PRIVACIDAD DE GRUPO: UN RETO PARA EL DERECHO A LA PROTECCIÓN DE DATOS A LA LUZ DE LA EVOLUCIÓN DE LA INTELIGENCIA ARTIFICIAL[1]

Group privacy: a challenge for data protection law in the light of the evolution of artificial intelligence

JOSÉ ANTONIO CASTILLO PARRILLA
Universidad de Granada
castillop@ugr.es

Cómo citar/Citation
Castillo Parrilla, J. A. (2023).
Privacidad de grupo: un reto para el derecho a la protección de datos a la luz de la evolución de la inteligencia artificial.
Derecho Privado y Constitución, 43, 53-88.
doi: https://doi.org/10.18042/cepc/dpc.43.02
(Recepción: 11/08/2023; aceptación tras revisión: 16/10/2023; publicación: 29/12/2023)

Resumen

Uno de los derechos fundamentales que más afectados se ven por el desarrollo de la inteligencia artificial (IA) es el derecho a la protección de datos, que hasta ahora se ha caracterizado como un derecho de no injerencia o de primera generación. Debido al desarrollo de la IA basada en datos y la analítica de datos en masa (que permite microsegmentar a la población), el derecho a la protección de datos ha adquirido una dimensión colectiva que lo acerca a derechos de tercera generación, como el derecho a un medio ambiente saludable o el derecho de consumidores.

[1] Esta publicación es parte del contrato RYC2021-031430-I, financiado por MCIN/AEI/10.13039/501100011033 y por la Unión Europea, «NextGenerationEU». Se desarrolla en el marco del Proyecto GOIA, financiado por MCIN/AEI/TED2021-12902B-C22 y por la Unión Europea, «NextGenerationEU». Gran parte de la investigación se realizó durante la estancia desarrollada en la Universidade Nova de Lisboa durante los meses de abril a junio de 2023, financiada por el Programa José de Castillejo (CAS22/0473).

La expresión «privacidad de grupo» ha sido precisada como la privacidad correspondiente a grupos definidos por cualquier característica o combinación de estas. En este trabajo propondremos una noción complementaria de privacidad de grupo, centrada en la defensa del derecho a un medio ambiente digital saludable.

Palabras clave

Privacidad de grupo; protección de datos; inteligencia artificial; perfilado; artículo 22 RGPD.

Abstract

One of the fundamental rights most affected by the development of AI is the right to data protection, which until now has been characterised as a non-interference or first generation right. Due to the development of data-driven AI and big data analytics (which allows for micro-segmentation of the population) the right to data protection has acquired a collective dimension that brings it closer to third generation rights such as the right to a healthy environment or consumer rights.

The term "group privacy" has been defined as privacy corresponding to groups defined by any characteristic or combination of characteristics. In this paper we will propose a complementary notion of group privacy, focusing on the defence of the right to a healthy digital environment.

Keywords

Group privacy; data protection; artificial intelligence; profiling; article 22 GDPR.

SUMARIO

I. INTRODUCCIÓN. ALGUNOS CASOS CONOCIDOS VISTOS DESDE LA ÓPTICA DE LA PRIVACIDAD DE GRUPO

¿Qué es lo primero que hacen cuando se despiertan por la mañana? Probablemente apagan la alarma del móvil o lo consultan para ver la hora, para revisar un periódico o para entrar en alguna red social. Muy probablemente mirar el móvil también sea lo último que hacen antes de dormir. Si tienen un reloj inteligente atado a su muñeca, probablemente curioseen la calidad de su sueño, los minutos exactos que han dormido (incluso cuántos corresponden a cada fase del sueño) o sus pulsaciones, y quizá no sean los únicos que lo curioseen[2]. Es probable que durante el desayuno comenten con su pareja, sus amigos o sus compañeros de trabajo alguna noticia que hayan leído (especialmente si es un vídeo o noticia que va encabezado por la palabra «zasca» o alguna parecida) ¿Escuchan la radio por internet? ¿Utilizan YouTube para buscar *podcasts*, entrevistas, música…? ¿Ven series en plataformas como Netflix, HBO, Amazon Prime, etc.? ¿Se han percatado de que en algunas de estas plataformas las sugerencias de contenido van acompañadas de un porcentaje que indica la probabilidad de que les guste? ¿Han probado a abrir

[2] Veliz (2020: 7-8) alerta sobre el interés de empresas en conocer estos datos de sus empleados.

la cuenta de su pareja, de un familiar o de un amigo en YouTube o en alguna plataforma (siempre con permiso de la persona)? Hagan la prueba. Verán que parece tratarse de dos plataformas completamente diferentes.

Estoy seguro de que no se les escapa que esto es posible gracias a que el historial de navegación, las conversaciones (a través del teléfono y en la calle, con algún teléfono cerca), la forma en que movemos el ratón[3], la ubicación, etc., están siendo rastreados y analizados, e introducidos en herramientas de analítica de datos en masa que permiten trazar un perfil muy preciso de cada persona. Los problemas relativos al perfilado no acaban con esto. Es probable que, incluso, si nuestra actividad en internet es escasa o nula, la cantidad de datos ya existentes[4] que vienen siendo objeto de procesado masivo y, sobre todo, la cantidad de perfiles abstractos que ya se han generado con dichos datos permitan trazar un perfil de nuestras características o de nuestra personalidad como el de aquellas personas que jamás se separan del teléfono móvil, tienen un *smartwatch*, una *smart TV*, y aceptan las *cookies* con la impaciencia de quien lo único que quiere es ver la información que hay detrás.

¿Qué ocurriría si como consecuencia de encajar en un determinado perfil social tuviéramos más probabilidades de ser investigados «aleatoriamente» por fraude? ¿Y si nuestras características encajan con un perfil crediticio de riesgo? ¿Qué pasa si un tribunal de justicia utiliza una herramienta que evalúa la probabilidad de que volvamos a cometer un delito, y esto condiciona decisiones que pueda tomar acerca de nuestro futuro? O, finalmente, ¿puede la microsegmentación de la población en perfiles abstractos ayudar a captar indecisos del partido o la opción contraria en un proceso electoral en distritos clave y alterar con ello el resultado de unas elecciones?

SyRI es un instrumento desarrollado por el Gobierno holandés para prevenir y combatir el fraude a la seguridad social que se sirve de un algoritmo de procesado de datos en masa, que son anonimizados y luego analizados y relacionados entre sí. Como resultado, emite informes de riesgo sobre la probabilidad de cometer fraude a la seguridad social a través de un uso inapropiado de fondos o del incumplimiento de la normativa vigente[5]. En febrero

---

[3] Los programas de *clickstream* registran cada movimiento de ratón para seguir la ruta de un usuario por las webs que visita, y dentro de estas webs, y, de este modo, medir la efectividad de los anuncios o el interés en los productos ofertados. Los datos de clics se recogen a través de *cookies* no técnicas que identifican al usuario y personalizan la navegación (Holmes, 2018: 26-29).

[4] La Comisión Europea (2020b) prevé que el volumen de datos producido en el mundo pase de 33 *zetabytes* en 2018 a 175 *zetabytes* en 2025.

[5] Corte de Distrito de La Haya (2020: pars. 3.1, 3.2 y 4.17). *Vid*. también Van Dalen *et al*. (2016: 12-13).

de 2020 la Corte de Distrito de La Haya consideró que SyRI no ofrecía suficientes garantías para lograr una mínima injerencia en la privacidad de acuerdo con el art. 8 CEDH[6].

Las últimas normas en materia de crédito responsable prevén la obligación de evaluar la solvencia del solicitante del crédito, con el objetivo de evitar el sobreendeudamiento. Así, por ejemplo, el art. 18.5 LCCI dispone que el prestamista solo ponga el crédito a disposición del consumidor si el resultado de la evaluación de solvencia indica que es probable que las obligaciones derivadas del contrato de crédito se cumplan según lo establecido en el contrato. De manera muy similar se expresa el art. 18 de la DCCC, de 18 de octubre de 2023 y que será objeto de transposición por los Estados miembros de la UE en los próximos años. Esta evaluación de solvencia puede tener lugar a través de perfilado o *credit scoring*. Como en el resto de las situaciones que estamos viendo, se relacionan datos de, en este caso, el solicitante de crédito con información recogida en perfiles abstractos de solvencia crediticia, lo que puede conducir a situaciones discriminatorias, bien porque se deniegue el crédito, bien porque el tipo de interés fluctúe dependiendo del perfil abstracto en que el solicitante de crédito se sitúe[7].

Uno de los algoritmos que más atención ha suscitado en la literatura jurídica es COMPAS (Correctional Offender Management Profiling for Alternative Sanctions). Se trata de una herramienta utilizada por algunos tribunales en Estados Unidos para evaluar el riesgo de reincidencia de los delincuentes. Si bien su uso fue avalado por el Tribunal Supremo de Wisconsin en el caso *Loomis*[8]*, se ha denunciado que la herramienta reproduce sesgos raciales (Angwin et al.*, 2016).

Cambridge Analytica es una consultora especializada en la recopilación y análisis de datos para campañas publicitarias y políticas. Según podemos leer en su web[9], utiliza modelos de datos y perfiles psicográficos para aumentar las audiencias, identificando personas influyentes y conectando usuarios de tal manera que se favorezca la interacción, utilizando como principal herramienta la escala OCEAN de personalidad, que valora los cinco grandes factores de la

6 Corte de Distrito de La Haya (2020: par. 6.7). La sentencia fue celebrada inmediatamente por el relator especial de la ONU para la extrema pobreza (Alston, 2020), que en su informe de 2019 citó el caso de SyRI como muestra de los riesgos de vigilancia del «estado del bienestar digital» (Alston, 2019: 16).

7 Mas Badía (2021: 359). Palma Ortigosa (2019: 15) recuerda que la evaluación previa de un cliente por parte de una empresa es algo totalmente legítimo. Lo novedoso, señala este autor, es que sea un programa informático el que decida si finalmente se le concede o deniega, por ejemplo, el préstamo solicitado.

8 De Miguel Beriain (2018: 47-48). Puede consultarse la sentencia en: https://tinyurl.com/3v53cxx6.

9 Véase https://tinyurl.com/n6m2ptsc.

personalidad: 1) apertura al cambio (*openness to experience*); 2) responsabilidad (*conscientiousness*); 3) extraversión (*extraversion*); 4) amabilidad (*agreebleness*), e 5) inestabilidad emocional (*neuroticism*) (Soto, 2018). En pocas palabras, se sirve de microsegmentación y perfilado para vender tanto unas zapatillas como un partido político al comprador idóneo en cada momento (Soriano Arnanz, 2021: 88-89).

