*Revista de Derecho Civil*
*http://nreg.es/ojs/index.php/RDC*
*ISSN 2341-2216*
*vol. XI, núm. 1 (enero-marzo, 2024)*
*Estudios, pp. 149-194*

# VULNERACIONES AUTOMATIZADAS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y MECANISMOS DE TUTELA[1]

*Paloma de Barrón Arniches*

Profesora contratada doctora
Universidad de Lleida

---

TITLE: *The Right to Personal Data Protection: Automated Violations and Legal Remedies*

RESUMEN: El presente trabajo analiza la vinculación entre las transacciones digitales y el uso de mecanismos automatizados para el tratamiento de los datos personales de los contratantes, mayoritariamente los consumidores. Con especial atención a la relación existente entre el régimen jurídico de protección de los datos personales y el derecho de consumo, porque la cesión de los propios datos para su tratamiento, acordada mediante la emisión del consentimiento, constituye una suerte de contrato de adhesión relativo a la privacidad de una de las partes contratantes. Entre los mecanismos de tutela que ofrece el ordenamiento jurídico, se pone el acento en la relevancia de las acciones de representación para la protección de los intereses colectivos de los usuarios con respecto a su imagen digital y a su privacidad.

ABSTRACT: *This paper analyzes the connection between digital transactions and the use of automated mechanisms for the processing of personal data of the individuals involved, mostly consumers. Special attention is paid to the relationship between data protection and consumer law, as the transfer of personal data for processing through the consent of its owner constitutes a type of adhesion contract. Additionally, emphasis is placed on the relevance of collective judicial actions to achieve real and effective protection of natural persons regarding their digital image and privacy.*

PALABRAS CLAVE: Datos personales, tratamiento automatizado, inteligencia artificial, consentimiento, acciones colectivas.

KEY WORDS: *Personal data, automated processing, AI, consent, collective judicial actions*.



---

[1] Artículo publicado dentro de las actividades del grupo de investigación consolidado de la Generalitat de Catalunya, *Dret privat comparat: fonaments i anàlisi,* nº 2021 SGR 00057. Este trabajo se terminó de redactar en julio de 2023. En la revisión de marzo de 2024 se da razón de los cambios legislativos acaecidos con posterioridad, y se confirman las fuentes consultables por internet.

## 1. INTRODUCCIÓN

La realidad tecnológica que estamos viviendo nos interpela, de nuevo, sobre la privacidad de los individuos. El derecho a la protección de los datos personales ya tiene un recorrido importante y se viene abordando por la doctrina desde hace años y, sin embargo, en nuestros días, las posibilidades que ofrecen los tratamientos automatizados y el empleo de algoritmos e inteligencia artificial han reabierto el debate sobre la eficacia del sistema previsto en el Reglamento General de Protección de Datos[2], y sobre las consecuencias que para el usuario se derivan de una generalizada y evidente pérdida de privacidad.

El objeto de este trabajo es analizar la situación fáctica que se produce como consecuencia de la vinculación entre las transacciones digitales que se realizan en el sector privado y el uso de mecanismos automatizados para el tratamiento de los datos personales por los prestadores de servicios digitales; *mapear* la dinámica de los mercados de datos y el papel que desempeña el consentimiento del sujeto en su configuración; sondear la realidad de las vulneraciones o intromisiones ilegítimas que afectan al derecho a la protección de los propios datos personales, y los cauces para su defensa.

El punto de partida es, por tanto, la situación del ciudadano que realiza cualquier tipo de transacción digital, o es usuario de redes sociales o de páginas web de entretenimiento, información etc., y constata el tratamiento automatizado (cada vez más frecuentemente a través de mecanismos de inteligencia artificial) de sus datos personales en pro, no de sus intereses, sino de los intereses del responsable de dicho tratamiento. Es, en la gran mayoría de los casos, un usuario que clicó en «Aceptar la política de privacidad» presentada por el prestador de servicios digitales[3], que aceptó

[2] 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 sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. En adelante, RGPD.

[3] Entiendo como prestador de servicios digitales tanto a las plataformas o webs de venta directa o que ofrecen al consumidor diferentes servicios digitales (como la banca a distancia, la contratación de seguros, o de viajes, o el acceso a películas o a música etc.), como a las plataformas intermediarias que ponen en contacto a terceros que desempeñan diferentes roles -vendedor y comprador, arrendatario y arrendador etc.-, y también a las redes sociales o motores de búsqueda, en tanto que acceden a información de los ciudadanos puesta en internet por terceros, la ordenan o indexan y la hacen accesible a quien realice una búsqueda mediante los datos de identificación del sujeto. Sobre este panorama social resulta inspiradora la lectura de WAGNER, Gerhard y EIDENMÜLLER, Horst, «Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions», *The University of Chicago Law Review,* Vol. 86 (2019), Nº. 2, pp. 581-609. Consultable en

las cookies de personalización que se le anunciaban al inicio de la navegación, que emitió, por tanto, su consentimiento para el tratamiento de sus datos personales.

El escenario tecnológico actual dificulta enormemente la comprobación de las entidades que llegan a disponer de los datos personales de un usuario, la interrelación entre las mismas, el tipo de datos tratados y cómo estos son compartidos, agregados e indexados. Además, la elaboración de perfiles para, en su caso, la adopción de decisiones automatizadas, es una realidad ampliamente extendida en el sector privado. Todo lo cual se traduce en un importante riesgo asociado para el derecho a la vida privada (y la propia imagen) en el ámbito digital, y para el poder de disposición y control sobre los propios datos personales que corresponde a cada persona física.

Para mostrar la realidad que acabo de describir, esta breve aportación se nutre de los supuestos hallados en la jurisprudencia, pero obviando aquellos en los que el tratamiento de datos personales aparece legitimado por razones diferentes al consentimiento de su titular y que, por tanto, afectan a ámbitos diferentes al de la entrega de bienes y prestación de servicios digitales por parte de las empresas.

Las cuestiones que pretendo destacar son dos. Por una parte, la relación cada vez más estrecha entre la protección de datos y el derecho de consumo y, en segundo lugar, la relevancia que adquieren las acciones de representación en la defensa real y efectiva de los intereses relacionados con la imagen digital y la privacidad de las personas.

## 2. MARCO LEGAL. LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL

### 2.1. *En Europa*

La regulación europea es prolija en materia de datos personales[4], y ha consolidado la condición de la privacidad como un derecho fundamental del individuo. La UE trata de

https://www.jstor.org/stable/pdf/26590566.pdf?refreqid=fastly-default%3A755536924ece88d0cf9478c400a018d0&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&origin=&initiator=search-results&acceptTC=1 (Fecha de la consulta 11.03.2024).

[4] Igual que con respecto a la jurisprudencia, en el marco legal obviaré las normas de protección de la privacidad dictadas en el ámbito de actuación de las autoridades policiales y de justicia penal, así como por los organismos públicos en general.

En lo que afecta al tratamiento de los datos personales de los individuos en el sector privado, a través de la regulación del mercado digital, los derechos de los consumidores y la economía digital, se han dictado en los últimos años, salvo error, las siguientes normas:

- Directiva 2002/58/CE, 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 (pendiente de ser reformada/derogada si se aprueba el Reglamento sobre el respeto de la vida privada y la protección de

fomentar una economía digital basada en los datos y en el desarrollo tecnológico, un espacio común europeo de datos, como un mercado interior en el que los datos pudieran utilizarse independientemente de su ubicación física de almacenamiento en la Unión, eso sí, respetando el Derecho aplicable. Este planteamiento es muy favorable a un rápido desarrollo de las tecnologías de inteligencia artificial y así lo expresa el legislador europeo:

> «El presente Reglamento [se refiere al R. 2022/868] debe tener como objetivo desarrollar en mayor medida el mercado interior digital sin fronteras y una sociedad y economía de los datos centradas en el ser humano, fiables y seguras» [5].

Se pretende desarrollar una economía de los datos que permita prosperar a las empresas europeas, garantizando la neutralidad en el acceso a los datos y su portabilidad e interoperabilidad[6]. En este contexto, la específica normativa europea protectora de la privacidad de los individuos viene a representar el contrapunto a la

---

los datos personales en el sector de las comunicaciones electrónicas, COM/2017/010 final - 2017/0003 (COD)).

- Directiva 2019/2161/UE, de 27 de noviembre de 2019 por la que se modifica la Directiva 93/13/CEE del Consejo y las Directivas 98/6/CE, 2005/29/CE y 2011/83/UE del Parlamento Europeo y del Consejo, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión (las Directivas modificadas, sobre todo la de 1993, también son aplicables a la protección de datos personales).
- Directiva 2019/770/UE, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales.
- Directiva 2020/1828/UE relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE.
- Reglamento 2022/868/UE, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).
- Reglamento 2022/2065/UE, de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE.
- Reglamento 2022/1925/UE de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales, solo aplicable a los grandes intermediarios en línea, prestadores de servicios digitales a los que se denomina «guardianes de acceso» por su actividad de intermediación y su importante presencia en el mercado, cfr. art.3.1). En adelante RMD.
- Reglamento 2023/2854/UE de 13 de diciembre de 2023 sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (el llamado Reglamento de Datos, que no entra en colisión, sino que refuerza y complementa las reglas sobre privacidad contenidas en el RGPD).

[5] Cfr. Considerando 3 del Reglamento 2022/868, que constituye toda una declaración de intenciones respecto al mercado de datos que genera la economía digital.

[6] El pasado 22 de diciembre se publicó el Reglamento 2023/2854, sobre normas armonizadas para un acceso justo a los datos y su utilización, que pretende contribuir al desarrollo de nuevos servicios, en particular en inteligencia artificial, donde se necesitan enormes cantidades de datos para el entrenamiento de algoritmos ya que, sostiene la Comisión, el 80% de los datos recopilados (personales y no personales) no llegan a utilizarse. Cfr. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202302854 (fecha de la consulta 11.03.2024).

tecnología sin límites que propugnan otros mercados como el americano o el asiático. Se entiende que esta política proteccionista ejercerá un efecto llamada en beneficio de las empresas europeas, respetuosas con la exigente normativa de protección de datos de la Unión. Por el contrario, los años transcurridos desde la entrada en vigor del RGPD nos muestran una realidad bien diferente, al menos en dos aspectos. El primero relativo a la percepción del ciudadano sobre una posible mayor garantía en las transacciones digitales realizadas en el entorno de la UE, y el segundo con respecto a la eficiencia de los mecanismos de defensa previstos por el ordenamiento ante las vulneraciones del derecho a la protección de datos[7]. Recordaré a continuación cuál es este marco legal europeo y señalaré, paralelamente, algunos ejemplos de su quiebra.

En primer lugar, el artículo 8 de la Carta de Derechos Fundamentales de la UE[8] -refrendado por el artículo 16 del Tratado de Funcionamiento de la Unión Europea[9]- consagra específicamente el derecho a la protección de los datos personales:

> «Toda persona tiene derecho a la protección de los datos personales que le conciernen. Dichos datos deben procesarse de manera leal para fines específicos y sobre la base del consentimiento de la persona interesada o alguna otra base legítima establecida por la ley. Toda persona tiene derecho a acceder a los datos que se hayan recabado que le conciernen, así como a que se rectifiquen. El cumplimiento de estas normas estará sujeto al control de una autoridad independiente.»

En segundo término, el Reglamento Europeo de Protección de datos es una normativa de aplicación directa en los Estados, una norma de desarrollo de este derecho consagrado como fundamental en Europa. Su objeto es la regulación de la recopilación y procesamiento de los datos personales de cada individuo, y de los tratamientos, automatizados o no, que se lleven a cabo sobre los datos recabados. El mecanismo empleado para ello es la determinación de unos principios básicos en los que se

[7] Como concluye el profesor y eurodiputado Juan Fernando López Aguilar: «Es verdad que corren malos tiempos para la privacidad». Aunque también han de reconocerse algunos «brotes verdes» como el nuevo Marco de Privacidad de Datos UE-EE.UU., adoptado por la Comisión Europea el pasado 10 de julio de 2023, que parece ser una respuesta a los motivos de inquietud puestos de manifiesto por el TJUE (de modo especial en la famosa sentencia *Maximilian Schrems y Data Protection Commissioner*, 6 octubre 2015, asunto C-362/14). Véase LÓPEZ AGUILAR, Juan Fernando, «La protección de datos en la UE: el punto de vista del parlamento europeo», en Rosario García Mahamut y Beatriz Tomás Mallén (edit.), *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,* Tirant lo Blanch, Valencia, 2019, p. 48.

[8] Carta de los Derechos Fundamentales de la Unión Europea «DO»2000, C 364/1.

[9] Tratado de la Unión Europea y Tratado de Funcionamiento de la Unión Europea «DOUE», Z 2010/70002.

asientan el resto de disposiciones relativas a los derechos de los titulares de los datos y a la responsabilidad derivada del tratamiento de los datos. Me centraré en los principios informadores.

2.1.1. Principio de lealtad y transparencia en el tratamiento de los datos de las personas físicas.

Aparece regulado en el art. 5.1.a) RGPD: el sistema de doble capa de protección al titular de los datos mediante la información básica sobre cómo se van a tratar sus datos personales, y una segunda capa consistente en la información completa sobre la política de privacidad de la empresa. Lealtad y transparencia aparecen interconectadas entre sí, y conducen directamente a las obligaciones de información sobre el destino y la utilización que piensa darse a los datos personales recabados en el momento de la celebración de un negocio jurídico. La transparencia del proveedor de internet, de la empresa con respecto al consumidor que solicita el bien o servicio, constituye el presupuesto para el ejercicio por parte de éste, de todos sus derechos, y se desarrolla normativamente en los artículos 12 a 15 RGPD, muy extensos y prolijos, sobre el contenido de la información que el usuario debe recibir. Asimismo, el artículo 15 desarrolla el contenido del derecho de acceso del interesado[10].

La información al usuario es una cuestión nuclear y me referiré a ella por extenso en el siguiente apartado, si bien cabe adelantar ahora la reflexión que surge de una primera lectura de estas disposiciones europeas: es tanto lo que se debe informar, son tan extensas las políticas de privacidad que ordena la norma que se presenten al usuario para su detenida lectura, que uno se pregunta si tal obligación de información, tal y como está formulada por el legislador, no encierra el peligro de conducir, paradójicamente, hacia escenarios de desinformación.

2.1.2. Principio de exactitud y minimización de los datos recabados

Aparece regulado en el art. 5.1.c) y d) RGPD[11]. Los datos serán exactos y, si fuere necesario, actualizados. Si no fuera así, deberá procederse a su rectificación o eliminación. Junto a ello, la minimización significa que únicamente deben requerirse y

[10] Cfr. STJUE 22 junio 2023, asunto C-579/21, (ECLI:EU:C:2023:501) que interpreta el artículo 15 RGPD en el sentido de que toda persona tiene derecho a la información relativa a operaciones de consulta de sus datos personales, y a las fechas y a los fines de estas operaciones, que deberá proporcionarle el responsable del tratamiento. El ejercicio del derecho de acceso es el paso previo y necesario para conocer, en el caso concreto, si se está produciendo o no una vulneración de la privacidad.
[11] En concordancia con el art. 13.2 a) y el art. 14.2 a) RGPD.

obtenerse los datos de la persona física que resulten necesarios en cada caso. Los datos personales tienen que ser los adecuados y pertinentes en relación con las finalidades para las cuales son recabados. Al respecto, hay que considerar que puede precisarse diferente información personal según el tipo de negocio jurídico concertado por vía electrónica de que se trate, por ejemplo, la compraventa de bienes corporales no exige más datos que los meramente identificativos y los necesarios para el pago del precio, mientras que el suministro de contenidos digitales puede implicar la necesidad de recabar más datos para hacer posible el ejercicio continuado de los servicios postventa, o el mantenimiento de la situación de conformidad de los contenidos digitales durante todo el tiempo que se prolongue el suministro (por ejemplo, la localización geográfica del consumidor cuando este dato sea necesario para saber si una aplicación móvil podrá funcionar correctamente, o para poder proporcionar las actualizaciones o reparar el software, si fuera necesario).

