. Singapur: World Scientific.

Guamán Hernández, Adoración y Moreno González, Gabriel. (2018). *Empresas transnacionales y Derechos Humanos. La necesidad de un Instrumento Vinculante*. Albacete: Editorial Bomarzo.

Gudín Rodríguez-Magariños, Faustino. (2018). *Nuevo Reglamento Europeo de Protección de Datos versus Big Data*. Valencia: Tirant Lo Blanch.

Guerrero Picó, María del Carmen. (2005). El derecho fundamental a la protección de los datos de carácter personal en la Constitución europea. *Revista de derecho constitucional europeo*, (4), 293-332.

Guerrero Picó, María del Carmen. (2006). *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*. Cizur Menor (Navarra): Aranzadi.

Häberle, Peter. (2001a). *El Estado constitucional*. México, D.F.: Universidad Nacional Autónoma de México.

Häberle, Peter. (2001b). La Jurisdicción Constitucional institucionalizada en el Estado constitucional. *Anuario iberoamericano de justicia constitucional*, (5), 169-182.

Häberle, Peter. (2003). *La libertad fundamental en el estado constitucional*. Granada: Comares.

Häberle, Peter. (2008). El valor de la autonomía como elemento de la cultura constitucional común europea. *Revista de derecho constitucional europeo*, (20), 347-354.

Habermas, Jürgen. (1981). *Historia y crítica de la opinión pública* (2ª.). Barcelona: Gustavo Gili, S.A.

Haenlein, Michael y Kaplan, Andreas. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California management review*, *61*(4), 5-14.

Hajian, Sara, Bonchi, Francesco y Castillo, Carlos. (2016). Algorithmic Bias: From Discrimination Discovery to Fairness-Aware Data Mining. En *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 2125–2126). New York, NY, USA: Association for Computing Machinery. doi:10.1145/2939672.2945386

Hallinan, Dara y de Hert, Paul. (2017). Genetic classes and genetic categories: protecting genetic groups through data protection law. En *Group Privacy* (pp. 175-196). Springer.

Han, Byung-Chul. (2018a). *En el enjambre* (1ª, 8ª imp.). Barcelona: Herder.

Han, Byung-Chul. (2018b). *La sociedad de la transparencia* (1ª, 9ª imp.). Barcelona: Herder.

Han, Byung-Chul. (2019). *La sociedad del cansancio* (2ª, 7ª imp.). Barcelona: Herder.

Harari, Yuval Noah. (2016a). *Homo Deus* (3ª.). Barcelona: Debate-Penguin Rabdom House.

Harari, Yuval Noah. (2016b). *Sapiens: de animales a dioses* (8ª.). Barcelona: Debate.

Harari, Yuval Noah. (2018). *21 lecciones para el siglo XXI*. Barcelona: Debate.

Harari, Yuval Noah. (2020, marzo 20). Yuval Noah Harari: the world after coronavirus. *Financial Times*. Recuperado de: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. (Última consulta: 20/10/2021).

Hart, Herbert L. A. (1997). Post Scriptum (El concepto de derecho). *Estudios Públicos*, (65), 225-263.

Hartzog, Woodrow y Richards, Neil. (2020). Privacy's Constitutional Moment and the Limits of Data Protection. *Boston College Law Review*, *61*(5), 1687-1761.

Hauben, Michael. (2017). History of ARPANET. *Site de l'Instituto Superior de Engenharia do Porto*, *17*, 1-20.

Helberger, Natali y Reyna, Agustin. (2017). The perfect match? A closer look at the relationship between EU consumer law and data protection law. *Common Market Law Review*, *54*(5).

Henderson, Loren, Herring, Cedric, Horton, Hayward Derrick y Thomas, Melvin. (2015). Credit Where Credit is Due?: Race, Gender, and Discrimination in the Credit Scores of Business Startups. *The Review of Black Political Economy*, *42*(4), 459-479.

Henochowicz, Anne, Creemers, Rogier, Gallagher, Mary, Miller, Blake Andrew Phillip y Ruan, Lotus. (2017). Can China's approach to internet control spread around the world? *China File*. Asia Society.

Heredero Higueras, Manuel. (1983). La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población de 1983. *Documentación Administrativa*, *abril-juni*(198), 139-158. Recuperado de: http://dialnet.unirioja.es/servlet/articulo?codigo=220507. (Última consulta: 20/10/2021).

Heredero Higueras, Manuel. (1988a). Nota preliminar. En *Informática. Leyes de protección de datos (III)* (Documentac.). Madrid: Dirección General de Organización, Puestos de Trabajo e Informática.

Heredero Higueras, Manuel. (1996). *La ley orgánica 5/1992, de regulación del tratamiento automatizado de los datos de caracter personal. Comentario y textos*. Madrid: Tecnos.

Heredero Higueras, Manuel. (1997). *La directiva comunitaria de protección de los datos de carácter personal. Comentario a la directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a l*. Cizur Menor (Navarra): Aranzadi.

Heredero Higueras, Manuel. (2001). Estudio crítico de la transposición de la Directiva 95/46/CE en el ordenamiento jurídico español por la L.O. 15/1999 de 13 de diciembre. *Revista jurídica de Navarra*, (31), 123-140.

Heredero Higueras, Manuel (trad. .. (Ed.). (1988b). *Informática. Leyes de protección de datos (III)* (Serie Verd.). Madrid: Dirección General de Organización, Puestos de Trabajo e Informática.

Hernández Llinás, Laura. (2020). Últimas tendencias de un modelo de protección antidiscriminatoria en constante evoluación: El caso J. D. y A. contra Reino Unido. *Anales de Derecho*, (Especial AdD: El TEDH en su sesenta aniversario), 1-26.

Herrán Ortiz, Ana Isabel. (2003). *El derecho a la protección de datos en la sociedad de la información* (Cuadernos.). Bilbao: Universidad de Deusto.

Herrero-Tejedor Algar, Fernando. (1990). *Honor, intimidad y propia imagen*. Madrid: Colex.

Heward-Mills, Dyann y Turku, Helga. (2020). California and the European Union Take the Lead in Data Protection. *Hastings Int'l & comp. Law Rev.*, *43*(2), 319-337.

Hijmans, Hielke. (2006). TheEuropean Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313-1342.

Hildebrandt, Mireille. (2013). Slaves to Big Data. Or Are We? *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, (17), 27-44.

Hildebrandt, Mireille. (2015). *Smart technologies and the End(s) of Law*. Cheltenham, UK-Northampton, Massachusetts: Edward Elgar Publishing.

Hildebrandt, Mireille. (2019). Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. *Theoretical Inquiries in Law*, *20*(1), 83-121.

Hindman, Matthew. (2008). *The Myth of Digital Democracy:* . Princeton University Press. doi:doi:10.1515/9781400837496

Hirsch, Dennis D. (2014). The glass house effect: Big Data, the new oil, and the power of analogy. *Maine Law Review*, *66*(2), 373-396.

Hoffman-Riem, Wolfgang. (2018). *Big Data. Desafíos también para el Derecho*. Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Hondius, Frits W. (1975). *Emerging Data Protection in Europe*. Amsterdam: North-Holland Publishing Company.

Hoofnagle, Chris Jay. (2014). The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS). *BERKELEY CENTER FOR LAW & TECHNOLOGY*, (july 15). doi:http://dx.doi.org/10.2139/ssrn.2466418. (Última consulta: 20/10/2021).

Huerta Anguiano, Julio A. (2020). "Naturaleza intrínseca", "contexto" o "finalidad" en la determinación del carácter sensible de los datos personales. *Estudios en derecho a la información*, *julio-dici*(10), 3-31.

Informática. Leyes de Protección de Datos. (1977) (Documentac.). Madrid: Servicio Central de Publicaciones/Secretaría General Técnica. Presidencia del Gobierno.

Iramina, Aline. (2020). RGPD V. LGPD: Adoção estratégica da abordagem responsiva na elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. *Revista de Direito, Estado e Telecomunicações*, *12*(2).

IT, Governance Privacy Team. (2019). *EU General Data Protection Regulation (GDPR). An implementation and compliance guide.* (3ª.). Ely, Cambridgeshire: IT Governance Publishing.

Ježová, Daniela. (2020). PRINCIPLE OF PRIVACY BY DESIGN AND PRIVACY BY DEFAULT. *Regional Law Review*, 127-139.

Jimena Quesada, Luis. (2019). La protección de datos y las personas vulnerables en el Consejo de Europa. En Rosario García Mahamut & Beatriz Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los dere* (pp. 585-608). Valencia: Tirant Lo Blanch.

Jiménez Asensio, Rafael. (2019). *Introducción al nuevo marco normativo de la protección de datos personales en el sector público*. Oñati: IVAP.

Jiménez Campo, Javier. (1987). La garantía constitucional del secreto de las comunicaciones. *Revista española de Derecho constitucional*, *Año 7*(20), 35-82.

Jiménez Campo, Javier. (1999). *Derechos fundamentales. Concepto y garantías*. Madrid: Trotta.

Jove, Daniel. (2017). Datos relativos a la salud y datos genéticos: consecuencias jurídicas de su conceptualización. *Revista Derecho y Salud*, (1), 55-66.

Jove, Daniel. (2018). La protección de datos: un derecho para el entorno digital. En Andrés Iván Dueñas Castrillo, Daniel Fernández Cañueto, & Gabriel Moreno González (Eds.), *Juventud y Constitución. Un estudio de la Constitución española por los jóvenes en su cuarenta aniversario* (pp. 79-102). Zaragoza: Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico.

Jove, Daniel. (2019). Peter Nowak v Data Protection Commissioner: Potential Aftermaths regarding Subjective Annotations in Clinical Records. *European Data Protection Law Review (EDPL)*, *5*(2), 175-183.

Jove, Daniel. (2020). Quo vadis, intimidad? En Antonio Pérez Miras, Germán M. Teruel Lozano, Edoardo C. Raffiotta, María Pia Iadicco, & Carmen Montesinos Padilla (Eds.), *Setenta años de Constitución Italiana y cuarenta años de Constitución Española. Vol. II* (pp. 151-166). Madrid: Centro de Estudios Políticos y Constitucionales y BOE.

Jove Villares, Daniel. (2019). La asistencia sanitaria transfronteriza a la luz del reglamento general de protección de datos. *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada = Law and the human genome review: genetics, biotechnology and advanced medicine*, (Extra 1), 511-523.

Jove Villares, Daniel. (2020). El derecho a la educación digital y su imprescindible fundamento democrático. En *XVIII Congreso de la Asociación de Constitucionalistas de España (ACE)*. Recuperado de: https://www.acoes.es/congreso-xviii/wp-content/uploads/sites/4/2020/03/Mesa__1_Daniel-Jove_El-derecho-a-la-educación-digital-y-su-imprescindible-fundamento-democrático.pdf. (Última consulta: 20/10/2021).

Jove Villares, Daniel. (2021). La inconstitucional habilitación a los partidos políticos para recabar datos sobre opiniones políticas. Comentario a la STC 76/2019, de 22 de mayo. *Revista Española de Derecho Constitucional*, (121), 303-331.

Jung, Gyuwon, Lee, Hyunsoo, Kim, Auk y Lee, Uichin. (2020). Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on

People With COVID-19 in South Korea. *Frontiers in Public Health*, *8*(305), 1-13. doi:10.3389/fpubh.2020.00305

Jurisprudencia Constitucional Extranjera, Núm. 33, IV. (1984). En *Boletín de Jurisprudencia Constitucional* (pp. 126-170).

Kahn, Paul W. (1999). *The cultural study of law*. Chicago: The University of Chicago Press.

Kaminski, Margot E. (2019). The right to explanation, explained. *Berkeley Technology Law Journal*, *34*, 189-218.

Kasirzadeh, Atoosa y Clifford, Damian. (2021). Fairness and Data Protection Impact Assessments. En *AIES '21.* (pp. 1-8). Virtual Event, USA.

Kaufmann, Arthur. (1984). Über den „Wesensgehalt" der Grund- und Menschenrechte. *RSP: Archiv Für Rechts- Und Sozialphilosophie / Archives for Philosophy of Law and Social Philosophy*, *70*(3), 384-399.

Keles, Betul, McCrae, Niall y Grealish, Annmarie. (2020). A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, *25*(1), 79-93.

Kent Jr., Michael B. (2009). Pavesich, Property and Privacy: The Common Origins of Property Rights and Privacy Rights. *Marshall L.J.*, *2*(1), 1-22.