En 2018 varios diarios denunciaron que la consultora Cambridge Analytica estaba utilizando datos personales de usuarios de Facebook, incumpliendo las políticas de privacidad de esta red social con la anuencia de la propia Facebook, para influir tanto en la campaña política de Donald Trump hacia la presidencia de Estados Unidos como en la campaña del *brexit* (en ambos casos, con éxito). En España, este escándalo motivó una modificación de última hora de la LOREG, incluida en la disposición final tercera de la LOPDgdd, para incluir un nuevo artículo 58 bis con la intención, según el grupo parlamentario que la propuso, de «impedir casos como el que vincula a Cambridge Analytica con el uso ilícito de datos de 50 millones de usuarios de Facebook para mercadotecnia electoral»[10].

Casos como los que acabamos de ver se consideran de alto riesgo de acuerdo con la Propuesta de Reglamento de Inteligencia Artificial (PRIA)[11]. A los efectos de este trabajo, interesa destacarlos a título de ejemplo acerca de los riesgos a los que nos vemos expuestos como individuos en la medida en la que se nos puede relacionar con una enorme cantidad de perfiles abstractos ya existentes. El nivel de contaminación digital (debido al altísimo volumen de datos que se recolectan y la creciente capacidad de interrelación y analítica en masa) se encuentra en un punto de no retorno. Actualmente es posible incluso crear datos sintéticos a partir de paquetes de datos ya existentes (Bousquette, 2023). Por eso, deben coordinarse medidas tendentes a reducir en lo posible el aumento de la contaminación digital con otras orientadas a defendernos jurídicamente de los potenciales efectos de esta.

Partiremos para ello de un análisis de la situación vista desde la óptica de la llamada «privacidad de grupo» acuñada por Luciano Floridi[12] para posteriormente analizar normas ya en vigor (principalmente, el Reglamento General de Protección de Datos) y normas en proceso de desarrollo (principalmente, la Propuesta de Reglamento de Inteligencia Artificial) en busca de herramientas que nos permitan continuar disfrutando del derecho a ser dejados en paz en un contexto de altísima contaminación digital.

---

10 Congreso de los Diputados (2018: 209). La STC 76/2019, de 22 de mayo, declararía inconstitucional el art. 58 bis.1 LOREG.

11 Anexo III PRIA, puntos 5.a, 5.b, 6.a y 8.a bis, respectivamente

12 Se ocupa de la privacidad de grupo en España Cotino Hueso (2022: 87-89).

II. EL DERECHO A LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL

1. DERECHO A LA PROTECCIÓN DE DATOS Y LIBRE CIRCULACIÓN DE LA INFORMACIÓN

Hasta ahora, el derecho a la protección de datos ha tenido como eje central el individuo[13]. El derecho a la protección de datos confiere a su titular la facultad de tomar decisiones[14] en torno a la utilización de los datos de cualquier naturaleza que nos identifican directa o indirectamente, y que potencialmente permiten reconstruir amplios aspectos de nuestra personalidad de tal manera que terceros pueden tomar decisiones sobre nosotros sin que seamos conscientes de ello y, consecuentemente, podamos contrarrestarlo (Lucas Murillo de la Cueva, 2021: 311; Cotino Hueso, 2022: 87).

El binomio «protección de datos personales y libre circulación de la información (incluidos los datos personales)» se ha mantenido desde el Convenio 108 hasta el RGPD, pasando por la Directiva 95/46/CE. En este sentido, en el preámbulo del Convenio 108 se afirma «la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos», y en su art. 12.2 se establece que «una parte no podrá, con el único fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de carácter personal con destino al territorio de otra parte». Por otro lado, la Directiva 95/46/CE afirma la necesidad «no sólo [de] la libre circulación de datos personales de un Estado miembro a otro, sino también [de] la protección de los derechos fundamentales de las personas» (cons. 3), en un contexto en que «el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos» (cons. 4). Esta idea permanece en el RGPD, en el que merece la pena destacar el art. 1.3, donde se afirma que «la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales»[15].

---

13 Floridi (2017: 2). Véase también la propia redacción del art. 4.1 RGPD o los FF. JJ. 6 y 7 de la STC 292/2000, de 30 de noviembre.

14 STC 292/2000, que define el derecho a la protección de datos como un poder de disposición y control sobre los propios datos personales. En igual sentido, Troncoso Reigada (2021: 852-854).

15 Otros puntos importantes del RGPD en este sentido son los considerandos 9, 13, 53, 123, 166 y 170. Véase Lucas Murillo de la Cueva (2021: 309).

El creciente uso de dispositivos interconectados (IoT), las cada vez más variadas redes sociales y la capacidad de analítica de datos en masa son algunos de los retos a los que se enfrenta en la actualidad el derecho a la protección de datos. El progreso tecnológico, que impulsa los retos que acabamos de mencionar, obliga también a interpretar a la luz de los tiempos el contenido del derecho a la protección de datos de tal manera que las mayores posibilidades de aprovechamiento de los datos vengan acompañadas de nuevas cautelas que preserven el equilibrio entre los dos elementos del binomio: protección de datos personales vs. libre circulación de la información[16].

En este contexto, juega un papel importante la promoción e impulso de la economía de datos, cuestión que en la Unión Europea pretende conjugarse de la manera más armoniosa posible con altos estándares de protección de datos personales[17].

2. ECONOMÍA DE DATOS Y CONTAMINACIÓN DE DATOS

Como puede intuirse, los datos ya eran un activo económico desde el principio (Comisión Europea, 2017b: 13). De otro modo difícilmente se entiende que las normas relativas al derecho a la protección de datos se refieran seguidamente a la garantía de su libre circulación. Con todo, no ha sido hasta la última década que han comenzado a realizarse estudios acerca de la llamada «economía de los datos», que se refieren no solo al valor global de los datos, sino al impacto económico que su uso e intercambio genera en el mercado.

De acuerdo con la Comisión Europea, la economía de los datos se caracteriza por ser un ecosistema donde diferentes tipos de agentes de mercado —como fabricantes, investigadores y proveedores de infraestructuras— colaboran para garantizar que los datos sean accesibles y utilizables (Comisión Europea, 2017a: 2). Este ecosistema permite a los agentes de mercado extraer valor de los datos, creando una variedad de aplicaciones con gran potencial para mejorar la vida cotidiana, como, por ejemplo, gestión de tráfico (Pereda y Jané, 2019), movimiento de población interurbana o medicina personalizada

[16] Cotino Hueso (2022: 71-73 y 82) que propone la actualización de facultades que integran el contenido de diversos derechos con un enfoque antropocéntrico y antropogénico, teniendo en cuenta la dimensión colectiva de los derechos derivada del desarrollo de la IA y el *big data*.

[17] Lo destaca la Estrategia Europea de Datos, en la que la UE se marca como objetivo la construcción de un espacio europeo de datos, donde estos puedan fluir en la UE y en todos los sectores, al tiempo que se respeten las normas y valores europeos, particularmente en materia de protección de datos, consumidores y competencia (Comisión Europea, 2020c: 6).

de precisión (Holmes, 2018: 99-101), entre otras ya en curso y, sobre todo, por desarrollar.

Una de las formas más importantes de recolección de datos (que posteriormente serán analizados y aprovechados económicamente) es el pago con datos en el entorno digital. La viabilidad jurídica del pago con datos ha suscitado una gran controversia, centrada en la posibilidad de comerciar con un derecho fundamental como es el derecho a la protección de datos. Es precisamente este aspecto uno de los que con más urgencia debe aclararse en el seno de las instituciones europeas si aspiramos a construir un Mercado Único Digital Europeo con la suficiente seguridad jurídica, también en materia de intercambio económico de datos[18].

Los datos aumentan de valor cuanto más se acumulan e interrelacionan entre sí (Gil González, 2022: 29) (justo al revés de como ocurre con carácter general en el resto de los activos económicos [Spanga, 2015: 61]), a lo que han contribuido de manera significativa la IA basada en datos y, particularmente, las técnicas de analítica de datos en masa y perfilado[19]. Si bien es cierto que el cumplimiento normativo en materia de protección de datos supone un coste económico para empresas cuyo modelo de negocio se basa en la analítica de datos, no lo es menos que el factor confianza comporta a medio plazo una ventaja competitiva importante (Gil González, 2022: 29). El valor de los conjuntos de datos está fuertemente ligado a la confianza que generan, y esta depende de factores como la calidad de los datos, los algoritmos que los procesan[20] o la seguridad de los entornos donde se almacenan[21].

El valor de la economía de los datos ha ido aumentando progresivamente en los últimos años. En 2019 superó el umbral de los 400 000 millones de euros para la UE de los 27 más el Reino Unido, con un crecimiento interanual del 7,6 % (Comisión Europea, 2020a: 7). En 2021 superó los 450 millones de euros para la UE de los 27 (con un crecimiento interanual del 3 %), y se estima que en 2022 habrá alcanzado los 500 millones de euros, con un crecimiento interanual del 8,9 %[22]; habiendo sido particularmente relevante respecto del

---

18 La viabilidad jurídica del pago con datos ha suscitado una gran controversia, centrada en la posibilidad de comerciar con un derecho fundamental como es el derecho a la protección de datos personales. *Vid.*, por todos, Supervisor Europeo de Protección de Datos (2017) y, crítico con la postura del SEPD, Metzger (2020: 25-46).

19 Valls Prieto (2021: 13). En igual sentido, Núñez Seoane (2020: 299-300).

20 Como se ha afirmado, los algoritmos sin datos están vacíos, y los datos sin algoritmos son ciegos (Balkin, 2017: 1220).

21 Véase cons. 45 PRIA.

22 Comisión Europea (2023b: 18). Los datos se publican a año vencido, por lo que no es posible disponer aún de datos sobre 2023.

crecimiento del último año el mercado de la analítica de datos (Comisión Europea, 2023a: 20). Pese a este considerable crecimiento, la importancia de la economía de datos de la UE sigue estando por detrás de la de otras regiones, aspecto del que viene alertando la UE desde hace algunos años (Comisión Europea, 2017a: 1).

La constatación del valor económico de los datos y el aumento considerable de este han derivado en una afirmación que se ha convertido en una suerte de lugar común: los datos son el nuevo petróleo[23].La metáfora es de lo más oportuna por cuanto permite transmitir gráfica e intuitivamente la dinámica de la nueva cadena de valor que constituye el eje central de la economía digital: la extracción, el procesado y el aprovechamiento de datos en masa. Ahora bien, si los datos son el nuevo petróleo en el entorno digital, también generan nuevas formas de contaminación en dicho entorno.

Por ejemplo, cuando pagamos con nuestros datos por ciertos bienes o servicios digitales estamos contaminando el entorno digital de un modo similar, salvando las distancias, a la contaminación que genera el uso de vehículos a motor. Contaminamos el entorno digital al permitir la recolección y análisis de nuestros datos personales, lo que deriva en un medio ambiente digital caracterizado por la hipervigilancia en masa y personalizada (al mismo tiempo), que se ha conocido como capitalismo de la vigilancia: una nueva forma de capitalismo que

> […] reclama para sí la experiencia humana, entendiéndola como una materia prima gratuita que puede traducir en datos de comportamiento […] como un excedente conductual privativo (propiedad) de las propias empresas capitalistas de la vigilancia [que] se usa como insumo de procesos avanzados de producción conocidos como inteligencia de máquinas, con los que se fabrican productos predictivos que prevén lo que cualquiera de ustedes hará ahora, en breve y más adelante (Zuboff , 2020: 21).

