Revista de Derecho Público: Teoría y Método
Marcial Pons Ediciones Jurídicas y Sociales
Vol. 3 | 2021 pp. 85-127
Madrid, 2021
DOI:10.37417/RPD/vol_1_2021_535

ISSN: 2695-7191
Recibido: 04/01/2021 | Aceptado: 03/03/2021

DECISIONES AUTOMATIZADAS: PROBLEMAS Y SOLUCIONES JURÍDICAS. MÁS ALLÁ DE LA PROTECCIÓN DE DATOS

AUTOMATED DECISIONS: LEGAL PROBLEMS AND SOLUTIONS. BEYOND DATA PROTECTION

Alba Soriano Arnanz*

RESUMEN: La creciente capacidad computacional de los sistemas automatizados de procesamiento de datos ha generado un aumento de su utilización en toda clase de actividades humanas. Estos sistemas pueden procesar cantidades masivas de datos y proporcionar resultados muy precisos, ayudando a los responsables de la toma de decisiones, tanto en el sector público como en el privado, a clasificar a los seres humanos y a predecir sus acciones. Sin embargo, en los últimos años se ha venido demostrando que estos sistemas pueden generar importantes riesgos para los derechos fundamentales y otros valores y principios democráticos. Hasta la fecha, las normas en materia de protección de datos han constituido el principal instrumento jurídico encargado de hacer frente a los riesgos y daños causados por el tratamiento automatizado de datos personales. El presente trabajo identifica los principales riesgos generados por el uso de sistemas algorítmicos, señala las deficiencias del marco jurídico en materia de protección de datos a estos efectos y pone de manifiesto la necesidad de una mayor intervención regulatoria en la utilización pública y privada de los sistemas automatizados de procesamiento de datos y toma de decisiones. También se formulan

---

* Este trabajó se finalizó el 8 de febrero de 2021.

Me gustaría agradecer las aportaciones y ayuda prestada en la elaboración de este trabajo por parte de Andrés Boix Palop, Gabriel Doménech Pascual y Clàudia Gimeno Fernández.

Investigadora en formación, Universitat de València. Este trabajo se ha desarrollado dentro de la SHINE Jean Monnet Network (Sharing Economy and Inequalities across Europe) donde varias universidades europeas, coordinadas por la Universitat de València, están estudiando estas cuestiones con el apoyo de la Comisión Europea (611585-EPP-1-2019-1-ES-EPPJMO-NETWORK).

una serie de breves propuestas que, de aplicarse, deberían contribuir a superar algunos de las insuficiencias del actual marco normativo en la prevención, gestión y solución de los riesgos y daños causados por los algoritmos.

PALABRAS CLAVE: algoritmos; automatización; tratamiento de datos; protección de datos; riesgos tecnológicos.

ABSTRACT: The growing implementation of algorithmic systems in all kinds of human activities is the result of their increasing computational capacity. These systems can process massive amounts of data and provide very accurate results that help decision-makers in both the public and private sector to classify humans and predict their actions. However, algorithms, and the actors that use them, are also increasingly producing significant harms to the fundamental rights of individuals and democratic principles and values. To date, informational privacy (data protection) regulatory frameworks, have been the main legal instruments tasked with protecting against the wide array of risks and harms caused by the automated processing of personal data. This paper maps the main hazards caused by algorithmic systems and aims to prove the shortcomings of the data protection framework in order to justify further regulatory intervention in the public and private use of automated systems. It also draws a series of brief proposals that, were they to be implemented, should help to overcome some of the ineffective aspects of the current regulatory framework when dealing with the risks and harms caused by algorithms.

KEYWORDS: algorithms; automatization; data processing; data protection; technological risks.

INTRODUCCIÓN

Un algoritmo es una secuencia de instrucciones que, contenida en un programa informático, puede realizar procesos similares a los llevados a cabo por seres humanos[1]. Estos programas pueden emplearse para la realización de tareas sencillas, como contar el número de personas matriculadas en un curso, o para la realización de tareas altamente complejas, como puede ser calcular el riesgo de reincidencia de las personas condenadas por distintas clases de delitos. Estos programas informáticos son en ocasiones denominados "modelos" porque representan un aspecto de la realidad —por ejemplo, un programa empleado para contar las personas matriculadas en un curso constituye una representación (o modelo) de un ser humano realizando la acción de contar—.

El uso de programas informáticos de procesamiento de datos en los procesos de toma de decisiones públicas y privadas no es un fenómeno nuevo. Desde hace años, las Administraciones públicas emplean sistemas automatizados sencillos para cruzar la información contenida en diferentes bases de datos[2]. También en el ámbito privado se han venido utilizando programas informáticos para la selección de personal o la concesión de préstamos[3].

Lo que sí es una novedad es la creciente capacidad computacional que tienen estos sistemas, así como su uso, cada vez más común, en la toma de decisiones, incluyendo la creación de perfiles[4], tanto en el ámbito público como en el ámbito privado. Es esta creciente capacidad computacional la que permite que se empleen programas informáticos con propósitos como el de predecir el riesgo de reincidencia de una persona condenada, evaluar la capacidad crediticia de un individuo o crear perfiles que ayuden a determinar qué clase de publicidad debe mostrársele a una usuaria de

---

[1] A lo largo del presente trabajo se emplearán, de manera indistinta, los términos o expresiones indicados a continuación para referirse a las tecnologías empleadas en la automatización de los procesos de toma de decisiones y creación de perfiles: "algoritmo", "tecnologías de procesamiento de datos", "sistema", "sistema automatizado", "programa" o "programa informático".

[2] Como trabajo esencial y pionero en la determinación del régimen jurídico de la actuación administrativa automatizada en España cabe hacer referencia a Isaac Martín Delgado, "Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada", *Revista de Administración Pública*, núm. 180, 2009, pp. 353-386.

[3] Roger Parloff, "Why deep learning is suddenly changing your life", *Fortune*, 28 de septiembre 2016. Disponible el 2 de diciembre de 2020 en *http://fortune.com/;* Marlies Van Eck, "Algorithms in public administration", 31 de enero de 2017. Disponible el 2 de diciembre de 2020 en *https://marliesvaneck.wordpress.com/*; Stella Lowry y Gordon Macpherson, "A blot on the profession", *British Medical Journal*, 5 de marzo de 1988, pp. 657-658.

[4] Así, el artículo 22 del Reglamento General de Protección de Datos (RGPD) reconoce 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". Es decir, considera la elaboración de perfiles como una forma más de tomar decisiones basadas en tratamiento automatizado.

una red social[5]. En estos casos, hablamos de algoritmos o programas con cierta autonomía, pues los resultados no vienen predeterminados por las personas encargadas de diseñarlos, sino que estas se limitan a alimentar los programas con grandes cantidades de datos para entrenarlos, proporcionándoles una serie de instrucciones más o menos extensas pero que, en todo caso, dejan un margen de apreciación al propio sistema.

Así, podemos establecer una distinción entre los sistemas clásicos, que denominaremos automáticos, y los sistemas más novedosos, a los que nos referiremos como sistemas de autonomía decisional o autónomos. Esta distinción puede ilustrarse a través del paralelismo que las dos clases de sistemas citados tienen con las potestades regladas y discrecionales de las Administraciones públicas[6]. Los sistemas automáticos son aquellos que establecen un resultado predeterminado frente al supuesto de hecho. Como en el caso de las potestades regladas, existirá un único resultado posible (consecuencia jurídica válida) frente a cada supuesto de hecho. En cambio, los sistemas de autonomía decisional valorarán el supuesto de hecho concreto en función de lo que han ido aprendiendo e irán ajustando los resultados a medida que cambie el contexto y que obtengan *feedback* sobre las decisiones previamente adoptadas. No existirá un único resultado posible frente al supuesto de hecho, sino que el algoritmo irá determinando, en cada caso, cual es la consecuencia más adecuada.

