CAPÍTULO IV

INTELIGENCIA ARTIFICIAL Y DERECHOS FUNDAMENTALES

LAURA GÓMEZ ABEJA
Universidad de Sevilla
lgomez2@us.es

1. INTRODUCCIÓN

Nuestras vidas han cambiado mucho en los últimos años gracias a los avances tecnológicos, que se encuentran estrechamente vinculados al uso del *big data* -también conocido como "macrodatos" o "datos masivos"- y a la inteligencia artificial. En efecto, la ingente -y siempre creciente- cantidad de datos disponible y los avances informáticos y algorítmicos han permitido a la inteligencia artificial facilitar nuestro día a día, con aplicaciones que nos ayudan -por ejemplo- a llegar a un lugar determinado, a saber cuántas calorías hemos consumido, o a identificar una canción que oímos y nos agrada, pero cuyo título y autor no conocemos o no recordamos; pero la IA también ha servido para afrontar grandes problemas a los que nos enfrentamos hoy como sociedad, como el tratamiento de algunas enfermedades crónicas, la prevención de otras graves, o la lucha contra el cambio climático[1]. Es evidente que desde esta perspectiva debe hacerse una valoración muy positiva de la IA y del *big data*, que han permitido unos avances inimaginables hasta hace pocos años. Pero el uso de estas herramientas también ha traído consigo un aspecto negativo. Y no es un problema menor, pues se trata de la vulneración -también masiva- de ciertos derechos fundamentales que, además, conforme avanza la acumulación y tratamiento de datos y el desarrollo de las nuevas tecnologías mediante la IA, se antoja cada vez más difícil de atajar. En estas páginas se van a hacer unas consideraciones generales al hilo del impacto del *big data* y el uso de algoritmos (para la toma de decisiones que afectan a personas) en dos derechos fundamentales: el derecho a la protección de datos personales (art. 18.4 CE) y el derecho a la no discriminación (art. 14 CE). Para ello, en primer lugar se harán las necesarias precisiones terminológicas. Después se expondrá cómo el uso de esas herramientas afecta en particular a los derechos mencionados. En tercer lugar se incidirá en las medidas -jurídicas- que se han adoptado para garantizar la protección de estos derechos y en algunas de las limitaciones que -a mi juicio- presentan las mismas. Finalmente se efectuarán a modo de conclusión algunos apuntes, con carácter esencialmente propositivo.

[1] Como indica la Comunicación de la Comisión de 25 de abril de 2018, al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo, y al Comité de las Regiones Inteligencia Artificial para Europa [COM (2018) 237 final].

2. PRECISIONES TERMINOLÓGICAS

Muchos de los conceptos relevantes en este contexto son relativamente recientes, o al menos novedosos para la mayoría de nosotros. Esto, junto al hecho de que habitualmente se trate de anglicismos (el de las TICs es uno de los muchos ámbitos en que los conceptos nuevos hacen fortuna en su versión inglesa), nos sitúa ante un sinfín de términos desconocidos -cada vez menos, eso sí- y exóticos, tales como *big data, data mining*, algoritmos, inteligencia artificial, *machine learning*, *privacy by design/by default*, o perfilado, entre muchos otros. Se hace necesario, pues, precisar algunos de estos conceptos.

En primer lugar, con el término *big data* se hace referencia, siguiendo lo dispuesto por el Parlamento Europeo, a "la recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personales (…), objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones"[2], a lo que debe añadirse que todo ello puede hacerse "a una gran velocidad de tratamiento" (Eguíluz Castañeira, 2020, 328). El concepto *big data* -de lo que también se habla como datos masivos o macrodatos- está asociado, por tanto, al de algoritmo. Con *algoritmo*, en el contexto que nos ocupa y en términos sencillos, nos estaremos refiriendo a la fórmula informatizada que se utiliza para calcular una predicción, mediante el uso de los datos disponibles. Es importante añadir que el algoritmo es una "creación humana" (Eguíluz Castañeira, 2020, 330), en el sentido de que son personas las que elaboran la fórmula que después será ejecutada por una computadora. Otra noción esencial es la de *inteligencia artificial,* con la que, según el Grupo de Expertos en Inteligencia Artificial de la Comisión Europea, se hace referencia a los sistemas que muestran un comportamiento inteligente, analizando su entorno y realizando acciones con cierta autonomía para lograr sus objetivos específicos[3]. La inteligencia artificial no puede entenderse sin la noción de algoritmo, a través del que se articula. Consecuentemente, su virtualidad -como

[2] Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)), en línea: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.pdf (última consulta: 22 de febrero de 2022).

[3] El Grupo de Expertos de Alto Nivel en Inteligencia Artificial se constituyó siguiendo lo previsto en la Comunicación de la Comisión sobre Inteligencia Artificial para Europa, de 25 de abril de 2018, dirigida al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y social Europeo, y al Comité de las Regiones. El documento, "Una definición de la Inteligencia Artificial: principales capacidades y disciplinas científicas", publicado el 18 de diciembre de 2018, está disponible en línea: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf (última consulta: 22 de noviembre de 2021).

la de aquél- depende también de la intervención humana, por eso la autonomía de la IA a la que se ha hecho referencia es sólo relativa, en el sentido de que se desarrollará, en principio, dentro de los parámetros previstos por las personas programadoras del sistema y creadoras de los algoritmos que lo integren.

Desde la perspectiva del debate jurídico, no en el sentido de que sean sinónimos desde un punto de vista técnico, por supuesto, algoritmo e inteligencia artificial se han llegado a utilizar indistintamente (Eguíluz Castañeira, 2020, 331). De otra parte, como se ha afirmado, "*big data* e inteligencia artificial se relacionan de manera bidireccional: por un lado, la IA necesita una gran cantidad de datos para el aprendizaje automático y, por el otro, el *big data* utiliza la IA y sus técnicas para extraer valor de los grandes volúmenes de información" (Arellano Toledo, 2019, 5). Los algoritmos y el *big data,* en fin, forman parte del universo de la inteligencia artificial. Todos ellos son, pues, conceptos íntimamente imbricados. A lo largo de estas páginas saldrán a colación otros conceptos propios del tema que nos ocupa. Por el momento basta con conocer los expuestos en las líneas previas.

3. DERECHOS FUNDAMENTALES EN JUEGO

El presente trabajo se centra en dos derechos -la protección de datos y la no discriminación- que resultan especialmente relevantes en este contexto, pero antes de profundizar en ellos debe al menos recordarse que existen otros derechos incididos a consecuencia del uso del *big data* y del desarrollo de la inteligencia artificial y sus avanzados algoritmos para la toma de decisiones, como el derecho a la tutela judicial (Castellanos Claramunt/Montero Caro, 2020), el derecho a la libertad de información (Cotino Hueso, 2017, 140), el derecho al sufragio (García Mahamuth, 2015) o el derecho de acceso a la información pública (Medina Guerrero, 2021).