3. LA SUBLIMACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS

Los derechos humanos nacen con una marcada impronta individualista, como libertades individuales que configuran la primera fase o generación de los derechos humanos para posteriormente verse completados por una segunda generación: los derechos económicos, sociales y culturales. Así, mientras que los derechos de primera generación se contemplan como derechos de defensa o de no injerencia por parte del Estado, los derechos de segunda generación

[23] Por citar solo algunas de las personas que han empleado la expresión: Gil González (2022: 25) y Mas Badía (2021: 357). Se han utilizado otras metáforas como que los datos son la sangre en las venas de la economía digital (Lohsse *et al.*, 2017: 15).

requieren una política activa por parte de los poderes públicos. Estas primeras dos generaciones se encuentran reflejadas en textos jurídicos como los Pactos de Nueva York o en los catálogos de derechos recogidos en nuestra Constitución. Junto con estas dos generaciones iniciales, «los derechos y libertades de tercera generación se presentan como una respuesta al fenómeno de la denominada contaminación de libertades (*liberties pollution*), término con el que algunos sectores de la teoría social anglosajona aluden a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías». Si bien es difícil cerrar unas características comunes en estos «derechos de nueva generación», podríamos decir que una característica común es que intentan hacer frente a problemas de carácter universal que exigen esfuerzos de la comunidad en su conjunto, incluso superando las fronteras estatales. Quizás el ejemplo que mejor represente esto sea el derecho a un medio ambiente saludable, o el derecho de consumidores (Pérez Luño, 1993: 187; Cotino Hueso, 2022: 81).

Señalaba Pérez Luño (1991: 208), en un contexto tecnológico donde aún no había eclosionado la analítica de datos en masa, lo siguiente respecto de la entonces llamada libertad informática:

> Nuestra vida individual y social corren, por tanto, el riesgo de hallarse sometidas a lo que se ha calificado, con razón, de juicio social permanente. Ya que, en efecto, cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida, que afecta potencialmente incluso a los aspectos más sensibles de su vida privada; aquellos que en épocas anteriores quedaban fuera de todo control por su variedad y multiplicidad.

El derecho a la protección de datos se ha encuadrado tradicionalmente en la primera generación de derechos humanos, y es perfectamente razonable que haya sido así. Esta ubicación y, consecuentemente sus características y modos de defensa no deben entenderse cuestionados por la evolución tecnológica, en la medida en que sus vulnerabilidades no se han disipado. Sin embargo, el desarrollo de la IA y el *big data* hacen necesario añadir una dimensión colectiva a este derecho, en la medida en que se han generado nuevos riesgos que afectan a la sociedad en su conjunto que ya no pueden resolverse *ex post* y de manera reactiva. La importancia de estos riesgos colectivos contrasta, además, con la casi imperceptible dimensión de los daños individuales que generan «acciones contaminantes», como, por ejemplo, aceptar las *cookies* no técnicas de una página web (Cotino Hueso, 2022: 78-80; Jaume Palasí, 2020: 32-34).

Actualmente es posible realizar análisis sofisticados de grandes cantidades de datos que permiten descubrir información no observable a simple

vista. Por ejemplo, cada vez es más sencillo reidentificar datos previamente anonimizados, e incluso identificar o inferir características de personas a partir de datos anónimos o de perfiles abstractos que no se han nutrido de datos de dichas personas (Romeo Casabona, 2021: 584; Gil González, 2022: 29). Todo ello acentúa la vis expansiva del RGPD, cuyo ámbito objetivo pivota en torno a la noción de dato personal, que crece tanto como las posibilidades de identificar a una persona[24]. Esta situación obliga a subrayar que los datos inferidos son también datos personales (Grupo de Trabajo del Artículo 29, 2007: 6), pero, sobre todo, a observar el derecho a la protección de datos más allá de la lógica de la no injerencia: desde un punto de vista colectivo, en el sentido del derecho a un medio ambiente digital no contaminado.

Entendemos por medio ambiente tecnológico contaminado aquel en el que la ingente cantidad de datos y la potencia de las herramientas de analítica de *big data* no permiten a los individuos desenvolverse en el entorno digital con unas mínimas expectativas de anonimato que garanticen el libre desarrollo de su personalidad[25]. El anonimato de los individuos puede ser directo (que no estén identificados o sean fácilmente identificables) o indirecto (que los perfiles abstractos existentes no permitan inferir características de su personalidad con un sencillo proceso de «aplicación» del perfil a la persona).

La contaminación de datos a la que nos vemos expuestos, incluso sin interactuar en entornos digitales, permite elaborar perfiles tan precisos como variopintos referidos a grupos de personas sin que estas puedan hacer nada, individual o colectivamente, para impedir que se desarrollen y tampoco para evitar verse afectadas en su día a día por estas técnicas. Estos perfiles, si bien abstractos (es decir, no asociados a una persona concreta), se refieren a características comunes que compartimos en cuanto que individuos pertenecientes a un grupo. La singularidad en la analítica de datos en masa es que este grupo no tiene que ser conocido socialmente (p. ej., edad, género, distrito urbano, raza, nacionalidad…), sino que se creará de manera funcional dependiendo de la configuración y objetivos de cada algoritmo de analítica de datos.

---

[24] Cons. 26 RGPD: «Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios […] teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos». Véase Romeo Casabona (2021: 589).

[25] Alerta Zuboff de que «los procesos automatizados llevados a cabo por máquinas no sólo conocen nuestra conducta, sino que también moldean nuestros comportamientos en igual medida», por lo que «la afirmación del libre albedrío es también una afirmación del derecho al tiempo futuro como una condición de una vida plenamente humana» (2020: 21 y 447).

Llegamos así a un elemento clave en el análisis de la privacidad de grupo: la constitución dinámica y funcional de los grupos sobre los que se construyen perfiles comportamentales abstractos.

III. LA CONSTITUCIÓN DINÁMICA DE GRUPOS Y SUS CONSECUENCIAS EN LA ATRIBUCIÓN Y DEFENSA DE DERECHOS COLECTIVOS

El concepto de grupo en la privacidad de grupo es un concepto funcional que depende de las elecciones previamente establecidas por cada operación de analítica de datos en materia de 1) elementos observables, 2) fines con los que se observa, y 3) limitaciones de los conjuntos analizados[26]. Es precisamente esta analítica de datos la que permite el desarrollo de perfiles abstractos grupales que podrán posteriormente ser aplicados a individuos concretos con la misma sencillez que una llave magnética se aplica a una puerta para abrirla (Floridi, 2017: 2-4). Los perfiles abstractos no tienen un listado de integrantes, pueden desarrollarse sin que medie acción alguna de los sujetos y alimentarse con datos agregados y otro tipo de datos no personales, de tal manera que, si no se «aplican» a nadie, no son datos personales (Cotino Hueso, 2022: 88). En este sentido, ¿es suficiente con el catálogo de derechos del RGPD para afrontar los retos de su dimensión colectiva?; ¿qué cambios o ampliaciones serían necesarios?; ¿cómo podrían hacer valer sus derechos los grupos que se vieran afectados por la dimensión colectiva del derecho a la protección de datos?

De acuerdo con Floridi, la agrupación de personas según criterios específicos crea un individuo que, como tal, puede ser sujeto de derechos y hacerlos valer. Entiende este autor que existen derechos que pertenecen al grupo como tal y no a los individuos que lo conforman y que en estos casos el grupo actúa como individuo. Esta afirmación no parece discutible respecto de grupos cuyas características son estáticas y observables (p. ej., consumidores). Floridi va más allá y considera que también es posible la atribución y ejercicio de derechos colectivos a grupos funcionales. Si bien admite que los individuos perfilados pueden no saber que lo han sido, entiende que son las mismas prácticas interesadas que determinan la agrupación de las personas las que

[26] Cotino Hueso (2022: 87). Véase también Núñez Seoane (2020: 300): «Para elaborar perfiles y para adoptar decisiones automatizadas se utilizan algoritmos diseñados con distintas funcionalidades: i) aglutinar a diferentes sujetos (algoritmos de agrupamiento); ii) conocer los hábitos y comportamientos de los sujetos (algoritmos de clasificación); iii) predecir mediante pronósticos basados en datos objetivos (algoritmos de regresión)». En igual sentido, Soriano Arnanz (2021: 93-94).

también configuran dichos grupos como titulares potenciales de un derecho a la privacidad que, por tanto, pueden hacer valer (Floridi, 2017: 8-11).

En la cultura jurídica anglosajona, las llamadas acciones de clase se han revelado útiles debido a ventajas como las siguientes: 1) economía procesal; 2) evitación de procesos contradictorios; 3) reforzamiento de la defensa del grupo a través de una única defensa letrada; 4) permitir el acceso a la justicia de reclamaciones de poca monta individualmente consideradas, y 5) distribución equitativa de las indemnizaciones cuando la suma debida por el empresario no satisfaga a todos los damnificados (Carrasco Perera y González Carrasco, 2001: 1900-1901). Pueden ser, además, un mecanismo disuasorio que permita a grupos de damnificados forzar acuerdos transaccionales con compañías cuya imagen pueda verse afectada al verse demandadas en un proceso de este tipo (*ibid.*: 1903).

La importación de las llamadas acciones de clase en el proceso civil español resulta problemática. Se ha introducido, y de manera muy limitada, en el art. 11 LEC, relativo a la legitimación para la defensa de derechos e intereses de consumidores y usuarios. Incluso en este caso una acción de clase en el ordenamiento español presenta, entre otras, las siguientes dificultades[27]: 1) no están claros los criterios ni la instancia para definir el grado necesario de representatividad en caso de que los afectados sean una pluralidad indeterminada de consumidores y usuarios (art. 11.3 LEC); 2) ni está clara la interrelación entre las distintas legitimaciones concurrentes (grupos de afectados y asociaciones de consumidores; asociaciones de consumidores y afectados individuales); 3) la posibilidad de sumarse individualmente a una ejecución de una sentencia de condena crea problemas de identificación de los sujetos que pueden adherirse; 4) no hay controles de justificación previa acerca de la conveniencia de colectivizar el proceso en un caso concreto, y 5) la fijación cuantitativa del daño individual en las acciones de clase resulta impracticable.

Añádase a todo lo anterior que, en el caso de la privacidad de grupo, la construcción funcional de los grupos dificulta tanto su eventual atribución de derechos como, consecuentemente, su eventual ejercicio. Un grupo variable y funcional, que depende de cada decisión de analítica de datos, genera un grado de incertidumbre infinitamente mayor en cuanto a su determinación que otros de carácter fijo y que atienden a características objetivas y observables de ciertos individuos (p. ej., consumidores, consumidores vulnerables, adherentes, usuarios profesionales…). Si en el caso del art. 11 LEC es criticable la falta de controles para definir el grado de representatividad de una

[27] Con mayor profundidad, Carrasco Perera y González Carrasco (2001: 1900-1910).

asociación, en el caso de un grupo difícilmente determinable resulta directamente imposible imaginar siquiera la constitución de una asociación.