Este último tipo de algoritmos es el que, en la actualidad, genera mayores problemas para el Derecho y el que ha despertado el interés de una importante parte de la doctrina jurídica por los riesgos que entraña para los valores y principios sobre los que se asientan los Estados democráticos y los derechos fundamentales de la ciudadanía. En todo caso, y aunque el presente trabajo se centra en el uso de algoritmos con autonomía decisional, es importante no menospreciar la incidencia y efectos que los algoritmos de funcionamiento automático pueden también tener en la esfera jurídica de las personas.

El presente trabajo se ocupa, en primer lugar, de identificar los principales problemas y riesgos generados por los sistemas automatizados de toma de decisiones. A continuación, se establecen las razones por las que la normativa en materia de protección de datos constituye, hasta la fecha, el instrumento jurídico principal dirigido a lidiar con los diferentes problemas derivados del uso de algoritmos. Una vez determinada esta cuestión, se procede a examinar la estructura del marco jurídico europeo de protección de datos y a señalar sus límites y deficiencias en la protección frente a los muchos y diversos riesgos derivados del uso de algoritmos. Finalmente, se realizan

---

[5] M.ª Dolores Mas Badía, "Credit-based insurance scores: some observations in the light of the european general data protection regulation", *Cuadernos Europeos de Deusto*, núm. 62, 2020, pp. 155-186; Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin Books, Londres, 2017.

[6] Sobre potestades regladas y discrecionales ver, por ejemplo, Eduardo García De Enterría y Tomás-Ramón Fernández Rodríguez, *Curso de Derecho Administrativo I*, Thomson Reuters – Aranzadi, Cizur Menor (Navarra), 2020, pp. 496-500; y José Esteve Pardo, *Lecciones de Derecho Administrativo*, 6.ª ed. Marcial Pons, Barcelona, 2016, pp. 103-104.

algunas propuestas para una regulación más completa y adecuada del uso de sistemas automatizados de procesamiento de datos y toma de decisiones.

1. PROBLEMAS DERIVADOS DEL CRECIENTE USO DE SISTEMAS ALGORÍTMICOS

Esta sección se ocupa de identificar los principales problemas y riesgos derivados del creciente uso de sistemas algorítmicos tanto por actores públicos como por actores privados. Se identifican tres clases principales de problemas: i) los que afectan, sobre todo, a las personas sometidas a procesos automatizados de toma de decisiones; ii) los fallos de mercado que contribuyen a justificar la intervención en el uso privado de sistemas algorítmicos y iii) las rupturas que la creciente utilización de algoritmos por las Administraciones públicas provoca con las normas y requisitos específicamente aplicables y exigibles a estas.

1.1. Riesgos para la protección de los derechos de las personas sometidas a procesos automatizados de toma de decisiones

Las próximas páginas se ocupan de determinar los posibles efectos negativos que los procesos automatizados de toma de decisiones pueden tener sobre las personas afectadas por ellos. Nos encontramos con algoritmos que contienen sesgos, que cometen errores, que producen resultados discriminatorios o que son empleados para manipular a las personas, entre otras cuestiones. Además, en el último epígrafe de esta sección se aborda la forma en que la opacidad algorítmica, la falta de reconocimiento de un "proceso justo tecnológico"[7] y la dificultad de determinar quiénes son las personas responsables del procesamiento pueden contribuir a exacerbar los daños causados a las personas afectadas por los procesos de toma de decisiones automatizadas y menoscabar sus derechos.

1.1.1. Sesgos y errores

La toma de decisiones llevada a cabo por seres humanos no es objetiva. Cuando los seres humanos decidimos, tendemos a hacerlo basándonos en información parcial y atajos mentales denominados "heurísticas"[8]. Por ejemplo, si nos preguntan si es más probable que una persona definida como "tímida" desarrolle su actividad profesional como bibliotecaria o como comercial, generalmente daremos como res-

[7] Danielle Citron, "Technological due process", *Washington University Law Review*, vol. 85, núm. 6, 2008, pp. 1249-1313.

[8] Amos Tversky y Daniel Kahneman, "Judgment under uncertainty: heuristics and biases", *Science*, vol. 147, núm. 4157, 1974, pp. 1124-1131.

puesta la primera. Esta respuesta no se basa necesariamente en la realidad sino en estereotipos que son comúnmente compartidos y aceptados. Si bien el uso de estos atajos o heurísticas puede ser eficaz, también puede propiciar decisiones basadas en información parcial y, por tanto, puede generar sesgos cognitivos[9].

Los sistemas automatizados de toma de decisiones se alimentan de enormes cantidades de información (inasumibles para un ser humano) relativas al fenómeno que debe ser procesado y analizado por la máquina. Estos programas tienden, por tanto, a ofrecer resultados más objetivos y precisos que los obtenidos cuando es una persona la encargada de tomar una decisión[10]. Asimismo, dada su gran capacidad computacional, estos sistemas son capaces de producir resultados (decisiones) de manera mucho más rápida, generando así un significativo aumento de la eficiencia de todos aquellos procesos en los que son empleados[11].

Sin embargo, a pesar de que las decisiones tomadas por sistemas automatizados suelen ser más precisas que las decisiones tomadas por seres humanos en contextos similares, estos programas también pueden arrojar resultados erróneos o sesgados. Las máquinas fallan. Pueden producirse errores de todo tipo derivados, por ejemplo, de la forma en que el sistema fue programado, que hagan que el programa no realice correctamente la tarea que tiene asignada. Estos errores pueden darse incluso en aquellos casos en los que el algoritmo es empleado para analizar fenómenos fácilmente medibles, como puede ser la cantidad de un determinado compuesto químico en un producto.

En segundo lugar, ya en el ámbito que nos ocupa y preocupa, cuando un sistema automatizado es empleado para analizar y tomar decisiones sobre la realidad social, es mucho más fácil que estas no sean correctas o estén basadas en información sesgada. Aunque los algoritmos son capaces de procesar enormes cantidades de datos, es muy difícil operacionalizar todos los aspectos relevantes de una realidad social, es decir, convertirlos en variables medibles. Es más, en la operacionalización de los diferentes elementos que pueden considerarse relevantes, las personas encargadas de la programación pueden obviar algunas variables, introducir sesgos en el sistema o escoger bases de datos que ofrecen una representación parcial de la realidad. Asimismo, los seres humanos tienen la capacidad de apreciar determinados elementos intangibles que no son captados por los sistemas automatizados[12].

---

[9] *Idem*, p. 1131.

[10] Alexandra Chouldechova, "Fair prediction with disparate impact: a study of bias in recidivism prediction instruments", 2016, pp. 1-17 (p. 5), disponible el 6 de diciembre de 2020 en *https://arxiv.org/;* Alex P. Miller, "Want less-biased decisions? Use algorithms", *Harvard Business Review*, 26 de Julio de 2018, disponible el 6 de diciembre de 2020 en *https://hbr.org*.

[11] Cary Coglianese y David Lehr, "Regulating by robot: administrative decision making in the machine-learning era", *The Georgetown Law Journal*, vol. 105, núm. 5, 2017, pp. 1147-1223 (p.1162); Cathy O'neil, *Weapons of Math Destruction…*, *cit.*, 2017, p. 70.

[12] En este sentido, resultan especialmente relevantes e interesantes las reflexiones acerca de la falta de empatía de la inteligencia artificial realizadas por el profesor Juli Ponce en: Juli Ponce Solé, "Inteli-

También es importante tener en cuenta que las conclusiones alcanzadas por estos sistemas se basan en correlaciones (las personas que compran freidoras suelen tener malos hábitos alimenticios) y no en causalidad (la compra de una freidora provoca malos hábitos alimenticios)[13]. Los grandes volúmenes de datos de que se dispone actualmente y la capacidad de los sistemas automatizados para procesar dicha información hacen que las decisiones tomadas por los algoritmos basados en correlaciones se consideren suficientemente fiables aunque no exista una prueba de causalidad. Por consiguiente, los resultados finales se basan en correlaciones, pero se tratan como relaciones causales, generándose así el riesgo de que se produzcan inferencias erróneas[14]. Volviendo al ejemplo de antes, es probable que exista una correlación entre las compras de freidoras realizadas por internet y malos hábitos alimenticios. Sin embargo, puede ser que, en un caso concreto, una persona compre una freidora como regalo. Si esta información llega a los algoritmos empleados por su seguro médico, que desconocerán el propósito con el cual se ha comprado la freidora, este dato podría contribuir a aumentar la prima de seguro de esa persona[15].