3.1. El derecho a la protección de datos personales

Uno de los derechos que se ha visto gravemente cuestionado a consecuencia de la acumulación masiva de datos es el derecho a la protección de los datos personales. Gran parte de la información del *big data* son datos de carácter personal. La tecnología permite que empresas privadas y poderes públicos utilicen masivamente datos personales en la realización de sus actividades. Por su parte, las personas físicas divulgan cada vez más información personal al público en general[4]. En este último caso, los datos

[4] Así lo señala el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en su considerando sexto.

proceden esencialmente de las redes sociales, pero las fuentes que proporcionan esta clase de información al *big data* son muy diversas, desde los dispositivos inteligentes -en general, el "internet de las cosas"- hasta las empresas con las que se efectúan transacciones, que proporcionarán información sobre pagos o datos administrativos[5]. Como es obvio, las posibilidades de control de esa información por parte de sus titulares se difuminan en un universo de trasiego constante y masivo de datos, por los que todos pujan. Y es que ello sucede sobre todo por el gran interés que existe en los datos, de los que se ha hablado como el petróleo del siglo XXI, pues se han convertido en un activo patrimonial de un valor económico sin precedente en los mercados (Sancho López, 2019, 3):

> Los datos son hoy el propulsor de crecimiento y transformación, como lo fue el petróleo en su momento. Y los flujos de datos configuran hoy nuevas infraestructuras, nuevos modelos de negocio y nuevas economías, con nuevos actores en posición de monopolio y políticas estatales diferenciadas según las ventajas de partida para beneficiarse de las reglas de mercado (Moreno Muñoz, 2017, 9, citado en Sancho López, 2019, 3).

Que el sector de los macrodatos esté "creciendo a un ritmo del cuarenta por ciento anual, siete veces más rápidamente que el del mercado de las tecnologías de la información" (Parlamento Europeo, 2017, considerando K) o que se calculase que en Europa el *big data* implicaría un incremento adicional del PIB de un uno coma nueve por ciento para 2020 (Cotino Hueso, 2019, 9), son elementos que corroboran sin atisbo de duda el valor que han alcanzado los macrodatos. Se ha hablado, en este sentido, del *big data* como "*big deal*: el *big data* es un gran negocio. Los datos personales se capitalizan y se comercializan por completo" (Han, 2014, 98, citado en Sancho López, 2019, 4).

Más allá del valor que tienen actualmente *per se* en los mercados, ¿cómo y para qué se utilizan los datos? Pues con ellos, como explica L. Cotino, se hace una "estadística del todo", combinándose miles de datos de forma prácticamente aleatoria: "frente a la contrastación de una hipótesis a partir de los datos, se descubren correlaciones sin conocer previamente la causa. Así sucede al probar casi aleatoriamente la posible correlación entre datos en principio totalmente distantes" (Cotino Hueso, 2017, 133, citando a Martínez, 2014, 3). Las conexiones resultantes permiten generar patrones de tendencias de futuro, a lo que se puede dar una diversidad de usos, válidos para todos los

[5] Así se ha puesto de manifiesto en el documento de la *European Union Agency for Fundamental Rights*, "*BigData: Discrimination in data-supported decision making*", disponible en línea: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf (última consulta: 21 de febrero de 2022).

sectores de actividad (tanto para el ámbito público como privado): mejor conocimiento del cliente, del mercado, personalización de productos y servicios, mejora y rapidez en la toma de decisiones, o previsión del comportamiento (AEPD-ISMS, 2017, 6-7). Y el beneficio que se obtiene por el uso de datos es incontestable: las empresas que basan la toma de decisiones en los conocimientos procedentes de datos experimentan un aumento aproximado de la productividad de un cinco con seis por ciento[6].

Expuesto cuanto antecede, puede comprenderse por qué los datos (que a menudo serán datos de carácter personal) tienen tanto valor y por qué en la actualidad hemos llegado a una suerte de "expropiación de la privacidad sin precedentes" (Sancho López, 2019, 24).

3.2. El derecho a la no discriminación

Otra consecuencia del uso del *big data* y los algoritmos es la posible lesión del derecho a no ser discriminado. Concretamente, en términos del Parlamento Europeo, los macrodatos pueden resultar en un tratamiento diferenciado injustificado "y en una discriminación indirecta de grupos de personas con características similares, en particular en lo que se refiere a la justicia e igualdad de oportunidades en relación con el acceso a la educación y al empleo, al contratar o evaluar a las personas o al determinar los nuevos hábitos de consumo de los usuarios de los medios sociales" (Parlamento Europeo, 2017, consideración general decimonovena). La discriminación se puede producir en distintas fases del proceso de toma de decisiones mediante el uso de datos: desde el momento en que estos son recogidos hasta el de la aplicación del algoritmo por el que se toma la decisión de que se trate.

En un primer momento podría pensarse que estas técnicas presentan una objetividad intachable, pero no es así, o al menos no siempre lo es. Son personas las que fijan las reglas sobre qué datos se van a utilizar y cómo, por lo que estas decisiones inevitablemente tienen una vertiente subjetiva. Las creencias o los valores de quienes deciden qué datos recabar y cómo utilizarlos podrían quedar reflejados en su recogida y tratamiento. En muchas ocasiones el sesgo no será evidente, e incluso puede ocurrir que la persona que trabaja con el sistema en cuestión no esté reflejando en el proceso ideas o valores discriminatorios, pero que el resultado finalmente sí lo sea. Siguiendo el ejemplo de Zuiderveen Borgesius (2018:17), una empresa podría utilizar un algoritmo para la contratación de su personal en el que la "variable objetivo" (que define lo que se quiere encontrar) sea "ser un buen profesional", y usar para su determinación

[6] Así puede leerse en la edición de *El país* de 13 de octubre de 2014, en línea: https://elpais.com/tecnologia/2014/10/13/actualidad/1413199836_461461.html (última consulta: 22 de febrero de 2022).

una "etiqueta de clase" (que divide los datos en categorías) relativa a la puntualidad, en la que se indique que "rara vez llega tarde". Las personas más pobres suelen vivir en el extrarradio y deben viajar más lejos que otros trabajadores para llegar al centro de trabajo. En consecuencia, la gente más pobre suele llegar tarde al trabajo más habitualmente que otros, por los atascos y problemas con el transporte público. Además, estos grupos humanos están integrados muy a menudo por inmigrantes. Si la empresa utiliza la etiqueta "raramente llega tarde" para determinar si un empleado es un buen profesional, se estaría poniendo en desventaja a la población inmigrante y más pobre, aunque sean mejores en otros aspectos (contemplados o no en otras etiquetas).

Puede suceder también, claro está, que el sesgo se introduzca de forma deliberada. Siguiendo con el ejemplo de Zuiderveen (2018: 22), una empresa podría servirse de un algoritmo que permite predecir el embarazo (que utilizan algunas compañías con fines de marketing) para evitar contratar a mujeres embarazadas, discriminándolas deliberadamente[7]. O podrían introducirse sesgos para dirigir determinados comportamientos y -o- crear opiniones políticas, como sucedió en las elecciones estadounidenses con *Cambridge Analytica* (Arellano Toledo, 50, 2019, 8).

El hecho de que quienes determinen la forma en que se van a recabar los datos y quienes creen los algoritmos sean personas supone además que pueda distinguirse un grupo privilegiado en este sentido, el de quienes pueden leer los datos, que pueden impedir a los demás el acceso a esos datos o el acceso al conocimiento generado gracias a los mismos. En el extremo opuesto, siendo objeto de especial discriminación, se encontrarían los marginados del *big data*, que sencillamente no aportan datos al mismo, millones de personas cuyas "preferencias y necesidades están en riesgo de ser ignoradas en las decisiones que se basen en el *big data* y la inteligencia artificial" (Cotino Hueso, 2017, 138).