Todo lo anterior nos lleva a afirmar que, si bien debe constatarse la privacidad de grupo como un fenómeno digno de consideración a efectos jurídicos, probablemente la mejor manera de hacerle frente no sea la atribución de derechos colectivos (cuyo ejercicio se canalizaría a través de acciones de clase) a grupos difícilmente determinables y muy variables[28]. A no ser, claro está, que entendamos por "grupos afectados" la ciudadanía en su conjunto. Sin embargo, esto nos lleva a orientar la estrategia hacia medidas similares (salvando las distancias) a las que se desarrollan para proteger el medio ambiente, cuyo mantenimiento o degradación nos afecta igualmente a la ciudadanía en conjunto.

En la medida en que toda la sociedad puede ver cómo sus datos alimentan la elaboración de perfiles y, sobre todo, sus características exteriores y actos de todo tipo pueden servir para que se les apliquen perfiles abstractos ya creados, los riesgos derivados de la microsegmentación de la población a través de perfiles abstractos de grupos funcionales guardan cierta relación con los propios de la contaminación medioambiental (del entorno físico). En este sentido, es posible diseñar estrategias encaminadas a lograr un medio ambiente digital más saludable en cada una de las fases del desarrollo de sistemas IA (basados en datos) que operan a través de perfilado de grupos funcionales: 1) fase de recolección de datos; 2) fase de construcción del modelo, y 3) fase de implementación del modelo (Lazcoz Moratinos, 2021: 283-294; Sancho Villa, 2021: 1730-1732; Gil González, 2022: 33-49). Nos centraremos en tres acciones fundamentales:

1) Reducir la «emisión de consentimientos» al tratamiento de datos personales durante la fase de recolección de datos.

[28] Véase, en contra, Floridi (2017: 10). Señala este autor que existen ciertos derechos que pertenecen a grupos en cuanto tales y no como suma de individuos, y que en estas situaciones es el propio grupo quien actúa como individuo para la defensa de sus derechos, y esto puede entenderse en un sentido suave (serán los individuos del grupo quienes ejerzan individualmente derechos atribuidos al colectivo) o fuerte (serán los colectivos como tales quienes ejerzan los derechos del colectivo actuando a estos efectos como individuos). Cotino Hueso (2022: 83-85) se muestra partidario de extender la lógica de las acciones de consumidores al ámbito de la protección de datos. Recuerda, en este sentido, que el art. 73.3 de la Propuesta de RGPD (actual art. 80) reconocía a asociaciones sin ánimo de lucro y otras entidades el derecho a reclamar ante una autoridad de control por violación de protección de datos sin necesidad de reclamación previa de un interesado.

2) Controlar los estándares de calidad de los datos durante la fase de construcción del modelo (perfil abstracto); teniendo en cuenta la importancia de prevenir los sesgos como criterio de calidad (fases de recolección de datos y de construcción del modelo).
3) Subrayar la necesidad de una aplicación integral del RGPD a toda actividad de tratamiento de datos, tanto la consistente en utilizar los datos (personales o no) para durante el desarrollo del modelo como aquella para la posterior aplicación de perfiles a personas concretas durante la fase de implementación del modelo.

IV. MEDIDAS PARA UN MEDIO AMBIENTE DIGITAL SALUDABLE

1. PREVENIR LA SOBREEMISIÓN DE CONSENTIMIENTOS

El consentimiento se ha erigido como la base de legitimación estrella para el tratamiento de datos personales[29], si bien nunca ha sido la única base de legitimación para el tratamiento de datos ni debe entenderse que ocupe una posición jerárquicamente superior al resto ya que no existe jerarquía entre las bases de legitimación del art. 6 RGPD. Se trata, eso sí, de la base de legitimación más cómoda y que mayor nivel de seguridad jurídica ofrece desde la perspectiva del responsable del tratamiento de los datos, ya que necesita menor profundidad de estudio y resulta más fácilmente adaptable a cada caso. No menos importante es la (apariencia de) protección de la autonomía individual del interesado que esta base de legitimación genera. Durante la vigencia de la Directiva 95/46/CE se formularon críticas al consentimiento, centradas en la presunción de que el consentimiento permite una elección consciente y razonada y la realidad práctica de que no es así (Gil González, 2022: 55-61).

El consentimiento como base de legitimación está demostrando ser susceptible de uso abusivo debido a razones como las siguientes:

— La realidad del pago con datos contribuye decididamente al alto nivel de emisión de consentimientos (Schermer *et al.*, 2014: 11-12; Gil González, 2022: 83-85).
— Los responsables de tratamiento redactan cláusulas excesivamente amplias, lo que, unido a la dinámica de recolección de datos a través de *cookies*, dificulta que los titulares de datos tomen verdadera

[29] Véase el art. 8.2 Carta Europea de los Derechos Fundamentales, que distingue entre el consentimiento y el resto de las bases de legitimación.

conciencia de lo que consienten (Comisión Europea, 2010: 7; Gil González, 2022: 69).

— Los titulares de datos no reparan en los términos en que se otorga este consentimiento y su trascendencia individual y colectiva[30].

De acuerdo con el art. 4.11 RGPD, el consentimiento del titular de los datos a su tratamiento debe ser libre, específico, informado e inequívoco. El carácter específico e inequívoco del consentimiento está enteramente relacionado con la redacción concreta del formulario de consentimiento. La redacción de formularios de consentimiento amplios puede ser contraria al principio de minimización de datos. No obstante, en la práctica, y sin perjuicio del riesgo de sanción que implica para el responsable del tratamiento, comporta igualmente ventajas: cuanto más amplia es la finalidad del tratamiento, mayor margen de maniobra tiene su responsable y más son también los potenciales tratamientos ulteriores compatibles[31].

No debe olvidarse, por otra parte, que el consentimiento al tratamiento de datos sirve también como instrumento de pago en manos del consumidor (en su doble condición de consumidor y titular de sus propios datos personales) para disfrutar de ciertos bienes y servicios en el entorno digital. En este sentido, una interpretación rígida o expansiva del RGPD frenaría la emisión de consentimientos y las consecuencias negativas asociadas a ello, pero también el desarrollo e impulso de la economía de datos en la UE. Puede observarse esta tensión en la recolección de datos personales a través de *cookies*. Las *cookies* no técnicas son quizá la herramienta más importante para recolectar datos personales de consumidores en el entorno digital, y esto, a su vez, es fundamental en los modelos de negocio basados en la monetización de datos y la publicidad comportamental (Gil González, 2022: 62), por lo que no es baladí el examen de la viabilidad jurídica del pago con datos (canalizado, por ejemplo, a través de muros de *cookies*).

No podemos ocuparnos de este aspecto en detalle, pero sí ofrecer dos muestras de la tensión existente en torno a este problema: 1) la antinomia

---

30 Schermer *et al.* (2014: 10) y Gil González (2022: 97). Cotino Hueso (2022: 86) lamenta que «lo que era una garantía ha sido totalmente contraproducente», en la medida en que «las recompensas a corto plazo llevan a no valorar racionalmente los peligros y daños futuros».

31 Entre los criterios que tener en cuenta para examinar la compatibilidad de usos ulteriores de datos se encuentra el de la cercanía entre el propósito originario de tratamiento y el propósito del uso ulterior (Grupo de Trabajo del Artículo 29, 2013: 3). No obstante, resulta muy difícil prever los potenciales usos ulteriores de los datos (Cotino Hueso, 2022: 85).

entre el art. 6.3 LOPDgdd y el art. 119 *ter* TRLGCU, y 2) la interpretación forzada de la reciente *Guía AEPD sobre el uso de las cookies* en relación con el pago con datos como alternativa al monetario.

Art. 6.3 LOPDgdd	*Art. 119 ter.2 TRLGDCU*
No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.	La resolución no procederá cuando la falta de conformidad sea de escasa importancia, salvo en los supuestos en que el consumidor o usuario haya facilitado datos personales como contraprestación […].

Directrices 5/2020 CEPD	*Guía AEPD sobre el uso de las cookies (2023)*
39. Para que el consentimiento se manifieste libremente, el acceso a los servicios y funcionalidades no puede supeditarse a que el usuario preste su consentimiento al almacenamiento de información, o al acceso a la información ya almacenada, en el equipo terminal del usuario (las denominadas «barreras de *cookies*»).	Siguiendo las directrices del CEPD sobre el consentimiento, para que este se dé libremente, el acceso a los servicios y funcionalidades no debe supeditarse a la aceptación por el usuario del uso de *cookies*. Por ello, no podrán utilizarse los denominados «muros de *cookies*» que no ofrezcan una alternativa al consentimiento […].
33. Ejemplo 6: Un banco […]. Si la negativa del cliente a dar su consentimiento a dicho tratamiento diera lugar a la negativa por parte del banco de prestar sus servicios, al cierre de la cuenta bancaria o, dependiendo del caso, a un aumento de las comisiones, el consentimiento no podría darse libremente.	Podrán existir determinados supuestos en los que la no aceptación de la utilización de *cookies* impida el acceso al sitio web o la utilización total o parcial del servicio, siempre que se informe adecuadamente al respecto al usuario y se ofrezca una alternativa, no necesariamente gratuita, de acceso al servicio sin necesidad de aceptar el uso de *cookies* […].

Relacionado con lo anterior está el poco detenimiento y reflexión de los interesados acerca de la trascendencia de consentir el tratamiento de sus datos personales. Hemos destacado como ventaja del consentimiento como base de legitimación el mantenimiento de la autonomía individual del interesado en cuanto que titular de los datos; sin embargo, puede alegarse que se trata más de una apariencia que de una realidad. Si bien el RGPD ha reforzado

esta base de legitimación a través del endurecimiento de algunos requisitos ya existentes, como la mayor amplitud de la información que debe darse a los interesados, cabe preguntarse si estas medidas contribuyen a un consentimiento más consciente por parte de los interesados.

Todo lo que hemos visto contribuye a un excesivo nivel de «polución de consentimientos» por parte de aquellos interesados que estén más preocupados por disfrutar de un bien o servicio en el entorno digital que por preservar su privacidad y la de los demás. En palabras de Barocas y Nissebaum, nos enfrentamos a la «tiranía de la minoría»: los datos que voluntariamente comparten unos pocos individuos pueden revelar la misma cantidad de información sobre otros semejantes que no han decidido dar su consentimiento en la medida en que estos datos (que sí están recabados directamente de una persona identificada o identificable) sirven para inferir características de una mayoría que no ha consentido (2014: 61-63). Queda por saber cómo de numerosa es esa «minoría».