Kerr, Orin S. (2007). Four Models of Fourth Amendment Protection. *Stanford Law Review*, *60*(2), 503-551.

Kistermann, Friedrich W. (1991). The Invention and Development of the Hollerith Punched Card: In Commemoration of the 130th Anniversary of the Birth of Herman Hollerith and for the 100th Anniversary of Large Scale Data Processing. *Annals of the History of Computing*, *13*(3), 245-259.

Kiviat, Barbara. (2019). The moral limits of predictive practices: The case of credit-based insurance scores. *American Sociological Review*, *84*(6), 1134-1158.

Klamert, Marcus. (2019). Article 16. Treaty on the Functioning of the European Union. En Manuel Kellerbauer, Marcus Klamert, & Jonathan Tomkin (Eds.), *Commentary on the EU Treaties and the Charter of Fundamental Rights* (pp. 405-410). Oxford: Oxford University Press.

Kleinberg, Jon, Ludwig, Jens, Mullainathan, Sendhil y Sunstein, Cass R. (2018). Discrimination in the Age of Algorithms. *Journal of Legal Analysis*, *10*, 113-174.

Kokott, Juliene y Sobotta, Christoph. (2013). The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, *3*(4), 222-228.

Koops, Bert-Jaap. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

Kotschy, Waltraut. (2020a). Article 30. Records of proccessing activities. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 616-624). Oxford: Oxford University Press.

Kotschy, Waltraut. (2020b). Article 6 Lawfulness of processing. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR)* (pp. 321-344). Oxford: Oxford University Press.

Kranenborg, Herke. (2014). Commentary to article 8: Protection of Personal Data. En Steve Peers, Tamara Hervey, Jeff Kenner, & Angela Ward (Eds.), *The EU Charter of Fundamental Rights. A Commentary* (pp. 223-266). Oxford, Portland: Hart Publishing.

Kuru, Taner. (2021). Genetic Data: The Achilles' Heel of the GDPR? *European Data Protection Law Review*, *7*(1), 45-58.

La Ley noruega de protección de datos personales (Ley de 9 de junio de 1978, núm. 47). Presentación y Traducción de Manuel Heredero Higueras. (1981). *Documentación Administrativa*, (189).

Lazcoz Moratinos, Guillermo. (2020). Análisis de la propuesta de Reglamento sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas. *IUS ET SCIENTIA*, *6*(2), 26-41. doi:https://doi.org/10.12795/IETSCIENTIA.2020.i02.03. (Última consulta: 20/10/2021).

Lazcoz Moratinos, Guillermo y Castillo Parrilla, José Antonio. (2020). Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI. *Revista chilena de derecho y tecnología*, *9*(1), 207-225.

Lazpita Gurtubay, Maria. (1994). Análisis comparado de las Legislaciones sobre Protección de Datos de los Estados Miembros de la Comunidad Europea. *Informática y Derecho: Revista iberoamericana de derecho informático*, (6-7), 397-420.

Leczykiewicz, Dorota. (2019). The Charter of Fundamental Rights and the EU's Shallow Constitutionalism. En Nick W. Barber, Maria Cahill, & Richard Ekins (Eds.), *The Rise and Fall of the European Constitution* (pp. 125-154). Oxford: Hart.

Linde Paniagua, Enrique. (2008). El ámbito de aplicación el talón de Aquiles de la Carta de los Derechos Fundamentales de la Unión Europea. *Revista de derecho de la Unión Europea*, (15), 27-44.

Litman-Navarro, Kevin. (2019). We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. *The New York Times*. Recuperado de: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html. (Última consulta: 20/10/2021).

Litman, Jessica. (2000). Information Privacy/Information Property. *Stanford Law Review*, *52*(5), 1283-1313.

Llaneza González, Paloma. (2018). Dataísmo, transparencia y protección de datos. En Sara Rodríguez Marín, Alfredo Muñoz García, & Fran Rodríguez Martínez (Eds.), *Aspectos legales de la economía colaborativa y bajo demanda en plataformas digitales* (pp. 199-219). Madrid: Wolters Kluwer.

Llaneza González, Paloma. (2019). *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*. Barcelona: Editoral Planeta-Ediciones Deusto.

Lletget Pizarro, Marcos. (2021). Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado (Comentario al artículo 14 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1381-1416). Cizur Menor (Navarra): Civitas Thomson Reuters.

López Aguilar, Juan Fernando. (2017). La proteccion de datos personales en la más reciente jurisprudencia del TJUE: Los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EUUU. *Teoria y Realidad Constitucional*, (39), 557-581. doi:10.5944/trc.39.2017.19165

López Aguilar, Juan Fernando. (2019). La protección de datos en la UE: El punto de vista del Parlamento Europeo. En Rosario García Mahamut & Beatriz Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales* (pp. 31-55). Valencia: Tirant Lo Blanch.

López Calvo, José. (2017). *Comentarios al Reglamento Europeo de Protección de Datos*. Madrid: Sepín.

López Castillo, Antonio. (2019). Estudio introductorio. En Antonio (dir. .. López Castillo (Ed.), *La Carta de Derechos Fundamentales de la Unión Europea. Diez años de jurisprudencia* (pp. 31-59). Valencia: Tirant Lo Blanch.

Lucas Murillo de la Cueva, Pablo. (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

Lucas Murillo de la Cueva, Pablo. (2003). La Constitución o el derecho a la autodeterminación informativa. *Cuadernos de Derecho Público*, (19-20), 27-44.

Lucas Murillo de la Cueva, Pablo. (2009). La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad. En *El derecho a la autodeterminación informativa* (pp. 11-80). Madrid: Fundación Coloquio Jurídico Europeo.

Lucas Murillo de la Cueva, Pablo. (2021). El objeto del Reglamento General de protección de datos y de la Ley Orgánica de protección de datos personales y garantía de los derechos digitales (Comentario al artículo 1 RGPD y al artículo 1 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 303-324). Cizur Menor (Navarra): Civitas Thomson Reuters.

Lucena-Cid, Isabel-Victoria. (2014). El concepto de la intimidad en los nuevos contextos tecnológicos. En Alfonso Galán Muñoz & Mónica Arribas León (Eds.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación* (pp. 15-54). Valencia: Tirant Lo Blanch.

Luhmann, Niklas. (1996). El concepto de riesgo. En Anthony Giddens, Zigmunt Bauman, Niklas Luhmann, & Ulrich Beck (Eds.), *Las consecuencias perversas de la modernidad* (pp. 123-153). Barcelona: Anthropos.

Lynskey, Orla. (2014). Deconstructing Data Protection: The «Added-Value» of a Right to Data Protection in the EU legal order. *International and Comparative Law Quarterly*, *63*(3), 569-597. doi:10.1017/S0020589314000244

Lynskey, Orla. (2017). The «Europeanisation» of data protection law. *Cambridge Yearbook of European Legal Studies*, *19*, 1-35.

Lynskey, Orla. (2020). Article 8: The Right to Data Protection. En Michal Bobek & Jeremias Adams-Prassl (Eds.), *The EU Charter of Fundamental Rights in the Member States* (pp. 353-369). Oxford: Hart.

Mac Síthigh, Daithí y Siems, Mathias. (2019). The Chinese social credit system: A model for other countries? *The Modern Law Review*, *82*(6), 1034-1071.

Maddox, Thomas M., Rumsfeld, John S., y Payne, Philip R. O. (2019). Questions for artificial intelligence in health care. *Jama*, *321*(1), 31-32.

Madrid Conesa, Fernando. (1984). *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia.

Mangas Martín, Araceli. (2008). Introducción. El Compromiso con los derechos fundamentales. En Araceli (dir. .. Mangas Martín (Ed.), *Carta de los Derechos*

Fundamentales de la Unión Europea. Comentario artículo por artículo (pp. 29-75). Bilbao: Fundación BBVA.

Mangas Martín, Araceli y Liñán Nogueras, Diego J. (2020). *Instituciones y derecho de la Unión Europea* (10ª.). Madrid: Tecnos.

Manokha, Ivan. (2018). The Cambridge analytica scandal contextualized: Platform capital, surveillance, and data as a new 'fictitious commodity. *Cultures et Conflits, 109*(1), 30-59.

Mantelero, Alessandro. (2020). The future of data protection: Gold standard vs. global standard. *Computer Law & Security Review*, *2020*(November), 1-5.

Martín-Retortillo Baquer, Lorenzo. (2010). El sistema europeo de derechos fundamentales tras la entrada en vigor del Tratado de Lisboa. *Anuario jurídico de La Rioja*, (15), 11-98.

Martín y Pérez de Nanclares, José. (2014). Cita con la ambición: el Tribunal de Justicia ante el desafío de la adhesión de la Unión el CEDH. *Revista de Derecho Comunitario Europeo*, *18*(48), 379-399.

Martín y Pérez de Nanclares, José. (2015). El TJUE pierde el rumbo en el Dictamen 2/13 ¿merece todavía la pena la adhesión de la UE al CEDH? *Revista de Derecho Comunitario Europeo*, *19*(52), 825-869.

Martínez Alarcón, María Luz. (2019). Artículo 8. Protección de datos de carácter personal. En Antonio (dir. .. López Castillo (Ed.), *La Carta de Derechos Fundamentales de la Unión Europea. Diez años de jurisprudencia* (pp. 219-260). Valencia: Tirant Lo Blanch.

Martínez de Pisón Cavero, José. (1992). *El derecho a la intimidad en la jurisprudencia constitucional*. Madrid: Civitas.

Martínez López-Sáez, Mónica. (2017a). Los nuevos límites al derecho al olvido en el sistema jurídico de la Unión Europea la difícil conciliación entre las libertades económicas y la protección de datos personales. *Estudios de Deusto: revista de la Universidad de Deusto*, *65*(2), 139-176.

Martínez López-Sáez, Mónica. (2017b). Nuevos perfiles del derecho al olvido en Europa y España. *Anuario de la Facultad de Derecho*, (10), 231-266.

Martínez López-Sáez, Mónica. (2018a). Towards a digital european integration: Constitutionalization of EU law and europeanization of constitutional law in the field of data protection. *Revista de estudios europeos*, (71), 23-37.

Martínez López-Sáez, Mónica. (2018b). *Una revisión del derecho fundamental a la protección de datos de carácter personal: Un reto en clave de diálogo judicial y constitucionalismo multinivel en la Unión Europea*. Valencia: Tirant Lo Blanch.

Martínez López-Sáez, Mónica. (2019). El nuevo derecho a la portabilidad de datos personales a la luz del RGPD y la LOPDGDD ¿Objetivo ambicioso o misión imposible? En Rosario García Mahamut & Beatriz Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales* (pp. 265-286). Valencia: Tirant Lo Blanch.

Martínez López-Sáez, Mónica. (2020). *El encaje constitucional del derecho al olvido en el ordenamiento jurídico estadounidense. Nuevas garantías y reconfiguración de viejas fórmulas jurídicas ante la europeización en materia de protección de datos*. Valencia: Tirant Lo Blanch.

Martínez Martínez, Ricard. (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson-Civitas.

Martínez Martínez, Ricard. (2007). El derecho fundamental a la protección de datos: perspectivas. *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, (5), 47-61.

Martínez Martínez, Ricard. (2014). Privacidad, Estados Unidos y España. Tan lejos, tan cerca. *Telos: Cuadernos de comunicación e innovación*, *febrero-ma*(97), 48-56.

Martínez Martínez, Ricard. (2019a). ¿Derecho al olvido o a borrar la historia? *LOPD y seguridad (Blog)*. Recuperado de: http://lopdyseguridad.es/derecho-al-olvido-o-a-borrar-la-historia/. (Última consulta: 20/10/2021).

Martínez Martínez, Ricard. (2019b). El principio de responsabilidad proactiva y la protección de datos desde el diseño. En Rosario García Mahamut & Beatriz Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los dere* (pp. 311-341). Valencia: Tirant Lo Blanch.

Martínez Martínez, Ricard. (2020). Schrems II. Una breve reflexión desde los derechos fundamentales. *La Ley Privacidad*, (5), 2.

Martínez Martínez, Ricard. (2021a). ¿Proteger o gestionar los datos? *Diario La Ley*, (47).

Martínez Martínez, Ricard. (2021b). El ecosistema normativo del dato. *La Ley Privacidad*, *abril-juni*(8).