Puede compartirse pues la afirmación de que "los algoritmos no son imparciales" (Arellano Toledo, 2019, 8). Y debe añadirse que tampoco son exactos. Las personas que trabajan creando los sistemas de inteligencia artificial pueden equivocarse y los errores se reflejarán en los resultados que el sistema arroje; pero es que, además, en contra de la creencia general que atribuye una alta precisión a los sistemas de IA, el *big data* no es siempre fiable. Las interrupciones y las pérdidas de datos que se producen con frecuencia en el mundo virtual producen errores en los resultados algorítmicos (Cotino Hueso, 2017, 134).

[7] Explica el autor (Zuiderveen Borgesius, 2018, 22 y 23) que la cadena estadounidense de tiendas *Target* creó un sistema de predicción de embarazo por puntuación basado en unos veinticinco productos, analizando el comportamiento de los clientes en sus compras. Si una mujer compra algunos de esos productos, *Target* puede predecir con bastante certeza que está embarazada.

Conviene citar -para concluir- las palabras del Parlamento Europeo en su Resolución de 2017:

> Los datos y/o los procedimientos de baja calidad en los que se basan los procesos de toma de decisiones y las herramientas analíticas podrían dar lugar a algoritmos sesgados, correlaciones falsas, errores, una subestimación de las repercusiones éticas, sociales y legales, el riesgo de utilización de los datos con fines discriminatorios o fraudulentos y la marginación del papel de los seres humanos en esos procesos, lo que puede traducirse en procedimientos deficientes de toma de decisiones con repercusiones negativas en las vidas y oportunidades de los ciudadanos, en particular los grupos marginalizados, así como generar un impacto negativo en las sociedades y empresas (Parlamento Europeo, 2017, considerando M).

4. RECONOCIMIENTO DE LOS DERECHOS INCIDIDOS Y MEDIDAS ADOPTADAS RECIENTEMENTE PARA SU PROTECCIÓN

Los derechos a la protección de datos personales y a la no discriminación, como es bien conocido, encuentran amparo en el ordenamiento jurídico español al más alto nivel normativo, en la Constitución, y su contenido ha sido desarrollado y delimitado por el máximo intérprete de la norma fundamental, el Tribunal Constitucional. Algo similar sucede a nivel regional europeo, con las normas *cuasi* constitucionales y los tribunales a los que corresponde su interpretación. El uso de la IA, también es sabido, ha provocado nuevas formas de lesión e invasión en estos derechos. Los mecanismos para su protección han ido quedando obsoletos, y han tenido que crearse nuevas fórmulas para luchar contra la invasión en estas libertades, mediante la aprobación de normas y la creación de órganos *ad hoc*, como se verá enseguida. Especialmente en la Unión Europea se ha llevado a cabo una constante actividad en este sentido desde sus distintas instancias.

4.1. El derecho a la protección de datos personales

4.1.1. Reconocimiento multinivel del derecho

El apartado cuarto del artículo 18 de la Constitución Española establece una genérica limitación legal del "uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", y el Tribunal Constitucional determinó que el mismo ampara un derecho fundamental a la protección de los datos personales; derecho que tiene, por un lado, carácter *instrumental*, al configurarse como un "un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos" (STC 292/2000 FJ 5, que cita la STC 254/1993, FJ 6) y, por otro lado, naturaleza de derecho *autónomo*, que faculta a

"controlar el flujo de informaciones que conciernen a cada persona" (STC 94/1998, FJ 6). El contenido de este derecho "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso" (STC 292/2000, FJ 7).

En el contexto del Consejo de Europa, el Convenio número 108 del Consejo de Europa de 1981 -recientemente modificado por el Protocolo de Enmienda de 2018 (Convenio número 223 del Consejo de Europa)- dispone en su artículo primero que su objetivo es proteger a todas las personas físicas en lo que respecta al tratamiento de datos personales, para lo que establece una serie de garantías y limitaciones al acceso y tratamiento de los datos por terceros. En el ámbito de la Unión Europea, el artículo 16 del Tratado de Funcionamiento de la Unión Europea dispone que "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan", y el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea lo reconoce en los mismos términos[8].

Conforme el derecho fundamental a la protección de datos se ha ido viendo más comprometido a medida que se ha desarrollado el *big data*, la Unión Europea ha venido alertando de este problema y desde sus propias instituciones ha intentado adoptar soluciones para conciliar ese desarrollo con el respeto a la privacidad de las personas en este contexto. Destaca en este sentido la labor realizada por el conocido como Grupo de Trabajo del artículo 29, un órgano de naturaleza consultiva, actualmente extinto -llamado así porque fue creado al amparo de lo dispuesto por el artículo 29 de la derogada Directiva 95/46/CE relativa a la protección de datos de las personas físicas- del que pueden reseñarse diversos trabajos en los que manifestaba su preocupación por la protección de los datos personales ante los retos actuales de las nuevas tecnologías[9]. Debe destacarse, por lo que aquí interesa, su Declaración sobre el

[8] El apartado segundo dispone que "Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación". El apartado tercero, finalmente, establece que "El respeto de estas normas quedará sujeto al control de una autoridad independiente".

[9] Como el Dictamen 02/2013, de 27 de febrero, sobre las aplicaciones de los dispositivos inteligentes; el Dictamen 13/2011, de 16 de mayo, sobre los servicios de geolocalización en los dispositivos móviles inteligentes; la Opinión 03/2013, de 2 de abril, sobre la "limitación del propósito" (para el uso de datos, también en el *big data*); o el Dictamen 9/2011 sobre la propuesta de la industria revisada para un marco de evaluación de impacto de protección de datos y privacidad para aplicaciones RFID.

impacto del desarrollo del *big data* en la protección de las personas con respecto al procesamiento de sus datos personales en la UE[10]. Por su parte, el Parlamento Europeo había manifestado en una Resolución de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea[11], que la Directiva 95/46/CE no alcanzaba a proteger este derecho frente a los nuevos riesgos a los que se encuentra expuesto debido a los recientes desarrollos tecnológicos. En este sentido, interesan también lo dispuesto por la Comisión Europea[12], el Comité Económico y Social Europeo, y el Comité de las Regiones[13]. Se hacía necesaria una nueva regulación que garantizase la protección de este derecho y mediante la que se homogeneizasen las diversas normativas internas. Dicha norma sería el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE.

4.1.2. El derecho a la protección de datos en el RGPD

El RGPD ha supuesto un importante avance para la protección de los datos personales. Entre los aspectos que pueden subrayarse, destaca el hecho de que el Reglamento haya ampliado su ámbito de aplicación, que ponga nuevos derechos a disposición de los titulares de los datos, que cree nuevas figuras ordenadas a la satisfacción de esa protección, y que introduzca una importante novedad que supone un cambio respecto de la anterior concepción del funcionamiento, por así decir, de la protección de datos, en relación con quiénes son responsables de su satisfacción. Todo ello, como no podía ser de otra manera, ha sido recogido por la Ley Orgánica 3/2018, de 5 de diciembre, de

[10] Puede consultarse en línea: https://es.calameo.com/aec/read/0018452803697a312e27b?authid=X62stTIQh47x&page=1 (última consulta: 22 de febrero de 2022).