En general, hay una gran cantidad de posibilidades de que se produzcan errores o se introduzcan sesgos durante el desarrollo de los sistemas algorítmicos e incluso tras su puesta en funcionamiento. Es por ello que esa "mayor objetividad" de los algoritmos debe cuestionarse y deben diseñarse e implementarse mecanismos de control jurídico e informático que traten de prevenir y lidiar con los errores y sesgos producidos por los procesos de toma de decisiones automatizadas.

1.1.2. Discriminación

No solo existe una justificada preocupación por los errores y sesgos que pueden generar los sistemas automatizados de toma de decisiones sino que, en los últimos años, también se han detectado múltiples casos en los que el uso de estos sistemas produce resultados especialmente perjudiciales para las personas pertenecientes a grupos vulnerables o históricamente desaventajados, habiéndose demostrado la especial incidencia que el uso de algoritmos tiene en la perpetuación de las estructuras sociales de desigualdad y subordiscriminación[16].

Desde una perspectiva jurídica, la discriminación puede definirse como la acción de tratar a una persona física o jurídica o a un grupo de personas de manera me-

---

gencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", *Revista General de Derecho Administrativo*, núm. 50, 2019, pp. 1-52.

[13] Brendt Mittelstadt *et al.*, "The ethics of algorithms: mapping the debate", *Big Data & Society*, julio-diciembre de 2016, pp. 1-21 (p. 5).

[14] Solon Barocas, "Data mining and the discourse on discrimination", *Proceedings of the Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining (KDD)*, 2014, pp. 1-4 (p. 2).

[15] Steve Lohr, "Sizing up big data, broadening beyond the Internet", *The New York Times BITS Blog*, 29 de junio de 2013, disponible el 6 de diciembre de 2020 en *https://bits.blogs.nytimes.com/*.

[16] Alba Soriano Arnanz, "Decisiones automatizadas y discriminación: aproximación y propuestas generales", *Revista General de Derecho Administrativo*, núm. 56, 2021.

nos favorable que a otras personas que se encuentran en una situación comparable. Por consiguiente, la discriminación puede producirse en una amplia variedad de contextos y situaciones. Sin embargo, ciertas acciones discriminatorias reciben una consideración específica, como especialmente perjudiciales, por los Estados democráticos y los instrumentos internacionales de derechos humanos. Se trata de casos de discriminación que se producen por categorías o motivos que son *a priori* "sospechosos", como la raza o el sexo. La razón de establecer estas categorías especialmente protegidas es que es inaceptable basar las decisiones en motivos (características) que son, en principio, inmutables (como la raza o el sexo) o que pertenecen a la esfera de la autonomía del individuo (como la religión y las opiniones políticas), sobre todo cuando dichas características no son relevantes en el contexto en el que se adopta la decisión [17].

Dentro de cada categoría protegida existen ciertas subcategorías que identifican a las personas pertenecientes a grupos considerados especialmente vulnerables o que han sufrido una situación histórica de opresión o desventaja, como las poblaciones no blancas, las mujeres o las personas procedentes de entornos socioeconómicos con menor poder adquisitivo. Las personas pertenecientes a estos grupos siguen siendo objeto de un trato discriminatorio como resultado de los estereotipos y prejuicios que se tienen contra ellas y de las normas e instituciones sociales que se han construido desde la perspectiva de y para quienes han ocupado tradicionalmente posiciones de poder.

Los algoritmos son diseñados por seres humanos que, de manera voluntaria o involuntaria, pueden introducir en los sistemas que programan los prejuicios y estereotipos que tienen sobre determinados grupos sociales. Una de las razones que se ha apuntado como causante de la incorporación de estos sesgos a los sistemas automatizados de toma de decisiones es la composición, en gran medida homogénea, de los equipos de personas que programan estos sistemas, ya que normalmente estamos hablando de hombres blancos heterosexuales, que proceden de entornos socioeconómicos acomodados [18] y que, en algunos casos, han llegado a apoyar, de manera pública, determinados discursos que perpetúan la idea de que las personas pertenecientes a grupos históricamente discriminados son "inferiores" [19].

Asimismo, puesto que los sistemas automatizados de toma de decisiones procesan la realidad social, y esta está construida sobre estructuras que discriminan a las perso-

---

[17] Janneke Gerards, "The discrimination grounds of article 14 of the European Convention on Human Rights", *Human Rights Law Review*, vol. 13, núm. 1, 2013, pp. 99-124 (p. 114).

[18] Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York University Press, New York, 2018, p. 80.

[19] *Idem*, p. 2: "en medio de una investigación federal sobre la supuesta persistente brecha salarial de Google, en la que las mujeres reciben sistemáticamente menos sueldo que los hombres en la plantilla de la empresa, en agosto de 2017 se hizo viral un manifiesto 'anti diversidad' escrito por James Damore, apoyado por muchos empleados de Google, en el que se argumentaba que las mujeres son psicológicamente inferiores e incapaces de ser tan buenas en la ingeniería de software como los hombres, entre otras afirmaciones patentemente falsas y sexistas" (traducción propia).

nas pertenecientes a grupos desaventajados, los algoritmos incorporan, reproducen y perpetúan estas estructuras de discriminación[20].

Durante los últimos años han salido a la luz numerosos casos en los que el uso de sistemas automatizados en ámbitos como la selección de personal, la determinación de la capacidad crediticia o en la prestación de servicios públicos y adjudicación de ayudas, ha generado situaciones de discriminación que han perjudicado a las personas pertenecientes a grupos desaventajados o especialmente vulnerables[21]. La aparente objetividad de estos sistemas no puede hacernos obviar que estos son creados y se desarrollan en un contexto social asentado sobre unas estructuras de desigualdad que los algoritmos pueden fácilmente incorporar y ayudar a reproducir y perpetuar.

1.1.3. Riesgos para la singularidad, autonomía e intimidad de los individuos

Aunque los sistemas automatizados de toma de decisiones son capaces de crear perfiles muy precisos, estos perfiles son creados considerando la pertenencia de la persona a diferentes grupos. Es decir, no se consideran las especificidades y singularidad propias de cada uno de los seres humanos que el sistema analiza, sino que la representación virtual de cada persona es el producto de su posición con respecto a otros individuos. Esto puede conducir a la toma de decisiones erróneas ya que, lo que es verdad para el grupo, no tiene por qué serlo necesariamente para una persona en concreto[22].

Estos sistemas también pueden aprender o ser diseñados para manipular a los seres humanos, limitando su autonomía de la voluntad a la hora de tomar decisiones[23]. Por ejemplo, los algoritmos empleados en el contexto de la publicidad dirigida pueden ser creados con el objetivo de atraer consumidoras y usuarias en situación de vulnerabilidad hacia el consumo de productos de baja calidad o que pueden resultarles perjudicales. Si bien esto es algo que se lleva haciendo desde hace ya mucho tiempo en el ámbito de la publicidad (piénsese, por ejemplo, en el caso de los anuncios de préstamos con cláusulas que rozan o son directamente abusivas o de casas de apuestas), lo que resulta especialmente preocupante en el contexto que nos ocupa, es la creciente

---

[20] Solon Barocas y Andrew Selbst, "Big data's disparate impact", *California Law Review*, vol. 104, núm. 3, 2016, pp. 671-732.

[21] Doris Allhutter, *et al.*, "Algorithmic profiling of job seekers in Austria: how austerity politics are made effective", *Frontiers in Big Data*, vol. 3, 2020, pp. 1-17; Stephanie Bornstein, "Antidiscriminatory algorithms", *Alabama Law Review*, vol. 70, núm. 2, 2019, pp. 519-572; Safiya Noble, *Algorithms of Oppression*, *cit.*, 2018; Sofia Ranchordás y Ymre Schuurmans, "Outsourcing the welfare state: the role of private actors in welfare fraud investigations", *European Journal of Comparative Law and Governance*, vol. 7, núm. 2, 2020, pp. 5-42.