Pues bien, la realidad nos muestra que, a través de las cookies y otros mecanismos automatizados, los prestadores de servicios, por regla general, acceden a datos personales adicionales a los estrictamente necesarios para el desarrollo de su actividad, o los emplean para fines diferentes a los estrictamente relacionados con el contrato principal. Ello ocurre por ejemplo, en aquellos casos en que el consumidor abre una cuenta en una red social y facilita un nombre y una dirección de correo electrónico, y estos se utilizan para fines que no son exclusivamente el suministro de los contenidos o servicios digitales, o cuando da su consentimiento para que cualquier material que constituya datos personales, como fotografías o mensajes que cargue, sea tratado por el empresario con fines comerciales[12]. La red social Facebook ha sido protagonista de la sentencia del TJUE de 15 junio 2021[13] porque, mediante cookies, complementos sociales (social plug-ins) y píxeles, recogía información sobre los hábitos de navegación tanto de los poseedores de una cuenta de Facebook como de personas no usuarias de los servicios de Facebook. Estos elementos permiten obtener determinados datos de un internauta que consulta una página web que los contenga, como la dirección de esa página, la «dirección IP» del visitante de dicha página y la fecha y la hora de la consulta en cuestión, todo ello sin solicitar su consentimiento. Esto es lo que la autoridad de control belga solicita a Facebook que cese de hacer, sin éxito, motivo por el cual la propia agencia interpone la acción judicial ante tribunal belga, y exclusivamente para la protección de los internautas de dicha nacionalidad.

[12] En EEUU tuvo mucha repercusión mediática en su día la demanda interpuesta por el fiscal general de Nuevo México contra Google por recopilar datos de estudiantes a través de Chromebooks - The Verge. Consultable en https://www.theverge.com/2020/2/20/21145698/google-student-privacy-lawsuit-education-schools-chromebooks-new-mexico-balderas (Fecha de la consulta 11.03.24).
[13] STJUE 15 junio 2021, asunto C-645/19. TJCE\2021\159.

En nuestro país la Agencia española de Protección de Datos (en adelante, AEPD) ha resuelto muchos casos sobre exceso de datos recabados, como la resolución que afecta a una web de venta de cosméticos en la que, tras la denuncia del usuario sobre su falta de libertad para rechazar las cookies de la página, la Agencia comprueba que, «al entrar en la página principal y sin realizar ninguna acción sobre la mismas ni aceptar las cookies, se utilizaban cookies que no son técnicas o necesarias», es decir, aquellas que precisan un consentimiento explícito del usuario para su validez[14]. Otro supuesto es el de la empresa que capta datos personales del perfil público del usuario en *Linked in* y los emplea para para enviarle publicidad no deseada al correo electrónico. En esta ocasión la AEPD se refiere no solo al RGPD sino también a la Ley de Servicios de la Sociedad de la Información[15], en su artículo 21.1, que prohíbe de forma expresa «el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas»[16].

El principio de minimización de los datos también hace referencia al plazo de tiempo durante el que el prestador de servicios dispondrá de esta información personal. Si no es posible fijar un plazo, sí deberán al menos establecerse los criterios que permitan determinarlo. Pero lo cierto es que, generalmente, el usuario no sabe durante cuánto tiempo se conservará su información personal por el prestador de servicios, y si quiere que sea eliminada, debe ejercer el derecho de supresión dirigiéndose al responsable del tratamiento. De ahí el auge, en los últimos tiempos, del llamado derecho al olvido digital que se identifica con la facultad de la persona de controlar y limitar la difusión de información antigua que afecte a su vida privada, ya sea mediante motores de búsqueda, redes sociales, o medios de comunicación digital.

Así, la primera sentencia española que condenó a una hemeroteca digital (del diario El País) al pago de una indemnización en aplicación del derecho al olvido digital contemplaba el supuesto de una noticia muy antigua que hacía referencia a dos personas perfectamente identificables y que podía encontrarse, en primer lugar, mediante los motores de búsqueda en Internet y, en segundo lugar, mediante el

[14] Cfr. AEPD, EXP202206594, consultable en https://www.aepd.es/es/documento/ps-00315-2022.pdf. (Fecha de la consulta: 11.03.2024).

[15] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico [BOE núm. 166, de 12/07/2002]. En adelante, LSSI.

[16] Cfr. AEPD, EXP202105347, consultable en https://www.aepd.es/es/documento/reposicion-ps-00173-2022.pdf; véase también, AEPD, EXP202201719, consultable en https://www.aepd.es/es/documento/ps-00227-2022.pdf; AEPD, EXP202103886, consultable en https://www.aepd.es/es/documento/ps-00032-2022.pdf; AEPD, EXP202103404, consultable en https://www.aepd.es/es/documento/ai-00031-2022.pdf. (Fecha de la consulta 11.03.24).

buscador interno del propio periódico[17]. Esta situación se debía a que el periódico no solo no había eliminado los datos personales en cuestión, sino que además permitía la indexación por todo tipo de buscadores mediante el llamado código fuente de la página (las instrucciones del lenguaje en el que dicha página estaba escrita). La indexación se permitía activamente, al constar en dicho código los comandos *index* y *follow*, mediante los cuales la página web informa a los buscadores de que pueden copiarla en su caché y seguir buscando otros enlaces a partir de aquélla. El propósito último era lograr un aumento del número de visitas de la web del diario, con el consiguiente eventual aumento de ingresos en concepto de publicidad por los anuncios que aparecen en dichas páginas. El derecho al olvido digital ha quedado vinculado por la doctrina y la jurisprudencia al derecho de oposición, a pesar de que el RGPD lo incardina en el art. 17 como una manifestación del derecho de supresión[18].

2.1.3. Deber de integridad y confidencialidad con respecto a los datos recabados. La cesión de datos a terceros

Aparece regulado en el art. 5.1 f) RGPD. Afecta a responsables y encargados del tratamiento de datos, así como a todas las personas que intervengan en cualquier fase de éste. Configura una obligación general que resulta complementaria de los deberes de secreto profesional que afectan a los empresarios o prestadores de servicios, en función del ámbito de su actividad profesional. La confidencialidad que afecta a los datos recabados también implica la adopción de medidas técnicas y de organización que permitan asegurar la conservación y la no transmisión de estos datos a terceros sin permiso de su titular: la responsabilidad de quien los recaba alcanza la protección contra el tratamiento no autorizado o ilícito por parte de terceros, y contra su pérdida, destrucción o daño accidental.

De nuevo la red social Facebook, esta vez junto con la empresa Fashion ID, protagonizó un trasvase inconsentido de datos, que constituye el caso analizado por la sentencia del TJUE de 29 julio 2019[19]: cuando un visitante consulta el sitio de Internet de Fashion ID, se transmiten a Facebook Ireland automáticamente los datos personales de ese visitante. Esa transmisión se efectúa sin que dicho visitante sea consciente de ello, o

[17] STS 15 octubre 2015, RJ 2015\4417. Véase el comentario de RUDA GONZÁLEZ, Albert, «Indemnización por daños al derecho al olvido. La responsabilidad por la no exclusión de la indexación de una hemeroteca digital por los buscadores generales (Caso El País)», *Cuadernos Civitas de Jurisprudencia Civil* (2016), nº 101, pp. 289-332.

[18] Cfr. SANTOS MORÓN, María José, «Los contornos del derecho al olvido en España. La aplicación por los tribunales españoles de la jurisprudencia europea», *Revista de Derecho Civil,* vol. IX, (2022), nº 2, p. 73.

[19] STJUE 29 julio 2019, asunto C-40/17. ECLI:EU:C: 2019:629.

sea sin otorgar su consentimiento, y con independencia de si es miembro o no de la red social, o de si clicó en el botón «me gusta» de Facebook. Se pregunta al TJUE si Fashion ID puede ser considerado responsable del tratamiento ulterior que Facebook haga de los datos personales recabados en su sitio de internet. Señala el Tribunal de Justicia:

> «[…] puede considerarse, sin perjuicio de las comprobaciones que incumbe efectuar al órgano jurisdiccional remitente, que Fashion ID y Facebook Ireland determinan, conjuntamente, los fines de las operaciones de recogida y de comunicación por transmisión de datos personales de que se trata en el litigio principal […] la responsabilidad del administrador de un sitio de Internet como Fashion ID, respecto del tratamiento de datos personales de esas personas resulta aún mayor, pues la mera consulta de tal sitio, que contiene el botón «me gusta» de Facebook, parece desencadenar el tratamiento de sus datos personales por Facebook Ireland (véase, en este sentido, la sentencia de 5 de junio de 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, apartado 41) […] En consecuencia, resulta que Fashion ID puede ser considerada responsable, en el sentido del artículo 2, letra d), de la Directiva 95/46, conjuntamente con Facebook Ireland, de las operaciones de recogida y de comunicación por transmisión de datos personales de los visitantes de su sitio de Internet».

Como se refleja en este ejemplo, el objetivo de estos trasvases de datos suele ser la publicidad, los fines de mercadotecnia. El trasvase de datos suele realizarse mediante redes de afiliación, que son plataformas que actúan como intermediarios entre los afiliados (creadores de contenido) y los anunciantes (empresas que quieren ser anunciadas). Los anunciantes y los afiliados se ponen en contacto a través de estas plataformas. Y son éstas las que actúan como regulador, al mismo tiempo, para ambos[20]. A través de las redes de afiliación se formalizan contratos entre los prestadores de servicios digitales y las empresas o redes sociales que «alquilan» sus «webs» para usarlas ubicando o remitiendo anuncios a las personas físicas que han celebrado con ellos acuerdos, en virtud de los cuales consienten en recibir publicidad de un sector determinado, sobre todo el financiero, y el de seguros. Esta situación queda regulada, desde 2022 por el Reglamento (RMD), que afecta a las plataformas intermediarias también llamadas «guardianes de acceso»[21]. El Reglamento detecta la ventaja competitiva de los denominados guardianes de acceso, que recogen directamente datos personales de los usuarios finales con el fin de prestar servicios de

[20] Cfr. SAN 19 enero 2023, ECLI:ES:AN:2023:33, por la que se establece que el responsable del tratamiento es la red de afiliación, la plataforma que pone en contacto a las partes, no la empresa que se anuncia, ni la red social en la que se anuncia.

[21] Reglamento 2022/1925, ya reseñado en nota 4. Reproduzco parcialmente los Considerandos 36 y 37, que se refieren a esta cuestión.

publicidad en línea cuando los usuarios finales utilizan sitios web y aplicaciones informáticas de terceros. Pero no solo eso, porque también los terceros facilitan a los guardianes de acceso datos personales de sus usuarios finales para hacer uso de determinados servicios básicos que ofrece la plataforma. Todo ello les proporciona ventajas potenciales en términos de acumulación de datos que perjudica al mercado, dado que tratan datos personales de un número considerablemente mayor de terceros que otras empresas. Así pues, establece el legislador europeo que:

> «Para garantizar que los guardianes de acceso no menoscaben deslealmente la disputabilidad de los servicios básicos de plataforma, dichos guardianes deben permitir que los usuarios finales puedan elegir libremente participar en tales prácticas de tratamiento de datos e inicio de sesión ofreciéndoles una alternativa menos personalizada, aunque equivalente, y sin condicionar el uso del servicio básico de plataforma o de determinadas funcionalidades de este al consentimiento del usuario final […] El presente Reglamento se entiende sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679, incluido su marco de ejecución, que sigue siendo plenamente aplicable con respecto a cualquier reclamación de los interesados relacionada con una vulneración de sus derechos amparados por dicho Reglamento».

Hay que tener en cuenta también la importante presencia en el mercado de empresas norteamericanas titulares de plataformas intermediarias. Estas empresas no quedan sujetas a los reglamentos europeos sino solo – para el caso de que interactúen con empresas o ciudadanos europeos- al llamado Marco de Privacidad de Datos UE-EE.UU., adoptado en su última versión por la Comisión Europea el pasado 10 de julio de 2023[22], al que pueden voluntariamente adherirse. En caso de que lo hagan se comprometen a cumplir una serie de obligaciones detalladas de privacidad, por ejemplo, a borrar los datos personales cuando ya no sean necesarios para el fin que hubiera motivado su recogida, y a garantizar la continuidad de la protección en caso de compartir los datos de carácter personal con terceros. Además, en caso de tratamiento indebido de sus datos por parte de las empresas estadounidenses, los ciudadanos de la UE se beneficiarán de varias vías de reparación, entre ellas unos mecanismos de resolución independiente y gratuita de controversias, y un tribunal arbitral. Es de esperar que estos mecanismos recién implantados tengan un recorrido práctico adecuado y sirvan para conminar a las empresas estadounidenses a respetar los estándares de privacidad de la UE, básicamente los relativos al consentimiento informado.

[22] Consultable en https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_es. (Fecha de la consulta 11.03.24).

### 2.1.4. Los datos personales y la IA. Elaboración de perfiles

Junto con todos estos principios recogidos en el RGPD, merece capítulo aparte la Propuesta de regulación europea en materia de Inteligencia artificial (en adelante IA), que inició su andadura el pasado 21 de abril de 2021, y se encuentra muy cerca de convertirse en Reglamento[23]. En efecto, uno de los aspectos clave de este proyectado Reglamento europeo es la prohibición de ciertas prácticas relacionadas con la IA consideradas inaceptables, porque pueden llegar a manipular el comportamiento humano de forma no transparente, o a violar la privacidad de las personas en contra de su voluntad. Para evitarlo se pretende imponer una serie de obligaciones a los desarrolladores y usuarios de sistemas de IA, en función de su riesgo potencial y su nivel de impacto. Así mismo se establecerá un sistema de gobernanza mediante el nombramiento de una autoridad europea de supervisión que garantice el cumplimiento de todas estas normas[24].

Cabe concluir que una de las principales preocupaciones del legislador europeo es que determinados sistemas de IA, a los que denomina de alto riesgo, puedan impactar negativamente en los derechos fundamentales de las personas, entre ellos el derecho a la protección de sus datos personales. Las aplicaciones de inteligencia artificial que suponen una amenaza clara para los derechos fundamentales –como los sistemas de categorización biométrica basados en características sensibles, los de puntuación social o los que buscan manipular el comportamiento humano- quedarán prohibidos en la UE. En este sentido, será necesario vincular esta normativa con lo que ya ha quedado establecido en el artículo 22 RGPD, según el cual:

[23] 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, COM(2021) 206 final.
Consultable en https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF (Fecha de la consulta 11.03.2024, la votación en el Parlamento europeo tendrá lugar la mañana del 13 de marzo).