Si bien es cierto que no se concede al consentimiento al tratamiento de datos la importancia que merece, no es menos cierto que la responsabilidad no descansa únicamente (ni de manera principal) en la ciudadanía. En el entorno digital encontramos ejemplos de buena praxis en relación con la reducción de la llamada «fatiga de consentimientos», pero también (cierto que cada vez menos) webs que como alternativa al consentimiento ofrecen al usuario una yincana interminable de pantallas sobre «configuración de *cookies*» que, en la práctica, supone un muro difícilmente franqueable[32].

En definitiva, es necesario reducir la «polución de consentimientos» a través de tres ejes de actuación:

— Vigilancia activa por parte de las autoridades de control de la amplitud con que se informa de la finalidad del tratamiento de datos a fin de que el consentimiento que emitan los interesados sea realmente explícito y específico; así como de que los métodos de recolección de consentimiento no están diseñados de tal manera que poder eludir entregar los propios datos sea una odisea infinita de saltos de pantalla.
— Clarificación a nivel europeo acerca de la legalidad (y, en su caso, requisitos y garantías) del pago con datos de ciertos bienes y servicios digitales, y especialmente los usos ulteriores compatibles de los datos que sirven como pago.

[32] El Comité Europeo de Protección de Datos (2020: 19) alertó sobre la fatiga de consentimientos por parte de los usuarios.

— Concienciación a la ciudadanía acerca de la importancia no solo individual, sino social, de consentir el tratamiento de los propios datos personales.

2. CONTROLAR LA CALIDAD DE LOS DATOS

La Propuesta de Reglamento de Inteligencia Artificial (PRIA) se refiere al principio de calidad de los datos en relación con los llamados sistemas de alto riesgo, entendiendo que la alta calidad de los datos, entre otros requisitos, es «esencial para el funcionamiento de muchos sistemas de IA, especialmente cuando se utilizan técnicas que implican la formación de modelos» (cons. 44), y necesaria «para mitigar los riesgos para los derechos fundamentales y la seguridad que plantea la IA y que no están cubiertos por otros marcos jurídicos existentes»[33].

El cumplimiento de los estándares de calidad debe buscarse desde el inicio del diseño del sistema IA, que debe estar sujeto a prácticas adecuadas de gobernanza y gestión de datos orientadas a lograr la mejor calidad de estos[34]. Se entiende que los conjuntos de datos (que han de utilizarse para la formación, validación y prueba de sistemas de IA) son de calidad cuando cumplen los siguientes requisitos:

— Son suficientemente relevantes, representativos, libres de errores y completos teniendo en cuenta la finalidad prevista del sistema[35].
— Tienen las propiedades estadísticas adecuadas, incluso en lo que se refiere a las personas o grupos de personas sobre los que se pretende utilizar el sistema IA, como, por ejemplo, las características o elementos del entorno geográfico, conductual o funcional específico en que se pretende utilizar dicho sistema[36].
— Para garantizar el control, detectar y corregir la parcialidad en los sistemas IA de alto riesgo podrán tratarse categorías especiales de datos[37].

El principio de calidad de los datos solo será exigible respecto de aquellos sistemas considerados como de alto riesgo (art. 10.1 PRIA). Si se observan las finalidades de los sistemas considerados de alto riesgo en el anexo III PRIA

33 PRIA, p. 9.
34 Véase el art. 10.2 PRIA.
35 Cons. 44 y art. 10.3 PRIA.
36 Cons. 44 y puntos 3 y 4 del art. 10 PRIA.
37 Cons. 44 y art. 10.5 PRIA.

podrá constatarse que una parte importante de los objetivos que estos sistemas IA persiguen puede lograrse a través del perfilado de grupos funcionales. Por destacar únicamente situaciones ya comentadas más arriba[38], se consideran de alto riesgo aquellos sistemas IA:

— Destinados a ser utilizados por las autoridades públicas o en nombre de ellas para evaluar el derecho de las personas físicas a las prestaciones y servicios de asistencia pública, así como para conceder, reducir, revocar o reclamar dichas prestaciones y servicios.
— Destinados a ser utilizados para evaluar la solvencia de las personas físicas o establecer su puntuación de crédito.
— Destinados a ser utilizados por las autoridades policiales para realizar evaluaciones de riesgo individuales de personas físicas con el fin de evaluar el riesgo de una persona física de delinquir o reincidir o el riesgo para las posibles víctimas de delitos.
— Destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de personas físicas en el ejercicio de su voto en elecciones o referendos[39].

Independientemente de si el sistema de IA en cuestión debe ser considerado de alto riesgo o no, el principio de calidad de los datos (PRIA) puede servir como criterio interpretativo de los principios de tratamiento de los datos (RGPD)[40]. Ello tendría como ventaja inmediata la mejor concreción de principios relativos al tratamiento de datos cuando este tiene lugar en el marco de analítica de datos a través de IA[41]. Además, una vez aprobado el Reglamento, permitiría extender la aplicación del principio de calidad de los datos a sistemas IA que no fueran considerados de alto riesgo de manera indirecta, en la medida en que se sirvieran del tratamiento de datos personales.

La diferencia fundamental entre el principio de calidad de los datos y los principios relativos al tratamiento de datos se debe a los textos normativos donde se insertan: el incumplimiento del primero dará lugar a las sanciones

38 *Vid*. apdo. 1.

39 PRIA, anexo III, puntos 5.a, 5.b, 6.a y 8.a bis, respectivamente.

40 El término de referencia en la Directiva 95/46/CE (art. 6) y la LOPD/1999 (art. 4.1) era la «calidad de los datos». El art. 4.1 LOPD/1999 entiende por datos de calidad aquellos que son «adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades […] para las que se hayan obtenido».

41 Véase Cotino Hueso (2022: 85), que recuerda que por el momento el régimen de protección de datos es prácticamente el único aplicable a la IA y el *big data*.

oportunas contra los responsables[42], mientras que el incumplimiento de los segundos faculta al interesado para ejercer ciertos derechos que le concede el RGPD[43], al margen de la potestad sancionadora de las autoridades de control[44].

Por lo demás, se trata de principios muy cercanos en cuanto a su contenido. De acuerdo con la PRIA, se consideran datos de calidad aquellos que son «relevantes, representativos, libres de errores y completos», siendo fundamental para concretar estas cualidades en cada caso la finalidad del sistema IA de que se trate. Por otro lado, de acuerdo con el RGPD, los datos personales deben ser «adecuados, pertinentes y limitados a lo necesario» (p. de minimización, art. 5.1.c RGPD) y «exactos y, si fuera necesario, actualizados» (p. de exactitud, art. 5.1.d RGPD). En ambos casos, en relación con los fines para los que son tratados, que deberán ser «determinados, explícitos y legítimos» (p. de limitación de finalidad, art. 5.1.b).

Una buena calidad de los datos no necesariamente implica una mejor protección de los individuos en el contexto de la privacidad de grupo. Pueden generarse perfiles abstractos con datos de buena calidad cuya aplicación a individuos les afecte significativamente, lo que socavaría el derecho al libre desarrollo de la personalidad (Sancho Villa, 2021: 1729), desde una perspectiva tanto individual como colectiva (Cotino Hueso, 2022: 81). Esto lleva a detenernos en la ausencia de sesgos como criterio de calidad de los datos.

2.1. La ausencia de sesgos como criterio de calidad de los datos

La prevención de sesgos y discriminación forma parte importante de los criterios de calidad de los datos. Tanto es así que en las enmiendas presentadas a la PRIA por parte del Parlamento Europeo (2023) se propone la ampliación del cons. 44 en términos como los siguientes: «[…] los sesgos tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente, en particular con respecto a las personas pertenecientes a determinados grupos vulnerables o étnicos o comunidades racializadas».

De acuerdo con el art. 10.5 PRIA, «en la medida en que sea estrictamente necesario para garantizar la supervisión, la detección y la corrección

[42] Véanse arts. 71 y 72 PRIA.

[43] Por ejemplo, en caso de incumplimiento del principio de minimización, se podrá solicitar la supresión de los datos que no sean necesarios para la finalidad del tratamiento (art. 17.1.a RGPD), y, en caso de incumplimiento del principio de exactitud, la rectificación de los datos (art. 16 RGPD) o su limitación (art. 18.1.a RGPD).

[44] Véanse cons. 129 y art. 58.2 RGPD.

de sesgos en relación con los sistemas de IA de alto riesgo, los proveedores de dichos sistemas podrán tratar las categorías especiales de datos personales»[45]. Este tratamiento de categorías especiales de datos se considera de interés público esencial de acuerdo con el cons. 44 PRIA, lo que implica que desde la perspectiva del RGPD el tratamiento está permitido de acuerdo con el art. 9.2.g, siempre que el tratamiento de datos sea proporcional al objetivo perseguido y se establezcan medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Los sesgos son, desde un punto de vista puramente estadístico, cualquier desviación o distorsión respecto de lo estándar; sin que esto condicione su valor ético o normativo. No obstante, esta perspectiva no tiene por qué comportar repercusiones jurídicas. Es más, puede que los sesgos relevantes a efectos jurídicos no lo sean desde un punto de vista estadístico (Lazcoz Moratinos, 2023: 94). Los sesgos de los sistemas IA pueden producirse durante todo su proceso (recolección de datos, construcción del modelo e implementación del modelo). Por razones evidentes, los sesgos relativos a calidad de los datos sucederán fundamentalmente en la fase de recolección de datos, aunque no solo. Algunos de los principales problemas de calidad de los datos relacionados con sesgos son los siguientes[46]:

1) Los datos introducidos son incorrectos, irrelevantes o incompletos. Esto tiene lugar, por ejemplo, cuando un colectivo está infrarrepresentado y el algoritmo arroja resultados distorsionados respecto de dicho grupo (Soriano Arnanz, 2021: 91-92).
2) Las variables sufren de una distribución desigual real (sesgos sociales). En estos casos, los datos son correctos desde el punto de vista técnico/estadístico, pero reflejan situaciones reales que son desiguales o discriminatorias[47].
3) Se producen fallos durante el proceso de ETL (extracción, transformación y carga)[48].

---

45 Se refiere no solo a los datos del art. 9.1 RGPD, sino también a los del art. 10 de la Directiva UE 2016/680, y a los del art. 10.1 del Reglamento UE 2018/1725.

46 Los dos primeros problemas destacados tendrán lugar durante la fase de recolección de datos, mientras que este último podrá tener lugar tanto durante la fase de recolección de datos como durante la fase de construcción del modelo.

47 Lazcoz Moratinos (2023: 94-100). *Vid*., asimismo, Soriano Arnanz (2021: 92-93).

48 Durante este proceso, los datos primarios se mueven desde sus fuentes de origen, se depuran, se preparan para su posterior análisis y se cargan en un repositorio común (Gil González, 2022: 37-39).