[11] Resolución del Parlamento Europeo, de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea, en línea: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//ES (última consulta: 22 de febrero de 2022).

[12] Comunicación de la Comisión, de 10 de junio de 2009, al Parlamento Europeo y al Consejo "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos − Programa de Estocolmo", en línea: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52009DC0262&from=es (última consulta: 22 de febrero de 2022).

[13] Dictámenes publicados respectivamente (según dispone al principio el RGPD), en el DOC 229, de 31 de julio de 2012 (p. 90), en línea: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.C_.2012.229.01.0090.01.SPA&toc=OJ%3AC%3A2012%3A229%3AFULL, y en el DOC 391, de 18 de diciembre de 2012 (p. 127), en línea: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.C_.2012.391.01.0127.01.SPA&toc=OJ%3AC%3A2012%3A391%3ATOC (última consulta: 3 de marzo de 2022).

Protección de datos personales y garantía de los derechos digitales[14], aprobada para armonizar la legislación española con lo previsto en el Reglamento, aplicable desde mayo de ese mismo año.

En cuanto a su ámbito territorial, el Reglamento señala que "será de aplicación a quienes lleven a cabo sus actividades en la Unión, y en ese contexto traten datos personales, *aunque el tratamiento* de los datos personales *no se haga en el territorio de la Unión*" (cursiva añadida. RGPD, considerando 22).

Por lo que hace a los derechos que puede ejercer el titular de los datos personales, los clásicos derechos ARCO (acceso, rectificación, cancelación y oposición) se modifican, en parte, y se amplían con otros nuevos. El Reglamento reconoce los derechos de acceso (art. 15), rectificación (art. 16), supresión, que equivale al derecho de cancelación y que alcanza al "nuevo" derecho al olvido (art. 17), el derecho a la limitación del tratamiento (art. 18), a la portabilidad (art. 20), y a la oposición (art. 21).

Destaca la creación del Comité Europeo de Protección de Datos como organismo de la Unión (art. 68) y, a nivel interno, de los delegados de protección de datos, que deben ser designados por los responsables o encargados del tratamiento de los datos personales (art. 37). Su designación será obligatoria cuando el tratamiento de los datos personales los lleve a cabo una autoridad u organismo público (excepto los tribunales), y en un gran número de supuestos (desarrollados a nivel nacional por el art. 34 de la LOPDGDD), cuando el tratamiento de los datos lo efectúe una empresa privada. El delegado tiene atribuidas una variedad de funciones, como la de informar y asesorar al responsable o al encargado del tratamiento, y a los empleados que se ocupen del tratamiento, de las obligaciones que les incumben en relación con la protección de datos, o la de supervisar el cumplimiento de lo dispuesto en el Reglamento y las demás normas relativas a la protección de datos (art. 39).

Finalmente, como se ha señalado, se introduce una novedosa modificación en cuanto a quién se exige la satisfacción de las obligaciones impuestas por el Reglamento. La norma transfiere a los responsables del tratamiento la obligación de velar por su cumplimiento, refiriéndose en su artículo 5.2. a lo que llama "responsabilidad proactiva". Desde esta premisa, se exige la protección de datos "desde el diseño y por defecto" (art. 25), de modo que, desde el inicio -tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento-, la privacidad se

[14] A ésta la habían precedido la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD, y la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, que se aprobó para trasponer al Derecho español la Directiva 95/46/CE.

integre en el tratamiento de los datos. Para ello, el RGPD pone a disposición del responsable del tratamiento (empresa privada u organismo público) medidas técnicas y organizativas para satisfacer su deber de garantizar la protección de datos personales. Se les exige, por ejemplo, que los datos estén limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos) (art. 5.1.c); se prevé que, si es necesario, se proceda a la seudonimización y cifrado de los datos (art. 32) o que se realice una evaluación de impacto relativa a la protección de datos. Sobre esta evaluación, en particular, el artículo 35.1 dispone que "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales".

4.1.3. Visión crítica. El limitado alcance del RGPD para la protección del derecho a la protección de datos

Sin negar los avances que el RGPD ha traído consigo, ni su voluntad de garantizar la protección de los datos personales, no pueden orillarse los muchos problemas que la norma presenta para la eficacia real de los principios que proclama y los derechos que reconoce.

Una primera cuestión clave tiene que ver con el consentimiento, en torno al que ha girado siempre el tratamiento de los datos personales. El RGPD mantiene este planteamiento, exigiendo que los datos sean tratados de forma lícita, lo que en principio sucederá si "el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos" (art. 6.1.a). Se ha señalado que este planteamiento está superado, pues a día de hoy no existe un control efectivo de los datos personales a través del consentimiento y los derechos a través de los que se articula. "La sociedad no está dispuesta a renunciar al uso de las IT y no tiene una fuerte cultura de la privacidad, lo que lleva a hacer casi irreal o inefectiva la garantía del consentimiento", el cual "se torna en una carta blanca al descontrol del flujo de los datos personales (...). El consentimiento acaba configurándose como un simbolismo que conlleva, a la postre, al fracaso de la privacidad pretendida y a la inoperancia del sistema de protección" (Oliver Lalana y Muñoz Soro, 2014, 163).

También puede considerarse desacertado el modo en que el Reglamento ha hecho recaer su cumplimiento en los responsables del tratamiento de los datos. A tal efecto, estos deben llevar a cabo una importante inversión en medios y preparación, así como una amplísima dedicación para el control del cumplimiento, exigencias todas que en muchos casos (pymes, autónomos) se antojan imposibles. Si a ello se añade que las nuevas previsiones normativas no

cuentan con la connivencia de las grandes corporaciones del *big data*, puede dudarse de la virtualidad del Reglamento en cuanto a que suponga una gran mejora para la protección de los datos personales desde esta perspectiva (Sancho López, 2019, 9).

Otro asunto controvertido es el hecho de que, pese a la teórica "responsabilidad proactiva" de los responsables del tratamiento, la protección de datos -en el Reglamento y también, claro, en la LOPDGDD- parece descansar asimismo, o al menos confiar, en una importante participación activa del ciudadano. Así lo acreditan la "artillería" de derechos que se le reconocen, la forma en que estos se articulan, y la realidad frente a la que están reconocidos, en la que lo habitual es que los productos que se adquieren estén preconfigurados para que la persona acepte el máximo nivel de cesión de sus datos personales, para todos los fines posibles. Pues bien, este planteamiento sería inadecuado, de un lado, porque se le presumen al ciudadano unos conocimientos técnicos de los que muy bien puede adolecer y, de otro, sobre todo, porque no parece la opción más adecuada para la protección de un derecho fundamental. Muy al contrario, de este modo se formaliza una lógica opuesta a la que subyace al sistema de garantía y protección de los derechos fundamentales propio de un Estado democrático de Derecho, y se provoca, asimismo, el indeseado *chilling effect* o efecto desaliento en los ciudadanos, quienes además ya "perciben la pérdida de privacidad como una consecuencia inevitable del progreso tecnológico, o como el precio que debemos de pagar si queremos evitar el aislamiento social" (Sancho López, 2019, 19).