[24] Puede verse un resumen del contenido de la propuesta en MARTÍNEZ ESPÍN, Pascual, «La propuesta de marco regulador de los sistemas de inteligencia artificial en el mercado de la UE», *Revista CESCO de Derecho de consumo* (2023), nº 46, pp.1-20; MARTÍN CASALS, Miquel, «Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial», *InDret* 3/2023, pp. 55-100; DOI: 10.31009/InDret.2023.i3.02. En nuestro país, contamos desde el año 2021 con un Anteproyecto de ley de IA publicado por el Ministerio de Asuntos Económicos y Transformación digital, que pretende ser un trasunto de la proyectada norma europea, incidiendo en una serie de principios éticos que deben observarse en el empleo de sistemas de IA.

> «Todo interesado tendrá derecho a no ser 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 de modo similar».

La interpretación mayoritaria que realiza la doctrina, a la que me adhiero, conduce a entender que el art. 22 RGPD contiene una verdadera prohibición de realizar tratamientos automatizados bajo esas circunstancias, que no es, únicamente, un argumento de defensa para el interesado que se vea sometido a estos tratamientos automatizados[25]. Es lo cierto que este principio general contiene tres excepciones en las que el algoritmo podrá analizar los datos recabados del individuo con fines de predicción y perfilado de clientes, recreando a partir de una información real patrones humanos de comportamiento. En concreto, en el sector privado la excepción legitimadora es el consentimiento del usuario. Pero también en estos supuestos ordena el legislador al responsable del tratamiento que adopte las medidas adecuadas para salvaguardar los derechos y libertades, y los intereses legítimos del interesado. Entre estas medidas está la obligación de elaborar un estudio previo de impacto en el derecho de protección de datos, de cualquier sistema de IA que desee implementar.

La elaboración de perfiles puede definirse como un tratamiento automatizado que permite inferir datos personales no recabados del sujeto a partir de los sí recabados, con la particularidad de que los datos inferidos pueden ser datos sensibles (como la afiliación política, la etnia o la salud[26]) que el algoritmo deduce a partir de datos personales no sensibles como los de identificación, o el lugar de residencia, o simplemente a partir del historial de búsquedas del sujeto en internet. Un supuesto recientemente resuelto por el TJUE, el asunto C-300/21, recoge un ejemplo muy claro de perfilado de un sujeto que produjo efectos significativos para él[27]. En este caso, la empresa nacional de correos austríaca trató los datos personales de los ciudadanos con la finalidad de inferir, mediante un algoritmo, su potencial afiliación política. La finalidad era remitir la propaganda electoral *ad hoc* a cada ciudadano. La empresa de correos no había informado ni recibido el consentimiento para dicho tratamiento. A raíz de una solicitud de acceso (art. 15 del RGPD), el demandante se enteró de que la

[25] Véase VILASAU I SOLANA, Mónica, «La realización de perfiles y la salvaguardia de los derechos y libertades del afectado», en *Retos jurídicos de la inteligencia artificial,* coord. por Agustí Cerrillo i Martínez y Miguel Peguera Poch, Aranzadi, Cizur Menor, 2020, pp. 182-183; DÍAZ LAFUENTE, José, «Los desafíos de la sociedad global digitalizada y la protección de datos personales. Análisis de la elaboración de perfiles en el Reglamento General de Protección de datos de la Unión Europea», *op. cit*., p. 298 y ss.

[26] Cfr. art. 9 RGPD. Así como su relación con el art. 22.4 del Reglamento, que permite el tratamiento de categorías especiales de datos personales si hay consentimiento explícito del interesado conforme al art. 9.2 a).

[27] Cfr. STJUE 4 mayo 2023, ECLI:EU:C:2023:370.

demandada había presumido su afinidad política con el Partido Liberal de Austria (FPÖ). La información relativa a la afinidad del sujeto se obtuvo mediante el uso de un algoritmo para definir las «direcciones del grupo objetivo» según las características sociodemográficas. El demandante se sintió ofendido y humillado por ser catalogado como partidario de extrema derecha En consecuencia, solicitó la supresión del tratamiento y una indemnización por los daños y perjuicios inmateriales sufridos. Sin perjuicio de que el algoritmo se equivocara en este caso, no puede negarse que pretender «gestionar» la campaña electoral de un país con base en los perfiles predeterminados por una máquina, sobre la afiliación política de los ciudadanos, de suyo ya es un grave atentado contra la libertad. Ello, además de la gravedad previa y objetiva que reviste el hecho de estar tratando sin permiso una categoría especial de dato personal, tal y como la define el RGPD[28].

En otro orden de cosas, la creación de perfiles sobre solvencia crediticia de los sujetos, que empieza a generalizarse en el sector bancario por la aplicación de sistemas de IA, puede resultar muy relevante y afectar significativamente a las oportunidades (por ejemplo, de obtener un crédito bancario) de los sujetos, generando sesgos discriminatorios de incalculables consecuencias. Podría pensarse que la obligación del prestamista de evaluar la solvencia del prestatario, tan desarrollada a partir de la Directiva 2014/17/UE y que está vigente en nuestro país a partir de la Ley de contratos de crédito inmobiliario, ampara la elaboración de perfiles de solvencia crediticia de los sujetos sin su consentimiento[29], si bien es precisamente lo contrario: solo un tratamiento automatizado conocido y consentido por el ciudadano objeto del mismo, se convierte en una actuación lícita para el potencial prestamista.

El mecanismo más generalizado para el perfilado de los sujetos con fines de mercadotecnia es un amplio y exhaustivo seguimiento y control de los comportamientos *on line* de los usuarios para identificar patrones generales de comportamiento y correlaciones entre determinados rasgos y decisiones individuales.

[28] En la sentencia, origen de la referenciada cuestión prejudicial, dictada el 15 de abril de 2021 por el Tribunal Supremo austriaco (Oberste Gerichtshof, OGH) se establece que el tratamiento de datos sobre la afinidad del sujeto con un partido político constituye una categoría especial de datos personales. Esto se aplica incluso si los datos en cuestión se basan en encuestas y estadísticas anónimas. Sobre este supuesto fáctico enjuiciado por el TJUE he publicado un artículo divulgativo en la publicación *The Conversation.* Puede consultarse en https://theconversation.com/como-las-empresas-de-internet-deducen-nuestra-ideologia-politica-y-otra-informacion-personal-sin-preguntarnos-202412

[29] Ley 5/2019, de 15 de marzo, reguladora de los contratos de crédito inmobiliario. Véase el art. 11.6 de esta norma: «Cuando se deniegue la solicitud de préstamo, el prestamista informará por escrito y sin demora al potencial prestatario y, en su caso, al fiador o avalista de su respectivo resultado advirtiéndoles, de forma motivada de dicha denegación y, si procede, de que la decisión se basa en un tratamiento automático de datos».

Ello resulta admitido siempre que los sujetos lo consientan, tras una previa y adecuada información. El empresario digital, realmente, no necesita esta información para desarrollar su negocio, lo cual le excluye a priori de la segunda excepción contemplada en el artículo 22.2.a) RGPD: que la decisión basada en tratamientos automatizados sea estrictamente necesaria para la celebración o la ejecución del contrato. Lo que ocurre es que el desarrollo vertiginoso de la tecnología le permite obtener cada vez más provecho de esta información adicional, y el prestador de servicios digitales accede a ella porque su análisis le produce beneficios económicos relevantes[30]. Las decisiones automatizadas, cuando afectan a las personas físicas, pueden referirse a la interacción de la persona en su contexto social, como sería el acceso a un contrato o servicio, o a la personalización de dicho servicio, como podría ser la personalización en los mandos de un coche realizada a partir de los datos personales del concreto comprador que va a adquirir el vehículo[31]. Las decisiones de la IA, a su vez, conducen a poder hacer predicciones sobre la evolución del sujeto, a realizar una evaluación sobre el estado actual de éste, o a decidir la ejecución de un conjunto de acciones en su nombre. Todo lo cual, puede afirmarse sin lugar a dudas, disminuye la ratio de decisiones libres del sujeto, y precisa de una suficiente justificación, más allá de la pura ganancia económica de los prestadores de servicios digitales[32].

A mi juicio, el régimen previsto actualmente en el RGPD resulta insuficiente para solventar muchos de los problemas que plantea la personalización, por eso cabe aplaudir la creación de una normativa específica para los sistemas de IA, como el Reglamento europeo en ciernes.

[30]Señala Antonio Rubí que «A mayor número de datos y a mayor complejidad y granularidad, más probabilidades de que la personalización sea más efectiva», RUBÍ PUIG, Antonio, «Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores», *Revista de educación y derecho* (2021), nº 24, p. 9.

[31] Este ejemplo concreto lo emplea la AEPD, en su Guía sobre IA, a la que luego volveré a referirme: «Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción», consultable en https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf. (Fecha de la consulta. 11.03.24).

[32] Cfr. ANTÓN JUÁREZ, Isabel, «Personalización de precios a través de la inteligencia artificial y el Big Data», en *El sistema jurídico ante la digitalización: estudios de Derecho privado*, Manuel Paniagua Zurera (Dir.), Tirant lo Blanch, Valencia, 2021, pp. 379-416; BINNS, Reuben, VEALE, Michael, «Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR», *Internet Data Privacy Law* (2021), pp. 1-14. Consultable en https://doi.org/10.1093/idpl/ipab020. (Fecha de la consulta 11.03.24); CASEY, Bryan, FARHANGI, Ashkon, VOGL, Roland, «Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise», *Berkeley Technology Law Journal* (2019), nº 34, 1, pp. 143-188; MAGGIOLINO, Mariateresa, «Personalized Prices in European Competition Law», *Bocconi Legal Studies* (2017), Research Paper No. 2984840, Consultable en http://dx.doi.org/10.2139/ssrn.2984840. (Fecha de la consulta 11.03.2024).

## 2.2. *En España*

### 2.2.1. Artículo 18.4 CE

La configuración de la protección de datos como un derecho fundamental del individuo es un dato indiscutible en nuestros días, en el ordenamiento jurídico español. El artículo 18, apartado 4 de la Constitución Española (en adelante CE) así como su interpretación por parte del Tribunal Constitucional no deja lugar a dudas. Queda explicitado en la CE:

> «La ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

A partir de ahí, el Tribunal Constitucional ha desarrollado la teoría de un derecho independiente respecto del derecho a la intimidad desligándolo de la protección de la Ley Orgánica 1/1982[33] para encontrarle un ámbito específico de protección. Es relevante la sentencia nº 254/1993[34], en la que se define por primera vez el llamado «derecho a la libertad informática», y la sentencia nº 292/2000[35], en la que se remarca su existencia independiente respecto del derecho a la intimidad, definiendo el derecho a la protección de datos como la potestad de control del individuo sobre sus datos personales[36]. Se ha destacado que existen diferencias en cuanto al objeto, y al contenido y alcance de este derecho. En primer lugar, porque la libertad informática excede la intimidad protegida por el art 18.1 CE, el derecho fundamental a la protección de datos vincula aquellos datos que tengan una incidencia o afectación en cualquier derecho de la persona, sean o no constitucionales y se refieran o no al honor e intimidad personal o familiar. Por lo tanto, el objeto es más amplio, se refiere a cualquier dato personal, cuyo conocimiento o tratamiento por terceras personas pueda inferir en los derechos de la persona, aun cuando estos no sean fundamentales. En segundo lugar, por lo que hace al contenido de este derecho fundamental, consiste en una facultad de control y disposición sobre los datos de índole personal, que supera nuevamente el contenido del derecho fundamental a la intimidad personal y familiar.

[33] LO 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen [BOE núm. 115, de 14/05/1982]. En adelante, LO 1/1982.
[34] STC 254/1993 de 20 julio, RTC\1993\254.
[35] STC 292/2000 de 30 noviembre, RTC\2000\292.
[36] Cabe mencionar también la STC 94/1998, de 4 de mayo (ECLI:ES:TC:1998:94), en la que se define este derecho fundamental como la garantía de que la persona tiene el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para su dignidad; de esta forma, el derecho a la protección de datos se concreta, como una de sus manifestaciones, en la facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

Estos poderes se concretan jurídicamente en el derecho de información, acceso, rectificación, supresión, oposición, así como el consentimiento explícito para el almacenamiento y tratamiento de los datos por un tercero[37].

Sin embargo, en la práctica, la delimitación total entre los derechos contenidos en el artículo 18 CE no es tan clara, por el contrario, existen supuestos en los que determinadas vulneraciones de la protección de datos personales pueden ser enfrentadas también a través de la aplicación de la LO 1/1982 para la defensa del honor, la intimidad y la propia imagen (también la digital) del individuo, es decir, supuestos en los que la lesión al derecho fundamental de protección de datos se realiza mediante conductas que también lesionan el honor o la propia imagen (digital) de la persona concernida[38]. Además, esto es lo que nos muestra la jurisprudencia actual, solo cuando la lesión del derecho fundamental protegido por el art. 18.4 CE lesiona, además, el derecho protegido por el art. 18.1 CE, el sujeto reclama y en su caso obtiene una indemnización económica para resarcirle por los daños y perjuicios materiales o inmateriales sufridos.

Este solapamiento se observa muy claramente en una sentencia del TS en la que el tribunal falló sobre la colisión entre la libertad de información y el derecho a la propia imagen[39]. En este supuesto, un medio de comunicación digital difundía la fotografía que una persona había subido a su perfil de una red social. Tal uso personal de la imagen, entiende el Tribunal Supremo, lo lleva a cabo el titular del derecho con los terceros, permitiéndoles el acceso al contenido de esa red social, pero no conlleva, como consecuencia natural, la autorización para que un medio de comunicación digital reproduzca esos contenidos. La publicación de una fotografía por parte de una persona en su red social no constituye el consentimiento expreso a que se refiere el artículo 2.2 LO 1/1982, excluyente de la ilicitud, dado que la persona afectada en este caso no era un personaje público cuya vida personal tuviera un interés general.

La consecuencia de la estimación de la acción civil es la indemnización al perjudicado con una cantidad, por el daño moral que ha sufrido. Así, la sentencia de 13 de enero de

[37] CABEDO MALLOL, Vicente, «El derecho fundamental a la protección de datos personales», en *Marco jurídico de la ciencia de datos*, Francisca Ramón Fernández y Alicia Barnard Amozurrutia (eds.), Tirant lo Blanch, Valencia, 2020, p. 86 y ss.
[38] GRIMALT SERVERA, Pedro, «Intromisiones ilegítimas en los derechos al honor, a la intimidad y a la propia imagen: tutela civil versus tutela administrativa», en *Protección de Datos Personales,* coord. por Isabel González Pacanowska, Tirant lo Blanch, Valencia, 2020, p. 356 y ss.
[39] Cfr. STS 17 mayo 2021; RJ 2021\2889.

2022[40] recoge el supuesto de reclamación porque la imagen de un menor aparece en un periódico digital informando de que había sido condenado por la comisión de un delito. El tribunal estima la vulneración del derecho fundamental a la propia imagen, porque no se había consentido ni por el menor ni por sus representantes la publicación de la fotografía, que no aparecía pixelada y permitía identificar perfectamente a la persona concernida, con claro perjuicio para sus intereses. Se aplica el art. 20.4 CE, que refuerza la obligación de proteger estos derechos de la personalidad cuando se trata de menores.