3. INTERPRETACIÓN INTEGRAL DEL RGPD, Y PARTICULARMENTE DEL ARTÍCULO 22

El art. 22.1 RGPD establece que «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», salvo que se dé alguna de las excepciones previstas en el art. 22.2 RGPD: 1) es necesaria para la celebración de un contrato entre el interesado y el responsable del tratamiento[49]; 2) está autorizada por el derecho de la UE o de los Estados miembros, o 3) se basa en el consentimiento explícito del interesado. Se ha afirmado que el art. 22 RGPD consagra el derecho a la intervención humana (Sancho Villa, 2021: 1739-1742) en la toma de decisiones automatizadas en un contexto tecnológico en que ya ha eclosionado la industria del *big data* (*ibid.*: 1727), lo cual no necesariamente protege a la persona afectada debido, entre otras razones, a la influencia de los llamados sesgos de confirmación o complacencia[50].

Como ya se ha dicho, el proceso completo de un sistema IA abarca tres fases: 1) recolección de datos; 2) construcción del modelo, e 3) implementación del modelo. El art. 22 RGPD y el RGPD en su conjunto son aplicables tanto en el momento en que los datos personales alimentan la elaboración de perfiles abstractos (fase 1) como en el momento en que perfiles abstractos se aplican a una persona concreta (fase 3), ya que en ambos momentos se producen actividades de tratamiento de datos personales. Es tratamiento de datos «cualquier operación»[51] realizada sobre datos personales, como, por ejemplo, su «organización, estructuración, conservación, adaptación o modificación» (fase 2, desarrollo del modelo), o su

---

49 No todo tratamiento de datos exigido en un contrato tiene el contrato como base de legitimación del art. 6 ni, por tanto, encaja tampoco aquí.
Debe prestarse atención a que no se camufle el tratamiento en las condiciones generales de un contrato de adhesión, o a que el tratamiento de datos se produzca como condición de acceso a redes sociales para posteriormente recibir publicidad comportamental. En estos casos no existiría un consentimiento.

50 Véase Romeo Casabona (2021: 610-611). Son elementos para descartar estos sesgos que 1) la intervención humana venga de una persona con suficiente autoridad para desobedecer la decisión/sugerencia automatizada; 2) que la decisión automatizada cumpla con los principios del art. 5 RGPD, y que 3) no haya rutina en el seguimiento de los resultados algorítmicos (Lazcoz Moratinos, 2023: 282). Sobre las posiciones doctrinales acerca de la intervención humana significativa en el marco del art. 22 RGPD, Sancho Villa (2021: 1732-1734).

51 Art. 4.2 RGPD.

«consulta [y] utilización» (fase 3, aplicación del modelo), y, por supuesto, su tratamiento a gran escala[52].

Por otra parte, toda información sobre una persona física identificada o identificable es un dato personal (art. 4.1 RGPD), incluida información inferencial resultante de asociar un perfil abstracto y una persona. Teniendo todo esto en cuenta, conviene volver al párrafo primero del art. 22: «[…] todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles […]». Esta afirmación puede interpretarse de dos maneras diferentes (y complementarias) dependiendo de la fase de tratamiento de los datos a que nos estemos refiriendo: 1) el derecho del interesado a que sus datos no alimenten la elaboración de perfiles, durante la fase de construcción del modelo, y 2) el derecho del interesado a que no se le apliquen perfiles, durante la fase de implementación del modelo.

3.1. Derecho a no ser objeto de decisión automatizada durante la fase de construcción del modelo

Todo interesado tiene derecho a que sus datos personales no alimenten la elaboración de perfiles, algo que se produce a través de un tratamiento automatizado de datos después de su recogida. Es decir, todo interesado tiene derecho a no verse incluido o asociado automáticamente entre quienes forman parte de un determinado grupo funcional (del que saldrá un perfil abstracto asociado a las características de este grupo). Esto tendría lugar durante la fase de construcción del modelo, cuando se realiza la analítica de datos y se buscan correlaciones y patrones para crear un nuevo conocimiento: el perfil comportamental de un determinado grupo.

En esta fase es importante vigilar y fomentar la transparencia y explicabilidad de los algoritmos como método para reducir en lo posible que los sesgos, prejuicios y errores humanos se trasladen al algoritmo y supongan un factor de cristalización en el futuro (Gil González, 2022: 40-41). El análisis de estos aspectos, si bien importante para los problemas que nos ocupan, queda fuera de las cuestiones estrictamente relacionadas con el tratamiento de datos.

En lo que se refiere al tratamiento de datos, hay dos aspectos importantes para tener en cuenta: 1) los usos ulteriores de datos obtenidos de muy diversas fuentes, y 2) la anonimización de datos durante esta fase.

---

[52] Véase el cons. 91 RGPD. Sobre los criterios para entender que estamos ante un tratamiento de datos a gran escala, Grupo de Trabajo del Artículo 29 (2017a: 8).

Si algo caracteriza a la analítica de datos en masa es el elevado volumen de datos que utiliza, y que la diferencia de la estadística tradicional (que se sirve de pequeñas muestras) (Gil González, 2015: 21). En este punto debe traerse a colación el principio de limitación de la finalidad del tratamiento, tal como viene recogido en el art. 5.1.b RGPD, según el cual los datos personales 1) no serán tratados ulteriormente de manera incompatible con los fines para los que fueron recabados, salvo que 2) el tratamiento ulterior de los datos personales se realizase con fines de archivo en interés público, investigación o estadísticos, en cuyo caso se considerará que los segundos usos son compatibles con los iniciales siempre que se cumpla con las garantías del art. 89.1 RGPD, que se refieren al principio de minimización de datos, incluida la pseudonimización[53]. También debe tenerse en cuenta el principio de minimización, de partida difícilmente conjugable con la analítica de datos en masa (Cotino Hueso, 2022: 85).

La elaboración de perfiles puede considerarse tanto una actividad de investigación como una actividad estadística (Grupo de Trabajo del Artículo 29, 2017b: 7), por lo que, en principio, puede entenderse como un uso posterior compatible de datos personales, siempre que se cumpla con las garantías adecuadas para proteger los derechos y libertades de los interesados, y se respete el principio de minimización de datos, particularmente por lo que se refiere a la pseudonimización (véase el art. 89.1 RGPD). La pseudonimización de los datos no es un problema para la elaboración de perfiles, puesto que la identidad de la persona no es relevante para la construcción del perfil (Jaume Palasí, 2020: 28): lo importante son sus características funcionales. Cuestión diferente es el diseño de «garantías adecuadas» para proteger los derechos y libertades de los interesados, que variarán dependiendo del tipo de perfil que se elabore y, sobre todo, de sus usos potenciales previstos o posibles.

De acuerdo con el cons. 26 RGPD y con una interpretación a contrario (y evidente) del art. 1.1 RGPD, este no debe entenderse aplicable a la información anónima, es decir, a todos aquellos datos que no guarden «relación con una persona física identificada o identificable», ni tampoco «a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo».

Desde un punto de vista técnico, resulta sumamente difícil someter datos personales en origen a procesos de anonimización completa. Pero sí cabe preguntarse qué procesos de pseudonimización de datos y establecimiento de

[53] Véase Grupo de Trabajo del Artículo 29 (2013: 3-4), que recuerda que los tratamientos ulteriores de datos ya recogidos deben analizarse caso por caso teniendo en cuenta que no debe asumirse por defecto que existe incompatibilidad.

garantías[54] serían suficientes a efectos de que el titular de los datos dejase de considerarse «identificable». Para determinar si una persona es identificable, deben tenerse en cuenta todos los medios que puedan utilizar tanto el responsable como cualquier otra persona para reidentificar al titular de los datos, de tal manera que, si existe una probabilidad razonable de reidentificación, los datos sigan siendo pseudonimizados (cons. 26 RGPD). Esto implica igualmente que, si la probabilidad de reidentificación está por debajo de lo razonable, podemos entender que se trata de datos anonimizados a efectos del RGPD (Romeo Casabona, 2021: 616-619).

La probabilidad «razonable» de reidentificación es un concepto jurídico indeterminado, que habrá de concretarse en cada caso. En el ámbito que nos ocupa es importante atender al nivel de granularidad en la exposición de la información. Qué se considera un nivel adecuado de granularidad puede explicarse fácilmente con un ejemplo que de un tiempo a esta parte se ha puesto de moda tras unas elecciones: el célebre «conoce cómo han votado tus vecinos» (Sánchez y Oliveres, 2023) de muchos diarios en la jornada postelectoral. ¿Cuándo los datos sobre voto (por barrios, por calles, por distritos, por extensión en km^2 —cuánta—) convierten a «tus vecinos» en personas identificables? Dependerá de cada caso, pero deberá tratarse de datos suficientemente agregados como para que no resulte fácil asociar vecinos concretos y sentido de su voto. En España, y debido a nuestro sistema electoral, esas noticias solo sirven para el cotilleo del café de la mañana siguiente, pero imaginen su importancia en sistemas donde es posible modificar la configuración de los distritos electorales cada cierto tiempo[55].

3.2. Derecho a no ser objeto de una decisión automatizada durante la fase de aplicación del modelo

Todo interesado tiene derecho a que no se le aplique un perfil comportamental abstracto ya creado referido a un determinado grupo funcional. En este caso, también se estaría viendo incluido o asociado como parte de los

[54] Véase el art. 89.1 RGPD.

[55] En Estados Unidos la redistribución de distritos se lleva a cabo por el Poder Legislativo de cada estado. Existe abundante jurisprudencia acerca de la prohibición de prácticas de distribución interesada o partidista de distritos electorales (*gerrymandering*) por considerarlas contrarias a la Constitución de Estados Unidos. Pese a todo, a la luz del abundante número de casos, parece difícil desterrar esta intención de la voluntad de los partidos políticos; existiendo en la actualidad intentos de redistribución partidista de los distritos electorales de similar intensidad a cuando se acuñó el término en la segunda mitad del siglo XIX (Kang, 2019: 1380-1387).

individuos pertenecientes o cercanos a ese grupo funcional, pero en una fase posterior, como es la de implementación del modelo[56]. Los perfiles abstractos no son datos personales mientras no están asociados a una persona concreta y, por lo tanto, no les resulta de aplicación el RGPD[57]. Sin embargo, cuando estos perfiles se aplican a una persona concreta ya sí se está realizando un tratamiento de datos personales en la medida en que el perfil abstracto deja de ser tal para convertirse en el perfil en que se ha categorizado a una persona concreta. Esto ya sí es un tratamiento de datos personales y una decisión (automatizada o no) que afecta al interesado[58]. Conviene distinguir entre personas cuyos datos son recopilados para la elaboración de perfiles (fase 1) y personas a las que los perfiles ya elaborados se les aplican (fase 3); aunque en ambos casos se producen actividades de tratamiento de datos, en ambos casos se producen actividades de perfilado, y, por lo tanto, en ambos casos resulta de aplicación el RGPD (Gil González, 2022: 43-46).