Martínez Saura, Fulgencio. (1996). La «llíada» y el «Corpus Hippocraticum». *Espacio, Tiempo y Forma*, (9), 169-193.

Martinón Quintero, Ruth. (2016). Los derechos humanos en la Unión Europea. En especial, el problema de la adhesión de la Unión al Convenio Europeo de

Derechos Humanos. *Revista Europea de Derechos Fundamentales*, (28), 49-71.

Marzal Herce, Gloria. (1996). *Bases de datos personales requisitos para su uso : comentarios a la LORTAD y normativa complementaria*. Bilbao: Deusto.

Mason, Lance E., Krutka, Dan, y Stoddard, Jeremy. (2018). Media literacy, democracy, and the challenge of fake news. *Journal of Media Literacy Education*, *10*(2), 1-10.

Mayer-Schönberger, Viktor y Ramge, Thomas. (2021). *Fuori i Dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*. Milán: Egea.

Mayer, Jonathan, Mutchler, Patrick y Mitchell, John C. (2016). Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences*, *113*(20), 5536-5541.

McCullagh, Karen. (2007). Data sensitivity: Proposals for resolving the conundrum. *J. Int'l Com. L. & Tech.*, *2*(4), 190-201.

Medina Guerrero, Manuel. (2019). Categorías especiales de datos. En Artemi Rallo Lombarte (Ed.), *Tratado de Protección de Datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales* (pp. 251-273). Valencia: Tirant Lo Blanch.

Medina Guerrero, Manuel. (2020). Encuesta sobre la protección de datos personales. *Teoria y Realidad Constitucional*, (46), 15-118.

Medina Guerrero, Manuel. (2021). De algoritmos y otras palabras inquietantes. Recuperado de: https://www.acoes.es/de-algoritmos-y-otras-palabras-inquietantes/. (Última consulta: 22/10/2021).

Merino, Marcos. (2019). Crean un sistema de cifrado «inquebrantable» a prueba de ordenadores cuánticos, basado en el uso de luz para codificar datos. *Genbeta*. Recuperado de: https://www.genbeta.com/seguridad/crean-sistema-cifrado-inquebrantable-a-prueba-ordenadores-cuanticos-basado-uso-luz-para-codificar-datos. (Última consulta: 20/10/2021).

Messner, Claudius. (2012). "Living" Law: Performative, Not Discursive. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *25*(4), 537-552.

Milkaite, Ingrida, y Lievens, Eva. (2019). *The GDPR Child's Age of Consent for Data Processing across the EU – One Year Later*. Gent. Recuperado de: https://biblio.ugent.be/publication/8621651. (Última consulta: 20/10/2021).

Miller, Arthur R. (1969). Personal privacy in the computer age: the challenge of a new technology and information oriented society. *Michigan Law Review*, *67*(6), 1089-1246.

Miller, Arthur R. (1971). *Assault on Privacy: Computers, Data Banks and Dossiers*. Ann Arbor: The University of Michigan Press.

Minero Alejandre, Gemma. (2014). A vueltas con el «derecho al olvido». Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital. *Revista jurídica Universidad Autónoma de Madrid*, (30), 129-155.

Miralles López, Ramón. (2017). Desvinculando datos personales. Seudonimización, desidentificación y anonimización. *I+S: Revista de la Sociedad Española de Informática y Salud*, *abril*(122), 7-9.

Miralles López, Ramón Martín. (2021). Protección de datos desde el diseño y por defecto (Comentario al art. 25 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1813-1818). Cizur Menor (Navarra): Civitas Thomson Reuters.

Miralles López, Ramón Martín. (2021). La evaluación de impacto relativa a la protección de datos (Comentario al artículo 35 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 2137-2162). Cizur Menor (Navarra): Civitas Thomson Reuters.

Missika, Jean-Louis y Verdier, Henri. (2021). La democracia, rehén de los algorítmos. *Agenda Pública*. Recuperado el 20 de septiembre de 2021 de: https://agendapublica.es/la-democracia-rehen-de-los-algoritmos/. (Última consulta: 20/10/2021).

Mogensen, Andreas. (2019). Racial profiling and cumulative injustice. *Philosophy and Phenomenological Research*, *98*(2), 452-477.

Monereo Atienza, Cristina y Monereo Pérez, José Luis. (2012). Prólogo. En Cristina Monereo Atienza & José Luis Monereo Pérez (Eds.), *La Europa de los Derechos. Estudio sistemático de la Carta de los Derechos Fundamentales de la Unión Europea* (pp. XIII-XVIII). Granada: Comares.

Moraes, Thiago Guimarães, Almeida, Eduarda Costa y de Pereira, José Renato Laranjeira. (2020). Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces. *AI and Ethics*, (pre-print), 1-14. doi:10.1007/s43681-020-00014-3

Morgan, Susan. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*, *3*(1), 39-43.

Morozov, Evgeny. (2013). *To save everything, click here. The folly of technological solutionism*. Nueva york: PublicAffairs.

Morrow, Susan. (2019). 50 shades of privacy: Consent and the fallacy that will prevent privacy for all. *Information-age*. Recuperado de: https://www.information-age.com/consent-privacy-gdpr-privacy-by-design-default-123482351/. (Última consulta: 20/10/2021).

Mota Pinto, Paulo y Reis, Raquel. (2006). A protecção da vida privada na jurisprudência do Tribunal Constitucional. En *VIII Conferencia Trilateral* (pp. 1-52). Recuperado de: https://www.tribunalconstitucional.es/es/trilateral/documentosreuniones/30/ponencia portugal 2006.pdf. (Última consulta: 20/10/2021).

Mund, Brian. (2018). Social Media Searches and the Reasonable Expectation of Privacy. *Yale JL & Tech*, *19*(1), 238-273.

Muñoz, Joaquín. (2018). Principios de proteccion de datos: licitud, lealtad, transparencia, minimización, exactitud, integridad y confidencialidad. *Economist & Jurist*, *26*(217), 18-23.

Muñoz Ontier, Joaquín. (2018). Disposiciones Generales (Arts.1-5). En José López Calvo (Ed.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos: adaptado al Proyecto de Ley orgánica de Protección de Datos de 10 de noviembre de 2017* (pp. 335-351). Madrid: Wolters Kluwer-Bosch.

Navarro Ruiz, José Carlos. (1992). Algunas consideraciones sobre la tramitación parlamentaria de la LORTAD. *Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol*, (1), 98-107.

Neiazy, Victoria. (2021). Invalidation of the EU–US Privacy Shield: impact on data protection and data security regarding the transfer of personal data to the United States. *International Cybersecurity Law Review*, *2*(1), 27-35. doi:10.1365/s43439-021-00018-7

Network, US Indigenous Data Sovereignty. (s. f.). Promoting indigenous data sovereignty through decolonizing data and indigenous data governance. *https://usindigenousdata.org/*. (Última consulta: 20/10/2021).

Ni Loideain, Nora. (2016). The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law. *Journal of Internet Law*, *19*(8), 7-14.

Nicolás Jiménez, Pilar. (2006). *La protecciñon jurídica de los datos genéticos de carácter personal*. Bilbao-Granada: Cátedra Interuniversitaria de Derecho y Genoma Humano-Comares.

Nicolás Jiménez, Pilar. (2021). Garantías y excepciones aplicables al tratamiento con fines de investigación biomédica. Reglamento General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de investigación biomédica (Comentario al artícul. En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de*

Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 2 (pp. 3395-3427). Cizur Menor (Navarra): Civitas Thomson Reuters.

Niedermeier, Robert y Mpame, Mario Egbe. (2019). Processing Personal Data under Article 6 (f) of the GDPR: The Concept of Legitimate Interest. *International Journal for Data Protection Officer, Privacy Officer & Privacy Couns.*, *3*(6), 18-28.

Nieto Manibardo, Enrique. (2019). Anonimización, seudonimización y disociación. Tratamiento de los conceptos en la Legislación española. En Federico Bueno de Mata & Irene González Pulido (Eds.), *Fodertics 7.0: estudios sobre derecho digital* (pp. 141-149). Granada: Comares.

Niger, Sergio. (2006). *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*. Padova: CEDAM.

Nimmer, Melville B. (1954). The Right of Publicity. *Law and Contemporary Problems*, *19*(2), 203-223.

Nissenbaum, Helen. (1999). The meaning of anonymity in an information age. *The Information Society*, *15*(2), 141-144.

Norris, Pippa. (2015). Movilización política y redes sociales: El ejemplo de la Primavera Árabe. *Infoamérica: Iberoamerican Communication Review*, (9), 17-36.

Nuñez García, José Leandro. (2019). Responsabilidad y obligaciones del responsable y del encargado del tratamiento. En Artemi Rallo Lombarte (Ed.), *Tratado de Protección de Datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales* (pp. 353-386). Valencia: Tirant Lo Blanch.

Núñez García, José Leandro. (2016). El encargado del tratamiento. En José Luis Piñar Mañas, María Álvarez Caro, & Miguel Recio Gayo (Eds.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 321-334). Madrid: Reus.

Núñez García, José Leandro. (2019). Responsabilidad y obligaciones del responsable y del encargado del tratamiento. En Artemi Rallo Lombarte (Ed.), *Tratado de Protección de Datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales* (pp. 353-386). Valencia: Tirant Lo Blanch.

Obar, Jonathan A. y Oeldorf-Hirsch, Anne. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147.

Ocón García, Juan. (2021). *Derecho fundamental al secreto y las tecnologías avanzadas de comunicación*. Madrid: Centro de Estudios Políticos y Constitucionales.

Ohm, Paul. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, *57*, 1701-1777.

Olsen, Johan P. (2002). The many faces of Europeanization. *JCMS: Journal of Common Market Studies*, *40*(5), 921-952.

Öman, Sören. (2004). Implementing data protection in law. *Scandinavian Studies in Law*, *47*, 389-403.

Orito, Yohko y Murata, Kiyoshi. (2005). Privacy protection in Japan: cultural influence on the universal value. *Electronic proceedings of Ethicomp*, *5*, 1-9.

Ortega Giménez, Alfonso. (2016). Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield. *Revista Lex Mercatoria*, (4), 85-90.

Ortega Giménez, Alfonso. (2021). China aprueba la nueva Ley de Seguridad de Datos (DSL). *Diario La Ley*, (9926).

Ortega y Gasset, José. (1965). *Meditación de la Técnica* (Colección.). Madrid: Espasa-Calpe.

Padín, Alejandro. (2020). Estados Unidos: Nueva ley de protección de datos en California: ¿en la senda del RGPD?. Análisis de la California Consumer Privacy Act (CCPA). *La Ley Privacidad*, (3), 20.

Pajunoja, Lauri Johannes. (2017). *The Data Protection Directive on Police Matters 2016/680 protects privacy: The evolution of EU´s data protection law and its compatibility with the right to privacy*. Helsingfors universitet.

Palma Ortigosa, Adrián. (2018a). Ámbito de aplicación y definiciones del RGPD. En Juan Pablo Murga Fernández, María de los Angeles Fernández Scagliusi, & Manuel Espejo Lerdo de Tejada (Eds.), *Protección de datos, responsabilidad activa técnicas de garantía* (pp. 25-38). Madrid: Reus.

Palma Ortigosa, Adrián. (2018b). Principios relativos al tratamiento de datos personales. En Juan Pablo Murga Fernández, María de los Ángeles Fernández Scagliusi, & Manuel Espejo Lerdo de Tejada (Eds.), *Protección de datos, responsabilidad activa técnicas de garantía. Curso de «Delegado de Protección de Datos», adaptado a la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (pp. 39-49). Madrid: Reus.

Papakonstantinou, Vagelis y De Hert, Paul. (2014). The EDPS as a unique stakeholder in the European data protection landscape, fulfilling the explicit and non-explicit expectations. En *How to Restore Trust? Contributions in*

Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014) (pp. 237-252). Amberes: Intersentia.

Pascua Mateo, Fabio Antonio. (2019). Un nuevo capítulo en la tutela del derecho a la protección de datos personales: Los datos de contenido político. Comentario a la sentencia del Tribunal Constitucional 76/2019, de 29 de mayo, en el recurso de inconstitucionalidad núm. 1405-2019. *Revista de las Cortes Generales*, (106), 549-558.

Pascual Huerta, Pablo. (2016). *La génesis del derecho fundamental a la protección de datos personales*. Universidad Complutense.