Es frecuente también que se declare como una lesión al honor y a propia imagen el trasvase inadecuado o no consentido de los datos personales de los sujetos a ficheros de morosidad[41]. Está claro que una información inexacta o negativa del sujeto concernido que se propague en internet mediante tratamientos automatizados tiene consecuencias importantes para él, no solo morales, sino también económicas: puede afectar a la búsqueda de empleo, a la posibilidad de obtener crédito, al éxito de determinadas operaciones mercantiles, entre otras. El usuario debe ser consciente de las repercusiones futuras del consentimiento a la cesión de sus datos a terceros, ya sean motores de búsqueda, redes sociales u otros prestadores de servicios digitales.

2.2.2. Las directrices de la Agencia Española de Protección de Datos sobre IA y sobre el uso de las cookies

La vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LO 3/2018)[42], desarrolla el derecho fundamental consagrado por nuestra Constitución. Se ha destacado el proceso de mejora que experimentó el inicial proyecto de ley durante su tramitación parlamentaria y, concretamente, en relación con la delimitación del objeto de la norma, que no solo persigue adaptar el ordenamiento jurídico español al RGPD, sino

[40] Cfr. STS 13 enero 2022, RJ 2022\423, en la que se hace referencia a una extensa y consolidada doctrina jurisprudencial en esta materia. Se condenó al periódico a indemnizar al menor con 4.000 €.

[41] Cfr. STS 13 enero 2022, RJ 2022\425, en la que el demandante presentó demanda de juicio ordinario contra Experian Bureau de Crédito, S.A., como entidad responsable y titular del fichero Badexcug, en ejercicio de acción conjunta de protección de los derechos fundamentales al honor y a la protección de datos de carácter personal, al haber sido incluido indebidamente en un registro de morosos. El demandante obtuvo una indemnización de 6.000 €.

[42] Y su norma de desarrollo, el todavía vigente Reglamento de la derogada Ley 15/199 (aunque sólo en lo que no se oponga al RGPD y a la LO 3/2018, y a la espera de que se desarrolle reglamentariamente la vigente Ley Orgánica). Es el Real Decreto 1720/2007, de 21 de diciembre.

también garantizar los derechos digitales de la ciudadanía conforme al mandato contenido en el artículo 18.4 CE[43].

El Título VII de la LO 3/2018, en cumplimiento de lo dispuesto por el RGPD (arts. 51 y ss.) regula la existencia y competencias de la AEPD y de las agencias autonómicas, donde las hay[44]. Las autoridades de control independientes adquieren una relevancia especial desde el momento en que lo que salvaguardan es un derecho fundamental, son las encargadas de realizar un control eficaz y fiable del cumplimiento de las normas de la UE sobre protección de datos personales[45]. En el mes de mayo de 2023 se ha aprobado una reforma que afecta a la forma de gestionar y resolver los procedimientos sobre protección de datos por parte de la AEPD[46]. Reforma que pone de manifiesto el considerable incremento de los expedientes tramitados por la autoridad de control española, que trata de paliarse, entre otras medidas, mediante el alargamiento de los plazos de resolución y la imposición de formularios a los usuarios que quieran presentar reclamaciones ante la Agencia. Asimismo, esta podrá realizar, no sólo investigaciones presenciales, sino también remotas.

En ejercicio de las funciones que la Ley le confiere, la AEPD publicó un documento en 2020 referido a los supuestos de tratamiento automatizado de los datos con tecnologías de Inteligencia Artificial[47]. Este documento normativo señala que la Inteligencia Artificial es un componente más de los tratamientos de datos realizados por los responsables y que, en muchos casos, aparece en forma de soluciones

[43] GARCÍA MAHAMUT, Rosario, «Del Reglamento General de Protección de datos a la LO 3/2018 de protección de datos personales y garantías de los derechos digitales», *op. cit.,* p. 115.

[44] En la actualidad existen autoridades de control en las Comunidades Autónomas de Cataluña, País Vasco y Andalucía, siendo el objeto de las dos últimas más limitado que el que se prevé para la Agencia Catalana de Protección de Datos. Véase, https://apdcat.gencat.cat/ca/autoritat/estructura/autoritat_catalana_de_proteccio_de_dades/ (Fecha de la consulta: 11.03.24).

[45] A este respecto, la denominada sentencia *Schrems* del TJUE (6 octubre 2015, asunto C-362/14) supuso un fuerte espaldarazo para estas instancias administrativas creadas por los Estados para contribuir a la aplicación coherente y uniforme del RGPD en toda la UE. Sobre la sentencia y, sobre todo, sobre las facultades de las agencias de control como guardianes de los derechos fundamentales de los individuos, puede consultarse: PUERTO, M.ª Isabel, y SFERRAZZA Pietro, «La sentencia Schrems del Tribunal de Justicia de la unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional», en *Revista Derecho del Estado* (2018), nº 40, pp. 209-236.

[46] Se reforma la LO 3/2018 mediante la Disposición Final 9ª de la Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos. Consultable en https://www.boe.es/boe/dias/2023/05/09/pdfs/BOE-A-2023-11022.pdf (Fecha de la consulta 11.03.2024).

[47] AEPD, «Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción», *cit*.

desarrolladas por terceros (esto es, mediante subcontratación de los prestadores de servicios digitales a programadores y desarrolladores de productos, que logran un aprovechamiento infinitamente superior de los datos recabados a los usuarios). Ello, a priori, tiene dos consecuencias, la primera, que esos terceros también acceden y tratan los datos de la persona física (¿con o sin su consentimiento expreso?) y la segunda, que los mecanismos de IA empleados pueden proporcionar una utilidad nueva a los datos recabados, (¿distinta respecto a la autorizada en su momento por el usuario?).

A la vista de este potencial gigante aplicable al tratamiento de datos de las personas físicas, la AEPD recuerda que la entidad que decide tratar los datos de los interesados con estos sistemas para sus propios fines, es la responsable de dicho tratamiento, esto es, será quien responda en su caso del cumplimiento del Reglamento europeo, y de las posibles vulneraciones que se produzcan. Lo que en ningún caso es sostenible es trasladar la responsabilidad al propio sistema de IA.

También introduce algunas recomendaciones sobre la obligación de información al usuario cuando se emplee esta tecnología:

a) La información que cada responsable ha de proporcionar a los interesados se tendrá que adaptar a la etapa del ciclo de vida de la IA en la que se esté realizando el tratamiento;

b) En cuanto a las dos capas de información, en la primera de ellas deberá informarse al usuario de que el tratamiento incluye la elaboración de perfiles o decisiones automatizadas, informarle de su derecho a oponerse a la adopción de decisiones individuales automatizadas, proporcionarle información significativa sobre la lógica aplicada, y sobre las consecuencias previstas de dicho tratamiento para el interesado;

c) Por último, si los datos personales objeto del tratamiento no han sido obtenidos directamente del afectado, la información básica incluirá también las categorías de datos objeto de tratamiento y las fuentes de las que procedan esos datos.

Otro documento publicado por la AEPD que incide directamente en los tratamientos automatizados de los datos personales es la denominada *Guía sobre el uso de las cookies*[48]. En ella la AEPD, según determina literalmente en la introducción del documento, no pretende ofrecer «una solución general y uniforme para el cumplimiento de la ley, sino servir de guía para que las entidades afectadas reflexionen

[48] Cfr. https://www.aepd.es/es/documento/guia-cookies.pdf (Fecha de la consulta 11.03.2024).

y adopten decisiones sobre la solución más adecuada a sus intereses y modelo de negocio». Un planteamiento bastante tenue si tenemos en cuenta que las cookies constituyen el principal mecanismo a través del cual los prestadores de servicios recaban la información sobre los usuarios, especialmente sobre sus hábitos en internet y sobre sus pautas habituales de consumo digital. Me refiero a las tecnologías que permiten almacenar y recuperar datos de un equipo terminal (por ejemplo, un ordenador, un teléfono móvil o una tablet) de una persona física o jurídica. No debe olvidarse que el Art. 22.2 LSSI vincula la obtención del consentimiento sobre estas técnicas a la información que se facilite al usuario, de modo que el consentimiento que, en su caso, preste el usuario sea realmente, un consentimiento informado.

En definitiva, el marco legal europeo y nacional expuesto hasta aquí nos conducen directamente a la cuestión del consentimiento informado que exige la normativa aplicable, y a la que dedicaré el siguiente apartado.

## 3. TRATAMIENTOS INCONSENTIDOS O *DEFICIENTEMENTE CONSENTIDOS* DE LOS DATOS PERSONALES

El modelo europeo de protección de datos en las relaciones entre empresario digital y consumidor se estructura en torno al consentimiento explícito del sujeto: se presume que, si los individuos tienen información sobre los datos a los que se acceden y al tratamiento que eventualmente se les puede dar, entonces podrán configurar la política de privacidad en cada caso, de acuerdo con sus preferencias. Este modelo, por tanto, tiene un corte privatista claro: los datos personales son objeto de propiedad y el individuo decide sobre ellos mediante el ejercicio de su autonomía privada. Un sistema que sitúa al individuo en el centro del régimen jurídico, como legitimado para tomar decisiones sobre su privacidad y modularla según sus preferencias.

Sin embargo, unos pocos años después de la entrada en vigor del RGPD, y ante una situación de imparable avance de la tecnología, puede sostenerse que existe consenso entre la doctrina en el hecho de que el régimen jurídico europeo y nacional en materia de protección de datos no resulta suficiente, a los efectos de proteger adecuadamente al usuario en los supuestos en los que la cesión de la privacidad se produce mediante la emisión del consentimiento[49]. Más bien podría decirse que una legislación amplia,

[49] Señala Mireia Artigot que «La aplicación práctica de este modelo privado y autodeterminista cuestiona, de forma significativa, su eficacia», véase ARTIGOT GALOBARDES, Mireia, «Las inherentes limitaciones del modelo autodeterminista de protección de datos en Europa», *Revista General de Derecho de los Sectores Regulados* (2021), nº 8, p. 3. Por su parte, Mariam Blandino indica que «El nuevo enfoque del RGPD, al situar el consentimiento del interesado al mismo nivel que las restantes causas habilitantes del tratamiento de los datos personales, implica desconocer el valor fundamental de la

detallada y aparentemente exigente, al final se queda corta en la creación de incentivos suficientes para que los responsables de los tratamientos de datos prefieran cumplir con la normativa de privacidad que incurrir en incumplimientos.

La información al sujeto y la transparencia se erigen por el legislador como la solución mágica que legitima la introducción de todo tipo de técnicas automatizadas en el tratamiento de los datos personales, por cuanto se presume que el sujeto consentirá libre y conscientemente a su utilización. Pero tal consentimiento no se produce. Trataré, a continuación, del binomio entre información y consentimiento, y de la configuración del negocio por el que se ceden los propios datos personales como un contrato digital de adhesión.

### 3.1. *La tesis de la mala calidad del consentimiento emitido por el usuario*

Las condiciones que debe tener el consentimiento se recogen en el RGPD, primero por vía de definición, en el art. 4.11 RGPD[50], y después por vía de principios informadores, en el artículo 7 titulado «Condiciones para el consentimiento». De ambos preceptos pueden colegirse las siguientes características del consentimiento que legitima el tratamiento de los datos personales de un sujeto: primero, se emite tras la pertinente información inteligible, de fácil acceso, diferenciada de la referida al objeto del contrato y, segundo, es un consentimiento libre y esencialmente revocable. Junto a ello, para el supuesto concreto recogido en el ya mencionado artículo 22 RGPD (para la toma de decisiones sobre la base de tratamientos automatizados[51]), la norma exige que el consentimiento sea explícito, luego no podrá inferirse del silencio del afectado. Además, el principio de equivalencia funcional que afecta a todas las transacciones digitales[52], y que también proclama el art. 80 de la LO 3/2018 cuando se refiere a la

autodeterminación como mecanismo legitimador del tratamiento de los datos de carácter personal»; cfr. BLANDINO GARRIDO, M.ª Amalia, «El consentimiento del interesado al tratamiento de sus datos personales en las comunicaciones electrónicas», *Revista de Derecho civil*, vol. IX, (2022), nº 4, p. 225. También puede consultarse GARCÍA-RIPOLL MONTIJANO, Martin, «El consentimiento al tratamiento de datos personales», *op. cit*., p. 149 y ss.; VILASAU SOLANA, Mònica, «Las exigencias de información en el RGPD y en la LO 3/2018 de Protección de Datos y Garantía de los Derechos Digitales, ¿contribuyen a la formación de un consentimiento de mejor calidad?», *op. cit.,* pp. 209-236.

[50] Art. 4.11): «Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen».

[51] Véase también arts. 6.1 y 6 bis de la Directiva 2011/83/UE, sobre los derechos de los consumidores (reformado por la Directiva (UE) 2019/2161 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019), que recoge la obligación de informar a los consumidores cuando se pretende elaborar perfiles con finalidades de personalización.

[52] Cfr. ILLESCAS ORTIZ, Rafael, *Derecho de la contratación electrónica*, Thomson Reuters, Cizur Menor, 2019, p. 57.

neutralidad de internet, exige que este consentimiento libre e informado sobre la cesión de los propios datos no sea diferente del que una persona emite cuando firma un contrato de adhesión recogido en un documento físico. Por lo tanto, en la propia definición de consentimiento se incluye la necesidad de información previa.

Veamos si el elemento de la información tiene algo que ver con la idea generalizada en nuestra sociedad de que el consentimiento emitido por la gran mayoría de los usuarios, al aceptar el tratamiento de sus datos personales, es, cuanto menos, defectuoso, susceptible de mejora. En efecto, las empresas digitales comunican los fines para los que recaban la información privada del individuo, pero ¿los comunican bien? ¿contribuye su información a la emisión de un consentimiento informado por parte del usuario? Mientras preparaba este trabajo, inicié una conversación con el chat GPT sobre el tema, y esta herramienta señaló literalmente:

> «es importante que las empresas adapten su información al usuario y lo hagan de manera fácil de entender. Por ejemplo, algunas empresas están optando por utilizar lenguaje sencillo, gráficos e infografías para explicar cómo se utilizan los datos personales. Otras empresas están utilizando técnicas de gamificación para fomentar la participación del usuario en el proceso de protección de sus datos personales […]».

Parece que la herramienta de IA generativa se está refiriendo a una suerte de *data protección by design*, mediante la implantación de técnicas que hagan posible la efectiva transmisión de la información al usuario de bienes y servicios digitales. Realmente, no es fácil conjugar la exigencia de proporcionar la información necesaria con el mandato de hacerlo de forma clara, sencilla y accesible. Pero tampoco parece que las empresas digitales hayan invertido demasiado en la búsqueda del equilibrio entre contenido y sobrecarga informativa[53]. Entiendo que sería necesario que los organismos encargados de proporcionar la tutela a los usuarios perjudicados en materia de privacidad (autoridades de control independientes, y tribunales) entraran a valorar el cómo (la forma en que se traslada la información al usuario) y no solo el qué (el contenido de la información proporcionada)[54].

[53] La profesora Vilasau realiza sugerentes propuestas al efecto, como recurrir a etiquetas o iconos de privacidad o generalizar la intervención de terceros, ya sea para asesorar antes de emitir el consentimiento, ya sea para certificar la idoneidad de la información procurada por la empresa digital a sus usuarios. Cfr. VILASAU SOLANA, Mònica, «Las exigencias de información en el RGPD y en la LO 3/2018 de Protección de Datos y Garantía de los Derechos Digitales, ¿contribuyen a la formación de un consentimiento de mejor calidad?», *op. cit.*, p. 228 y ss.