Una última cuestión es relativa a la no aplicación de la normativa de protección de datos a la información anonimizada. El Reglamento dispone que "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable". Será también de aplicación a los datos personales seudonimizados, que son aquéllos que "cabría atribuir a una persona física mediante la utilización de información adicional". En cambio, tales principios "no deben aplicarse a la información anónima, es decir, información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo" (considerando 26). Teóricamente la anonimización puede evitar toda posibilidad de reidentificar al individuo. Sin embargo, actualmente -se ha señalado- es imposible lograr la anonimización absoluta pues, dada la inmensa -y cada vez mayor- cantidad de datos de que dispone el *big data,* siempre existe un riesgo de que a través de los datos anonimizados se pueda reidentificar a las personas a las que están vinculados

(Morales Barceló, 2017, 6; y Gil González, 2016, 83)[15]. Qué decir, pues, de los datos que "sólo" han sido seudonimizados. Se pone en peligro de esta forma la privacidad, y el Reglamento, sencillamente, parece orillar este espinoso asunto. La LOPDGDD sí aborda algo la cuestión, aunque básicamente para garantizar que se evite la reidentificación en el ámbito del tratamiento de los datos personales de salud[16]. La norma también preceptúa como una infracción muy grave "la reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados" (art. 72.1 p LOPDGDD).

En relación con la obligación de realizar una evaluación de impacto en el caso de determinados tratamientos de datos (art. 35), cabría preguntarse si esta exigencia podría llegar a convertirse en una mera formalidad previa al tratamiento de los datos, cuando el informe sobre la evaluación de impacto es obligatorio.

A las críticas expuestas cabría añadir que el Reglamento abusa del uso de conceptos jurídicos indeterminados, y efectúa excesivas remisiones a las normativas internas[17]. Interesa incidir, a modo de conclusión, en el hecho de que las limitaciones que presenta el RGPD -para alzarse como una verdadera herramienta para garantizar el derecho a la protección de datos personales- tienen que ver con que la protección de datos no es el único objetivo, quizá tampoco el primero, perseguido por el Reglamento, que tiene como especial interés "asegurar el libre flujo de datos entre los Estados parte" (Sancho López, 2019, 14). El considerando segundo es clarificador en este sentido: "El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".

[15] Ambas autoras se encuentran citadas en la siguiente entrada del portal *Legaltoday*, en línea: https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/datos-anonimizados-fuera-de-la-normativa-de-proteccion-de-datos-2020-10-01/ (última consulta: 23 de febrero de 2022). El Grupo de Trabajo del artículo 29 había advertido también sobre el riesgo de reidentificación del titular de los datos, en su Dictamen 5/2014.

[16] La disposición adicional décimo séptima de la LOPDGDD, relativa a "Tratamientos de datos de salud", prevé "una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación" (apartado 2, d.1), y la realización de una evaluación de impacto que "incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos" (apartado 2, f.1).

[17] Esto se contradice con lo que cabría esperar de una norma que se adoptó para homogeneizar y superar la disparidad normativa de los Estados miembros. A nivel interno, en cuanto a la LOPDGDD, coincido con Sancho López (2019:7) en que no ha supuesto una gran mejora en relación con las dificultades que presenta el Reglamento, y en que precisamente genera más interrogantes que respuestas.

5. EL DERECHO A LA NO DISCRIMINACIÓN

5.1. Reconocimiento multinivel del derecho a la no discriminación

El artículo 14 de la Constitución española proclama la igualdad ante la ley, "sin que pueda haber discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social". Se trata de la igualdad formal, que determina, por un lado, que la ley ha de ser aplicada por igual a todos; que el legislador no puede dispensar injustificadamente tratos diferenciados a quienes se encuentran en situaciones jurídicas similares (igualdad en la ley); y, por otro, que los jueces han aplicar la ley por igual a quienes se encuentren en la misma situación, salvo que el cambio de criterio sea motivado y razonable (igualdad en la aplicación de la ley).

La norma, no obstante, sí puede introducir diferenciaciones entre categorías de personas que aparentemente se encuentren en la misma situación si la diferencia de trato resulta justificada de forma objetiva y razonable, y siempre que la diferenciación supere el juicio de proporcionalidad (STC 76/1990, FJ 9, STC 22/1981, FJ 3, y STC 49/1982, FJ9). Además, de esta forma (introduciendo diferenciaciones entre categorías de personas para que un colectivo o grupo pueda disfrutar como los demás del ejercicio de un derecho), el legislador satisface la igualdad material, reconocida en el artículo 9. 2 CE, según el cual "corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas".

Interesa también distinguir entre discriminación directa e indirecta, siendo la primera la que se produce cuando una persona es tratada de modo menos favorable que otra en una situación análoga a causa de su género, raza, o cualquier otra circunstancia personal o social. La discriminación indirecta, en cambio, se produce cuando una norma, actuación, o criterio aparentemente neutral genera una específica desventaja a un grupo de personas por alguna condición personal o social. El Tribunal Constitucional se pronunciaría sobre la discriminación indirecta al hilo de la discriminación por razón de sexo, afirmando que la prohibición de discriminación por razón de sexo consagrada en el art. 14 CE, "comprende no sólo la discriminación directa, es decir, el tratamiento jurídico diferenciado y desfavorable de una persona por razón de su sexo, sino también la indirecta, esto es, aquel tratamiento formalmente neutro o no discriminatorio del que se deriva, por las diversas condiciones fácticas que se dan entre trabajadores de uno y otro sexo, un impacto adverso sobre los miembros de un determinado sexo" (STC 253/2004 (FJ 7), citando la STC 198/1996, FJ 2; y, en sentido idéntico, las SSTC 145/1991, 286/1994 y 147/1995).

En el ámbito del Consejo de Europa, el artículo 14 del CEDH establece que el goce de los derechos y libertades del Convenio ha de ser asegurado sin distinción alguna, mencionándose también una serie de causas específicas de discriminación. Por lo que hace al contexto de la Unión, el artículo 21 de la Carta de los derechos fundamentales de la UE prohíbe toda discriminación, y el artículo 10 del TFUE dispone que la Unión tratará de luchar contra ella en cualquiera de sus manifestaciones. Desde la perspectiva jurisprudencial, es indudable la importancia de la labor del TEDH en la construcción de los conceptos y en la determinación del contenido de la igualdad y la no discriminación[18], aunque los pronunciamientos del TJUE en materia de discriminación indirecta parecen ser el principal referente para la jurisprudencia constitucional española[19].

Desde la perspectiva legislativa o infraconstitucional, ni a nivel nacional ni a nivel comunitario existe una única norma reguladora de la igualdad con carácter general, sino diversas normas que regulan la igualdad y la no discriminación en distintos ámbitos. En el ámbito de la Unión destacan un importante número de Directivas: sobre la no discriminación por razón del origen étnico o racial, la Directiva 2000/43/CE; sobre la no discriminación en el ámbito laboral (por razones de edad, discapacidad, religión u orientación sexual), la Directiva 2000/78/CE; y sobre no discriminación por razón de género, la Directiva 2002/73/CE (para el ámbito laboral), la Directiva 2004/113/CE, y la Directiva 2006/54/CE (también para el ámbito laboral).