[22] Tal Zarsky, "Transparent predictions", *University of Illinois Law Review*, vol. 2013, núm. 4, 2013, pp. 1503-1570 (pp. 1560-1561).

[23] Juli Ponce Solé, "El derecho a una buena administración y la personalización de los servicios públicos" en Beltrán Puentes Cociña y Andrei Quintiá Pastrana, (dirs.), *El Derecho ante la Transformación Digital*, Barcelona, Atelier, 2019, pp. 51-71 (p. 68).

capacidad de que se dispone para configurar y hacer llegar esta publicidad de manera altamente personalizada exactamente a aquellas personas que son especialmente vulnerables y susceptibles de ser manipuladas y de contratar esta clase de productos[24].

Por último, como se verá más adelante, los daños más evidentes producidos por las tecnologías de procesamiento de datos son los que se generan en el ámbito de la intimidad o privacidad de las personas. Es más, en no pocas situaciones, la invasión en el ámbito de la intimidad de una persona que tiene lugar cuando se recogen y procesan sus datos ocurre sin que aquella comprenda ni consienta plenamente dichas acciones ni los fines para los que se llevan a cabo.

1.1.4. Transparencia, proceso justo y atribución de la responsabilidad

Los próximos párrafos se refieren, brevemente, a aquellos elementos que contribuyen a intensificar los riesgos y daños generados a los seres humanos cuando son sometidos a procesos automatizados de toma de decisiones al dificultar el acceso y comprensión de los sistemas empleados, la posibilidad de recurrir las decisiones y los obstáculos que pueden encontrarse al tratar de concretar quiénes son las personas físicas responsables del procedimiento.

Uno de los elementos más problemáticos de los sistemas automatizados de toma de decisiones es su falta de transparencia. Esta se refleja, en primer lugar, en la propia utilización de estos sistemas. No son pocas las ocasiones en que una persona que está siendo analizada por uno de estos sistemas no es consciente de que dicho procesamiento está siendo efectuado[25]. En segundo lugar, el aspecto que ha sido principalmente abordado por la doctrina es la falta de transparencia de los propios algoritmos, ya sea porque el código fuente no se hace público o porque el sistema es tan complejo que comprenderlo resulta imposible[26]. La falta de transparencia de los sistemas algorítmicos dificulta el control general de legalidad de los programas empleados en la toma de decisiones automatizadas y limita la posibilidad que los individuos afectados tienen de impugnar los resultados obtenidos. Resulta altamente complejo argumentar que una decisión es errónea si se desconoce su lógica subyacente.

La opacidad que caracteriza a muchos de los algoritmos que están siendo empleados de manera creciente en toda clase de contextos no es el único elemento que dificulta el acceso de las personas afectadas a un "proceso justo tecnológico"[27]. En general, existe una patente falta de implementación de mecanismos y procedimientos

---

[24] Cathy O'Neil, *Weapons of Math Destruction…*, *cit.*, 2017, p. 70; Karen Yeung, "'Hypernudge': Big data as a mode of regulation by design", *Information, Communication & Society*, vol. 20, núm. 1, 2017, pp. 118-136.

[25] Solon Barocas y Andrew Selbst, "The intuitive appeal of explainable machines", *Fordham Law Review*, vol. 87, núm. 3, 2018, pp. 1085-1139 (pp. 1091-1092).

[26] Jenna Burrell, "How the machine 'thinks': understanding opacity in machine learning algorithms", *Big Data & Society*, vol. 3, núm. 1, 2016, pp. 1-12 (p. 5).

[27] Danielle Citron, "Technological due process", *cit.*, 2008, pp. 1249-1313.

que, de manera sencilla, permitan a los individuos afectados por procesos de toma de decisiones automatizadas defender sus derechos e intereses[28].

Cabe también añadir, en el contexto de la transparencia algorítmica y el proceso justo tecnológico que, incluso cuando se ofrece una suerte de explicación, puede ser que esta no sea intuitiva. En tales casos nos encontramos ante un importante dilema. Puesto que los algoritmos son capaces de procesar enormes cantidades de información, es posible que obtengan resultados basados en lógicas difíciles de comprender. Es decir, que carezcan de la motivación suficiente por ser el producto de correlaciones inesperadas[29]. Así, un algoritmo puede llegar a la conclusión de que existe una correlación entre realizar compras de calcetines de personajes de dibujos animados por internet e incumplir las condiciones de devolución de un préstamo. En estos casos, resulta importante determinar si se debe priorizar la eficiencia y supuesta mayor precisión del sistema sobre los elementos que tradicionalmente se valoran para determinar que una decisión se encuentra debidamente justificada y es conforme a la legalidad.

Como último elemento a mencionar en relación con la necesaria construcción de mecanismos que garanticen un proceso justo tecnológico, cabe destacar la dificultad en la atribución de la responsabilidad por algunas de las decisiones tomadas por sistemas automatizados. Si hablamos de sistemas automáticos, en los que el resultado se encuentra totalmente predeterminado, no existen grandes problemas en determinar quién es el ser humano responsable. Sin embargo, en el caso de los sistemas autónomos, cuya programación inicial va evolucionando a medida que se van retroalimentando de los efectos de las decisiones que han tomado y de la realidad en la que operan, resulta mucho más difícil atribuir la responsabilidad a un ser humano en concreto[30]. Esta cuestión ha sido en parte resuelta por el Reglamento General de Protección de Datos (RGPD)[31] que establece, de manera lo suficientemente clara, la atribución de responsabilidad en relación con las cuestiones derivadas del procesamiento a los responsables[32] y encargados del tratamiento de datos[33]. Sin embargo,

---

[28] Cathy O' Neil, *Weapons of Math Destruction…*, *cit.*, pp. 3-11; Margot KAMINSKI, "Binary governance: Lessons from the GDPR's approach to algorithmic accountability", *Southern California Law Review*, vol. 92, núm. 6, 2019, pp. 1529-1616 (pp. 1538-1539).

[29] Solon Barocas y Andrew Selbst, "The intuitive appeal of explainable machines", *cit.*, 2018, pp. 1085-1139 (p. 1091); Kriel Brennan-Marquez, "'Plausible cause': explanatory standards in the age of powerful machines", *Vanderbilt Law Review*, vol. 17, núm. 4, 2017, pp. 1249-1301 (p. 1288).

[30] Brendt Mittelstadt *et al.*, "The ethics of algorithms…", *cit.*, 2016, pp. 1-21 (p. 6).

[31] 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.

[32] Art. 4.7 RGPD: «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

[33] Art. 4.8 RGPD: «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

en aquellos casos en los que tanto los causantes como las víctimas de los daños no sean fácilmente identificables o no se puedan concretar, la efectividad de este sistema resulta dudosa.

1.2. Fallos de mercado e intervención en el sector privado

Hasta el momento se ha mostrado cómo el uso de sistemas automatizados puede provocar importantes daños a los derechos fundamentales de las personas. Para dar cumplimiento a las obligaciones positivas que los Estados tienen en relación con la protección de los derechos fundamentales[34], estos deben crear normas que protejan frente a los riesgos que el uso de sistemas algorítmicos genera, principalmente, para los derechos a la libertad (autonomía), igualdad, no discriminación, intimidad, protección de datos y un proceso justo. Cabe recordar, por ejemplo, que el art. 9.2 CE establece la obligación de promoción de la igualdad y libertad y la remoción de aquellos obstáculos que impidan su consecución plena.