[54] Véase SAINZ DE JUBERA HIGUERO, Beatriz, «Retos jurídicos de la inteligencia artificial en el ámbito del consentimiento contractual: una aproximación general», *Revista de Derecho civil*, vol. X, (2023), nº 2, p. 50. Esta autora se refiere al concepto de «explicabilidad de los algoritmos», empleado por el legislador

Respecto al segundo y también esencial requisito, que el consentimiento sea libre y explícito en su caso, sí suele haber pronunciamientos por parte de las autoridades de control y de los tribunales. Así, la AEPD ha tenido ocasión de señalar cómo debe ser el consentimiento para considerarse válido e inequívoco[55]:

> «[…] Para la utilización de las cookies no exceptuadas (no necesarias), será necesario obtener el consentimiento del usuario de forma expresa. Este consentimiento se puede obtener haciendo clic en, "aceptar" o infiriéndolo de una inequívoca acción realizada por el usuario que denote que el consentimiento se ha producido inequívocamente. Por tanto, la mera inactividad del usuario, hacer *scroll* o navegar por el sitio web, no se considerará a estos efectos, una clara acción afirmativa en ninguna circunstancia y no implicará la prestación del consentimiento por sí misma. Del mismo modo, el acceso a la segunda capa si la información se presenta por capas, así como la navegación necesaria para que el usuario gestione sus preferencias en relación con las cookies en el panel de control, tampoco es considerada una conducta activa de la que pueda derivarse la aceptación de cookies».

Por tanto, está prohibido presumir el consentimiento a partir de una actitud pasiva del afectado. En el mismo sentido, el TJUE ha precisado que no puede entenderse que hay consentimiento válido cuando se exige al interesado, para negarse a darlo, que cumplimente un formulario adicional en el que haga constar esa negativa[56]. Tampoco habrá un consentimiento prestado de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de cookies se autoriza mediante una casilla marcada por defecto, de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento[57]. Son ejemplos de supuestos en los que la causa de que el consentimiento no sea verdaderamente libre es, precisamente, el empleo de prácticas comerciales desleales por parte del prestador de servicios. Otro ejemplo muy claro, que se ventiló en sede contencioso-administrativa, es el que recoge la sentencia del TS de 18 de junio de 2020[58]. Se trata de un procedimiento judicial que se inicia con la resolución de la AEPD de imponer a la empresa una sanción de 7.500 €, a raíz de un cúmulo de denuncias presentadas por particulares. Estos recibían una llamada telefónica (procedente de una app de juegos y bromas) a partir de la cual la empresa recababa el dato del número de teléfono y de la voz del sujeto que recibía la llamada. Se sanciona el acceso a estos datos personales sin haber obtenido un consentimiento

europeo y por la doctrina para exigir a los prestadores de bienes y servicios digitales una clara y entendible información sobre el uso de los modelos de inteligencia artificial.

[55] Cfr. AEPD, EXP202206594, cit.

[56] STJUE 11 noviembre 2020, TJCE 2020\268.

[57] STJUE 1 octubre 2019, Asunto C-673/17, ECLI:EU:C:2019:801.

[58] Cfr. STS 18 junio 2020; RJ 2020\2168.

libre y no viciado del titular de los mismos. Argumenta el Tribunal Supremo que la solicitud de autorización tras escuchar la grabación de la llamada que se acaba de hacer al sujeto, el cual solo al final comprende que ha sido una broma (que le ha podido hacer gracia, pero también le ha podido originar dudas, sorpresa o alarma), difícilmente puede considerarse un consentimiento que cumpla con los requisitos estipulados en la Ley de protección de datos.

Así pues, en este punto la amonestación al prestador de servicios no se contrae al contenido y expresión de la información, sino al comportamiento leal que debe permitir al usuario, realmente, elegir. Con respecto a las plataformas intermediarias o guardianes de contenido, el RMD es muy claro cuando les exige que permitan al usuario decidir sobre la cesión de sus datos, ofreciéndoles un servicio alternativo para el caso de que no consientan dicha cesión:

> «La alternativa menos personalizada no debe ser diferente ni tener una calidad degradada en comparación con el servicio prestado a los usuarios finales que prestan su consentimiento, a menos que la degradación de la calidad sea consecuencia directa del hecho de que el guardián de acceso no pueda tratar dichos datos personales ni iniciar la sesión de los usuarios finales en un servicio. No prestar el consentimiento no debe ser más difícil que prestarlo»[59].

El cumplimiento de estas concretas directrices podría calificarse como un ejemplo de una verdadera responsabilidad proactiva del responsable del tratamiento[60]. Pero, ¿son estas prácticas las que observamos de manera habitual en las transacciones comerciales por internet?

Como ya he mencionado con anterioridad, a mi parecer disponemos de una normativa aparentemente muy exigente que, sin embargo, convive con una operativa práctica en la que la persona física está verdaderamente indefensa. El análisis de casos revela un número significativo de incumplimientos por parte de los prestadores de servicios[61]. Pero no es este el único problema que afecta al consentimiento relativo a la cesión de

[59] Reglamento (UE) 2022/1925, *cit*. Reproduzco parcialmente el Considerando 37.
[60] SANTOS MORÓN, María José, «Tratamiento de datos, sujetos implicados, responsabilidad proactiva», *op. cit*., 2020, p. 51.
[61] La Memoria de la AEPD correspondiente a 2022, indica que entre los diez tipos de reclamaciones que se presentan con mayor frecuencia, las relativas a los servicios de internet ocupa el primer lugar, y suponen el 15% del total, la misma proporción que las reclamaciones por videovigilancia. Ello teniendo en cuenta que de forma habitual son pocas las personas físicas que se toman la molestia de interponer reclamaciones en materia de protección de datos personales. Consultable en https://www.aepd.es/es/documento/memoria-aepd-2022.pdf (Fecha de la consulta: 11.03.2024).

la propia privacidad. Aun en el hipotético caso de que todos los empresarios digitales lo hicieran bien, el consentimiento del usuario de bienes y servicios por internet puede calificarse como defectuoso o de mala calidad porque, en la mayoría de los supuestos, no puede realizarse con clara conciencia de su alcance, sobre todo a largo plazo. No es posible emitir un verdadero consentimiento libre por las propias dificultades cognitivas del individuo, que impiden evaluar los efectos e impacto del tratamiento de sus datos para su bienestar futuro[62]. En línea con esta tesis, también cabe considerar la falta de alfabetización algorítmica de los ciudadanos: no hemos recibido una formación que nos habilite lo suficiente para entender cómo se lleva a cabo el tratamiento automatizado de nuestros datos personales, una vez hemos emitido el consentimiento. Así que parece que el sistema del consentimiento informado para el tratamiento de los propios datos personales dista mucho de ser perfecto y precisa ser sometido a revisión, rellenar las zonas grises del ordenamiento europeo para hacerlo eficiente y ajustar bien su alcance territorial[63].

### 3.2. *La tesis del contrato de adhesión encapsulado sobre la cesión de los propios datos personales*

Junto con la constatación de los problemas que afectan al consentimiento para el tratamiento de los propios datos personales, se ha destacado por la doctrina el hecho de que el RGPD configura el consentimiento como independiente del contrato principal que se celebrará *on line*, como un acto con trascendencia jurídica que produce el efecto de permitir al prestador de servicios acceder a la información personal del usuario, sin que tal acción pueda ser calificada como antijurídica. Sin embargo, ello no implica, para muchos autores, que se trate de un negocio jurídico, el de los datos personales, que se formalizaría por las partes con carácter previo al negocio principal. Se argumenta que se trata solo de una declaración de voluntad previa y, en algunos casos, necesaria para que se pueda llevar a cabo la adquisición del bien o servicio que el usuario desea

[62] Esta es la tesis que defiende (y a la que me adhiero, aunque quizá menos categóricamente) la profesora Artigot. Cfr. ARTIGOT GOLOBARDES, Mireia, «Las inherentes limitaciones del modelo autodeterminista de protección de datos en Europa», *op. cit.*, p. 1.

[63] «Hay quienes hablan de la "territorialización de internet", opción que, por el momento, se está usando más bien para la censura, por ejemplo, en China. En nuestro artículo proponemos que cualquier opción democráticamente saludable pasa por la adopción de un nuevo contrato social que establezca un equilibrio más justo entre usuarios/as (tanto personas como gobiernos) y las grandes corporaciones que exprimen el jugo de nuestros datos. En este contrato social, el derecho a los datos (*data rights*) y la alfabetización en datos (*data literacy*) deben ser pilares sólidos para que el click en la casilla de "*I accept*" pase a ser una rutina ejercida con conciencia ciudadana», GUTIÉRREZ Miren y DIAZ-SANZ, Marina, «Deperipheralisation of people and states in the algorithmic assemblage: court cases and a proposal for a new social contract», (Published online: 13 Mar 2023, consultable en https://doi.org/10.1080/04353684.2023.2182226 (Fecha de la consulta 11.03.2024).

contratar, pero no propiamente una prestación que este realice, ya que este consentimiento a la recabación ni siquiera es vinculante, por cuanto el usuario puede revocarlo en cualquier momento (art. 7.3 RGPD) [64].

Siendo absolutamente cierto este planteamiento, nada impide abordar también la cuestión de la analogía que se observa en cuanto a la asimetría en las posiciones de las partes, cuando se comparan los contratos de adhesión celebrados entre empresarios y consumidores en cualquier sector económico, y los acuerdos celebrados entre el prestador de servicios digitales y el usuario en relación con la recabación de los datos personales del segundo. Es decir, el empresario digital establece «las reglas del juego» necesarias para que se produzca el «consentimiento informado» del usuario: decide la información que proporciona -y la forma en que la proporciona- sobre su política de privacidad; establece los mecanismos tecnológicos a través de los cuales deberá el usuario, en su caso, consentir la recabación de sus datos. La persona física tiene la libertad de adherirse o no a este sistema predeterminado por el empresario. De manera que la cesión de los propios datos personales en internet viene a convertirse, con todos los matices necesarios, en una suerte de «contrato digital de adhesión» encapsulado dentro de un contrato de compraventa o prestación de servicios, que constituyen el negocio jurídico principal.

Esta analogía ya queda plasmada por el propio legislador europeo cuando, en el Considerando 43 del RGPD, señala que el consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal si se produce un desequilibro claro entre el interesado y el responsable del tratamiento. Y, como muestra de un supuesto en el que se entiende que hay desequilibrio, señala el caso en el que el cumplimiento de un contrato, incluida la prestación de un servicio, se hace depender del consentimiento del usuario a la recabación de sus datos, sobre todo si estos no son necesarios para dicho cumplimiento. Más expreso aún, el Considerando 42 cita la Directiva 93/13 sobre cláusulas abusivas en contratos celebrados con consumidores[65].

Por otro lado, la Directiva (UE) 2019/770, de 20 de mayo, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales, ya ha consagrado la posibilidad de que los sujetos intercambien bienes y servicios digitales

[64] Véase GARCÍA-RIPOLL MONTIJANO, Martin, «El consentimiento al tratamiento de datos personales», en *Protección de Datos Personales, op. cit*., p. 88 y ss., en la que se contienen otras referencias doctrinales.
[65] También lo hace el Considerando 9 del Reglamento 2023/2854 sobre normas armonizadas para un acceso justo a los datos, aprobado en diciembre de 2023.

por datos personales que, de este modo, se convierten en la contraprestación del usuario. Son los llamados «contratos gratuitos a cambio de datos»[66]. En este sentido, la posibilidad de equiparar el consentimiento de cesión de datos al consentimiento contractual se ciñe al caso en que la cesión se refiera, no sólo a los datos imprescindibles para la realización del negocio principal que las partes pretenden, dado que en este caso no habría realmente contraprestación[67], sino a los casos en los que se proporcionan al empresario digital datos adicionales (lo cual se produce en la mayoría de los supuestos de contratación digital entre personas físicas y prestadores de servicios digitales)[68].

Al tiempo que reconoce plenamente que la protección de datos personales es un derecho fundamental, por lo que los datos personales no pueden considerarse una mercancía (ni ser regulados como si fueran un bien mueble o inmueble objeto de comercio), la Directiva señala literalmente que se plantea como objetivo «garantizar que los consumidores, en el contexto de dichos modelos de negocio, tengan derecho a medidas correctoras contractuales»[69]. Es decir, que se les pueda aplicar la normativa europea de consumo en materia de cláusulas abusivas.

[66] Ya trabajé este asunto en 2019, en el artículo «La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)», en *Cuadernos Europeos de Deusto* (2019), nº 61, pp. 29-65. Más recientemente véase MARTÍNEZ CALVO, Javier, «Dualidad normativa en la regulación de los contratos gratuitos de suministro de contenidos y servicios digitales: la necesaria armonización entre la Directiva (UE) 2019/770 y el Reglamento (UE) 2016/679», *Actualidad jurídica iberoamericana* (2022), nº. 16, pp. 1168-1185.

[67] Señala el profesor Carrasco: «Ha de repararse que los datos personales pueden cursar como contraprestación cuando su entrega no fuera ya imprescindible para ejecutar el contrato. Si esto ocurriera, y tampoco se pagara dinero, no habría contraprestación, y tampoco habría contrato, porque el Derecho de consumo no puede oficiar de marco regulatorio de una relación negocial no onerosa» CARRASCO PERERA, Ángel, «Resolución de contrato pagado con datos personales como precio», *Revista CESCO*, consultable en https://centrodeestudiosdeconsumo.com/images/Resoluci%C3%B3n_de_contrato_pagado_con_datos_personales_como_precio.pdf. (Fecha de la consulta 11.03.2024)

[68] Véase el Considerando 24 de la Directiva 770/2019, en cuanto a la descripción de los supuestos que califica sin ambages como un contrato en el que los datos personales constituyen la contraprestación: «A menudo, los contenidos o servicios digitales se suministran también cuando el consumidor no paga un precio, pero facilita datos personales al empresario. Tales modelos de negocio ya se utilizan de diferentes formas en una parte considerable del mercado […]. Así, por ejemplo, la presente Directiva debe aplicarse en aquellos casos en que el consumidor abre una cuenta en una red social y facilita un nombre y una dirección de correo electrónico, y estos se utilizan para fines que no sean exclusivamente el suministro de los contenidos o servicios digitales, o distintos del cumplimiento de los requisitos legales. También debe aplicarse en aquellos casos en que el consumidor dé su consentimiento para que cualquier material que constituya datos personales, como fotografías o mensajes que cargue, sea tratado por el empresario con fines comerciales».

[69] De nuevo, Considerando 24 de la Directiva 770/2019, *cit*.

El derecho de consumo es la disciplina que se ha desarrollado al albur de los controles que se han ido estableciendo para los contratos predispuestos, bien diferentes a los negociados tanto en el elemento de la libertad como en el de la igualdad. Los contratos predispuestos constituyen una técnica útil y atractiva para el ámbito de las transacciones digitales, que racionaliza la actividad contractual de los empresarios y optimiza su organización interna y la utilización de sus recursos[70]. No obstante, este tipo de contratos digitales contienen un enorme potencial para generar abusos y desequilibrar la relación contractual, y por esta razón, toda la normativa sobre cláusulas generales de la contratación se dirige a evitar la hipertrofia de una de las partes contratantes, el predisponente, con la consiguiente reducción o atrofia para el otro, el sujeto adherente. Así pues, cuando se aplican a la cesión de los propios datos en internet las reglas sobre cláusulas predispuestas en los contratos de adhesión, adquieren sentido las exigencias relativas a la información precontractual que ya están plenamente implantadas, por ejemplo, en el sector bancario o en las compraventas de inmuebles a consumidores.