Pascual Huerta, Pablo. (2021a). El derecho a la limitación del tratamiento (Comentario al artículo 18 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1605-1632). Cizur Menor (Navarra): Civitas Thomson Reuters.

Pascual Huerta, Pablo. (2021b). El derecho de rectificación (Comentario al artículo 16 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1529-1555). Cizur Menor (Navarra): Civitas Thomson Reuters.

Pascual Huerta, Pablo. (2021c). Obligación de notificación relativa a la rectificación o supresión de datos personales (Comentario al artículo 19 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1635-1653). Cizur Menor (Navarra): Civitas Thomson Reuters.

Passaglia, Paolo. (2018). Privacy e nuovetecnologie, un raporto difficile, il caso emblemático dei social media, tra regole e ricerca di una specificità. En Ascensión Elvira Perales (Ed.), *El derecho a la intimidad* (pp. 205-238). Valencia: Tirant Lo Blanch.

Pavón Pérez, Juan. (2001). La protección de datos personales en el consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales. *Anuario de la Facultad de Derecho*, (19), 235-252.

Pendás, Benigno y Baselga, Pilar. (1995). *El derecho a la intimidad*. Madrid: Civitas.

Pérez-Ugena, María. (2012). Aspectos jurídico-constitucionales de los efectos del desarrollo tecnológico en los menores. En Yolanda Gómez Sánchez, Aurora Gutiérrez Nogueroles, Luis Jimena Quesada, Javier Tajadura Tejada, Pedro Tenorio Sánchez, & Carlos Vidal Prado (Eds.), *Constitución y Democracia:*

Ayer y Hoy. Libro homenaje a Antonio Torres del Moral (pp. 1835-1860). Madrid: Universitas.

Pérez de las Heras, Beatriz. (2008). *El mercado Interior Europeo: las libertades económicas: Las libertades económicas comunitarias: mercancías, personas, servicios y capitales*. *Universidad de Deusto* (2ª, vol. 8.). Bilbao: Universidad de Deusto.

Pérez Luño, Antonio Enrique. (1986). La defensa del ciudadano y la protección de datos. *Revista Vasca de Administración Pública*, *enero-abri*(14), 37-54.

Pérez Luño, Antonio Enrique. (2000). La tutela de la libertad informática en la sociedad globalizada. *Isegoría*, *0*(22), 59-68. doi:10.3989/isegoria.2000.i22.521

Pérez Luño, Antonio Enrique. (2004). *Los derechos fundamentales* (8ª (1ª ed.). Madrid: Tecnos.

Pérez Miras, Jorge. (2018). *El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos*. Universidad de Sevilla. Recuperado de https://idus.us.es/handle/11441/83475. (Última consulta: 20/10/2021).

Perotto, Pier Giorgio. (1995). *Programma 101. L'invenzione del personal computer: Una storia appassionante mai raccontata*. oldcomputers. Recuperado de: http://www.oldcomputers.it/parts/olivetti/programma101/docs/perotto_programma101.pdf. (Última consulta: 20/10/2021).

Petit de Gabriel, Eulalia W. (2020). El abuso de derecho en el artículo 54 de la Carta: Un linezo -casi- en blanco para el desarrollo jurisprudencial. En Ana Carmona Contreras (Ed.), *Las cláusulas horizontales de la Carta de Derechos Fundamentales de la Unión Europea: Manual de Uso* (pp. 223-267). Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Piñar Mañas, José Luis. (2009). Protección de datos: Origen, situación actual y retos de futuro. En Pablo Lucas Murillo de la Cueva & José Luis Piñar Mañas (Eds.), *El derecho a la autodeterminación informativa* (pp. 81-179). Madrid: Fundación Coloquio Jurídico Europeo.

Piñar Mañas, José Luis. (2016a). Introducción. Hacia un modelo europeo de protección de datos. En José Luis Piñar Mañas, María Álvarez Caro, & Miguel Recio Gayo (Eds.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (pp. 15-22). Madrid: Reus.

Piñar Mañas, José Luis. (2016b). Objeto del Reglamento. En José Luis (dir. .. Piñar Mañas, María Álvarez Caro, & Miguel (coords. .. Recio Gayo (Eds.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 51-62). Madrid: Reus.

Plana Arnaldos, Mª Carmen. (2020). Los datos personales como contraprestación. En *Protección de Datos Personales* (pp. 561-618).

Platero Alcón, Alejandro. (2019). La seguridad como elemento clave en el tratamiento de datos personales en Europa. Especial referencia al régimen de responsabilidad civil derivado de las brechas de seguridad. *Lex: Revista de la Facultad de Derecho y Ciencia Política de la Universidad Alas Peruanas*, *17*(23), 55-74.

Platón. (1991). Cratilo, o de la exactitud de las palabras. En Francisco de P. Samaranch (trad.) (Ed.), *Platón. Obras Completas* (2ª. 10ª re., pp. 508-552). Aguilar.

Podstawa, Karolina. (2018). Peter Nowak v Data Protection Commissioner: You Can Access Your Exam Script, Because It Is Personal Data. *European Data Protection Law Review (EDPL)*, *4*(2), 252-259.

Polčák, Radim. (2020). Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 398-412). Oxford: Oxford University Press.

Pollicino, Oreste. (2016). La tutela de la «privacy» digital. El diálogo entre el Tribunal de Justicia de la Unión Europea y las jurisdicciones nacionales. *Revista de estudios políticos*, (173), 195-244.

Polo Roca, Andoni. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, *1*(108), 165-194.

Polo Roca, Andoni. (2021). Datos, datos, datos: El dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos. *Estudios de Deusto*, *69*(1), 211-240.

Poscher, Ralf. (2017). The Right to Data Protection. A No-Right Thesis. En Russell A. Miller (Ed.), *Privacy and power: a transatlantic dialogue in the shadow of the NSA-affair* (pp. 129-141). Cambridge: Cambridge University Press.

Posner, Richard A. (1977). The Right of Privacy. *Georgia Law Review*, *12-primave*(3), 393-422.

Pratamasari, Annisa. (2020). South Korean Hurry-Hurry (빨리 빨리) COVID-19 Strategy: Privacy Concern, No-Lockdown, and Discriminations. *Jurnal Global & Strategis*, *14*(2), 29-48.

Presano, Federica. (2020). GDPR and Children Rights in EU Data Protection Law. *European Journal of Privacy Law & Technologies (EJPLT)*, *2020*, 32-42.

Prieto Hergueta, Julián. (2019). El Reglamento General de Protección de Datos y los códigos de conducta. En Rosario García Mahamut & Beatriz Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales* (pp. 343-368). Valencia: Tirant Lo Blanch.

Prins, Corien. (2006). When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter? *SCRIPTed: A Journal of Law, Technology and Society*, *3*(4), 270-303.

Prosser, William L. (1960). Privacy. *California Law Review*, *48*(3), 383-423.

Puente Escobar, Agustín. (2006). Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal. En *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos)*. Valencia: Tirant Lo Blanch.

Puente Escobar, Agustín. (2019). Principios y licitud del tratamiento. En Artemi Rallo Lombarte (Ed.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 115-168). Valencia: Tirant Lo Blanch.

Purtova, Nadezhda Nickolayevna. (2009). Property rights in personal data: Learning from the American discourse. *Computer Law & Security Review*, *25*(6), 507-521. doi:https://doi.org/10.1016/j.clsr.2009.09.004. (Última consulta: 20/10/2021).

Purtova, Nadezhda Nickolayevna. (2011). *Property rights in personal data: A European perspective*. Oisterwijk, Países Bajos: BOXPress BV.

Purtova, Nadezhda Nickolayevna. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

Quadra-Salcedo Janini, Tomás. (2011). Mercado interior y Directiva de servicios. *Revista catalana de dret públic*, (42), 257-293.

Quadri, Amanullah y Khan, Muhammad Khurram. (2020). The G-War: Race for Technological Supremacy in 5G and 6G The G-War: Race for Technological Supremacy in 5G and 6G. *Global Foundation for Cyber Studies and Research*. Recuperado de: https://www.gfcyber.org/download/policy-brief-february-2020-by-a-quadri-m-k-khan/?wpdmdl=1298&refresh=6135e9afb18aa1630923183. (Última consulta: 20/10/2021).

Queralt Jiménez, Argelia. (2007). Los usos del canon europeo en la jurisprudencia del Tribunal Constitucional una muestra del proceso de armonización

europea en materia de derechos fundamentales. *Teoría y realidad constitucional*, (20), 435-470.

Quintanilla Mendoza, Gabriela. (2020). Legislación, riesgos y retos de los sistemas biométricos. *Revista Chilena de Derecho y Tecnología*, *9*(1), 63-91.

Quintel, Teresa. (2018). Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive. *European Data Protection Law Review*, *4*, 104-109.

Rallo Lombarte, Artemi. (2014). *El derecho al olvido en internet. Google versus España*. Madrid: Centro de Estudios Políticos y Constitucionales.

Rallo Lombarte, Artemi. (2017a). De la 'libertad informática' a la constitucionalización de nuevos derechos digitales (1978-2018). *Revista de Derecho Político*, (100), 639-669.

Rallo Lombarte, Artemi. (2017b). El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet. *Teoria y Realidad Constitucional*, *39*(1), 583-610. doi:10.5944/trc.39.2017.19150

Rallo Lombarte, Artemi. (2018a). El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet. En Ascensión Elvira Perales (Ed.), *El derecho a la intimidad* (pp. 157-191). Valencia: Tirant Lo Blanch.

Rallo Lombarte, Artemi. (2018b). España en la vanguardia de la Protección de Datos: nuevos retos del Reglamento Europeo. En José López Calvo (Ed.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos: adaptado al Proyecto de Ley orgánica de Protección de Datos de 10 de noviembre de 2017* (pp. 75-79). Madrid: Wolters Kluwer-Bosch.

Rallo Lombarte, Artemi. (2019a). Del derecho a la protección de datos a la garantía de nuevos derechos digitales. En Artemi Rallo Lombarte (Ed.), *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 23-52). Valencia: Tirant Lo Blanch.

Rallo Lombarte, Artemi. (2019b). El nuevo derecho de protección de datos. *Revista Española de Derecho Constitucional*, *39*(116), 45-74.

Rallo Lombarte, Artemi, y Díaz Díaz, Efrén. (2014). Caso Google vs. España. Sentencia del TJUE 13 de mayo de 2014. *Actualidad jurídica Aranzadi*, (886), 8-9.

Ramopoulos, Thomas. (2019). Article 39. Treaty on European Union. En Manuel Kellerbauer, Marcus Klamert, & Jonathan Tomkin (Eds.), *Commentary on the EU Treaties and the Charter of Fundamental Rights* (p. 266). Oxford: Oxford University Press.

Rao, Radhika. (2000). Property, Privacy, and the Human Body. *Boston University Law Review*, *80*(2), 359-460.

Rebollo Delgado, Lucrecio. (2005). *El derecho fundamental a la intimidad*. Madrid: Dykinson.

Rebollo Delgado, Lucrecio. (2010). Vida privada y protección de datos: Un acercamiento a la regulación internacional europea y española. En Consuelo Maqueda Abreu & Víctor M. Martínez Bullé Goyri (Eds.), *Derechos Humanos: Temas y problemas* (pp. 263-318). México, D.F.: Instituto de Investigaciones Jurídicas-UNAM.

Rebollo Delgado, Lucrecio. (2014). *Vida privada y protección de datos en la Unión Europea*. Madrid: Dykinson.

Rebollo Delgado, Lucrecio, y Serrano Pérez, Mª Mercedes. (2008). *Introducción a la protección de datos* (2ª.). Madrid: Dykinson.

Rebollo Delgado, Lucrecio, y Zapatero Martín, Pilar. (2019). *Derechos Digitales*. Madrid: Dykinson.

Recuero Linares, Mikel. (2019a). *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado*. Madrid. Recuperado de: https://www.aepd.es/sites/default/files/2020-02/premio-2019-emilio-aced-accesit-mikel-recuero.pdf. (Última consulta: 20/10/2021).

Recuero Linares, Mikel. (2019b). Transferencias internacionales de datos genéticos y datos de salud con fines de investigación. *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada = Law and the human genome review: genetics, biotechnology and advanced medicine*, (Extra 1), 413-433.

Redondo Saceda, Lara. (2021). Las cláusulas de restricción en el Convenio Europeo de Derechos Humanos. *Teoria y Realidad Constitucional*, (47), 469-492.