En el orden interno pueden mencionarse la aprobación de la Ley 39/1999, de 5 de noviembre, para promover la conciliación de la vida familiar y laboral de las personas trabajadoras; la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, que trasponía el contenido de las dos primeras Directivas arriba citadas; la Ley Orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género, aprobada para erradicar esta particular forma de discriminación de la mujer; la Ley Orgánica 3/2007, del 22 de marzo, para la igualdad efectiva de mujeres y hombres, que pretendía integrar, trasponiéndolas, las Directivas 2002/73/CE y 2004/113/CE, ya mencionadas, y que se conoce como "Ley de Igualdad"; la Ley 3/2007, de 15 de marzo, reguladora de la rectificación registral de la mención

[18] Por todas, SSTEDH en los asuntos *D. H. y otros contra República Checa* (Gran Sala) núm. 57325/00, de 13 de noviembre de 2007, párrafo 175; o *Burden contra Reino Unido* (Gran Sala), núm. 13378/05, de 29 de abril de 2008, párrafo 60.

[19] Entre otras muchas, SSTJCE de 27 de junio de 1990, en los asuntos *Kowalska*; de 7 de febrero de 1991, *Nimz*; de 4 de junio de 1992, *Bötel*; o de 9 de febrero de 1999, en el *Asunto Seymour-Smith y Laura Pérez*, citadas en la STC 253/2004.

relativa al sexo de las personas; o la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte[20].

En el contexto de la inteligencia artificial, el tratamiento de datos masivos y el uso de algoritmos puede desembocar en estos tratos discriminatorios, como ya se señaló arriba. Un derecho que paliaría la eventual discriminación derivada del tratamiento de datos y de las decisiones automatizadas sería el derecho a la transparencia algorítmica[21], que consistiría en proporcionar al interesado la información relativa al algoritmo que se ha utilizado para adoptar una decisión, como los parámetros y las concretas operaciones realizadas por el mismo. El Reglamento no reconoce la transparencia algorítmica. Sí contempla la transparencia "a secas" (artículo 12), pero orientada a garantizar la protección de datos, y no la no discriminación[22]. En efecto, es transparencia en el sentido de permitir al individuo el acceso a la información personal de la que dispone el responsable del tratamiento, y el acceso a los fines a los que está orientado su uso. Transparencia para que el ciudadano pueda procurarse y asegurarse el respeto a su privacidad.

5.2. El derecho a la no discriminación y el RGPD

Aunque, como se ha dicho, El RGPD no reconoce la transparencia algorítmica, sí contiene algunas previsiones muy importantes que podrían evitar decisiones (automatizadas) discriminatorias, contenidas en los artículos 22, 15, y en el considerando 71. El Reglamento reconoce al interesado el derecho a obtener una decisión no basada exclusivamente en el tratamiento automatizado de datos si produce en él efectos jurídicos o le afecta de modo similar (22.1), o si la decisión incluye el tratamiento de datos de las categorías sensibles del art. 9.1 RGPD (art. 22.4), salvo en algunos supuestos, como que la decisión (automatizada) sea necesaria para celebrar o ejecutar un contrato con el responsable del tratamiento de los datos, o esté autorizada por el Derecho de la Unión o de los Estados miembros, o que el interesado consienta en que la decisión sea automatizada (22.2 a, b, c). Pero, incluso en estos supuestos, el interesado tiene derecho a obtener intervención humana (22.3). Por lo demás, tiene derecho a que se le informe de la existencia de decisiones automatizadas

[20] El amplio abanico de normas que se pueden añadir a estas, de rango reglamentario y autonómico, puede consultarse en https://www.europarl.europa.eu/RegData/etudes/STUD/2020/659297/EPRS_STU(2020)659297_ES.pdf

[21] Es importante recordar en este momento que, aunque nos centremos en la discriminación, la extensión del uso de algoritmos puede provocar la vulneración de otros derechos fundamentales (derecho a la tutela judicial, el derecho de acceso a la información pública), y que la transparencia algorítmica podría servir también para solventar la lesión de esos otros derechos.

[22] Con excepción de lo dispuesto en los artículos 22.1, 13.2.f, y 15.1.h.

y, si la decisión produce en él efectos jurídicos o similares, o maneja datos de las categorías sensibles del art. 9 RGPD (o sea, las decisiones sólo "parcialmente automatizadas") tendrá, en concreto, derecho a que se le proporcione "información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado" (art 15.1. h). En cambio, si se trata de decisiones "automatizadas puras" (art. 22.3), la interpretación del artículo 22.3 en conexión con lo dispuesto en el considerando 71 *in fine* determina que en estos supuestos habrá de proporcionarse la información específica al interesado, que tendrá derecho a obtener intervención humana, a expresar su punto de vista, y a recibir una *explicación* de la decisión tomada.

Otro precepto del RGPD que interesa desde la perspectiva de la no discriminación es su artículo 9.1, que prohíbe "el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física". El precepto proscribe el tratamiento de estos datos salvo que concurra alguna de las circunstancias del apartado segundo, como, por ejemplo, que el interesado haya dado su consentimiento explícito (a), que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física (c), o que el tratamiento se refiera a datos personales que el interesado ha hecho manifiestamente públicos (e). La especial protección de estos datos se debe a que el uso de alguna de estas categorías es automáticamente sospechoso de ser discriminatorio, pues históricamente -como ya se ha visto- han sido motivo de discriminación. La novedad que presenta el RGPD en relación con la protección de las categorías especiales de datos personales es la inclusión en ellas de los datos genéticos y los biométricos (que no aparecían en la Directiva 95/46/CE)[23].

La discriminación puede producirse, como ya se indicó, en cualquier momento del proceso, desde que los datos son recogidos hasta la aplicación del algoritmo por el que se toma la decisión. Interesa en este sentido la previsión del RGPD relativa a la obligación de realizar evaluaciones de impacto previamente a determinados tratamientos de datos, ya mencionada, del artículo 35. Con esta evaluación del impacto, los responsables del tratamiento podrían detectar, y prevenir, un riesgo de discriminación en el tratamiento de los datos y/o en el algoritmo a través del que se adopte una decisión automatizada.

[23] La LOPDGDD se refiere también a las categorías especiales de datos (a algunas de ellas) en su artículo 9.

Concretamente, el apartado segundo del artículo 35 establece que la evaluación de impacto relativa a la protección de los datos a que se refiere el apartado primero se requerirá, entre otros, "en caso de evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar" (a), y de "tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo" (b).

5.3. Apuntes críticos. Limitaciones del RGPD en relación con el derecho a la no discriminación

Lo primero que ha de señalarse es la ausencia de reconocimiento del derecho a la transparencia algorítmica en el Reglamento. Desde tiempo antes de la adopción de esta norma se había venido alertando del riesgo de que la extensión del uso de decisiones automáticas y análisis predictivos pudiese conducir a cambios indeseables en el desarrollo de nuestras sociedades, dirigiéndolas hacia la discriminación, el refuerzo de estereotipos ya existentes, la segregación social y cultural, y la exclusión[24]. Sin su inclusión en el Reglamento parece haberse perdido una gran oportunidad para el reconocimiento de este derecho, el mejor instrumento para que el interesado pueda cerciorarse de que no se le ha discriminado cuando se ha tomado una decisión automatizada (o semiautomatizada), pero también para la protección de otros intereses reglamentaria y constitucionalmente relevantes.