La intervención en el sector privado viene, asimismo, avalada por el principio de precaución[35] que justifica la imposición de mayores cargas y obligaciones sobre aquellas actividades económicas susceptibles de producir daños sobre los intereses públicos cuya magnitud es desconocida[36]. Si bien el principio de precaución ha venido desarrollándose sobre todo en relación con la protección del medioambiente[37], la propia Comisión Europea ya reconoció en el año 2000 que su ámbito de aplicación era mucho más amplio[38]. Es más, si bien no lo hace de manera directa, la propia Constitución Española prevé la aplicación del principio de precaución a las tecnologías de procesamiento de datos[39] al establecer que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[40].

---

[34] Gabriel Doménech Pascual, *Derechos Fundamentales y Riesgos Tecnológicos*, Centro de Estudios Políticos y Constitucionales, Madrid, 2006, p. 113.

[35] Clara Velasco Rico, "Vigilando al algoritmo. Propuestas organizativas para garantizar la transparencia", en Beltrán Puentes Cociña y Andrei Quintiá Pastrana, (dirs.), *El Derecho ante la Transformación Digital*, Barcelona, Atelier, 2019, pp. 73-89 (pp. 84-86).

[36] Sentencia del Tribunal General de la UE (Sala Tercera) de 11 de septiembre de 2002, C-T-13/99, Pfizer Animal Health SA y Consejo de la UE, párrafos 139, 144 y 147.

[37] Gabriel Doménech Pascual, *Derechos Fundamentales y Riesgos Tecnológicos, cit., 2006, pp. 255-256.*

[38] COMISIÓN EUROPEA, "Comunicación de la Comisión sobre el recurso al principio de precaución", COM/2000/0001 final, 1 de febrero de 2000, párrafo 3: "El principio de precaución no está definido en el Tratado, que sólo lo menciona una vez, para la protección del medio ambiente, pero, en la práctica, su ámbito de aplicación es mucho más vasto".

[39] Andrés Boix Palop, "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones", *Revista de Derecho Público: Teoría y Método*, vol. 1, 2020, pp. 223-270 (p. 239).

[40] Art. 18.4 CE.

A mayor abundamiento, desde una perspectiva económica, el creciente uso de sistemas automatizados de toma de decisiones se da en un contexto en el que se producen significativos fallos de mercado que, de manera breve, se abordan a continuación y que ofrecen un apoyo adicional a los argumentos relativos a la necesidad de intervenir en el sector privado. Estos fallos de mercado se concretan en la generación de externalidades negativas por parte de los actores privados que emplean sistemas automatizados de procesamiento de datos y toma de decisiones, la existencia monopolios digitales, las situaciones de información asimétrica y la irracionalidad en el comportamiento de los individuos a quienes pueden afectar los procesos de toma de decisiones automatizadas.

1.2.1. Externalidades negativas

El procesamiento de datos y toma de decisiones automatizadas por parte de empresas privadas produce resultados nocivos para terceras personas, así como para ciertos intereses públicos y valores compartidos que las democracias occidentales[41] y, en particular, los Estados miembros de la UE deben respetar. Estos resultados nocivos o daños no son internalizados por las empresas que los producen y tampoco pueden ser neutralizados mediante las técnicas propias del Derecho privado, como la responsabilidad contractual o extracontractual. A continuación, se ofrecen algunos ejemplos de estas externalidades negativas que ayudan a acreditar que, para lidiar con los riesgos y daños generados por el uso privado de algoritmos, no es posible recurrir, en exclusiva a soluciones propias del Derecho privado[42].

Resulta relevante volver sobre los daños causados a los derechos a la igualdad y no discriminación que no solo constituyen derechos fundamentales reconocidos a la ciudadanía de los Estados miembros de la UE, sino también principios y mandatos que deben vertebrar toda la actuación de los poderes públicos. La discriminación algorítmica no solo se da a través de tratamientos personalizados, sino también a través de la perpetuación de estereotipos perjudiciales para las personas pertenecientes a grupos especialmente protegidos, causando daños difusos que vulneran los principios y valores básicos sobre los que se asientan los Estados democráticos pero cuyas víctimas no son fácilmente identificables. Por ejemplo, los algoritmos empleados por motores de búsqueda contribuyen a perpetuar estereotipos sobre las minorías étnicas y raciales y sobre las mujeres al ofrecer imágenes sexualizadas de mujeres como resultado a determinadas combinaciones de palabras introducidas en el buscador[43].

La utilización por parte de empresas de sistemas de recogida y procesamiento automatizado de datos también produce otras externalidades negativas con las que el Derecho privado no es capaz de lidiar. Cabe destacar los casos en que ha salido a

---

[41] Omri Ben-Shahar, "Data pollution", *Journal of Legal Analysis*, vol. 11, 2019, pp. 104-159 (pp. 110-118).

[42] *Idem*, p. 115.

[43] Safiya Noble, *Algorithms of Oppression…*, *cit.*, 2018, p. 71.

la luz que las empresas tecnológicas de redes sociales compartían, sin autorización, los datos de sus usuarias y usuarios con terceros[44]. Otro claro supuesto lo constituye la difusión de noticias falsas y puntos de vista que aumentan la polarización de la sociedad y tienen por objeto manipular a las personas y que pueden llegar a reducir la legitimidad de las instituciones y procesos democráticos[45].

La relevancia de estos daños es el resultado de su valor agregado, esto es, del menoscabo a los principios y valores básicos de la democracia. Sin embargo, no resulta sencillo individualizar estos daños. Es más, incluso cuando es posible identificar a las víctimas, el daño individual es de escasa entidad, por lo que no existen incentivos para demandar a los causantes. Asimismo, no siempre es sencillo identificar a los causantes del daño, sobre todo en los supuestos en los que el *software* se encuentra abierto, facilitando la participación de muchas personas no identificadas en su desarrollo.

1.2.2. Monopolios digitales

Las sociedades occidentales se han construido sobre la idea de que el poder público implica coacción (y control) mientras que el desarrollo de actividades privadas es una expresión de la libertad[46]. El grado en que se mantiene esta noción de la dicotomía sector público/privado como regulación vs. libertad varía según la cultura y tradición política e ideológica de cada país, pero, en todo caso, existe un acuerdo general en relación con el reconocimiento de la libertad de actuación de los actores privados y la limitada posibilidad de intervención del poder público en la actividad de aquellos, que únicamente podrá regular el sector privado cuando se generen ciertos riesgos. Por consiguiente, la noción de que las organizaciones del sector privado puedan actuar como reguladores parece, a primera vista, contraintuitiva. Así pues, sugerir que restricciones similares a las impuestas al sector público deberían ser de aplicación también al desarrollo de determinadas actividades privadas puede resultar difícil de aceptar. Sin embargo, el poder adquirido por ciertas organizaciones privadas que actualmente poseen una gran cantidad de capital y, lo que es igual o incluso más importante, de información, hace que dichas organizaciones se comporten como cuasi reguladores[47].

Muchas de las empresas privadas que crean algoritmos y controlan gran parte de los datos del mundo se comportan como monopolios. Empresas como Alphabet (Google), Facebook, Apple o Amazon ocupan un segmento muy importante de los mercados en línea y son los principales recolectores de datos personales, que luego

---

[44] Josh Constine, "Facebook is shutting down its API for giving your friends' data to apps", *TechCrunch*, 28 de abril de 2015. Disponible el 8 de diciembre de 2020 en *https://techcrunch.com*.

[45] Yochai Benkler, Robert Faris y Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford University Press, Oxford, 2018.

[46] Lawrence LESSIG, *Code: Version 2.0*, Basic books, Nueva York, 2006, pp. 5-6.

[47] Nancy Kim y Jeremy Telman, "Internet giants as quasi-governmental actors and the limits of contractual consent", *Missouri Law Review*, vol. 80, núm. 3, 2015, pp. 723-770.

utilizan en beneficio propio o venden a terceros (incluidos los gobiernos). Por ejemplo, Google es el principal motor de búsqueda y proveedor de servicios de publicidad digitales y, de hecho, ha sido multada por la Comisión Europea por prácticas abusivas en el ámbito de la publicidad digital [48]. Además, las cuatro empresas mencionadas están siendo objeto de investigaciones por incumplimiento de las normas de competencia tanto en los Estados Unidos como en la Unión Europea.