Remotti Carbonell, José Carlos. (2020). El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal. En Teresa Freixes Sanjuán (Ed.), *Garantías del proceso debido y Unión Europea: implicaciones para los ordenamientos internos* (pp. 21-70). Madrid: Centro de Estudios Políticos y Constitucionales.

Requejo Pagés, Juan Luis. (2016). *El sueño constitucional*. Oviedo: KRK ediciones.

Requena, Miguel. (2017). *La desigualdad ante la muerte: educación y esperanza de vida en España* (No. 006). Barcelona: Centre d'Estudis Demogràfics. Recuperado de: https://ddd.uab.cat/record/174321. (Última consulta: 20/10/2021).

Resta, Eligio. (2008). *Diritto vivente*. Bari, Roma: Laterza.

Rey Martínez, Fernando. (2019). *Derecho Antidiscriminatorio*. Cizur Menor (Navarra): Thomson Reuters-Aranzadi.

Richards, Neil M. (2010). The puzzle of brandeis, privacy, and speech. *Vanderbilt Law Review*, *63*(5), 1295-1352.

Rihawi Pérez, Natalia. (2019). El papel de las redes sociales en la cibercultura: el caso de la" primavera árabe". *Ene*, *16*, 2.

Rodotà, Stefano. (1997). *Tecnopolitica. La democrazia e le nueve tecnologie della comunicazione*. Roma: Laterza.

Rodotà, Stefano. (2009). Data Protection as a Fundamental Right. En Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, & Nouwt Sjaak (Eds.), *Reinventing Data Protection?* (pp. 77-82). Dordrecht: Springer.

Rodotà, Stefano. (2014). *El derecho a tener derechos*. (Traducción de José Manuel Revuelta, Ed.). Trotta.

Rodotà, Stefano. (2019). *Il mondo nella Rete. Quali i diritti, quali i vincoli* (6ª.). Roma: Laterza.

Rodríguez-Izquierdo Serrano, Miryam. (2020). Artículo 51: El ámbito de aplicación de la Carta y su proyección sobre los Estados miembros. En Ana Carmona Contreras (Ed.), *Las cláusulas horizontales de la Carta de Derechos Fundamentales de la Unión Europea: Manual de Uso* (pp. 13-48). Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Rodríguez-Piñero y Bravo-Ferrer, Miguel. (2019). La Carta de Derechos Fundamentales de la Unión Europea, ámbito de aplicación y eficacia. En María Emilia Casas Baamonde, Román Gil Alburquerque, Ignacio García-Perrote Escartín, Adriano Gómez García-Bernal, & Antonio Vicente Sempere Navarro (Eds.), *Derecho Social de la Unión Europea: Aplicación por el Tribunal de Justicia* (pp. 53-75). Madrid: Francis Lefebvre.

Rodríguez Ayuso, Juan Francisco. (2020). La garantía de la privacidad de los menores de edad. *Actualidad jurídica iberoamericana*, (13), 1004-1023.

Rodríguez Lainz, José Luis. (2016). *El secreto de las telecomunicaciones y su interceptación legal*. Madrid: Sepín.

Rojas, Raul. (1997). Konrad Zuse's legacy: the architecture of the Z1 and Z3. *IEEE Annals of the History of Computing*, *19*(2), 5-16.

Romeo Casabona, Carlos María. (2002). La intimidad y los datos de carácter personal como derechos fundamentales y como bienes jurídicos penalmente protegidos. En *Estudios jurídicos en memoria de José María Lidón* (pp. 513-536). Bilbao: Universidad de Deusto.

Romeo Casabona, Carlos María. (2019). Revisión de las categorías jurídicas de la normativa europea ante la tecnología del big data aplicada a la salud. *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, (Número Extraordinario 2019 "Uso de datos clínicos ante nuevos escenarios tecnológicos y científi cos. Oportunidades e implicaciones jurídicas"), 85-127.

Romero Coloma, Aurelia María. (2001). *Honor, intimidad e imagen de las personas famosas*. Madrid: Civitas.

Rosenthal, Edward H. y Werbin, Barry. (2018). A Historical Retrospective on New York ' s Right of Privacy Law : 115 Years of New York Court of Appeals Jurisprudence. *NYSBA Entertainment, Arts and Sports Law Journal*, *29*(3), 35-39.

Rotenberg, Marc. (2001). Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get). *Stanford Technology Law Review*, (2001), 1-34.

Rouvroy, Antoinette. (2016). *"OF DATA AND MEN" FUNDAMENTAL RIGHTS AND FREEDOMS IN A WORLD OF BIG DATA*. Estrasburgo. Recuperado de: https://rm.coe.int/16806a6020. (Última consulta: 20/10/2021).

Rubio Llorente, Francisco. (2002). Mostrar los derechos sin destruir la Unión (Consideraciones sobre la Carta de Derechos Fundamentales de la Unión Europea). *Revista Española de Derecho Constitucional*, *22*(64), 13-52.

Rubio Núñez, Rafael. (2018). Los efectos de la posverdad en la democracia. *Revista de Derecho Político*, (103), 191-228.

Rudolph, Manuel, Feth, Denis y Polst, Svenja. (2018). Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior. En *International Conference on Human-Computer Interaction* (pp. 587-598). Cham: Springer.

Ruhdan, Uzun. (2020). National Interest vs. Online Freedom of Expression: The Discussions of Internet Users on the Blocking of 'Wikipedia'in Turkey. *Üsküdar Üniversitesi İletişim Fakültesi Akademik Dergisi Etkileşim*, (5), 10-22.

Ruipérez Alamillo, Javier. (2005). *El constitucionalismo democrático en los tiempos de la globalización. Reflexiones rousseaunianas en defensa del Estado constitucional democrático y social*. México: Universidad Nacional Autónoma de México.

Ruiz Miguel, Carlos. (1994). *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Madrid: Civitas.

Ruiz Miguel, Carlos. (1995). *La configuracion constitucional del derecho a la intimidad*. Madrid: Tecnos.

Ruiz Miguel, Carlos. (2003). El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea. Análisis crítico. *Revista de Derecho Comunitario Europeo*, *7*(14), 7-43.

Ruiz Tarrías, Susana. (2020). La Sentencia del Tribunal de Justicia de la Unión Europea en el asunto" Schrems II" o cómo los datos personales pueden terminar viajando sin equipaje. *Revista española de derecho europeo*, (76), 111-162.

Ryngaert, Cedric y Taylor, Mistale. (2020). The GDPR as global data protection regulation? *AJIL Unbound*, *114*, 5-9. doi:10.1017/aju.2019.80

Saiz Arnaiz, Alejandro. (2004). El Convenio Europeo de Derechos Humanos y la garantía internacional de los derechos. *Revista del Foro Constitucional Iberoamericano*, *julio sept*(7), 187-226.

Sáiz Peña, Carlos Alberto. (2019). Seguridad de los datos, evaluación de impacto, códigos de conducta y certificación. En Artemi Rallo Lombarte (Ed.), *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 387-430). Valencia: Tirant Lo Blanch.

Salami, Emmanuel. (2017). The impact of directive (EU) 2016/680 on the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movem. *Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of Such Data on the Existing Privacy Regime*, (Febreary 6), 1-19.

Salas Carceller, Antonio. (2014). El concepto de interés público: distinta visión del Tribunal Constitucional y del Tribunal Supremo. *Revista Aranzadi Doctrinal*, (1), 117-123.

Saldaña, María Nieves. (2012). «The right to privacy». La génesis de la protección de la privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Brandeis. *Revista de Derecho Político*, *septiembre*(85), 195-240.

Salinas Alcega, Sergio y Fernández-Rodríguez Fairén, Víctor. (2019). Derecho de la Unión Europea. *Anuario aragonés del gobierno local*, (11), 167-183.

Samuelson, Pamela. (2000). Privacy As Intellectual Property? *Stanford Law Review*, *52*(5), 1125-1173.

Sánchez Bravo, Álvaro A. (1998). *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla: Universidad de Sevilla, Secretariado de Publicaciones.

Sánchez Domingo, María Belén. (2017). La protección de datos personales en el espacio de libertad, seguridad y justicia. especial consideración a las transferencias de datos a terceros países y organizaciones internacionales según la directiva 2016/680. *Revista de estudios europeos*, (69), 17-36.

Sánchez González, María Belén. (2015). *Implicaciones institucionales de la Ley de Protección de Datos*. Universidad de Málaga.

Sánchez Muñoz, Óscar. (2020). *Libros Colecciones Consejo Editorial Novedades Normas Editoriales Revistas Revistas electrónicas Acceso al fondo histórico de revistas Suscripciones y tarifas Publicaciones Digitales Colección Foro Working Papers Otras publicaciones digitales Distribución*. Madrid: Centro de Estudios Políticos y Constitucionales.

Sancho Villa, Diana. (2021). Las decisiones individuales automatizadas, incluida la elaboración de perfiles (Comentario al artículo 22 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1725-1745). Cizur Menor (Navarra): Civitas Thomson Reuters.

Santamaría Ibeas, José Javier. (1994). La LORTAD. Breve análisis de sus antecedentes. *Informática y derecho: Revista iberoamericana de derecho informático*, (4), 261-276.

Santamaría Ramos, Francisco José. (2021a). El derecho a la portabilidad: un nuevo derecho esencial en materia de protección de datos (Comentario al artículo 20 RGPD y al artículo 17 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1655-1680). Cizur Menor (Navarra): Civitas Thomson Reuters.

Santamaría Ramos, Francisco José. (2021b). La designación del delegado de protección de datos (Comentario al artículo 37 RGPD y al artículo 34 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 2237-2265). Cizur Menor (Navarra): Civitas Thomson Reuters.

Santolaya, Pablo. (2014). El derecho a la vida privada y familiar (un contenido notablemente ampliado del derecho a la intimidad). En Javier García Roca & Pablo Santolaya (Eds.), *La Europa de los Derechos: El Convenio Europeo de Derechos Humanos*. Madrid: Centro de Estudios Políticos y Constitucionales.

Santos Morón, María José. (2020). Tratamiento de datos, sujetos implicados, responsabilidad proactiva. En Asociación de Profesores de Derecho Civil &

Isabel (coord. .. González Pacanowska (Eds.), *Protección de Datos Personales* (pp. 23-77). Valencia: Tirant Lo Blanch.

Sarkodie, Samuel Asumadu, Strezov, Vladimir, Jiang, Yijiao y Evans, Tim. (2019). Proximate determinants of particulate matter (PM2.5) emission, mortality and life expectancy in Europe, Central Asia, Australia, Canada and the US. *Science of The Total Environment*, *683*, 489-497. doi:https://doi.org/10.1016/j.scitotenv.2019.05.278. (Última consulta: 20/10/2021).

Sartori, Giovanni. (1998). *Homo Videns. La sociedad teledirigida*. Buenos Aires: Taurus.

Schermer, Bart W., Custers, Bart y van der Hof, Simone. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, *16*(2), 171-182.

Schwalbe, Nina y Wahl, Brian. (2020). Artificial intelligence and the future of global health. *The Lancet*, *395*(10236), 1579-1586.

Schwartz, Bernard. (1993). *A History of the Supreme Court*. Nueva york: Oxford University Press.

Schwartz, Paul M. (2009). Preemption and Privacy. *The Yake Law Journal*, *118*(5), 902-947.

Schwartz, Paul M. y Janger, Edward J. (2006). Notification of data security breaches. *Michigan Law Review*, *105*(5), 913-984.

Schwartz, Paul M. y Solove, Daniel J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, *86*, 1814-1894.

Seaver, Nick. (2019). Captivating algorithms: Recommender systems as traps. *Journal of Material Culture*, *24*(4), 421-436.

Seoane, José-Antonio. (2002a). De la intimidad genética al derecho a la protección de datos genéticos. la protección iusfundamental de los datos genéticos en el derecho español (a propósito de las SSTC 290/2000 y 292/2000, de 30 de noviembre) (Parte I). *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, (16), 71-106.

Seoane, José-Antonio. (2002b). De la intimidad genética al derecho a la protección de datos genéticos. la protección iusfundamental de los datos genéticos en el derecho español (a propósito de las SSTC 290/2000 y 292/2000, de 30 de noviembre) (Parte II). *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, (17), 135-175.

Serra Cristóbal, Rosario. (2021). De falsedades, mentiras y otras técnicas que faltan a la verdad para influir en la opinión pública. *Teoría y Realidad Constitucional*, (47), 199-235.