La versión en castellano del art. 4.4 del RGPD puede dar lugar a alguna confusión interpretativa en lo que acabamos de señalar: mientras que en la versión en inglés se habla de *profiling* (perfilado), la versión en castellano habla de «elaboración de perfiles». Pese a que el perfilado se define como «toda forma de tratamiento automatizado de datos personales», hablar de «elaboración de perfiles» puede dar lugar a pensar que el RGPD resulta únicamente aplicable a toda actividad relativa a perfilado durante las fases 1 (recolección de datos) y 2 (construcción del modelo), pero no durante la fase 3 (aplicación del modelo; aplicación del perfil). Esto no es así.

La aplicación de un perfil abstracto a una persona concreta es una actividad de tratamiento de datos como cualquier otra. Se trata de una operación realizada sobre datos personales, ya sea por procedimientos automatizados o no, orientada a evaluar determinadas características de una persona física. Da igual aquí si entendemos que la actividad de tratamiento se produce del perfil a la persona o de la persona al perfil: se está estableciendo una relación de semejanza suficientemente relevante entre el perfil abstracto (que ya es concreto) y la persona; se está afirmando que cierto perfil funciona para una persona concreta, y que cierta persona concreta es suficientemente semejante a dicho perfil, y, por tanto, previsiblemente se comportará del mismo modo.

---

56 Esto comporta el riesgo de que al clasificar a las personas en grupos funcionales se tomen decisiones discriminatorias basadas únicamente en esos perfiles (Romeo Casabona, 2021: 610-612).

57 *Vid*. cons. 26 y art. 4.1 RGPD, a contrario.

58 En este sentido, Cotino Hueso (2022: 88): «[…] estas clasificaciones, aunque no supongan un tratamiento de datos personales, pasan a serlo en el momento en que desprenden efectos sobre personas concretas».

Bien es verdad que los datos resultantes de aplicar un perfil abstracto a una persona física no deben tomarse como ciertos, sino como inferencias. Pero no es menos cierto que no por ello dejan de ser datos personales, ya que se refieren a una persona identificada o identificable.

Se trata de conocimiento nuevo (derivado de analítica en masa y micro-segmentación de la población en grupos funcionales) que será más o menos preciso en términos de probabilidad; pero que cumple con las condiciones necesarias para ser dato personal y, por tanto, queda sujeto al RGPD, igual que el resto de los datos personales[59]. No deja por ello de tratarse de una evolución del derecho a que nos dejen en paz, a la luz de la nueva realidad social derivada de la evolución tecnológica: el derecho a no ser agredidos, golpeados, juzgados, perseguidos, difamados (Warren y Brandeis, 1890: 205) o, en definitiva, perjudicados a través de la aplicación sobre nuestra persona de perfiles abstractos de grupos, por mucho que encajemos en las características exteriores y observables de dichos grupos.

V. CONCLUSIONES

El derecho a la protección de datos confiere a su titular la facultad de tomar decisiones en torno a la utilización de datos de cualquier naturaleza. Por su parte, el derecho a la intimidad protege frente a invasiones que puedan realizarse en el ámbito de la vida personal y familiar que la persona desee excluir del conocimiento ajeno. Tanto uno como otro derecho tienen una marcada impronta individualista o defensiva que los caracteriza como derechos de no injerencia o de primera generación.

El derecho a la protección de datos ha estado unido, desde sus inicios, a la garantía y fomento de la libre circulación de los datos (véase el art. 1.3 RGPD). El aumento de fuentes productoras de datos y el desarrollo de herramientas de recolección y análisis han permitido el impulso de la IA basada en datos (*machine learning*, *deep learning*), contribuyendo todo ello al desarrollo de la llamada economía de los datos, que estudia no solo el valor global de los datos, sino el impacto económico que su uso e intercambio generan en el mercado. El valor de la economía de los datos ha aumentado progresivamente en los últimos años. En 2021 superó los 450 millones de euros para la UE más el Reino Unido, y se estima que en 2022 superará los 500 millones de euros, a pesar de la salida del Reino Unido de la UE. Tanto la IA basada en datos como la economía de datos se retroalimentan: la infraestructura contractual

[59] Véase cons. 72 RGPD.

generada en torno a la economía de datos (por ejemplo, a través de pago con datos y muros de *cookies*) aumenta la cantidad de datos disponibles para su posterior análisis y generación de conocimiento nuevo.

El progreso tecnológico obliga también a interpretar a la luz de los tiempos el contenido del derecho a la protección de datos, de tal manera que las mayores posibilidades de aprovechamiento de los datos vengan acompañadas de nuevas cautelas. En este sentido, es importante ser conscientes de la contaminación que genera nuestra actividad en el entorno digital: cuando pagamos con nuestros datos estamos contaminando el entorno digital al permitir la recolección y análisis de nuestros datos personales, lo que deriva en un medio ambiente digital caracterizado por la hipervigilancia en masa y personalizada, y esto afecta de un modo diferente al hasta ahora conocido como derechos a la intimidad o la protección de datos. Por ello es necesario añadir a la tradicional perspectiva del derecho a la protección de datos aquella que nos permita desarrollar el derecho a disfrutar de un medio ambiente tecnológico saludable, entendido como aquel cuyo nivel de «contaminación de datos» no favorezca un juicio social permanente a individuos a través de análisis masivos de datos que no necesariamente están relacionados con su persona, pero que potencialmente podrían estarlo, y que se ven aplicados a través de perfiles abstractos asociados a grupos funcionales difícilmente determinables a través de técnicas de analítica de datos en masa.

Resulta necesario reflexionar acerca de los retos que plantea la perspectiva colectiva de la privacidad, vista como el derecho a disfrutar de un medio ambiente digital saludable. Mientras esto se produce, vale la pena diseñar o reforzar estrategias que mitiguen la nueva contaminación digital y sus efectos. Estas estrategias se podrán desarrollar en alguna de las tres fases de los sistemas de IA: recolección de datos, diseño del modelo o implementación del modelo.

El consentimiento al tratamiento de datos es una de las varias bases de legitimación que contempla el art. 6 RGPD. Pese a sus indudables ventajas (como la seguridad jurídica que ofrece al responsable del tratamiento), contribuye a un alto nivel de polución de consentimientos, debido a la realidad del pago con datos (incómoda y poco clara desde el punto de vista jurídico), a formularios de consentimiento excesivamente amplios, y al bajo (o nulo) nivel de reflexión de los titulares de datos, más interesados en disfrutar «gratis» de ciertos bienes y servicios en el entorno digital que en preservar su privacidad y la de los demás. En este sentido, las autoridades de control deben vigilar tanto la amplitud con que se informa de la finalidad del tratamiento cuando se recaba consentimiento del titular de los datos como que se reduce la llamada fatiga de consentimiento. También debe profundizarse en la concienciación ciudadana sobre la trascendencia individual y colectiva de consentir

el tratamiento de datos. Finalmente, se ha de aclarar la legalidad del pago con datos y sus métodos.

Por lo que se refiere al control de calidad de los datos, hay que comenzar destacando que la analítica de datos permite tomar decisiones mejor informadas, pero esto solo ocurrirá si se construyen sobre datos lo suficientemente relevantes, representativos, libres de errores y completos teniendo en cuenta la finalidad del sistema de IA. En otras palabras, si se utilizan datos de calidad. La Propuesta de Reglamento de Inteligencia Artificial se ocupa del principio de calidad de los datos en el art. 10 y en el cons. 46. La prevención de sesgos en los datos forma parte importante de la calidad de los datos, tanto que si fuera necesario se consideraría como de interés público esencial utilizar categorías especiales de datos para supervisar, detectar y corregir sesgos en sistemas de IA de alto riesgo (art. 10.5). Además, el principio de calidad de los datos de la PRIA puede servir como parámetro de interpretación de los principios del tratamiento de datos del art. 5 RGPD en la medida en que dicho tratamiento tenga lugar en el marco de un sistema de IA.

Como tercera estrategia, hay que subrayar que el RGPD, y particularmente su art. 22, resulta aplicable a cualquier operación de tratamiento de datos; lo que abarca potencialmente las tres fases de un sistema de IA: recolección de datos, construcción del modelo (perfil) e implementación del modelo. A los efectos de afrontar los retos de la privacidad de grupo, esto implica que cualquier persona tiene derecho a 1) que sus datos no alimenten la elaboración de perfiles durante la fase de construcción del modelo, salvo que sean sometidos a medidas adecuadas de salvaguarda de sus derechos y libertades, como la pseudonimización, y, también, a 2) que no se le apliquen perfiles abstractos ya creados, durante la fase de implementación del modelo.

Resulta particularmente importante subrayar el derecho de todo ciudadano a que no se le apliquen perfiles abstractos que permitan inferir (con mayor o menor probabilidad de acierto) comportamientos suyos pasados, presentes o futuros. Desde el punto de vista del derecho a la protección de datos, aplicar un perfil abstracto a una persona concreta es una actividad de tratamiento de datos, y, como tal, le resulta aplicable el RGPD. Por otra parte, no menos importante, la microsegmentación de la población en grupos funcionales difícilmente determinables con el objetivo de inferir aspectos de su vida o su personalidad genera una situación de indefensión tal que socaba la dignidad de la persona y el libre desarrollo de la personalidad.

Prestar atención al derecho a que no se nos apliquen perfiles abstractos ya creados es una buena estrategia reactiva habida cuenta de la gran cantidad de datos y perfiles abstractos ya creados que existen en la actualidad. Tanto la reducción de la emisión de consentimientos como el control de la calidad de los datos permiten construir un medio ambiente digital menos conta-

minado en el futuro. Pero, por el momento, como sociedad, debemos luchar con la mayor agilidad posible contra la microsegmentación social a través de perfilado que ya opera en múltiples facetas de nuestra vida cotidiana. Para ello, y haciendo uso de normas ya en vigor, podemos reclamar nuestro derecho a no ser objeto de perfilado (es decir, contribuir a la elaboración de perfiles sin las debidas garantías y, sobre todo, que no se nos apliquen perfiles), en la medida en que se trata de una decisión automatizada que nos afecta significativamente (art. 22.1 RGPD) socavando nuestra dignidad y perturbando el libre desarrollo de nuestra personalidad (art. 10 CE).

Bibliografía

Alston, P. (2020). Un fallo histórico de un tribunal holandés detiene los intentos del gobierno de espiar a los pobres (Informes ACNUDH. Comunicado Prensa). Ginebra: ACNUDH. Disponible en: https://tinyurl.com/5n6mespd.

Angwin, J., Larson, J., Mattu, S. y Kirchner, L. (2016). Machine bias. There's software used across the country to predict future criminals. And it's biased against blacks. *ProPublica* [blog], 23-5-2016. Disponible en: https://tinyurl.com/yyy6yc2y.

Balkin, J. M. (2017). The three laws of robotics in the age of big data. *Ohio State Law Journal*, 78, 1217-1241.

Barocas, S. y Nissebaum, H. (2014). Big data's end run around anonymity and consent. En J. Lane, V. Stodden, S. Bender y H. Nissebaum (eds.). *Privacy, big data and the public good. Frameworks for engagement* (pp. 44-75). Cambridge: Cambridge University Press. Disponible en: https://doi.org/10.1017/CBO9781107590205.004.