Sin embargo, por el momento, los instrumentos contenidos en la normativa en materia de competencia no han logrado reducir el poder monopolístico de estas empresas. En este contexto, el informe y las recomendaciones del sector demócrata del subcomité antimonopolio de la Cámara de Representantes de los Estados Unidos ofrece una visión muy ilustrativa de la necesidad de limitar el poder monopolístico de Alphabet (Google), Facebook, Apple y Amazon y de fortalecer y revitalizar las leyes antimonopolio [49]. Asimismo, recientemente, el Gobierno de los Estados Unidos ha interpuesto una demanda contra Facebook por prácticas monopolísticas y anticompetitivas dirigidas a controlar el mercado de las redes sociales [50].

Estas empresas operan espacios que forman una parte esencial de la vida diaria de muchas personas y, como propietarias de dichos espacios, regulan la manera en que se llevan a cabo muchas interacciones en ellos y toman decisiones que pueden tener un impacto muy significativo en los seres humanos que, directa o indirectamente, interactúan con la máquina [51]. Además, el control que estas empresas ejercen sobre su sector del "ciberespacio" [52], limitando la libre competencia a través del abuso de su posición en el mercado [53], conduce a la creación de arquitecturas de elección que limitan e influyen en gran medida en la autonomía de la voluntad de las personas, restringiendo la capacidad de decisión de estas [54].

Las organizaciones privadas que, como Google, son monopolios efectivos en su segmento de mercado deberían ser objeto de una regulación pública más intensa. El uso de sistemas algorítmicos por parte de estas empresas debería estar sujeto a requisitos similares a los aplicables al sector público y las garantías y protecciones recono-

---

[48] Comisión Europea, "Defensa de la competencia: la Comisión impone una multa a Google de 1,49 miles de millones de euros por prácticas abusivas en la publicidad en línea", 20 de marzo de 2019. Disponible el 8 de diciembre de 2020 en *https://ec.europa.eu*.

[49] Jerrold Nadler y David Cicilline, "Investigation of competition in digital markets", Subcommittee on antitrust, commercial and administrative law of the Committee on the judiciary, octubre 2020.

[50] Cecilia Kang y Mike Isaac, "U.S. and States Say Facebook Illegally Crushed Competition", *New York Times*, 9 de diciembre de 2020. Disponible el 10 de diciembre de 2020 en *https://www.nytimes.com*.

[51] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St Martin's Press, Nueva York, 2017; Safiya NOBLE, *Algorithms of Oppression*…, *cit.*, 2018; Cathy O'neil, *Weapons of Math Destruction*…, *cit.*, 2017.

[52] Lawrence Lessig, *Code: Version 2.0*, *cit.*, 2006, pp. 5-6.

[53] Sobre la figura y prohibición de abuso de la posición dominante en el mercado ver, por ejemplo, Julio Pascual y Vicente, "Prohibiciones del abuso de posición dominante" en *Tratado de Derecho de la competencia*, José María Beneyto Pérez (dir.) y Jerónimo Maillo González (coord.), Bosch, Barcelona, 2005, pp. 455-511.

[54] Karen Yeung, "'Hypernudge'…", *cit.*, 2017, pp. 118-136.

cidas a la ciudadanía contra esta forma de regulación algorítmica también deberían trazarse y estructurarse de manera similar a las otorgadas cuando los particulares interactúan con poderes públicos.

1.2.3. Información asimétrica, comportamientos irracionales y costes de transacción

Las personas no son conscientes ni del tipo de información que realmente proporcionan al interactuar en los espacios digitales ni de los fines para los que se puede utilizar su información, ni tampoco de la medida en que las tecnologías de procesamiento de datos pueden llegar a afectarles y, por ello, perciben que los riesgos de los sistemas de recogida y tratamiento de datos son pequeños e indirectos[55]. En este sentido, los encargados y responsables de la recogida y el tratamiento de datos tienden a ofrecer información parcial, expuesta de manera compleja y que dificulta la comprensión por parte de las personas interesadas.

Es más, aunque cuando son preguntadas sobre estas cuestiones, las ciudadanas y ciudadanos suelen expresar preocupación y una clara preferencia por proteger su intimidad, después no actúan en consecuencia y suelen compartir datos personales con cierta facilidad. Este fenómeno se ha denominado "paradoja de la privacidad"[56] y, en muchas ocasiones, es el resultado de la falta de alternativas a los servicios digitales que exigen a las y los usuarios que compartan sus datos[57].

Sin embargo, en otros casos, es la prioridad que las personas tienden a otorgar a los beneficios a corto plazo[58] del acceso a un servicio digital frente a los riesgos o daños a largo plazo que pueden causarles los datos que proporcionan a cambio de acceder a dicho servicio la que decanta la balanza y hace que no se ponderen suficientemente los perjuicios. Ello es así porque estos daños generalmente se caracterizan por su dispersión y falta de inmediatez, a lo que cabe añadir que, en muchos casos, son el resultado de datos compartidos por terceras personas y no por la propia persona a quien se causa el daño.

También debemos tener en cuenta los costes de transacción generados en torno al acceso a plataformas digitales. Cabe destacar, por ejemplo, el esfuerzo que requiere

---

[55] Mike Annany y Kate Crawford, "Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability", *New Media & Society*, vol. 20, núm. 3, 2018, pp. 973-989 (pp. 979-980).

[56] Spyros Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", *Computers & Security*, vol. 107, 2017, pp. 122-134 (p. 128).

[57] Bert-Jaap Koops, "The problem with European data protection law", *International Data Privacy Law*, vol. 4, núm. 4, 2014, pp. 250-261 (p. 251).

[58] El descuento hiperbólico de los riesgos es un sesgo cognitivo que deriva, entre otras cuestiones, de que los seres humanos tendamos a dar prioridad a los beneficios en el muy corto plazo sin valorar la verdadera entidad de los daños que se puedan dar a largo plazo como contraprestación a esos beneficios a corto plazo. Ariel Rubinstein, "Dilemmas of an economic theorist", *Econometrica*, vol. 74, núm. 4, 2006, pp. 865-883.

leer con atención las condiciones de acceso y uso de una página o aplicación web, así como rechazar una por una todas las opciones de recogida y procesamiento de datos. Como norma general, los individuos no están dispuestos a dedicar su tiempo a leer con atención cada aviso relativo a la protección de datos y suelen aceptar las condiciones de acceso.

1.3. Quiebras en la aplicación de los principios propios de la actuación de las Administraciones públicas

El empleo de sistemas automatizados de toma de decisiones por parte de los poderes públicos genera una serie de problemas específicos que no se dan, o al menos no con tanta intensidad, en el ámbito privado. Las próximas páginas se ocupan, por una parte, de cómo las mayores exigencias de transparencia y justificación de las decisiones públicas afectan al creciente uso de sistemas automatizados y, por otra, de los efectos de la externalización de funciones públicas en sistemas automatizados privados y de la utilización por los poderes públicos de programas diseñados por actores privados.

1.3.1. Transparencia y justificación de las decisiones públicas automatizadas

El establecimiento de mecanismos e instrumentos destinados a eliminar la opacidad algorítmica adquiere especial relevancia cuando se trata de programas que se encargan de la toma de decisiones públicas automatizadas[59], ya que el principio y mandato de transparencia desempeña un papel fundamental en los ordenamientos jurídico-administrativos de los Estados democráticos[60]. Hay varias formas en que la transparencia hace avanzar la democratización de las sociedades. En primer lugar, la transparencia empodera a la ciudadanía en la medida en que proporciona información sobre las acciones y procedimientos realizados por los poderes públicos, permitiendo a ciudadanos y ciudadanas la posibilidad de participar en los procesos de toma de decisiones que puedan interesarles. En segundo lugar, y en estrecha relación con el punto anterior, para que las instituciones públicas rindan cuentas no solo es necesario establecer procedimientos que permitan a los individuos defender sus derechos e intereses, sino también proporcionarles los conocimientos necesarios sobre la forma en que se ha adoptado una decisión que les afecta y que pueden desear impugnar. En tercer lugar, la transparencia también es necesaria para proporcionar a las personas

[59] Angelo Giuseppe Orofino, "The Implementation of the Transparency Principle in the Development of Electronic Administration", *European Review of Digital Administration & Law*, vol. 1, núm. 1-2, 2020, pp. 123-142.