Serrano Pérez, Mª Mercedes. (2021). Algunos elementos de los códigos de conducta: La autorregulación regulada. *AC Asuntos Constitucionales*, *enero-juni*(0), 151-168.

Shaban-Nejad, Arash, Michalowski, Martin y Buckeridge, David L. (2018). Health intelligence: how artificial intelligence transforms population and personalized health. *Nature Partner Journals*, *1*(1).

Simitis, Spiros. (1990). «Sensitive Daten»: zur Geschichte und Wirkung einer Fiktion. En Ernst Brem, Jean N. Druey, Ernst A. Kramer, & Ivo Schwander (Eds.), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (pp. 469-493). Bern: Stämpfli.

Simitis, Spiros. (1995). From the Market to the Polis: The EU Directive on the Protection of Personal Data. *Iowa Law Review*, *80*(3), 445-470.

Simitis, Spiros. (1999). *Revisiting Sensitive Data*. Estrasburgo. Recuperado de: https://rm.coe.int/09000016806845af. (Última consulta: 20/10/2021).

Simón Castellano, Pere. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*. Hospitalet de Llobregat: Bosch.

Slavin, Aiden. (2021). Digital identification for the vulnerable: continuities across a century of identification technologies. En Emre Eren Korkmaz (Ed.), *Digital Identity, Virtual Borders and Social Media* (pp. 33-51). Cheltenham, UK-Northampton, Massachusetts: Edward Elgar Publishing.

Sobrino García, Itziar. (2020). La invalidez del privacy shield y la supervivencia de las cláusulas contractuales tipo Sentencia del Tribunal de Justicia de 16 de julio de 2020, Asunto C- 311/18: Schrems II. *La Ley Unión Europea*, (84), 1-10.

Solove, Daniel J. (2002). Conceptualizing Privacy, *90*(4), 1087-1155. Recuperado de: https://doi.org/10.15779/Z382H8Q. (Última consulta: 20/10/2021).

Solove, Daniel J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477-560.

Solove, Daniel J. (2007). «I've Got Nothing to Hide» and Other Misunderstandings of Privacy. *San Diego Law Review*, *44*(289), 745-772.

Solove, Daniel J. (2011). *Nothing to Hide. The False Tradeoff between Privacy and Security*. New Haven y Londres: Yale University Press.

Solove, Daniel J., y Schwartz, Paul M. (2018). *Information Privacy Law* (6ª.). Nueva york: Wolters Kluwer Law & Business.

Solozabal Echavarria, Juan José. (2020). *Derechos Fundamentales y forma política*. Madrid: Centro de Estudios Políticos y Constitucionales.

Somaini, Laura. (2020). Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability. *European Data Protection Law Review (EDPL)*, *6*(1), 84-93.

Soriano Arnanz, Alba. (2021a). *Data Protection for the prevention of algorithmic discrimination*. Cizur Menor (Navarra): Thomson Reuters-Aranzadi.

Soriano Arnanz, Alba. (2021b). Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos. *Revista de Derecho Público: Teoría y método*, *3*, 85-127.

Spohr, Dominic. (2017). Fake news and ideological polarization: Filter bubbles and selective exposure on social media. *Business Information Review*, *34*(3), 150-160. doi:10.1177/0266382117722446

Stalla-Bourdillon, Sophie y Knight, Alison. (2016). Anonymous Data v. Personal Data -False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. *Wisconsin International Law Journal*, *34*(2), 284-322.

Steiker, Carol S. (2009). Brandeis in Olmstead: Our Government Is the Potent, the Omnipresent Teacher. *Mississippi Law Journal*, *79*(1), 149-178.

Steinfeld, Nili. (2016). "I agree to the terms and conditions":(How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior*, *55*, 992-1000.

Stengel, Richard. (2021). *Guerras de la información: Cómo perdimos la batalla global contra la desinformación y qué podemos hacer en el futuro*. Barcelona: Roca Editorial.

Stephens-Davidowitz, Seth. (2017). *Everybody lies. Big Data, new data, and what the Internet can tell us about who we really are*. Nueva York: HarperCollins.

Suárez Rubio, Soledad Mª. (2015). *Constitución y privacidad sanitaria*. Valencia: Tirant Lo Blanch.

Sulston, John. (2002). Intellectual Property and the Human Genome. En Peter Drahos & Ruth Mayne (Eds.), *Global Intellectual Property Rights* (pp. 61-73). Londres: Palgrave.

Sweeney, Latanya. (2000). *Simple Demographics Often Identify People Uniquely* (No. 3). Pittsburgh.

Tajadura Tejada, Javier. (2010). Derechos fundamentales e integración europea. *Estudios de Deusto: revista de la Universidad de Deusto*, *58*(1), 265-286.

Teague, Vanessa. (2021). Which E-Voting Problems Do We Need to Solve? En *Annual International Cryptology Conference* (pp. 3-7). Cham: Springer.

Tene, Omer y Polonetsky, Jules. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*(5), 239-273.

Teruel Lozano, Germán M. (2016). Perspectivas de los derechos fundamentales en la sociedad digital. *Fundamentos: Cuadernos monográficos de Teoría del estado, Derecho público e Historia constitucional*, (9), 215-243.

Tjong Tjin Tai, Eric. (2018). Data ownership and consumer protection. *Journal of European Consumer and Market Law = EuCML*, *7*(4), 136-140.

Todoruţ, Amalia Venera y Tselentis, Vasileios. (2018). Digital technologies and the modernization of public administration. *Quality-Access to Success*, *19*(165), 73-78.

Tomás Mallén, Beatriz. (2019). Las sinergias entre el Reglamento General de Protección de Datos de la Unión Europea y el Convenio 108+ del Consejo de Europa. En Rosario García Mahamut & Beatriz Romás Mallén (Eds.), *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los dere* (pp. 57-90). Valencia: Tirant Lo Blanch.

Toniatti, Roberto. (1991). Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada. *Revista Vasca de Administración Pública*, (29), 139-164.

Tosoni, Luca y Bygrave, Lee A. (2020). Article 4 (2). Processing. En Christopher Kuner, Lee A. Bygrave, Christopher Docksey, & Laura Drechsler (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 116-121). Oxford: Oxford University Press.

Tracol, Xavier. (2020). "Schrems II": The return of the Privacy Shield. *Computer Law & Security Review*, *39*, 1-11. doi:https://doi.org/10.1016/j.clsr.2020.105484. (Última consulta: 20/10/2021).

Trigo Aranda, Vicente. (2004). Historia y evolución de Internet. *Manual formativo de ACTA*, (33), 22-32.

Trinidad, Valentín. (2018). Del caso «Google Spain» al Reglamento Europeo de protección de datos. El derecho al olvido digital contra los motores de búsqueda. *Boletín del Colegio de Registradores de España*, (55).

Troncoso Reigada, Antonio. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant Lo Blanch.

Troncoso Reigada, Antonio. (2012). Hacia un nuevo marco jurídico europeo de la protección de datos personales. *Revista Española de Derecho Europeo*, (43), 25-184.

Troncoso Reigada, Antonio. (2018). Investigación, Salud Pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, (49), 187-266.

Troncoso Reigada, Antonio. (2021a). Las categorías especiales de datos personales y los tratamientos de datos de salud (Comentario al artículo 9 RGPD y a la Disposición adicional decimoséptima de la LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 2* (pp. 4623-4727). Cizur Menor (Navarra): Civitas Thomson Reuters.

Troncoso Reigada, Antonio. (2021b). Los principios relativos al tratamiento (Comentario al artículo 5 RGPD y al artículo 4 LOPDGDD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Volumen 1* (pp. 847-907). Cizur Menor (Navarra): Civitas Thomson Reuters.

Trotter, J. K. (2014). Public NYC Taxicab Database Lets You See How Celebrities Tip. *Gawker*. Recuperado de: https://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546. (Última consulta: 20/10/2021).

Turing, Alan M. (1937). On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, *s2-42*(1), 230-365.

Tussman, Jospeh y TenBroek, Jacobus. (1949). The equal protection of the laws. *California Law Review*, *37*(3), 341-381.

Tzanou, Maria. (2013). Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not so New Right. *International Data Privacy Law*, *3*(2), 88-99.

Urbaneja Cillán, Jorge, Ferrer Lloret, Jaume, Soler García, Carolina y Requena Casanova, Millán. (2020). *Introducción al Derecho de la Unión Europea*. (Jaume Ferrer Lloret, Ed.). Valencia: Tirant Lo Blanch.

Usero Sánchez, María Belén y Fernández, Zulima. (2006). La competencia dinámica entre pioneros y seguidores. Aplicación al sector de la telefonía móvil en Europa. *Cuadernos de Economía y Dirección de la Empresa*, (27), 85-113.

Valero Torrijos, Julián. (2013). *Derecho, Innovación y Administración electrónica*. Sevilla: Global Law Press-Editorial de Derecho Global.

van der Sloot, Bart. (2020). The quality of law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases. *Journal of Intellectual Property, Information Technology and E-Commerce Law: JIPITEC*, *11*(2), 160-185.

Van der Sloot, Bart. (2017). Legal Fundamentalism: Is Data Protection Really a Fundamental Right? En Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, & Paul De Hert (Eds.), *Data Protection and Privacy: (In)visibilities and Infrastructures* (pp. 3-30). Cham: Springer.

van der Sloot, Bart y van Schendel, Sascha. (2016). Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study. *JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law*, *7*(2), 110-145.

Van Outrive, Lode. (2001). Historia del Acuerdo y del Convenio de Schengen. *Revista CIDOB d'afers internacionals*, (53), 43-61.

Vander Maelen, Carl. (2021). First of Many? First GDPR Transnational Code of Conduct Officially Approved After EDPB Opinions 16/2021 and 17/2021. *European Data Protection Law Review*, *7*(2), 228-231.

Veale, Michael y Zuiderveen Borgesius, Frederik. (2021). Demystifying the Draft EU Artificial Intelligence Act. *SocArXiv Papers*, (6 julio), 1-27.

Vicario, Ignacio. (2004). *Nombres, referencia y valor cognoscitivo*. Universidad de Barcelona. Recuperado de https://www.tdx.cat/handle/10803/2098. (Última consulta: 20/10/2021).

Vidal Domínguez, Ignacio. (2002). El secreto profesional ante el notario. *Ius et Praxis*, *8*(2), 479-517.

Villalobos Guízar, Valeria. (2018). Cambridge Analytica. De la interfaz al régimen. *Revista de la Universidad de México*, (5), 131-135.

Villaverde Menédez, Ignacio. (1994). Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993. *Revista Española de Derecho Constitucional*, *mayo-agost*(41), 187-224.

Villaverde Menéndez, Ignacio. (2013). La intimidad, ese "terrible derecho" en la era de la confusa publicidad virtual. *Espaço Jurídico: Journal of Law*, *14*(3), 57-72.

Voigt, Paul y von dem Bussche, Axel. (2017). *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing.

Volosevici, Dana. (2019). Child Protection under GDPR. *Jus et Civitas*, *VI*(2), 17-22.

von Bogdandy, Armin, Kottmann, Matthias, Antpöhler, Carlino, Dickschen, Johanna y Hentrei, Simon. (2012). Reverse Solange-Protecting the essence of fundamental rights against EU Member States. *Common Market Law Review*, *49*(2), 489-519.

von Danwitz, Thomas. (2020). Adecuación de la protección garantizada por el Escudo de la Privacidad Unión Europea-Estados Unidos ante la reclamación de una persona física cuyos datos fueron transferidos de la Unión Europea a Estados Unidos. TJ, Gran Sala, S 16 Jul. 2020. Asunto C-311. *La Ley Unión Europea*, (84), 1-4.

von Grafenstein, Maximilian. (2018). *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation*. Baden-Baden: Nomos.

Wachter, Sandra y Mittelstadt, Brent. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, *2019*(2), 494-620.

Wachter, Sandra, Mittelstadt, Brent y Floridi, Luciano. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76-99.

Walters, Robert y Novak, Marko. (2021). Cyber Security, Artificial Intelligence, Data Protection & the Law. Singapur: Springer Nature.

Wang, Min y Jiang, Zuosu. (2017). The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World. *International Journal of Communication*, *11*, 3286–3305.

Wanvik Stenersen, Håvard. (2020). *Anonymization of Health Data. Anonymization Approaches, Data Utility and the GDPR*. University of Oslo. Recuperado de https://www.duo.uio.no/handle/10852/79902?show=full. (Última consulta: 20/10/2021).