Bousquette, I. (2023). AI-generated gata could be a boon for healthcare, if only it seemed more real. *The Wall Street Journal*, 2-8-2023. Disponible en: https://tinyurl.com/3j3skp6z.

Carrasco Perera, A. y González Carrasco, M. C. (2001). ¿Acciones de clase en el proceso civil? *Aranzadi Civil: Revista Quincenal*, 1, 1895-1912.

Comisión Europea (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of The Regions: a comprehensive approach on personal data protection in the European Union* (Report COM. Bulletin COM; 609 final). Brussels: COM. Disponible en: https://tinyurl.com/2efrbmrs.

——— (2017a). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: «La construcción de una economía de los datos europea»* (Report COM. Bulletin COM; 9 final). Brussels: COM. Disponible en: https://tinyurl.com/2p9a763k.

——— (2017b). *Commission staff working document: on the free flow of data and emerging issues of the European data economy. Building a European data economy*

(Report COM. Bulletin COM; SWD 2 final). Brussels: COM. Disponible en: https://tinyurl.com/2ud76ks2.

——— (2020a). *The european data market monitoring tool: key facts and figures, first policy conclusions, data landscape and quantified stories* (Report EC. Bulletin POEU; D2.9 Final Study Report). Luxembourg: EC. Disponible en: https://tinyurl.com/vbrzx8w5.

——— (2020b). *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza* (Informe COM. Boletín COM; 65 final). Brussels: COM. Disponible en: https://tinyurl.com/mvfveceu.

——— (2020c). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: una estrategia europea de datos* (Informe COM. Boletín COM; 66 final). Brussels: COM. Disponible en: https://tinyurl.com/23ysm7vt.

——— (2023a). *European data market study 2021-2023* (D2.4 Second Report on facts and figures). Brussels. Disponible en: https://tinyurl.com/w3pcja99.

——— (2023b). *European Data Market Study 2021-2023. Second Report on policy conclusions*. (Report COM. Bulletin COM; D2.5). Brussels: COM. Disponible en: https://tinyurl.com/2p8ca5s4.

Comité Europeo de Protección de Datos (2020). *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento UE 2016/679*. (Informe CEPD.) Bruselas: CEPD. Disponible en: https://tinyurl.com/yr44x52v.

Congreso de los Diputados (2018). *Enmiendas e índice de enmiendas al articulado. 121/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal*. Disponible en: https://tinyurl.com/3bcjduwd.

Corte de Distrito de La Haya (2020). *Legislación SyRI en conflicto con el Convenio Europeo de Derechos Humanos: C-09-550982-HA ES 18-388*. Disponible en: https://tinyurl.com/37dkj69y.

Cotino Hueso, L. (2022). Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial. En L. Cotino Hueso (dir.). *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (pp. 69-105). Navarra: Thomson Reuters Aranzadi.

De Miguel Beriain, I. (2018). Does the use of risk assessments in sentences respect the right to due process? A critical analysis of the Wisconsin vs. Loomis ruling. *Law, Probability and Risk*, 17 (1), 45-53. Disponible en: https://doi.org/10.1093/lpr/mgy001.

Floridi, L. (2017). Group privacy: a defence and an interpretation. En L. Taylor, L. Floridi y B. van der Sloot (eds.). *Group privacy: new challenges of data technologies* (pp. 103-123). Dordrecht: Springer. Disponible en: https://doi.org/10.1007/978-3-319-46608-8_5.

Gil González, E. (2015). *Big data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos. Disponible en: https://tinyurl.com/4t8zh4d2.

——— (2022). *El interés legítimo en el tratamiento de datos personales*. Madrid: Wolters Kluwer.

Grupo de Trabajo del Art. 29 (2007). *Opinion 4/2007 on the concept of personal data* (Report CE. Bulletin WP; 136). Brussels: CE Disponible en: https://tinyurl.com/cwwx5bhc.

——— (2013). *Opinion 03/2013 on purpose limitation* (Report EC. Bulletin WP; 203). Brussels: EC. Disponible en: https://tinyurl.com/9k5t3wah.

——— (2017a). *Guidelines on data protection impact assessment and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679.* (Report EC. Bulletin WP; 248). Brussels: EC. Disponible en: https://tinyurl.com/yc7htu56.

——— (2017b). *Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679* (Report EC. Bulletin WP; 251 rev. 01). Brussels: EC. Disponible en: https://tinyurl.com/yhp3382h.

Holmes, D. E. (2018). *Big Data. Una breve introducción*. Barcelona: Antoni Bosch.

Jaume Palasí, L. (2020). Cómo la inteligencia artificial está impactando en las sociedades. En A. Cerrillo i Martínez y M. Peguera Poch (dirs.). *Retos jurídicos de la inteligencia artificial* (pp. 27-39). Navarra: Thomson Reuters Aranzadi.

Kang, M. S. (2019). Hyperpartisan gerrymandering. *Boston College Law Review*, 61, 1379-1445.

Lazcoz Moratinos, G. (2021). Modelos algorítmicos, sesgos y discriminación. En F. Bueno de Mata (dir.). *FODERTICS 9.0. Estudios sobre tecnologías disruptivas y justicia* (pp. 283-294). Granada: Comares.

——— (2023). *Gobernanza y supervisión humana de la toma de decisiones automatizada basada en la elaboración de perfiles* [tesis doctoral inédita]. Universidad del País Vasco.

Lohsse, S., Schulze, R. y Staudenmayer, D. (2017). Trading data in the digital economy: legal concepts and tools. En S. Lohsse, R. Schulze y D. Staudenmayer (dirs.). *Trading data in the digital economy: legal concepts and tools* (pp. 13-26). Baden-Baden: Nomos. Disponible en: https://doi.org/10.5040/9781509921218.0005.

Lucas Murillo de la Cueva, P. (2021). El objeto del Reglamento General de protección de datos y de la Ley Orgánica de protección de datos personales y garantía de los derechos digitales. Comentario al art. 1 Reglamento General de Protección de Datos y al art. 1 Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales. En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 323-324). Navarra: Thomson Reuters Aranzadi.

Mas Badía, M. D. (2021). *Sistemas privados de información crediticia. Nueva regulación entre la protección de datos y el crédito responsable*. Valencia: Tirant lo Blanch.

Metzger, A. (2020). A market model for personal data: state of play under new Directive on digital content and digital services. En S. Lohsse, R. Schulze y D. Staudenmayer (dirs.). *Data as counter-performance: contract law 2.0?* (pp. 25-46). Baden-Baden: Nomos. Disponible en: https://doi.org/10.5771/9783748908531-23.

Núñez Seoane, J. (2020). El derecho de la información y acceso al funcionamiento de los algoritmos que tratan datos personales. En A. Huergo Lora (dir.). *La regulación de los algoritmos* (pp. 299-315). Navarra: Thomson Reuters Aranzadi.

Palma Ortigosa, A. (2019). Decisiones automatizadas en el Reglamento General de Protección de Datos. El uso de algoritmos en el contexto de la protección de datos. *Revista General de Derecho Administrativo*, 50.

Parlamento Europeo (2023). *Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión* (Informes COM. Boletín COD 0206/2021–C9-0146/2021–0106/2021). Bruselas: COM. Disponible en: https://tinyurl.com/mtyv2nnd.

Pereda, O. y Jané, C. (2019). El Instituto Nacional de Estadística paga medio millón por los datos de cómo se desplazan los españoles. *El Periódico*, 29-10-2019. Disponible en: https://tinyurl.com/4ak9ehpf.

Pérez Luño, A. E. (1991). Las generaciones de derechos humanos. *Revista del Centro de Estudios Constitucionales*, 10, 203-217.

——— (1993). El concepto de los derechos humanos y su problemática actual. *Derechos y libertades: Revista de Filosofía del Derecho y Derechos Humanos*, 1 (1), 179-196.

Romeo Casabona, C. M. (2021a). Limitación del tratamiento. Comentario al art. 4.3 del Reglamento General de Protección de Datos. En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 573-589). Navarra: Thomson Reuters Aranzadi.

——— (2021b). Datos personales. Comentario al art. 4.1 del Reglamento General de Protección de Datos. En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 573-589). Navarra: Thomson Reuters Aranzadi.

——— (2021c). Elaboración de perfiles. Comentario al artículo 4.4 del Reglamento General de Protección de Datos. En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 609-612). Navarra: Thomson Reuters Aranzadi.

——— (2021d). Seudonimización. Comentario al art. 4.5 del Reglamento General de Protección de Datos. En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 613-627). Navarra: Thomson Reuters Aranzadi.

Sánchez, R. y Oliveres, V. (2023). MAPA. ¿Qué votaron tus vecinos el 23J? Los resultados de las elecciones generales, calle a calle. *elDiario.es*, 24-7-2023. Disponible en: https://tinyurl.com/mrm8p869.

Sancho Villa, D. (2021). Las decisiones individuales automatizadas, incluida la elaboración de perfiles. Comentario al art. 22 Reglamento General de Protección de Datos. En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 1725-1745). Navarra: Thomson Reuters Aranzadi.

Schermer, B. W., Custers, B. y Van der Hof, S. (2014). The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, 16 (2), 171-182. Disponible en: https://doi.org/10.1007/s10676-014-9343-8.

Soriano Arnanz, A. (2021). Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos. *Revista de Derecho Público: Teoría y Método*, 3, 85-127. Disponible en: https://doi.org/10.37417/RPD/vol_3_2021_535.

Soto, C. J. (2018). Big five personality traits. En M. H. Bornstein, M. E. Arterberry, K. L. Fingerman y J. E. Lansford (eds.). *The SAGE encyclopedia of lifespan human development* (pp. 240-241). Sage: Thousand Oaks, C. A.

Spanga, C. (2015). Dei beni in generale. En P. Schlesinger (dir.). *Il Codice Civile Commentario: art. 810-821* (pp. 1-259). Milano: Giuffrè Editore.

Supervisor Europeo de Protección de Datos (2017). *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content* (Report SEPD.). Brussels: SEPD Disponible en: https://tinyurl.com/yckvj9yh.

Troncoso Reigada, A. (2021). Los principios relativos al tratamiento. Comentario al art. 5 Reglamento General de Protección de Datos y al art. 4 Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 847-907). Navarra: Thomson Reuters Aranzadi.

Valls Prieto, J. (2021). *Inteligencia artificial, derechos humanos y bienes jurídicos*. Navarra: Thomson Reuters Aranzadi.

Van Dalen, S., Gilder, A., Hooydonk, E. y Ponsen, M. (2016). *System risk indication: an assessment of the dutch anti-fraud system in the context of data protection and profiling. Public Interest Litigation Project, Nederlands Juristen Comité voor de Mensenrechte.* London: University of London. Disponible en: https://tinyurl.com/3udmxr87.

Veliz, C. (2020). *Privacy is power*. Madrid: Penguin Random House.

Warren, S. D. y Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4 (5), 193-220. Disponible en: https://doi.org/10.2307/1321160.

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