[60] Juan Francisco Mestre Delgado, "Una reflexión sobre la regulación constitucional del Derecho administrativo", *Corts: Anuario de Derecho Parlamentario,* núm. extra 31, 2018, pp. 367-386 (p. 384).

y organizaciones los conocimientos necesarios para impugnar e iniciar debates públicos sobre cualquier acción o decisión adoptada por los poderes públicos y, por lo tanto, para ejercer una supervisión efectiva sobre dichas acciones. Por último, como consecuencia de todo lo anterior, la transparencia ayuda a prevenir que se lleven a cabo conductas ilícitas y proporciona legitimidad a las instituciones públicas. Si la ciudadanía conoce las acciones y decisiones tomadas por los poderes públicos, cómo impugnarlas en caso de que les afecten y se les permite participar en los diferentes procesos de toma de decisiones, aumentará su confianza en el sistema.

Para poner en práctica un sistema eficaz de control y supervisión de los instrumentos algorítmicos son necesarios ciertos niveles de transparencia[61]. Dicha transparencia no debe referirse únicamente al código fuente sino, en ciertos casos, también a dar explicaciones comprensibles. La explicación o justificación de las decisiones públicas es especialmente relevante ya que estas tienen que estar correctamente motivadas, es decir, la actuación de las Administraciones públicas debe someterse a los fines que la justifican[62]. En consecuencia, será necesario garantizar que la toma de decisiones públicas automatizadas es capaz de producir justificaciones aceptables dentro del marco normativo actual. De lo contrario, deberemos aceptar un cambio de paradigma en las exigencias de motivación de los actos administrativos, aceptando explicaciones no intuitivas. En este segundo caso, se deberá garantizar el control de los sistemas automatizados empleados en el ámbito público a través de otra clase de mecanismos[63] que garanticen la protección de los derechos de las personas interesadas en el procedimiento[64], especialmente el ejercicio de potestades discrecionales[65].

1.3.2. La intervención privada en la provisión de servicios y realización de funciones públicas

Hay dos situaciones que se derivan de las interacciones entre sector público y privado en el desarrollo y uso de sistemas algorítmicos que provocan rupturas con las tradicionales formas de ejercicio del poder público.

---

[61] Agustí Cerrillo i Martínez, "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", *Revista General de Derecho Administrativo*, núm. 50, 2019, pp. 1-38 (p. 18).

[62] Art. 106 CE.

[63] Solon Barocas y Andrew Selbst, "The intuitive appeal of explainable machines", *cit.*, 2018, pp. 1085-1139 (p. 1138).

[64] Con respecto a las garantías en el uso de la inteligencia artificial por las Administraciones públicas ver, Julián Valero Torrijos, "The legal guarantees of artificial intelligence in administrative activity: reflections and contributions from the viewpoint of Spanish administrative law and good administration requirements", *European Review of Digital Administration & Law*, vol. 1, No. 1-2, 2020, pp. 55-62.

[65] Agustí Cerrillo i Martínez, "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", *cit.*, 2019, pp. 1-38 (pp. 20-24) y "¿Son fiables las decisiones de las Administraciones públicas adoptadas por algoritmos?", *European Review of Digital Administration & Law*, vol. 1, No. 1-2, 2020, pp. 18-36 (pp. 22-26); Juli Ponce Solé, "Inteligencia artificial, Derecho administrativo y reserva de humanidad…", *cit.*, 2019, pp. 1-52.

En primer lugar, debemos hacer referencia a la externalización de determinadas funciones públicas. Si bien la externalización de funciones públicas no es ninguna novedad, lo que si resulta especialmente preocupante es que la clase de actuaciones que se vienen externalizando a empresas privadas que se dedican al procesamiento de datos automatizado constituyen, en muchos casos, funciones públicas de autoridad que únicamente deben de ser llevadas a cabo por personal funcionario, es decir, funciones inherentemente públicas que corresponden al núcleo mismo del ejercicio de la actividad de los poderes públicos por la confianza y legitimidad democrática en ellos depositada. Por ejemplo, cada vez es más común que las Administraciones públicas contraten los servicios de empresas que emplean sistemas automatizados para detectar casos de fraude entre las personas receptoras de ayudas sociales[66]. Esta realidad es también preocupante por cuanto que la creciente eficiencia (entendida en un sentido y desde una perspectiva puramente económica) ofrecida por la capacidad computacional de los sistemas algorítmicos genera el riesgo de que se pierdan de vista otros objetivos de interés general como puede ser la protección de los segmentos más vulnerables de la población, contribuyendo así a la estigmatización de los colectivos solicitantes de ayudas sociales y a la perpetuación de la desigualdad.

En segundo lugar, los problemas y cuestiones que surgen en relación con el hecho de que los algoritmos empleados por el sector público sean adquiridos generalmente de empresas privadas o se desarrollen junto con ellas. Ello da lugar a un marco totalmente nuevo en la interacción entre las esferas de actividad privada y pública y plantea interrogantes sobre la medida en que esas empresas privadas ejercen potestades administrativas discrecionales e intervienen en las actividades de elaboración de políticas y programas que deberían llevar a cabo las y los representantes de la ciudadanía y el personal funcionario que tienen encomendado el ejercicio de funciones públicas de autoridad. Los instrumentos normativos tradicionales son generales y ambiguos para permitir su adaptación y aplicación a casos particulares. Por el contrario, los algoritmos deben programarse de manera muy específica. Aunque el conjunto de instrucciones que constituye el algoritmo variará una vez que se aplique a casos concretos, el nivel inicial de granularidad que requiere la programación algorítmica, conlleva un grado de precisión en las instrucciones proporcionadas que no se emplea en la creación de normas jurídicas. Esto implica que las personas y empresas que creen los algoritmos estarán interpretando y aplicando los instrumentos jurídicos de una manera muy específica que, en teoría debería corresponder a las y los representantes democráticamente elegidos o al personal funcionario[67].

Las situaciones descritas en los dos párrafos anteriores no serían tan problemáticas si las Administraciones públicas ejerciesen un control efectivo sobre los sistemas algorítmicos adquiridos o empleados por aquellas empresas en las que externalizan

---

[66] Sofia Ranchordás y Ymre Schuurmans, "Outsourcing the welfare state…", *cit.*, 2020, pp. 5-42.

[67] Marion Oswald, "Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power", *Philosophical Transactions of the Royal Society of London*, *Series A: Mathematical and Physical Sciences*, vol. 376, núm. 2128, 2018, pp. 1-20 (pp. 14-15).

sus funciones. Sin embargo, la Administración no dispone de los medios, y también parece carecer de la voluntad, para supervisar y controlar los sistemas automatizados empleados en estos contextos por lo que, en muchas ocasiones, se limita a aceptar su uso de manera acrítica.

Por último, con respecto a la adquisición y utilización por parte de las Administraciones públicas de programas desarrollados por el sector público, resulta preocupante el hecho de que, en algunos casos, las empresas privadas que crean estos sistemas, permitan su uso a las Administraciones públicas a cambio de datos que obran en poder de estas[68].

2. EL SISTEMA EUROPEO DE PROTECCIÓN DE DATOS: ESTRUCTURA Y LÍMITES

2.1. La protección de datos como principal mecanismo de salvaguarda frente a los riesgos generados por los sistemas algorítmicos

Muchos de los daños reales o potenciales causados por los algoritmos son el resultado de acciones de recogida y procesamiento de datos personales. Por consiguiente, los instrumentos jurídicos construidos desde la perspectiva de la protección de la privacidad (datos personales) son los mecanismos que, de manera más evidente, pueden proteger, en una primera aproximación, a las personas de los daños causados por las tecnologías de procesamiento de datos. A su vez, y dado que nos encontramos en muchos casos ante relaciones jurídicas privadas cuyos efectos se producen en la esfera privada de la vida de las personas, lo lógico también es, en principio, construir estas relaciones a partir de la autonomía de la voluntad de los individuos y el consentimiento, recurriendo a mecanismos de Derecho privado, como el Derecho de obligaciones y contratos, para su regulación.