Warren, Samuel D. y Brandeis, Louis D. (1890). Right to Privacy. *Harvard Law Review*, *4*(5), 193-220.

Weichert, Thilo. (2017). «Sensitive Daten» revisited. *Datenschutz und Datensicherheit-DuD*, *41*(9), 538-543.

Westin, Alan F. (1967). *Privacy And Freedom*. Nueva York: Athenum.

Wiggers, Kyle. (2021). 'Anonymized' X-ray datasets can reveal patient identities. *VentureBeat*. Recuperado de: https://venturebeat.com/2021/03/17/anonymized-x-ray-datasets-can-

reveal-patient-identities/amp/?__twitter_impression=true. (Última consulta: 20/10/2021).

Wituschek, Joe. (2021). 96% of iPhone users have opted out of app tracking since iOS 14.5 launched. *iMore*. Recuperado de: https://www.imore.com/96-iphone-users-have-opted-out-app-tracking-ios-145-launched. (Última consulta: 20/10/2021).

Wong, Rebecca. (2007). Alternative Approaches to Sensitive Data? *Journal of International Commercial Law and Technology*, *2*, 9-15.

Zabía de la Mata, Juan. (2021). Sobre el deber de información (Comentario al artículo 12 RGPD). En Antonio Troncoso Reigada (Ed.), *Comentario al Reglamento General de Proteción de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. Vol. 1* (pp. 1331-1355). Cizur Menor (Navarra): Civitas Thomson Reuters.

Zanfir-Fortuna, Gabriela. (2020a). Article 13. Information to be provided where personal data are collected from the data subject. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 413-433). Oxford: Oxford University Press.

Zanfir-Fortuna, Gabriela. (2020b). Article 14. Information to be provided where personal data have not been obtained from the data subject. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 434-448). Oxford: Oxford University Press.

Zanfir-Fortuna, Gabriela. (2020c). Article 15. Right of access by the data subject. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 449-468). Oxford: Oxford University Press.

Zanfir-Fortuna, Gabriela. (2020d). Article 21. Right to object. En Christopher Kuner, Lee A. Bygrave, & Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 508-520). Oxford: Oxford University Press.

Zarsky, Tal Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, *47*(4), 995-1020.

Zeidan, Rodrigo, Boechat, Claudio, y Fleury, Angela. (2015). Developing a Sustainability Credit Score System. *Journal of Business Ethics*, *127*(2), 283-296. doi:10.1007/s10551-013-2034-2

Zerón, Agustín. (2011). Biotipos, fenotipos y genotipos.¿ Qué biotipo tenemos. *Educación*, *2*(1), 22-33.

Žliobaite, Indre y Custers, Bart. (2016). Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models. *Artificial Intelligence and Law*, *24*(2), 183-201.

Zoco Zabala, Cristina. (2015). *Nuevas tecnologías y control de als comunicaciones*. Cizur Menor (Navarra): Aranzadi.

Zuboff, Shoshana. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, *30*(1), 75-89.

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

Zuiderveen Borgesius, Frederik. (2017). The breyer case of the court of justice of the european union: Ip addresses and the personal data definition. *European Data Protection Law Review (EDPL)*, *3*(1), 130-137.

Zwenne, Gerrit-Jan. (2013). *Diluted privacy law*. Leiden. Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2488486&download=yes. (Última consulta: 20/10/2021).

JURISPRUDENCIA

TRIBUNAL EUROPEO DERECHOS HUMANOS

- STEDH, asunto relativo a ciertos aspectos del régimen lingüístico en Bélgica, de 23 de julio de 1968
- STEDH, Irlanda c. Reino Unido, de 18 de enero de 1978
- STEDH, Leander contra Suecia, de 26 de marzo de 1987
- STEDH, López Ostra c. España, de 9 de diciembre de1994
- STEDH, Z c. Finlandia, de 25 de febrero de 1997
- STEDH, asunto Fressoz y Roire c. Francia de 21 de enero de 1999
- STEDH, Pretty contra Reino Unido, de 29 de julio de 2002
- STEDH, Peck c. Reino Unido, de 28 de enero de 2003
- STEDH, Sidabras y Džiautas c. Lituania, de 27 de julio de 2004
- STEDH, Bosphorus Airways c. Irlanda, de 30 de junio de 2005
- STEDH, Copland contra Reino Unido, de 3 de abril de 2007
- STEDH, McCann contra Reino Unido, de 13 de mayo de 2008
- STEDH, Liberty y otros contra Reino Unido, de 1 de julio de 2008
- STEDH, K.U. contra Finlandia, de 2 de diciembre de 2008
- STEDH, Karakó c. Hungría, de 28 de abril de 2009
- STEDH, Chapman contra Reino Unido, de 18 enero de 2011
- STEDH, V. C. contra Eslovaquia, de 8 de febrero de 2012
- STEDH, Bărbulescu contra Rumanía, de 12 de enero de 2016
- STEDH, asunto Çam c. Turquía, de 23 de febrero de 2016
- STEDH, asunto G.L. c. Italia, de 10 de septiembre de 2020

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (se incluyen sentencias del TJCE)

- **Sentencias:**
  - STJCE asunto C-29/69, Erich Stauder v City of Ulm, de 12 de noviembre de 1969
  - STJCE asunto C-11/70, Internationale Handelsgesellschaft mbH c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, de 17 de diciembre de 1970 (Solange I)
  - STJCE asunto C-4/73, J. Nold, de 14 de mayo de 1974
  - STJCE asunto 168/84, Bergholz, de 4 de julio de 1985

- STJCE asunto C-69/85, Wünsche Handelsgesellschaft GmbH & Co. c. Federal Republic of Germany, de 5 de marzo de 1986 (Solange II)
- STJCE asuntos acumulados C-465/00, C-138/01 y C-139/01, Rechnungshof c. Osterreichischer Rundfunk, de 20 de mayo de 2003
- STJUE asunto C-112/00, Eugen Schmidberger, Internationale Transporte und Planzüge y Republik Österreich, de12 de junio de 2003
- STJCE asunto C-101/01, Lindqvist, 6 de noviembre de 2003
- STJCE asunto C-524/06, Huber c. Alemania, de 16 de diciembre de 2006
- STJCE asunto C-524/06, Heinz Huber contra Bundesrepublik Deutschland [GS], 16 de diciembre de 2008
- STJCE asunto C-73/07, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy, Satamedia Oy, de 16 de diciembre de 2008
- STJCE asunto C-553/07, Coliege van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer, de 7 de mayo de 2009
- STJUE Comisión c. Alemania. Asunto C-518/07, Comisión c. Alemania, de 9 de marzo de 2010
- STJUE asunto C-28/08, Bavarian Lager, de 29 de junio de 2010
- SSTJUE asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke GbR c. Land Hessen y Eifert v. Land Hessen y Bundesantalt fur Landwirtschaft un Ernahrung, de 9 de noviembre de 2010
- STJUE asunto C-543/09, Deutsche Telekom AG c. Bundesrepublik Deutschland, de 5 de mayo de 2011
- STJUE asuntos acumulados C-468/10 y C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado, 24 de noviembre de 2011
- STJUE asunto C-614/10, Comisión Europea c. Austria, de 16 de octubre de 2012
- STJUE asunto C-473/12, IPI, de 7 de noviembre de 2013
- STJUE asuntos C-293/12 y C-594/12, Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, de 8 de abril de 2014
- STJUE asunto C 131/12, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014
- STJUE asuntos acumulados C-141/12 y C-372/12, YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie; Integratie en Asiel contra M y S, de 17 de julio de 2014

- STJUE asunto C-212/13, František Ryneš c. Úřad pro ochranu osobních údajů, de 11 de diciembre de 2014
- STJUE asunto C-580/13, Coty Germany Gmbh y Stadtsparkasse Magdeburg, de 16 de julio de 2015
- STJUE asunto C-230/14, Weltimmo s.r.o. c. Nemzeti Adatvedelmi es Informacioszabadsag Hatosag, de 1 octubre de 2015
- STJUE, Asunto C-362/14, Maximillian Schrems y Data Protection Commissioner, 6 de octubre de 2015
- STJUE asunto C-582/14, Patrick Breyer contra Bundesrepublik Deutschland, de 19 de octubre de 2016
- STJUE asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB, de 21 de diciembre de 2016
- STJUE C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce y Salvatore Manni, de 9 de marzo de 2017
- STJUE asunto C-13/16, Rīgas Satiksme, de 4 de mayo de 2017
- STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017
- STJUE asunto C-524/15, Menci, de 20 de marzo de 2018
- STJUE asunto C-210/16, Wirtschaftsakademie Schleswig-Holstein, de 5 de junio de 2018
- STJUE asunto C-25/17, Tietosuojavaltuutettu, de 10 de julio de 2018
- STJUE asunto C-40/17, Fashion ID, de 29 de julio de 2019
- STJUE asunto C 507/17, Google LLC y CNIL, de 24 de septiembre de 2019
- STJUE asunto C-311/18, Facebook Ireland & Maximillian Schrems, de 16 de julio de 2020
- STJUE asuntos C-511/18, C-520/18 y C-520/18, La Quadrature du Net y otros, de 6 de octubre de 2020

- **Otros:**

- Conclusiones del Abogado General presentadas el 10 de febrero de 2000, asunto C-369/98, The Queen c. Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher
- Conclusiones de la Abogada General presentadas el 12 de diciembre de 2013, asuntos acumulados C-141/12 y C-372/12, YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie; Integratie en Asiel contra M y S
- Dictamen 2/2013 del Tribunal de Justicia (Pleno), de 18 de diciembre de 2014
- Opinion TJUE 1/15, de 26 de julio de 2017, sobre los acuerdos entre Canadá y la UE

- Conclusiones del Abogado General presentadas el 19 de diciembre de 2018, asunto C-40/17, Fashion ID

TRIBUNAL CONSTITUCIONAL ESPAÑOL

- STC 11/1981, de 8 de abril
- STC 15/1982, 23 de abril
- STC 99/1985, de 5 de noviembre
- STC 254/1993, de 20 de julio
- STC 108/1999, de 14 de junio
- STC 202/1999, de 8 de noviembre
- STC 290/2000, de 30 de noviembre
- STC 292/2000, de 30 de noviembre
- STC 70/2009, de 23 de marzo
- STC 76/2019, de 22 de mayo

JURISPRUDENCIA EXTRANJERA

- **Estados Unidos**
  - Corte Suprema de Georgia en el caso Pavesich v. New England Life Ins. Co. - 122 Ga. 190, 50 S.E. 68 (1905)
  - Tribunal Supremo Olmstead v. United States, 277 U.S. (1928)
  - Hirabayashi v. United States, 320 U.S. 81 (1943)
  - Korematsu v. United States, 323 U.S. 214 (1944)
  - Tribunal Supremo Kovacs v. Cooper, 336 US (1949)
  - Tribunal Supremo Griswold v. Connecticut, 381 US (1965)
  - Tribunal Supremo Warden v. Hayden, 387 US (1967)
  - Tribunal Supremo Katz v. United States, 389 US (1967)
  - Graham v. Richardson, 403 U.S. 365 (1971)
  - Hollingsworth v. Perry, 570 U.S. 693 (2013)
  - Tribunal Supremo Carpenter v. United States, 585 U.S. (2018)

- **Alemania**
  - Sentencia del Tribunal Constitucional Federal Alemán (BVG) sobre la Ley del Censo, de 1983. BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983- 1 BvR 209/83 -, Rn. 1-215, Grunde C, II-1a)

LEGISLACIÓN Y OTROS DOCUMENTOS JURÍDICAMENTE RELEVANTES

UNIÓN EUROPEA

- Tratado Constitutivo de la Comunidad Europea
- Tratado de Ámsterdam, de 2 de octubre de 1997
- Tratado de Lisboa, 13 de diciembre de 2007
- Tratado de Funcionamiento de la Unión Europea
- Tratado de la Unión Europea
- Carta de Derechos Fundamentales de la Unión Europea
- Explicaciones sobre la Carta de los Derechos Fundamentales (2007/C 303/02) de 14 de diciembre de 2007

- Acuerdo de Schengen, de 14 de junio de 1985. Acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985. Diario Oficial n° L 239 de 22/09/2000 p. 0013 – 0018.
- Convenio de aplicación del Acuerdo de Schengen, de 19 de junio de 1990. Convenio Schengen entró en vigor en 1995. Diario Oficial n° L 239 de 22/09/2000 p. 0019 – 0062.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y la libre circulación de esos datos
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)
- Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público
- Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual

- Reglamento (UE, EURATOM) No 1141/2014 del Parlamento Europeo y del Consejo, de 22 de octubre de 2014, sobre el estatuto y la financiación de los partidos políticos europeos y las fundaciones políticas europeas.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en relación con el tratamiento de datos personales por parte de las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento penal delitos o la ejecución de sanciones penales, y sobre la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva 2016/680)
- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018.
- Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea
- Reglamento (UE, Euratom) 2019/493 del Parlamento Europeo y del Consejo, de 25 de marzo de 2019, por el que se modifica el Reglamento (UE, Euratom) n.° 1141/2014 en lo que respecta a un procedimiento de verificación relativo a las infracciones de las normas de protección de los datos personales en el contexto de las elecciones al Parlamento Europeo
- Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales
- Reglamento 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo.
- Reglamento 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816.

- Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público

Propuestas normativas, estrategias y otros documentos relevantes de la UE

- Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión
- Parlamento Europeo emitió una resolución el 21 de enero de 2021 en la que insta a la Comisión a elaborar una propuesta regulatoria que se regule el derecho a la desconexión digital
- Objetivos digitales de la Década Digital de Europa
- Estrategia Digital Europea
- Tratado por el que se instituye una Constitución para Europa
- Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre privacidad y comunicaciones electrónicas)
- Digital Single Market, elemento central de la estrategia europea para el período 2014-2019
- Estrategia Europea de Datos
- Estrategia Europea para la IA. La Comisión presentó, el 25 de abril de 2018, sus planes en relación con el uso de la IA, puede consultarse la Comunicación de la Comisión al Parlamento, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones
- Libro Blanco sobre Inteligencia Artificial: un enfoque europeo orientado a la excelencia y al confianza
- Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial).
- Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas.
- Decisión de ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
- Comunicación de la Comisión al Parlamento Europeo y al Consejo. Orientaciones sobre el Reglamento relativo a un marco para la libre

circulación de datos no personales en la Unión Europea, de 29 de mayo de 2019

- Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea elaboradas por la Comisión.
- Propuesta de Reglamento sobre gobernanza de datos de 25 de noviembre de 2020
- Propuesta de Reglamento del Parlamento y el Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE.
- Propuesta de Reglamento del Parlamento y del Consejo sobre mercados disputables y equitativos en el sector digital(Ley de Mercados Digitales)
- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una estrategia para el Mercado Único Digital de Europa, de 6 de mayo de 2015
- Communication from the Commisión to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World, de 10 de enero de 2017
- Comunicación de la Comisión al Parlamento Europeo y al Consejo acerca de la protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos, de 24 de junio de 2020

CONSEJO DE EUROPA

- Convenio Europeo de Protección de los Derechos Humanos y las Libertades Fundamentales
- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal + Protocolo adicional relativo a las autoridades de control y a los flujos transfronterizos de datos personales, de 8 de noviembre de 2001
- Convenio 108 actualizado, Protocolo de modificación del Convenio 108 (Protocolo CETS nº 223), de 18 de abril de 2018.
- Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
- Recomendación 509 de 31 de enero de 1968 de la Asamblea del Consejo de Europa, *Human rights and modern scientific and technological developments*.
- Resolución del Comité de Ministros del CdE 73(22), de 26 de septiembre de 1973, relativa a la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector privado.

- Resolución del Comité de Ministros del CdE 74(29), de 20 de septiembre de 1974, relativa a la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector público.
- Recomendación 80/3, del Comité de Ministros del Consejo de Europa de 18 de septiembre de 1980, relativa al intercambio de informaciones jurídicas en materia de protección de datos.
- Recomendación 83/10, del Comité de Ministros del Consejo de Europa de 23 de septiembre de 1983, en materia jurídica a los estados miembros relativa a la protección de los datos de carácter personal utilizados con fines de investigación científica y de estadísticas;
- Recomendación 85/20, del Comité de Ministros del Consejo de Europa de 25 de octubre de 1985, en materia jurídica a los estados miembros relativa a la protección de los datos de carácter personal utilizados con fines de marketing directo;
- Recomendación 89/2, del Comité de Ministros del Consejo de Europa, de 18 de enero de 1989, en materia jurídica a los estados miembros sobre la protección de los datos de carácter personal utilizados con fines de empleo;
- Recomendación 90/19, del Comité de Ministros del Consejo de Europa de 13 de septiembre de 1990, en materia jurídica a los estados miembros sobre la protección de los datos de carácter personal utilizados con fines de pago y otras operaciones conexas;
- Recomendación 95/4del Comité de Ministros del Consejo de Europa de 7 de febrero de 1995, en materia jurídica a los estados miembros sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación, en especial con relación a los servicios telefónicos;
- Recomendación 97/5, del Comité de Ministros del Consejo de Europa de 13 de febrero de 1997, relativa a protección de datos médicos; Convenio sobre los Derechos Humanos y la Biomedicina, Oviedo, 4 de abril de 1997 (Convenio de Oviedo).
- Recomendación 15 de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa

INSTRUMENTOS INTERNACIONALES

- Declaración Universal de los Derechos Humanos de 1948
- Pacto Internacional de Derechos Civiles y Políticos (1966)
- Pacto Internacional de Derechos Económicos, Sociales y Culturales, también de 1966
- Convención Americana sobre Derechos Humanos
- Resolución 45/95 de Naciones Unidas, de 14 de diciembre de 1990, en la que se establecen los Principios Rectores para la reglamentación de los ficheros computarizados de Datos Personales.

- Directrices del Consejo de la Organización para la Cooperación y el Desarrollo Económico (en adelante OCDE), sobre protección de la privacidad y el flujo transfronterizo de datos personales, de 23 de septiembre de 1980 + Memoria Explicativa de las Directrices
- Memoria Explicativa de las Directrices del Consejo de la Organización para la Cooperación y el Desarrollo Económico
- Principios rectores para la reglamentación de los ficheros computadorizados de datos personales, adoptados por la Asamblea de las Naciones Unidas por resolución 45/95, de 14 de diciembre de 1990
- Privacy Framework del Foro de Cooperación Económica Asia Pacífico, de noviembre de 2004
- Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el tratamiento de datos de carácter personal (Resolución de Madrid, 5 de noviembre de 2005)

ESPAÑA

- Constitución Española
- Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales (LOPDGDD)

Otros:

- Carta de Derechos Digitales (2021)

OTROS PAÍSES

- Austria:
  - Constitución de Austria
  - *Datenschutzgesetz* de Austria, aprobaba el 18 de octubre de 1978. Publicada en la BGBl. O. Nr. 565/1978, de 28 de noviembre de 1978

- Portugal:
  - Constitución portuguesa de 1976
  - Lei nº 58/2019, de 8 de agosto de 2019

- EEUU:

- Constitución de Estados Unidos
- New York Civil Rights Law
- Act to amend the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in United States currency be reported to the Department of the Treasury, and for other purposes, aprobada el 26 de octubre de 1970 (Fair Credit Reporting Act 1970)
- Equal Credit Opportunity Act de 1974
- The Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552ª)
- Right to Financial Privacy Act of 1978
- *Report of Secretary's Advisory Committee on Automated Personal Data System*
- California Consumer Privacy Act of 2018, especialmente desde su modificación por la California Privacy Rights Act of 2020

o Reino Unido:
- *Privacy: Younger committee's report*, de 6 de junio de 1973
- Data Protection Act de 23 de mayo de 2018

o Alemania:
- Constitución alemana de 1949
- Ley para la protección del mal uso de los datos personales a través de su tratamiento, *Bundesdatenschutzgesetz* (Ley federal de protección de datos). Aprobada el 27 de enero de 1977, no entraría en vigor hasta el 1 de enero de 1978. BGBl. I Nr. 7 S. 201
- *Datenschutzgesetz* (Ley de protección de datos) del *Land* de Hesse, de 12 de octubre de 1970.
- Ley de Renania-Palatinado de 24 de enero de 1974, "Ley contra la utilización abusiva de los datos" *Gesetz gegen mißbräuchliche Datennutzung* (*Landesdatenschutzgesetz -LDatG-*) Vom. 24. Januar 1974, VOBl. RP, 4 de febrero de 1974, Nº. 3, pp. 31-33.
- ley de Mecklemburgo-Pomerania Occidental: Ley para la protección de los ciudadanos en el tratamiento de sus datos. *Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz - DSG M-V) Vom 28. März 2002*)

o Suecia:
- Ley de Datos, *Datalag*, de 11 de mayo de 1973, SFS: 289
- Ley de Datos Personales, de 29 de abril de 1998, *SFS*: 204

o Francia:
- Constitución francesa de 1958

- Ley relativa a la informática, archivos y libertades, Ley n° 78-17 del 6 de enero de 1978.
- Declaración de Derechos del Hombre y del Ciudadano de 1789

- Dinamarca:
  - Leyes nº. 293 y 294, ambas del 8 de junio de 1978

- Italia:
  - Constitución italiana

- Noruega:
  - Ley de 9 de junio de 1978, núm. 47

- Gran Ducado de Luxemburgo:
  - Ley sobre la utilización de datos en tratamientos informáticos, de 1979

- Australia:
  - Privacy Act de 1988. Enmendada en julio de 2020 (Act. Nº. 11, 2020)

- Canadá:
  - La *Personal Information Protection and Electronic Documents Act* de 13 de abril del 2000, ha sido modificada en diversas ocasiones, incluida la modificación de 18 de junio de 2015, por la *Digital Privacy Act*

- Brasil:
  - Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados Pessoais

- India:
  - Personal Data Protection Bill, de 11 de diciembre de 2019

- China:
  - Cyber Security Law of the People's Republic of China
  - Ley para la Protección de la Información personal

GRUPO DE TRABAJO DEL ARTÍCULO 29, EDPB, EDPS, AEPD, ICO

- **GT29:**
  - Recomendación 4/99, de 7 de septiembre de 1999 del GT29, on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights
  - GT29, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», de 26 de febrero de 2010

- Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679
- GT29, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», de 26 de febrero de 2010
- Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679
- Dictamen 03/2013 sobre limitación a la finalidad, de 2 de abril de 2013
- Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, de 4 de abril de 2017
- Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, de 3 de octubre de 2017
- Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 3 de octubre de 2017
- Dictamen sobre algunas cuestiones fundamentales de la Directiva sobre protección de datos en el ámbito penal (UE 2016/680), de 29 de noviembre de 2017
- Dictamen 4/2007, sobre el concepto de datos personales, de 20 de junio de 2007
- Dictamen sobre Datos Genéticos, de 17 de marzo de 2004
- Opinion 05/2014 on Anonymisation Techniques, de 10 de abril de 2014.
- Dictamen 5/2009 sobre las redes sociales en línea, de 12 de junio de 2009
- Dictamen 3/2012, de 27 de abril de 2012, sobre la evolución de las tecnologías biométricas
- Advice paper on special categories of data ("sensitive data") de 20 de abril de 2011

- **Comité Europeo de Protección de Datos**:

- FAQ document on CJEU judgment C-311/18 (Schrems II) elaborado por el Comité Europeo de Protección de datos
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
- EDPB, Directrices 07/2020 sobre los conceptos de responsable y encargado en el RGPD, versión 1.0, adoptada el 2 de septiembre de 2020
- Directrices 1/2019 sobre códigos de conducta y organismos de supervisión con arreglo al Reglamento (UE) 2016/679
- EDPB, Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 4 de mayo de 2020
- Declaración 03/2021, relativa al Reglamento sobre la privacidad y las comunicaciones electrónicas, adoptada el 9 de marzo de 2021

- EDPB y Supervisor Europeo de Protección de datos, Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), de 9 de marzo de 2021

- **AEPD**:
  - Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD
  - 10 malentendidos relacionados con la anonimización
  - 14 equívocos con relación a la identificación y autenticación biométrica

- **ICO**:
  - Guide to the General Data Protection Regulation (GDPR) elaborada por el ICO
  - The Information Commissioner's (United Kingdom) response to A comprehensive approach on personal data protection in the European Union. A Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on 4 November 2010, de 14 de enero de 2011.
  - Proposed new EU General Data Protection Regulation: Article-by-article analysis paper, 12 de febrero de 2013