El reconocimiento en el Reglamento del derecho a que no se adopten decisiones individuales automatizadas es, en mi opinión, confuso. Se trata de un derecho complejo, con demasiadas excepciones, y que deja abiertas cuestiones importantes. ¿Hasta dónde alcanza el "derecho a la explicación" que puede deducirse del artículo 22.3 en conexión con el considerando 71? ¿Puede considerarse equivalente al derecho a la transparencia algorítmica? Por otro lado, ¿qué sucede con las decisiones en las que haya habido una intervención humana "menor", en el sentido de que básicamente ha sido una decisión algorítmica que una persona se ha limitado a plasmar? Parece que en estos casos no existiría el derecho a la explicación, en lo que quiera que consista.

Hasta aquí se ha abordado la cuestión de la discriminación desde una perspectiva individualizada, con referencia a garantías como la información de la lógica aplicada en la decisión que afecte al interesado, o el derecho a una

[24] En este sentido se pronuncia el Supervisor Europeo para la Protección de Datos, en su Opinión 7/2015, *Meeting the challenges of big data A call for transparency, user control, data protection by design and accountability*, en línea: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf (última consulta: 23 de febrero de 2022).

explicación sobre la misma. Algo puede decirse también en este apartado sobre las previsiones normativas que podrían proteger frente a la discriminación en los momentos anteriores del proceso de tratamiento de los datos. Concretamente, sobre la obligación de realizar una evaluación de impacto en el caso de determinados tratamientos de datos (art. 35 RGPD), más allá de las dudas sobre su virtualidad ya manifestadas al hilo del derecho a la protección de datos, cabría preguntarse si esta herramienta realmente puede servir para apreciar la posible discriminación, pues, como se señaló, en ocasiones el sesgo será difícil de detectar y la evaluación de impacto no está específicamente orientada a descubrir este tipo de discriminación.

6. APUNTES PROPOSITIVOS (Y CONCLUSIVOS)

A la vista de los problemas que presenta la legislación para garantizar una efectiva protección de los derechos incididos, pueden realizarse, a modo de conclusión, algunas reflexiones, principalmente sobre las propuestas que se han planteado para paliar estas dificultades.

1. Una primera cuestión tiene que ver con la importancia de la ética en este ámbito. Habida cuenta de la incapacidad de ciertos planteamientos clásicos para la protección de los derechos incididos, como hemos señalado en relación con el consentimiento y el derecho a la protección de datos, se ha reivindicado insistentemente la importancia de los principios éticos en este contexto, no sólo por parte de la doctrina científica, sino desde las instituciones más relevantes. Tal es el caso del Parlamento Europeo, que señala, en su Resolución de 2017 sobre las implicaciones de los macrodatos en los derechos fundamentales, que "son fundamentales normas científicas y éticas estrictas para gestionar la recopilación de datos y valorar los resultados" de los análisis basados en macrodatos (consideración segunda); y se refiere a la necesidad de que los Estados miembros "desarrollen un marco ético común sólido para el tratamiento transparente de los datos personales y la toma de decisiones automatizada que sirva de guía para la utilización de los datos y la aplicación en curso del Derecho de la Unión" (consideración vigésima). Claro que, a pesar de la importancia de establecer unos principios éticos fuertes en el ámbito de la inteligencia artificial, la ética no puede sustituir al Derecho. Derecho, además, en el que entiendo que ha de primar la heterorregulación frente a la autorregulación. En este sentido, la LOPDGDD prevé que los códigos de conducta, cuya adhesión es potestativa, sean complementarios.

2. Dada la incapacidad de ciertos derechos, o de sus versiones clásicas, para la protección de los intereses de las personas frente a las nuevas tecnologías, se ha planteado la importancia de reflexionar sobre la conveniencia de reconocer nuevos derechos en el contexto de la inteligencia artificial, que pudiesen incardinarse en su caso, entiendo, en el contenido del pertinente

derecho fundamental. Se habla, por ejemplo, de un "derecho a la criptografía" (Cotino Hueso, 2017, 137), como una nueva versión del derecho a la privacidad. Ejemplos de derechos nuevos en este contexto son el derecho al olvido (de naturaleza jurisprudencial hasta su reconocimiento por el RGPD) o el derecho a no ser objeto de una decisión "automatizada pura" en determinados supuestos.

3. Ante las limitaciones de las garantías subjetivas, por las dificultades de ejercer exitosamente un control de los datos personales, deben ganar importancia las garantías objetivas (Cotino Hueso, 2017, 146), de carácter preventivo, que se articulen en forma de obligaciones sobre los responsables del tratamiento de los datos. El RGPD establece, en este sentido, el respeto de la privacidad de los datos desde el diseño y por defecto, así como la obligación de efectuar una evaluación de impacto, o la de minimizar el uso de datos personales, entre otras. Para garantizar el cumplimiento de estas obligaciones, los poderes públicos deben buscar fórmulas para evitar que la adopción de las medidas sea excesivamente gravosa para los responsables del tratamiento y, a la vez, deben de ser muy estrictos en sus funciones de inspección y auditorías (que se atribuyen a las autoridades de control, que en España es la AEPD). Auditorías, por cierto, que deberían ser unas para la protección de datos y otras específicas para la protección frente a la no discriminación, especialmente enfocadas, entre otros aspectos, a la detección de sesgos algorítmicos.

4. En particular, en relación con el derecho a la protección de datos, un elemento que cabría introducir para mejorar su protección sería el establecimiento de una limitación temporal real -o, al menos, más efectiva- para la conservación de los datos. El artículo 14.2 RGPD dispone que el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: "a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo". Por supuesto, las empresas recurren siempre a esta segunda opción ("los criterios"). La LOPDGDD tampoco ha solucionado el problema. La cuestión de los plazos es especialmente sangrante en relación con el derecho al olvido en las búsquedas de internet. Si existe este derecho, cabe preguntarse si no debería obligarse a los motores de búsqueda a suprimir la información de las personas cuando devengan las circunstancias del artículo 93 RGPD o cuando pase cierto tiempo.

5. Debe ponerse en valor, a modo de conclusión, la importante labor jurisprudencial que está siendo llevada a cabo por algunos tribunales. En relación con el derecho a la no discriminación, existen novedosas decisiones judiciales que han hecho valer este derecho cuando ha resultado lesionado por el uso de un algoritmo discriminatorio, tanto frente al poder público como frente a los particulares (en el ámbito laboral). En relación con lo primero, tuvo

bastante repercusión una sentencia holandesa, dictada en el asunto *Siry* (*System Risk Indication*) por el Tribunal de Distrito de La Haya el 5 de febrero de 2020. En ella se declararía ilegal un sistema algorítmico utilizado por el Gobierno holandés con el que se trataba de prevenir y combatir el fraude fiscal y a la seguridad social. Al aplicarse sólo en determinadas zonas integradas por barrios cuya población se consideraba que tenía una mayor predisposición a este tipo de fraude, el sistema algorítmico lesionaba el derecho a la igualdad de trato de la población más pobre e inmigrante. Esta sentencia, además, estimaba que se producía también lesión del derecho a la privacidad del art. 8 CEDH, pues se habían utilizado una cantidad ingente de datos personales, de forma desproporcionada y con incumplimiento de los principios de limitación de la finalidad y minimización (uso de los datos necesarios) (*The technolawgist*, 2020).