Los tribunales han ido vinculando las obligaciones de información, cada vez más exigentes para el empresario, con la doctrina del error en el consentimiento de la persona física, que puede derivar, en su caso, en una declaración de nulidad contractual. Si se acredita que el consumidor ha emitido un consentimiento viciado por error, y que este resulta imputable a la parte más fuerte en la relación contractual, se declarará la nulidad radical del contrato de adhesión de que se trate[71]. Esto mismo debe poder predicarse de la cesión de los datos personales lograda por el prestador de servicios sin haber observado sus obligaciones relativas a la información precontractual. En esta dirección parecen ir los tribunales, en primer lugar el Tribunal Constitucional, que en su sentencia de 24 de febrero de 2020 y refiriéndose a la red social Facebook, ha identificado el consentimiento para el tratamiento de datos personales como un verdadero contrato de adhesión:

> «[…] Respecto a la alegada autorización del don I.I.L. para el uso de su imagen formulada en el momento de su inscripción y registro en Facebook, las denominadas "condiciones de servicio" incluidas en la "Declaración de derechos y responsabilidades" que necesariamente deben aceptar los usuarios de Facebook para poder utilizar la red revelan que el contrato suscrito por ambas partes es típicamente de los llamados de

[70] PAGADOR LÓPEZ, Javier, «Condiciones generales y cláusulas abusivas», en *La defensa de los consumidores y usuarios. Comentario sistemático del Texto Refundido aprobado por el Real Decreto Legislativo 1/2007*, Manuel Rebollo Puig y Manuel Izquierdo Carrasco, (Dirs.), Madrid, 2011, p. 1308.

[71] Véase por ejemplo entre las más recientes que afectan al sector bancario, las SSTS 28 febrero 2023 (ECLI:ES:TS:2023:667), y 8 marzo 2023 (ECLI:ES:TS:2023:1097).

> "adhesión", con la particularidad de que se formaliza mediante un clic en el botón de la aplicación digital previsto al efecto. Es decir, estamos en presencia de un contracto electrónico puro. El uso de condiciones generales empleado en este procedimiento de contratación online, sus características, y la falta de capacidad de los usuarios/consumidores para negociar el clausulado, arroja dudas relevantes sobre la existencia de una adecuada manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta indiscriminadamente el tratamiento de su imagen por cualquier tercero que pueda tener acceso a ella. Los avisos legales, las condiciones de uso y las políticas de privacidad están redactadas en un lenguaje generalista, de difícil comprensión para el usuario medio, de tal suerte que, a pesar de encontrarse recogidas en el sitio web, no alcanzan su finalidad última, que no es otra que la comprensión por el usuario del objeto, la finalidad y el plazo para el que otorga dicha autorización»[72].

Para concluir este apartado sobre la tesis del contrato de adhesión encapsulado sobre la cesión de los propios datos personales, es necesario abordar la cuestión de la esencial revocabilidad del consentimiento prestado en materia de datos personales.

El derecho de supresión que asiste a todos los sujetos (art. 17 RGPD), el derecho a retirar el consentimiento y, en consecuencia, la obligación del prestador de servicios de suprimir los datos recabados, trae causa de que la persona nunca pierde la titularidad sobre su información personal. Significa, en los tratamientos basados en el consentimiento del sujeto, que este puede cambiar de criterio en cualquier momento sobre la conveniencia de que sus datos personales sean tratados por el prestador de servicios, y retirar el consentimiento. Volviendo a la Directiva 770/2019 se observa cómo, el hecho de considerar los datos personales como verdadera contraprestación contractual (art. 59.4 Directiva), influye radicalmente en el régimen sobre el incumplimiento del prestador de servicios y los remedios al alcance del consumidor. En efecto, la norma prevé en estos supuestos que el consumidor pueda resolver el contrato, aunque la falta de conformidad sea de escasa importancia porque, como el consumidor no ha pagado precio monetario, no puede solicitar como primer remedio la rebaja del precio, por lo que procede directamente la medida de resolución contractual siempre que se haya intentado primero la reparación. De manera que la resolución contractual puede producirse mucho más frecuentemente en las transacciones digitales «gratuitas» a cambio de datos, en los casos de falta de conformidad del bien o servicio, y ello se entiende por el legislador como una manera de reforzar la posición de control del consumidor que ha «vendido» su privacidad.

[72] STC 24 febrero 2020, (ECLI:ES:TC:2020:27). Véase también SSTJUE 28 abril 2022, (C-319/20, ECLI:EU:C:2022:322), y 1 octubre 2019, (C-673/17, ECLI:EU:C:2019:801).

Sin embargo, al amparo del RGPD, el consumidor no necesita que se produzca una falta de conformidad para poder retirar el consentimiento que autoriza al prestador de servicios a tratar sus datos. Además, dispone la normativa europea que la retirada del consentimiento debe resultar tan fácil como la emisión del consentimiento. En estos casos, ¿se está contemplando una resolución contractual injustificada? ¿un derecho de desistimiento no sujeto a plazo? ¿o se trata de un incumplimiento contractual del consumidor que, por tanto, genera un derecho a ser resarcido, para el prestador de servicios? La Directiva no ha resuelto este problema, lo cual obliga a los Estados miembros a pronunciarse sobre el mismo en sede de trasposición de la directiva. En el caso de España la solución prevista en el artículo 119.ter, 7 del Real Decreto Legislativo 1/2007 (en adelante, TRLGDCU)[73], emplea el término «resolución del contrato», a diferencia del artículo 621-78 del Código civil catalán (en adelante, CCCat.)[74],que se refiere al «desistimiento del contrato». Sin embargo, ni el legislador estatal ni el autonómico entran a definir la revocación del consentimiento efectuada por el usuario, sino que se limitan a regular las consecuencias que la misma tiene para el prestador de servicios digitales. Estas son sustancialmente iguales en ambas normativas: el suministrador podrá dar por terminado el contrato y dejar de prestar el servicio, pero no podrá reclamar resarcimiento de ninguna clase al usuario que, en consecuencia, no incurre de ningún modo en incumplimiento contractual.

En definitiva, entiendo que la interacción entre el derecho contractual (de consumo) y el régimen de protección de datos puede ser conveniente y posible en algunos aspectos, aunque no en todos. Puede permitir la aplicación, por ejemplo, del régimen jurídico de los vicios del consentimiento, en especial el error imputable a la falta de información del prestador de servicios, o las normas imperativas de supresión de cláusulas abusivas en los contratos predispuestos. Pero no cabe obviar que siempre será una relación contractual *sui generis*, por la especial naturaleza de la información personal, que se convierte en objeto de comercio entre las partes.

[73] «7. El ejercicio por el consumidor o usuario de su derecho a retirar su consentimiento u oponerse al tratamiento de datos personales permitirá que el empresario resuelva el contrato siempre y cuando el suministro de los contenidos o servicios digitales sea continuo o consista en una serie de actos individuales y se encuentre pendiente de ejecutar en todo o en parte. En ningún caso el ejercicio de estos derechos por el consumidor supondrá el pago de penalización alguna a su cargo».

[74] «1. En caso de que el adquirente ejerza el derecho a revocar el consentimiento o a oponerse al tratamiento de sus datos personales, en los términos del Reglamento (UE) 2016/679, el suministrador que presta contenidos o servicios digitales de manera continuada durante un periodo de tiempo, o en una serie de actos individuales, puede desistir del contrato si este suministro se encuentra pendiente de ejecución en todo o en parte. 2. El suministrador no puede reclamar al adquirente ninguna indemnización por los daños y perjuicios que pueda causarle el ejercicio de los derechos mencionados».

## 4. MECANISMOS DE TUTELA Y PRETENSIONES DERIVADAS DE LA DEFENSA DEL DERECHO A LA PROTECCIÓN DE DATOS

En este apartado me centraré, ya no en las vulneraciones automatizadas del derecho a la protección de datos, sino en los mecanismos de tutela y en las pretensiones que a través de los mismos persigue el perjudicado.

En cuanto a los mecanismos de tutela, ya me he referido al solapamiento que cabe observar entre las reclamaciones que transitan por la vía administrativa (primero, frente a las autoridades de control y, en su caso, en la vía judicial si se incoa el posterior procedimiento contencioso-administrativo para confirmar o anular la resolución dictada por la Agencia) y las acciones civiles privadas. Y por lo que respecta a las pretensiones perseguidas por los perjudicados (entendiendo este término no desde una perspectiva estrictamente procesal sino más bien en el sentido de la intencionalidad que mueve al sujeto que acciona), pueden clasificarse en tres grandes grupos: a) la sanción punitiva al infractor, b) el resarcimiento económico al perjudicado, y c) la eficiencia de la reclamación de cara al futuro y con carácter general, es decir, conseguir que se generalicen los comportamientos ajustados a derecho por parte de los prestadores de servicios digitales.

Los procedimientos administrativos y contencioso-administrativos derivados de la invocación del RGPD ante las autoridades de control y ante los tribunales de la jurisdicción administrativa, son los que específicamente se dirigen a la imposición, si procede, de una sanción al infractor. El ciudadano ha ido interiorizando la vía de la reclamación ante la Agencia de Protección de datos como un mecanismo útil para sancionar al prestador de servicios digitales sin tener que incurrir en costes de abogado y procurador, en este sentido, como un recurso más barato y más fácil.

No obstante, el sistema se revela insuficiente. Las autoridades de control no imponen sanciones punitivas en todos los casos de infracción y, si lo hacen, no en una cuantía que realmente resulte disuasoria, al menos para las grandes empresas tecnológicas que tratan los datos del ciudadano en las transacciones digitales[75]. Al respecto, es relevante

[75] Siempre hay excepciones. Como la multa millonaria impuesta a Meta por la autoridad de control irlandesa (https://www.lainformacion.com/empresas/meta-facebook-multa-historica-europa/2886562/. Fecha de la consulta 11.03.2024). En España, la Memoria de la AEPD de 2022 habla de multas de 11 millones y medio de euros por infracciones en servicios de internet, pero también reconoce que la Agencia sólo ha impuesto el 2,5% de dichas multas. Puede consultarse en la página web de la AEPD, referencia en nota 61.

la reciente reforma de la LO 3/2018[76], que se adapta a la corrección de errores del RGPD, y de la que se desprende que el apercibimiento no es propiamente una sanción. Se configura como una medida de naturaleza no sancionadora, incluida dentro de los poderes correctivos de las autoridades de control. Y se «promociona» el recurso a la misma mediante la regulación de un procedimiento flexible y rápido, con una duración máxima de seis meses. En consecuencia, cabe sostener que el sistema de reclamaciones arbitrado en torno a las autoridades de control persigue fundamentalmente la rapidez en la respuesta a las reclamaciones de los ciudadanos, y establece la amonestación al responsable del tratamiento de los datos como la medida correctora preferente, para la gran mayoría de los supuestos.

Es cierto que, en ocasiones, la autoridad de control impone una multa como medida disuasoria, al responsable del tratamiento de los datos. Y puede adoptar otras medidas complementarias ex art. 58.2 RGPD, como la de imponer una limitación temporal o definitiva del tratamiento, incluso prohibirlo, ordenando la supresión de determinados datos personales o también la suspensión de los flujos de datos hacia un destinatario situado en un tercer país, o hacia una organización internacional. Pero lo cierto es que hoy por hoy no está sirviendo como incentivo suficiente para que dejen de realizarse determinadas conductas contrarias al derecho a la privacidad de los ciudadanos. Me centraré, por ello, en los otros dos grupos de pretensiones: recibir una compensación económica, y la garantía de que el comportamiento infractor no va a repetirse.

### 4.1. *El resarcimiento por los daños y perjuicios sufridos por la vulneración del derecho a la protección de los propios datos personales. Las acciones privadas*

En el sector privado los tribunales civiles son los competentes para conocer de las reclamaciones de resarcimiento económico que pueda interponer un sujeto perjudicado por cualquier intromisión ilegítima en su derecho fundamental a la protección de sus datos personales. De esta manera, pueden imponer al sujeto infractor, además o al margen del apercibimiento, o de las sanciones administrativas que hubiera recibido, el abono de una indemnización al perjudicado por los daños y perjuicios que hubiera sufrido.

[76] Ya referenciada en la nota 46.

En efecto, la normativa europea de protección de datos contempla el derecho a indemnización del perjudicado en el art. 82 RGPD[77] y, aunque la LO 3/2018 no ha regulado este derecho del ciudadano español[78], ello no debería ser un impedimento dado que el Reglamento europeo es de aplicación directa en todos los Estados de la Unión. Sin embargo, lo cierto es que se trata de un remedio privado incardinado en un sistema normativo con un elevado protagonismo del derecho público y regulatorio, y dependiente, en gran medida, de las normas sustantivas y procesales de cada Estado[79]. Todo lo cual desincentiva a los particulares para invocar su aplicación. Además, las incertidumbres relacionadas con la coordinación entre las reclamaciones civiles y los procedimientos seguidos ante la Agencia de Protección de Datos u otras autoridades de control también reducen el atractivo del art. 82 RGPD.

Por todo ello, la reciente STJUE dictada en el asunto C-300/21 resulta pionera, y puede significar el inicio de un cambio de tendencia con respecto a la solicitud de indemnización económica por lesión a la protección de los propios datos personales en las reclamaciones de los particulares.

Se trata de una cuestión prejudicial presentada por el Tribunal Supremo austriaco en un asunto en el que resulta acreditada la infracción por parte del responsable del tratamiento de los datos[80]. La invocación del art. 82 RGPD suscita dudas prácticas en el tribunal nacional relativas a la carga probatoria del daño, así como a la compatibilidad de la norma europea con un umbral mínimo de daño para ser indemnizado (porque el demandante solo había reclamado 1000 € en concepto de indemnización por daños morales). Las Conclusiones del Abogado General, de fecha 6 de octubre de 2022, contienen ciertas consideraciones (teóricas, de principios), claramente reticentes a la opción de que el ciudadano sea resarcido siempre que se acredite la vulneración de la normativa europea de protección de datos:

[77] Art. 82.1 RGPD: «Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos».

[78] Solo su artículo 30 cita de pasada el 82 RGPD, para establecer la responsabilidad solidaria de los responsables o encargados del tratamiento no establecidos en la Unión Europea. Por el contrario, su precedente legislativo, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal sí que recogía el derecho del ciudadano a un resarcimiento económico en su artículo 19.

[79] Ya manifestó este tipo de problemas para la consolidación práctica del artículo 82 RGPD el profesor Rubí, véase RUBÍ PUIG, Antoni, «Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español», *Derecho Privado y Constitución* (2019), nº 34, pp. 197-232.

[80] Supuesto referenciado en la nota 27.