Por lo que hace a la eficacia horizontal del derecho a la no discriminación, destaca una sentencia italiana, dictada por el Tribunal ordinario de Bolonia, en la que la magistrada concluiría que el algoritmo utilizado por la empresa Deliveroo para organizar los horarios de los repartidores (*riders*) era discriminatorio. El repartidor podía reservar un tramo horario de reparto (en función de unos órdenes preestablecidos de selección de los mismos). Si anulaba el tramo elegido se le penalizaba y perdía su lugar en el turno de elección. La penalización era aún mayor si no lo anulaba y no acudía a repartir. Esto era así independientemente del motivo por el que lo hiciese, que sencillamente no podía alegarse, lo que, a juicio de la magistrada, suponía una discriminación indirecta: "El sistema de perfilación del *rider* adoptado por la plataforma Deliveroo, basado sobre los dos parámetros de la reputación o confianza y la participación, al tratar del mismo modo a quien no participa por motivos fútiles y a quien no participa porque hace huelga (o porque está enfermo, o lesionado, o asiste a un menor enfermo, etc), discrimina en concreto a este último, marginándolo del grupo prioritario y por lo tanto reduciendo significativamente sus futuras ocasiones de acceso al trabajo" (Baylos Grau, 2021).

6. Algunos tribunales, por tanto, están marcando pautas interesantes para el respeto de los derechos aquí incididos. Por lo que hace al derecho a la protección de datos, la labor judicial se ha desarrollado al máximo nivel, pues es el Tribunal Superior de Justicia de la Unión el que nos ha dejado ya relevantes sentencias para garantizar su protección. No puede dejar de mencionarse el *caso Costeja* (2014). Desde esta polémica decisión (STJUE en el asunto *Google contra AEPD*), bien conocida, se reconoce el derecho al olvido frente a los motores de búsqueda en internet. Otras dos importantes decisiones del TJUE son las adoptadas en el caso *Schrems (I y II)* (2015 y 2020) en que se cuestiona, a raíz de las revelaciones del analista Snowden sobre la inteligencia norteamericana, la existencia de un adecuado nivel de protección de los datos personales transferidos a ese país. En ambas sentencias -en las que invalida los

sistemas que daban cobertura a la transferencia de datos personales desde la UE a EEUU, conocidos como *Safe Harbour* (2015) y *Privacy Shield* (2020)- el TJUE sostiene que la comunicación de los datos personales debe contar con el consentimiento del afectado o tener un fundamento legalmente previsto (art. 8 CDFUE), y que cualquier normativa que autorice el acceso *generalizado* a los datos personales sin establecer ninguna salvaguarda vulnera el contenido esencial del derecho a la vida privada y familiar (art. 7 CDFUE) (Fuentes Máiquez, 2020).

Finalmente, también en el ámbito de la jurisprudencia constitucional española debe destacarse algún pronunciamiento. En concreto la STC 76/2019, que declaró inconstitucional la habilitación legal que permitía a los partidos la elaboración de perfiles políticos de los ciudadanos para personalizar los mensajes de propaganda. Fue el Defensor del pueblo quien interpuso el recurso de inconstitucionalidad contra el nuevo artículo 58 bis de la Ley Orgánica del Régimen Electoral General (LOREG), introducido -precisamente- por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. El Tribunal Constitucional consideró, en efecto, que ese artículo que posibilitaba el *profiling* político era lesivo del derecho a la protección de datos del artículo 18.4 CE.

7. BIBLIOGRAFÍA

AEPD - ISMS Forum (eds.), Aced, Emilio *et al.* (coords.) (2017), *Código de buenas prácticas en protección de datos para proyectos de Big Data*, AEPD e ISMS Forum, Madrid.

Arellano Toledo, Wilma, (2019), "El derecho a la transparencia algorítimica en *big data* e inteligencia artificial", en: *Revista General de Derecho Administrativo*, 50, 1-28.

Baylos Grau, Antonio (2021), "El algoritmo no es neutral. No permite ejercer derechos fundamentales a los trabajadores de plataformas", en: *Blog de Antonio Baylos*, disponible en línea: https://baylos.blogspot.com/2021/01/el-algoritmo-no-es-neutral-no-permite.html (última consulta: 2 de marzo de 2022).

Castellanos Claramunt, Jorge, y Montero Caro, María Dolores (2020), "Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales", en: *Ius et Scientia*, 6, 2, 72-82.

Cotino Hueso, Lorenzo (2017), "*Big data* e inteligencia artificial, una aproximación a su tratamiento jurídico desde los derechos fundamentales", en: *Dilemata*, 24, 131-150.

— (2019), "Riesgos e impactos del *big data*, la inteligencia artificial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho", en: *Revista General de Derecho Administrativo*, 50, 1-37.

Eguíluz Castañeira, Josu Andoni (2020), "Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales", en: *Estudios de Deusto*, 68, 2, 325-368.

Fuentes Maíquez, Antonio (2020), "Comentario de la STJUE de 16 de Julio de 2020, C-311/18 (Schrems II)", en: *Icade: Revista de la Facultad de Derecho*, 110, 1-10.

García Mahamud, Rosario (2015), "Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español", en: *Teoría y Realidad Constitucional*, 35, 309-338.

Gil González, Elena, 2016, *Big data, privacidad y protección de datos*, Agencia Estatal de Protección de Datos-Boletín Oficial del Estado, Madrid.

Han, Byung-Chul (2014), *Psicopolítica, Neoliberalismo y nuevas técnicas de poder*, Herder, Barcelona.

Martínez, Ricard (2014): "Ética y privacidad de los datos", en: *Big Data: de la investigación científica a la gestión empresarial* (jornadas), Fundación Ramón Areces, 3 de julio de 2014, disponible en línea: http://sgfm.elcorteingles.es/SGFM/FRA/recursos/conferencias/ppt/1776180509_1472014102438.docx (22/2/2022).

Medina Guerrero, Manuel (2021), "De algoritmos y otras palabras inquietantes", en: *Blog de Asociación de Constitucionalistas de España*, disponible en línea: https://www.acoes.es/de-algoritmos-y-otras-palabras-inquietantes/ (1/3/2022).

Morales Barceló, Judith (2017), "Big Data y Protección de Datos: especial referencia al consentimiento del afectado", en: *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 44, 137-164.

Moreno Muñoz, Miguel (2017), "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", en: *Dilemata*, 24, 1-23.

Oliver Lalana, Daniel y Muñoz Soro, José Félix (2014): "El mito del consentimiento, o por qué un sistema individualista de protección de datos (ya) no sirve para (casi) nada", en: Valero Torrijos, Julián (coord.), *La protección de los datos personales en Internet ante la innovación tecnológica*, Aranzadi, Cizur Menor, 153-196.

Sancho López, Marina (2019), "Estrategias legales para garantizar los derechos fundamentales frente a los desafíos del *big data*", en: *Revista General de Derecho Administrativo*, 50, 1-28.

Thetechnolawgist (2020), "Derechos humanos en un mundo de algoritmos. La sentencia histórica que ata en corto la implantación de modelos opacos", en el portal *Thetechnolawgist.com*, disponible en línea: https://www.thetechnolawgist.com/2020/02/12/derechos-humanos-en-un-mundo-de-algoritmos-la-sentencia-historica-que-ata-en-corto-la-implantacion-de-modelos-opacos/ (última consulta: 3 de marzo de 2022).

Zuiderveen Borgesius, Frederik (2018), *Discrimination, artificial intelligence, and algorithmic decision-making*, Consejo de Europa, Estrasburgo.