> «Desde una perspectiva teórica, una interpretación que, en ausencia de cualquier daño, confíe a la responsabilidad civil la función punitiva crea el riesgo de convertir los mecanismos indemnizatorios en redundantes con los sancionadores. En la práctica, la facilidad para obtener una ganancia «punitiva» a título de indemnización podría inclinar a los interesados a preferir esta vía a la del artículo 77 del RGPD. De generalizarse, se privaría a las autoridades de control de un elemento útil (la reclamación del interesado) para conocer y, por tanto, investigar y sancionar posibles infracciones del RGPD, en detrimento de los instrumentos más apropiados para la defensa del interés general. […] Ante la evidencia del valor de los datos (personales y no personales) para el progreso económico y social en Europa, el RGPD no pretende magnificar el control del individuo sobre la información que le concierne, plegándose sin más a sus preferencias, sino reconciliar el derecho a la protección de los datos personales de cada uno con los intereses de terceros y de la sociedad».

El TJUE, en la Sentencia de 4 de mayo de 2023, atiende estas consideraciones y resuelve que, de la interpretación sistemática del RGPD se desprende que la mera infracción de la norma no es suficiente para solicitar una indemnización, dado que también se requiere la existencia efectiva de daños y perjuicios, y una relación de causalidad entre los daños y la infracción, resultando estos tres requisitos acumulativos. Ello, a pesar de la dicción literal del apartado tercero del art. 82 RGPD, que conduce inevitablemente a la traslación de la carga de la prueba de la concurrencia del tercer requisito (la relación de causalidad) al responsable o encargado del tratamiento, ya que establece que este «resultará exento de responsabilidad si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios».

También señala el TJUE que no es compatible con el derecho de la Unión la exigencia austríaca de un umbral mínimo de gravedad, sería contradictorio únicamente indemnizar los daños graves. Ahora bien, en cualquier caso, corresponde al afectado probar la existencia de estos daños inmateriales, por mínimos que sean. En tercer lugar, en relación con la cuestión de la cuantificación del daño, el TJUE establece que, siempre que se respeten los principios de equivalencia y efectividad del Derecho de la Unión, los jueces deben aplicar las normas internas de cada Estado para cuantificar la indemnización, dado que no hay ninguna disposición del RGPD que regule cómo proceder y calcular la misma.

En definitiva, habrá que estar a la espera de los efectos de esta Sentencia en el futuro. Dado que el TJUE ha establecido que no existe un umbral mínimo indemnizable, cabe prever un aumento de las reclamaciones judiciales por daños y perjuicios en la UE, si bien no es tan esperable que ello ocurra en concreto en España. En nuestro país, la

posibilidad de reclamar una indemnización al perjudicado por lesiones a su imagen (digital) se concreta en la invocación del art. 9.3 L.O. 1/1982, que establece precisamente lo contrario a lo que ha resuelto el TJUE para el art. 82 RGPD. Dice literalmente el 9.3:

> «La existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima»[81].

Otra cuestión determinante con respecto a la pretensión de indemnización es la relativa a la cuantificación del daño. Señala el TJUE que este elemento queda en manos de los tribunales nacionales, que aplicarán el derecho nacional y, en este sentido, pueden resolver de forma bien diferente en un Estado u otro. Pero es que, además, desde una perspectiva objetiva, el problema de la cuantificación del daño deriva de la especial naturaleza de los datos personales. ¿cuál es el daño causado por la publicación del nombre de usuario y la contraseña de acceso a una red social de un individuo? ¿cuál es el daño causado por la publicación de las características personales sociales y económicas de un individuo? Una persona puede ver vulnerada su privacidad y, solo por ello, el daño indudablemente existe. Pero ¿cómo cuantificarlo?

Las dificultades relativas a la cuantificación de los daños resultantes de la vulneración de la privacidad de los individuos diluyen la estructura de incentivos del régimen de protección de datos y, al mismo tiempo, anticipando la improbable acción judicial de la víctima, las páginas web, plataformas y aplicaciones digitales tampoco tienen incentivos para tomar medidas efectivas que protejan los datos y la privacidad de sus usuarios.

A partir de esta constatación, procede analizar a continuación las acciones de representación para la defensa de los intereses colectivos relacionados con la privacidad. El derecho a la protección de los datos personales no tiene una lógica

[81] Ya he citado *supra* la primera vez que el Tribunal Supremo condenó a pagar una indemnización por vulneración del derecho al olvido digital mediante sentencia de 15 de octubre de 2015 y, en la actualidad, existe una jurisprudencia consolidada en la materia. Es significativa a este respecto la sentencia de 17 de mayo de 2021 (RJ 2021\2889, que resume una serie de criterios jurisprudenciales sobre la indemnización por daños morales: «1) el hecho de que la valoración del daño moral no pueda obtenerse de una prueba objetiva no excusa ni imposibilita legalmente a los tribunales para cuantificarla, a cuyo efecto ha de tenerse en cuenta y ponderar las circunstancias concurrentes en cada caso; 2) no son admisibles las indemnizaciones de carácter meramente simbólico; 3) se trata de una valoración estimativa, que, en el caso de daños morales derivados de la vulneración del derecho fundamental del artículo 18.1 CE, ha de atender a los parámetros previstos en el artículo 9.3 LO 1/1982, utilizando criterios de prudente arbitrio».

únicamente individual. Despliega también una dimensión colectiva, por ejemplo, a partir del fenómeno de la elaboración de perfiles, que los sistemas de IA han hecho proliferar exponencialmente. El suministro de datos efectuado libremente por una persona impacta en todas las otras personas con las que guarda afinidad (entendiendo por grupo de afinidad el compuesto por todas las personas automáticamente agrupadas por el algoritmo, desde el momento en que este les atribuye los mismos intereses). Es necesario, por tanto, adentrarse en el análisis de la eficiencia de una eventual salvaguarda de los intereses generales, que puede contar con ventajas comparativas frente al ejercicio de las acciones privadas[82].

### 4.2. *Las acciones de representación para la defensa de los intereses colectivos relacionados con la privacidad de las personas*

Existen intereses colectivos dignos de salvaguarda en materia de protección de datos. En concreto, la pretensión de lograr la eficiencia de la reclamación de cara al futuro, es decir, conseguir que se generalicen los comportamientos ajustados a derecho por parte de los prestadores de servicios digitales (especialmente los gigantes tecnológicos a los que difícilmente pueden doblegar las multas punitivas) solo cabe obtenerla por esta vía.

En efecto, muchas de las cuestiones que han ido aflorando al hilo del análisis jurisprudencial, tales como la mejorable calidad del consentimiento del usuario, o las exigencias que debe observar la información precontractual que proporciona el prestador de servicios, o la necesidad de lograr la cesación de determinadas prácticas desleales en la obtención y en el tratamiento de los datos, se convierten en objetivos que deberían abordarse colectivamente, en beneficio de todos los usuarios. Se trata de luchar frente a determinadas conductas cuya perpetración afecta, directa o indirectamente, al colectivo de las personas físicas que contratan por internet y, previamente, ceden su información personal. Se trata de conductas que tienen la vocación de reproducirse en el tiempo, o lo que es lo mismo, presentan un carácter continuado. Pero ¿cuál es el estado de la cuestión con respecto a las acciones colectivas en materia de privacidad?

[82] RUBÍ PUIG, Antonio, «Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español», *op. cit*., p. 208; WACHTER, Sandra, «Affinity Profiling and Discrimination by Association in Online Behavioural Advertising», *Berkeley Technology Law Journal* (2020), nº 35-2, consultable en: https://ssrn.com/abstract=3388639. (Fecha de la consulta 11.03.2024).

Comenzando por el propio RGDP, resulta que el art. 80 por un lado permite que cualquier interesado otorgue mandato en favor de una organización o asociación de las que cumplen los requisitos previstos en la norma para que presente en su nombre una reclamación, y por otro lado permite que los Estados miembros dispongan lo procedente para que estas entidades, actuando sin mandato, puedan presentar una reclamación colectiva ante la autoridad administrativa o ante los tribunales civiles, si considera que los derechos colectivos de los interesados han sido vulnerados. De manera que las acciones colectivas instadas por mandato de un grupo de ciudadanos para defender su privacidad ya están consagradas en la norma europea, y se aplican directamente, y las acciones colectivas sin mandato dependen del desarrollo legislativo que tenga lugar en cada Estado miembro. Las acciones colectivas que dependen de un mandato expreso de los ciudadanos no siempre funcionan[83], y hay un ejemplo paradigmático que pone de manifiesto el estado de la cuestión en nuestro país: se trata de la sentencia del Tribunal Constitucional de 7 de mayo de 2012[84], en la que, precisamente la defensa de la privacidad de los ciudadanos, se volvió en contra de los propios consumidores[85].

En segundo lugar, la Directiva 2020/1828 del Parlamento europeo y del Consejo de 25 de noviembre de 2020 relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22 (en adelante Directiva 2020/1828[86]), insta a los Estados miembros a que regulen esta cuestión y permitan, así, a las organizaciones que ellos consideren que presenten acciones colectivas para obtener tanto medidas de cesación como medidas resarcitorias en nombre de grupos de consumidores. Se trata de una norma que

[83] Cfr. SANDE MAYO, María Jesús, *Las acciones colectivas en defensa de los consumidores*, Aranzadi, Cizur Menor (Navarra), 2018. Véase especialmente pp. 196 y ss.

[84] RTC\2012\96.

[85] Concretamente, la asociación ADICAE pretendía presentar acción de cesación de conductas contrarias a la legislación en materia de cláusulas abusivas, a la que se acumularían otras como la acción de nulidad contractual por vicios del consentimiento y acciones restitutorias e indemnizatorias. Para contactar con los consumidores a los que pretendía proteger, a los efectos de que estos, si así lo estimaban adecuado, les otorgaran mandato de representación, ADICAE instó petición de diligencias preliminares para que la entidad financiera le entregara los listados diferenciados por productos financieros con los datos personales (nombre y apellidos, DNI, dirección postal actualizada, y número de teléfono, fax y correo electrónico, si estuvieren disponibles), de los clientes personas físicas que, en toda España, hubieran contratado con dicha entidad bancaria determinados productos financieros (los famosos swap). Lo que se inició como una solicitud de diligencias preliminares para la interposición de una acción civil se tornó un Recurso de Amparo ante el Tribunal Constitucional a instancias de una poderosa entidad financiera como el BBVA, que obtuvo del TC la declaración de inconstitucionalidad del Auto judicial que obligaba al banco a proporcionar los datos de los usuarios que habían contratado estos productos.

[86] Consultable en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020L1828. (Fecha de la consulta 11.03.2024). Cfr. AGULLÓ AGULLÓ, Diego, *La acción en defensa de los consumidores. Aspectos nacionales y transfronterizos*, Atelier, Barcelona, 2023, especialmente pp. 55-68.

debería haber sido ya objeto de transposición en nuestro país[87], y que en su Anexo I, dentro del listado de normas susceptibles de ser protegidas a través de las acciones colectivas, incorpora el RGPD[88].

Por lo tanto, el legislador europeo habilita a las organizaciones u organismos públicos designados por los Estados miembros para obtener, tanto medidas de cesación como medidas resarcitorias, en nombre de grupos de consumidores recurriendo a las acciones de representación (incluidas las transfronterizas). Una medida de cesación es una orden provisional o definitiva de dejar de realizar una práctica, o que prohíbe la misma. También puede conllevar, en su caso, la obligación de publicar el fallo judicial o una declaración de rectificación. La entidad habilitada no tendrá la obligación de demostrar que se ha producido una pérdida, daño o perjuicio efectivo en los usuarios afectados por la infracción, ni tampoco que se ha producido dolo o negligencia, en nuestro caso, imputable al empresario digital. En cuanto a las medidas resarcitorias, sirven para exigir al empresario que proporcione soluciones, ya sea la indemnización u otras, según corresponda y se disponga de ellas en virtud del Derecho de la Unión o la legislación nacional. Así que reviste una especial importancia el modo en que finalmente se produzca la trasposición de la Directiva 2020/1828 en España[89].

La viabilidad de ejercitar acciones colectivas en defensa del derecho a la protección de datos es una cuestión que el TJUE ya ha tenido que plantearse. El supuesto más representativo es el que resuelve mediante sentencia de 28 de abril de 2022, en el

[87] La fecha límite para su plena aplicación en los Estados miembros era el 25 de junio de 2023.

[88] Por si esto fuera poco, el Considerando 17 de la Directiva 2020/1828 deja claro que el Anexo I no pretende «fosilizar» el *corpus* normativo que aparece listado y, por supuesto, autoriza a los Estados miembros a ampliar, si lo consideran oportuno el ámbito de aplicación.

[89] La futura normativa española sobre acciones de representación para la protección de los intereses colectivos de los consumidores se encuentra en plena tramitación. El 12 de marzo de 2024 el Consejo de Ministros ha aprobado un anteproyecto de ley en el que el Ministerio de Derechos Sociales, Consumo y Agenda 2030 es co-proponente junto con el Ministerio de Justicia. Se denomina Anteproyecto de la Ley Orgánica de Medidas en Materia de Eficiencia del Servicio Público de Justicia y de Acciones Colectivas para la Protección de los Derechos e Intereses de los Consumidores y Usuarios. Todo indica que el legislador optará finalmente, con carácter general, por el sistema de vinculación a la acción colectiva por defecto (opt-out), permitiendo solo de forma excepcional la vinculación por adhesión (opt-in). Entre la doctrina procesalista parece haber algún recelo con respecto a este mecanismo (Cfr. https://almacendederecho.org/vinculacion-por-defecto-opt-out-en-las-acciones-de-representacion.Fecha de la consulta 11.03.2024). No entraré en esta cuestión que excede el objeto del trabajo y de los conocimientos de quien lo suscribe, si bien, a la espera de poder disponer de un texto legal vigente, parece que podría resultar más eficiente una acción colectiva en defensa de la privacidad de los usuarios -hasta el punto de hacer cambiar las prácticas de los empresarios digitales-, si se mantiene el sistema propuesto, de adhesión por defecto. Así, los efectos de la acción colectiva podrían alcanzar a un grupo mucho mayor de personas.

asunto C-319/20[90]. Es un caso en el que la Federación alemana de Asociaciones de Consumidores había presentado un litigio contra Meta (Facebook) instando a la cesación de determinadas prácticas para la obtención de los datos de los usuarios, que consideraba desleales. El TJUE entiende que el artículo 80 RGPD permite que los Estados miembros habiliten a las asociaciones de consumidores para ejercitar acciones contra las vulneraciones de los derechos relacionados con los datos personales, y ello sin que sea preciso que tales asociaciones se constituyan de forma concreta para proteger este derecho de las personas físicas:

> «El artículo 80, apartado 2, 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, debe interpretarse en el sentido de que no se opone a una normativa nacional que permite a una asociación de defensa de los intereses de los consumidores ejercitar acciones judiciales sin mandato conferido a tal fin y con independencia de la vulneración de derechos concretos de los interesados, contra el presunto infractor de la normativa en materia de protección de datos personales, invocando el incumplimiento de la prohibición de prácticas comerciales desleales, de una ley en materia de protección de los consumidores o de la prohibición del uso de condiciones generales nulas, toda vez que el tratamiento de los datos de que se trate pueda afectar a los derechos que este Reglamento confiere a personas físicas identificadas o identificables»[91].

De esta manera el TJUE está vinculando formalmente la cuestión de los datos con el derecho de consumo, de la misma forma que lo hace la Directiva 2020/1828, que permite a las entidades habilitadas interponer, tanto acciones representativas, a través de las que se defienden derechos de particulares concretos, como acciones destinadas a la defensa de un interés general. En el mismo sentido la Directiva 770/2019 sobre

[90] TJCE\2022\85. Cfr. TORRALBA MENDIOLA, Elisa, «Las asociaciones de defensa de los intereses de los consumidores pueden ejercer acciones colectivas en materia de protección de datos», *Revista CESCO de Derecho de consumo*, 2022, pp. 1-5. Consultable en https://centrodeestudiosdeconsumo.com/images/Las_asociaciones_de_defensa_de_los_intereses_de_los_consumidores_pueden_ejercer_acciones_colectivas_en_materia_de_proteccion_de_datos.pdf (Fecha de la consulta 11.03.2024).

[91] También la STJUE 15 junio 2021 (cit.) había resuelto una cuestión prejudicial en el sentido de admitir la facultad de las autoridades de control para poner en conocimiento de los órganos jurisdiccionales de ese Estado miembro cualquier supuesta infracción de dicho Reglamento y, si procede, para iniciar o ejercitar acciones judiciales en lo que respecta a un tratamiento de datos transfronterizo, aunque no sea la «autoridad de control principal», siempre que se respeten los procedimientos de cooperación y de coherencia establecidos por dicho Reglamento.

suministro de contenidos digitales[92], propugna el derecho, tanto de las autoridades de control como de las asociaciones de consumidores para instar acciones, tanto administrativas como civiles, en defensa de los intereses colectivos de los ciudadanos. Todo lo cual avala la tesis de que las condiciones generales que el usuario ha de consentir cuando acepta la política de privacidad de un prestador de servicios digitales, son comprendidas por el legislador y también por el juzgador europeo, como un verdadero contrato de adhesión. Se puede sostener que protección de datos y derechos contractuales de los consumidores, a pesar de ser dos materias diferentes en cuanto a su contenido, aparecen muy conectadas en el contexto de la economía digital y de la protección de la que Europa pretende dotar a las personas físicas. Por eso ambas materias reciben una regulación entrelazada, en la Directiva sobre contratos de suministro de contenidos digitales. Habrá que ver si la futura ley de acciones de representación incluye la protección de datos en su ámbito objetivo de aplicación, lo cual obviamente sería lo deseable[93].

Teniendo en cuenta el protagonismo que tanto el artículo 80 RGPD como la propia Directiva 1828/2020 atribuyen a la regulación nacional de los diferentes Estados miembros sobre las acciones de representación, es preciso remitirse al vigente artículo 15.bis de nuestra Ley de Enjuiciamiento Civil. Esta norma permite la intervención voluntaria, o a instancia del órgano judicial, de las autoridades de control tanto la estatal como las autonómicas, en los procesos que afecten a cuestiones relativas a la aplicación del RGPD. Ahora bien, esta intervención no se realiza en condición de parte en el proceso, ni en representación de ningún colectivo, sino que su función se reduce a aportar información relevante o a realizar observaciones escritas u orales, que puedan ayudar al órgano jurisdiccional a adoptar la resolución correspondiente. Esta norma fue incorporada a la LEC en virtud de la Disposición final 7ª de la LO 3/2018, y ahora debería someterse a revisión con ocasión de la elaboración de la norma que acomete la trasposición de la Directiva europea. Porque, a la luz de la Directiva 2020/1828 y de la dicción del artículo 80 RGPD nada impediría al Estado español habilitar para el ejercicio

[92] Cfr. Cdo. 79: «Las personas o las organizaciones que según el Derecho nacional tienen un interés legítimo en proteger los derechos contractuales de los consumidores y en materia de protección de datos deben tener derecho a iniciar procedimientos para garantizar que se apliquen las disposiciones nacionales por las que se transponga la presente Directiva a Derecho interno, ya sea ante una autoridad administrativa o un órgano jurisdiccional competente para decidir sobre las reclamaciones o iniciar los procedimientos judiciales oportunos».

[93] El artículo 828.1 (Ámbito de aplicación del presente título) del Anteproyecto no lo hace: «1. Las disposiciones de este título serán aplicables a los procesos en que se ejerciten acciones de representación frente a conductas de empresarios o profesionales que infrinjan los derechos e intereses colectivos de los consumidores y usuarios».
Cfr.https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/Anteproyecto%20de%20Ley%20acciones%20representativas.pdf (Fecha de la consulta 13.03.24).

de las acciones colectivas relacionadas con la vulneración de la privacidad de los ciudadanos a las agencias de protección de datos. También, por el contrario, puede optar por la solución de ampliar expresamente el objeto sobre el que recae la función de protección que ejercen las asociaciones de consumidores.

Si las autoridades de control ostentan la legitimación activa para interponer acciones colectivas, simplemente alegando que determinado tratamiento de datos puede afectar a los derechos que el RGPD confiere a personas físicas identificadas o identificables, entonces decaería la función «pericial» que les atribuye el artículo 15 bis LEC, porque no se puede intervenir en el proceso en calidad de perito o experto independiente, si ya se interviene como parte actora.

Insiste el legislador español en que la Directiva europea no diseña un procedimiento colectivo por el que deban sustanciarse las acciones de representación, y ni siquiera articula las fases de una estructura procedimental. Por el contrario, esta tarea corresponde a los Estados miembros que deben configurar las dos modalidades (acciones de cesación y acciones resarcitorias) de acuerdo con su propia tradición jurídica. Así pues, el Estado español entiende que la tutela colectiva de los consumidores debe vehicularse exclusivamente ante los órganos jurisdiccionales civiles, y en ningún caso, ante autoridades administrativas. Por ello se propone la modificación de la normativa procesal civil, y la regulación de las entidades habilitadas para ejercer las acciones de representación para la protección de los intereses colectivos de los consumidores.

En este contexto, entiendo que en el futuro pueden adquirir especial relevancia las acciones colectivas de cesación que puedan interponerse con el objeto de frenar determinados mecanismos automatizados y técnicas de recopilación de datos empleadas en la actualidad por los gigantes tecnológicos, los llamados «guardianes de acceso» [94]. Estos procedimientos obligarían a ponderar los intereses en juego y concluirían con importantes resoluciones civiles en las que se irían sentando criterios de prevalencia, en cada caso, de los intereses que entran en colisión.

## 5. REFLEXIONES CONCLUSIVAS

Tras lo expuesto, las cuestiones que resaltaré son dos. Por una parte, la relación cada vez más estrecha entre la protección de datos y el derecho de consumo. Y ello por el fundamento legal que sustenta la cesión de los datos personales a los prestadores de

[94] Que se encuentran sujetos al Reglamento 2022/1925.

servicios digitales (el consentimiento de su titular), y por la fórmula empleada/impuesta por el mercado (la prestación del consentimiento mediante asentimiento global a toda la política de privacidad). Entiendo que la interacción entre el derecho contractual (de consumo) y el régimen de protección de datos puede ser conveniente y posible en algunos aspectos, por ejemplo, mediante la aplicación del régimen jurídico de los vicios del consentimiento, en especial el error imputable a la falta de información del prestador de servicios, o de las normas imperativas de supresión de cláusulas abusivas en los contratos predispuestos.

En segundo lugar, quiero destacar la relevancia que pueden llegar a tener las acciones de representación en defensa de los intereses colectivos de las personas físicas, si se emplean para lograr una tutela real y efectiva de los intereses de la persona con respecto a su imagen digital y a su privacidad.

## BIBLIOGRAFÍA

AGULLÓ AGULLÓ, Diego, *La acción en defensa de los consumidores. Aspectos nacionales y transfronterizos*, Atelier, Barcelona, 2023.

ANTÓN JUÁREZ, Isabel, «Personalización de precios a través de la inteligencia artificial y el Big Data», en *El sistema jurídico ante la digitalización: estudios de Derecho privado*, Manuel Paniagua Zurera (Dir.), Tirant lo Blanch, Valencia, 2021, pp. 379-416.

ARTIGOT GALOBARDES, Mireia, «Las inherentes limitaciones del modelo autodeterminista de protección de datos en Europa», *Revista General de Derecho de los Sectores Regulados* (2021), nº 8, pp. 1-27.

BINNS, Reuben, VEALE, Michael, «Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR», *Internet Data Privacy Law* (2021), pp. 1-14.

BLANDINO GARRIDO, M.ª Amalia, «El consentimiento del interesado al tratamiento de sus datos personales en las comunicaciones electrónicas», *Revista de Derecho civil*, vol. IX (2022), nº 4, pp. 195-228.

CABEDO MALLOL, Vicente, «El derecho fundamental a la protección de datos personales», *Marco jurídico de la ciencia de datos*, Francisca Ramón Fernández y Alicia Barnard Amozurrutia (eds.), Tirant lo Blanch, Valencia, 2020, pp. 81-92.

CARRASCO PERERA, Ángel, «Resolución de contrato pagado con datos personales como precio», *Revista CESCO de Derecho de consumo*, pp. 1-2.

CASEY, Bryan, FARHANGI, Ashkon, VOGL, Roland, «Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise», *Berkeley Technology Law Journal* (2019), nº 34, 1, pp. 143-188.

DE BARRÓN ARNICHES, Paloma, «La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)», *Cuadernos Europeos de Deusto* (2019), nº 61, pp. 29-65.

DÍAZ LAFUENTE, José, «Los desafíos de la sociedad global digitalizada y la protección de datos personales. Análisis de la elaboración de perfiles en el Reglamento General de Protección de datos de la Unión Europea», en *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*, Rosario García Mahamut y Beatriz Tomás Mallén (edit.), Tirant lo Blanch, Valencia, 2019, pp. 287-310.

GARCÍA MAHAMUT, Rosario, «Del Reglamento General de Protección de datos a la LO 3/2018 de protección de datos personales y garantías de los derechos digitales», en *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*, Rosario García Mahamut y Beatriz Tomás Mallén (edit.), Tirant lo Blanch, Valencia, 2019, pp. 95-131.

GARCÍA-RIPOLL MONTIJANO, Martin, «El consentimiento al tratamiento de datos personales», en *Protección de Datos Personales*, coord. por Isabel González Pacanowska, Tirant lo Blanch, Valencia, 2020, pp. 79-160.

GRIMALT SERVERA, Pedro, «Intromisiones ilegítimas en los derechos al honor, a la intimidad y a la propia imagen: tutela civil versus tutela administrativa», en *Protección de Datos Personales*, coord. por Isabel González Pacanowska, Tirant lo Blanch, Valencia, 2020, pp. 309-372.

GUTIÉRREZ Miren y DIAZ-SANZ, Marina, «Deperipheralisation of people and states in the algorithmic assemblage: court cases and a proposal for a new social contract» (Published online: 13 Mar 2023, consultable en https://doi.org/10.1080/04353684.2023.2182226).

ILLESCAS ORTIZ, Rafael, *Derecho de la contratación electrónica*, Thomson Reuters, Cizur Menor (Navarra), 2019.

LÓPEZ AGUILAR, Juan Fernando, «La protección de datos en la UE: el punto de vista del parlamento europeo», en *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*, Rosario García Mahamut y Beatriz Tomás Mallén (edit.), Tirant lo Blanch, Valencia, 2019, pp. 31-55.

MAGGIOLINO, Mariateresa, «Personalized Prices in European Competition Law», *Bocconi Legal Studies* (2017), Research Paper Nº 2984840, Consultable en https://ssrn.com/abstract=2984840

MARTÍN CASALS, Miquel, «Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial», *InDret* (2023), 3, pp. 55-100.

MARTÍNEZ CALVO, Javier, «Dualidad normativa en la regulación de los contratos gratuitos de suministro de contenidos y servicios digitales: la necesaria armonización entre la Directiva (UE) 2019/770 y el Reglamento (UE) 2016/679», *Actualidad jurídica iberoamericana* (2022), nº 16, pp. 1168-1185.

MARTÍNEZ ESPÍN, Pascual, «La propuesta de marco regulador de los sistemas de inteligencia artificial en el mercado de la UE», *Revista CESCO de Derecho de consumo* (2023), nº 46, pp.1-20.

PAGADOR LÓPEZ, Javier, «Condiciones generales y cláusulas abusivas», en *La defensa de los consumidores y usuarios. Comentario sistemático del Texto Refundido aprobado por el Real Decreto Legislativo 1/2007,* Manuel Rebollo Puig y Manuel Izquierdo Carrasco (Dirs.), Madrid, 2011, pp. 1306-1442.

PUERTO, M.ª Isabel y SFERRAZZA Pietro, «La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional», en *Revista Derecho del Estado* (2018), nº 40, pp. 209-236.

RUBÍ PUIG, Antonio:

- «Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores», *Revista de educación y derecho* (2021), nº 24, pp. 1-24.

- «Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español», *Derecho Privado y Constitución* (2019), nº 34, pp. 197-232.

RUDA GONZÁLEZ, Albert, «Indemnización por daños al derecho al olvido. La responsabilidad por la no exclusión de la indexación de una hemeroteca digital por los buscadores generales (Caso El País)», *Cuadernos Civitas de Jurisprudencia Civil* (2016), nº 101, pp. 289-332.

SAINZ DE JUBERA HIGUERO, Beatriz, «Retos jurídicos de la inteligencia artificial en el ámbito del consentimiento contractual: una aproximación general», *Revista de Derecho civil*, vol. X, (2023), nº 2, pp. 41-70.

SANDE MAYO, María Jesús, *Las acciones colectivas en defensa de los consumidores*, Aranzadi, Cizur Menor, 2018.

SANTOS MORÓN, María José:

- «Los contornos del derecho al olvido en España. la aplicación por los tribunales españoles de la jurisprudencia europea», *Revista de Derecho Civil*, vol. IX (2022), nº 2, pp. 71-112

- «Tratamiento de datos, sujetos implicados, responsabilidad proactiva», en *Protección de Datos Personales,* coord. por Isabel González Pacanowska, Tirant lo Blanch, Valencia, 2020, pp. 23-78.

TORRALBA MENDIOLA, Elisa, «Las asociaciones de defensa de los intereses de los consumidores pueden ejercer acciones colectivas en materia de protección de datos», *Revista CESCO de Derecho de consumo* (2022), pp. 1-5.

VILASAU I SOLANA, Mónica:

- «La realización de perfiles y la salvaguardia de los derechos y libertades del afectado», en *Retos jurídicos de la inteligencia artificial,* coord. por Agustí Cerrillo i Martínez y Miguel Peguera Poch, Aranzadi, Cizur Menor, 2020, pp. 182-183

- «Las exigencias de información en el RGPD y en la LO 3/2018 de Protección de Datos y Garantía de los Derechos Digitales, ¿contribuyen a la formación de un consentimiento de mejor calidad?», en *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,* Rosario García Mahamut y Beatriz Tomás Mallén (edit.), Tirant lo Blanch, Valencia, 2019, pp. 209-236.

WACHTER, Sandra, «Affinity Profiling and Discrimination by Association in Online Behavioural Advertising», *Berkeley Technology Law Journal* (2020), nº 35-2, Consultable en: https://ssrn.com/abstract=3388639.

WAGNER, Gerhard y EIDENMÜLLER Horst, «Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions», *The University of Chicago Law Review*, Vol. 86 (2019), nº 2, pp. 581-609.

Fecha de recepción: 27.07.2023

Fecha de aceptación: 21.03.2024