Sin embargo, como ya se ha indicado, muchos de los daños causados por el uso de tecnologías de procesamiento de datos personales afectan a derechos fundamentales y principios democráticos básicos que los poderes públicos tienen la obligación de proteger. Asimismo, concurren fallos de mercado, arriba detallados, que impiden que los mecanismos de Derecho privado sean totalmente eficaces al abordar los problemas generados por el sector de los servicios de datos y, más concretamente, por las tecnologías de procesamiento de datos[69].

---

[68] Sam Shead, "Google DeepMind is giving the NHS free access to its patient monitoring app", *Business Insider*, 24 de junio de 2017. Disponible el 10 de diciembre 2020 en *https://www.businessinsider.com*.

[69] Omri Ben-Shahar, "Data pollution", *cit.*, 2019, pp. 104-159 (pp. 110-118).

En este contexto en el que la protección de la privacidad o intimidad informativa frente a los riesgos generados por los sistemas automatizados de toma de decisiones produce tensiones entre los marcos de Derecho privado y público, la Unión Europea ha desarrollado su estructura jurídica de protección de datos. El marco de protección de datos tiene por objeto proporcionar una serie de mecanismos jurídicos dirigidos a lidiar con muchos de los riesgos generados por el creciente uso de tecnologías de tratamiento de datos personales. Esta vocación de abarcar cuantos aspectos problemáticos del tratamiento de datos personales sea posible, ha conllevado el reconocimiento, por parte de la UE, del carácter público de algunos de los daños generados por estas actividades. Así pues, nos encontramos con una serie de instrumentos jurídicos que, si bien son construidos principalmente desde una perspectiva jurídico-privada, incorporan mecanismos y mandatos de intervención propios del Derecho público.

2.1. La estructura del ordenamiento jurídico europeo en materia de protección de datos

El núcleo del régimen de protección de datos personales de la UE lo constituye la libre determinación en materia de información personal. Este régimen jurídico se basa principalmente en un marco que, en teoría, proporciona a las personas autoridad sobre cómo y cuándo compartir sus datos. No obstante, este régimen de derechos individuales, cuyas influencias principales se encuentran en las construcciones propias del Derecho privado, establece también una serie de mandatos que los responsables del control y el tratamiento deben cumplir en todos los casos cuando procesan datos personales. Esto significa que algunas de las obligaciones comprendidas en los derechos reconocidos a las personas no solo se activan a petición del o la interesada, sino que siempre deben ser cumplidas por la persona física o jurídica que trata o utiliza los datos. Por ejemplo, los arts. 13 y 14 del RGPD establecen obligaciones de divulgación de información para los responsables del tratamiento.

Además, el sistema de protección de datos personales de la Unión Europea también establece una serie de instrumentos de supervisión que se han desarrollado combinando instrumentos jurídicos de *hard* y *soft law* a fin de producir un sistema que tenga por objeto prevenir y hacer frente a los riesgos y daños causados por el tratamiento de datos personales. Por último, al establecer una red de autoridades públicas de protección de datos, se transmite claramente la forma en que la Unión Europea reconoce las insuficiencias de abordar exclusivamente los peligros generados por las tecnologías de tratamiento de datos mediante instrumentos tradicionales de Derecho privado.

Si bien a lo largo del presente trabajo nos referimos principalmente al Reglamento General de Protección de Datos, no debemos olvidar que las normas europeas en este ámbito se extienden más allá. Conviene así hacer referencia, principalmente, a la Di-

rectiva de protección de datos personales en el ámbito penal (Directiva 2016/680)[70] y también, aunque no sea tan relevante para el objeto de estudio del presente trabajo pues no se centra tanto en la protección como en la libre circulación de datos, el Reglamento Europeo de libre circulación de datos no personales[71]. Por su parte, los Estados miembros de la UE también han adoptado normas propias en materia de protección de datos. Sin embargo, dado que todas ellas son el resultado de la trasposición del RGPD y de la Directiva 2016/680, que no hay diferencias muy significativas entre Estados en la regulación y que la mayor parte de la doctrina se ha centrado en el estudio de las normas europeas, también en el presente trabajo abordamos, exclusivamente, dicha normativa.

Cabe destacar también que el marco jurídico europeo en materia de protección de datos se centra en todo tipo de tratamiento o procesamiento de datos, se utilicen programas informáticos o no. Sin embargo, como es evidente, en el marco del presente trabajo nos centramos exclusivamente en los efectos que dichas normas tienen para el tratamiento de datos y la toma de decisiones automatizadas.

El sistema europeo en materia de protección de datos articula tres clases de mecanismos que se estructuran sobre los principios generales contenidos en los arts. 5 del RGPD y 4 de la Directiva 2016/680 (licitud, lealtad, transparencia, limitación de la finalidad y del plazo de conservación, minimización de datos, exactitud, integridad y confidencialidad)[72].

El primer mecanismo dirigido a la protección de datos es el que establece prohibiciones de procesamiento. Por una parte, los arts. 9 RGPD y 10 de la Directiva 2016/680 establecen la prohibición de procesar categorías especiales de datos. Estas categorías especiales de datos se solapan, en su mayoría, con las categorías sospechosas de producir discriminación. Por otra parte, el art. 22 RGPD establece el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles. Sin embargo, el Grupo de Trabajo del Artículo 29[73] ya determinó que dicho derecho debía, en realidad, ser considerado como una prohibición[74]. Por su parte, el art. 11 de la Directiva 2016/680 sí dispone la prohibi-

---

[70] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[71] Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

[72] Ver, en general, Adrián Palma Ortigosa, "Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos", *Revista General de Derecho Administrativo*, núm. 50, 2019 y Margot Kaminski, "Binary governance…", *cit.*, 2019, pp. 1529-1616.

[73] El Grupo de Trabajo del Artículo 29 se encargaba de interpretar las disposiciones contenidas en la Directiva de Protección de Datos y, posteriormente, en el RGPD, hasta que fue sustituido por el Comité Europeo de Protección de Datos en 2018.

[74] Grupo de Trabajo del Artículo 29, "Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679", 17/ES, WP 251rev.01, 6 de febrero

ción explícita de basar decisiones únicamente en tratamientos automatizados, incluida la elaboración de perfiles. Estas prohibiciones pueden ser exceptuadas en algunos casos, por ejemplo, cuando la persona interesada da su consentimiento.

El segundo mecanismo lo conforman todos aquellos derechos dirigidos a la conformación de un sistema de proceso tecnológico justo. Estos derechos vienen acompañados de correlativas obligaciones para los responsables y encargados del tratamiento de datos personales y se refieren a la información y acceso a los datos y a otros extremos relativos al procesamiento (arts. 12 a 15 RGPD y Directiva 2016/680); a rectificar y suprimir sus datos (arts. 16 y 17 RGPD y 16 Directiva 2016/680); a oponerse al tratamiento (art. 21 RGPD) y a recurrir los perfiles creados y/o decisiones tomadas ante autoridades de protección de datos y órganos judiciales (arts. 77 a 79 RGPD y 52 a 54 Directiva 2016/680).

Finalmente, se incluyen también instrumentos dirigidos a controlar, de manera general, los procesos de tratamiento de datos personales. Estos mecanismos incluyen la obligación de realizar evaluaciones de impacto, especialmente cuando estos sistemas entrañen un alto riesgo para las libertades y derechos fundamentales de las personas (arts. 35 RGPD y 27 Directiva 2016/680), un sistema de sanciones (arts. 84 RGPD y 57 Directiva 2016/680) y entidades públicas independientes de supervisión y control de protección de datos (Capítulo VI RGPD y Directiva 2016/680). Ademas, el RGPD (y no así la Directiva 2016/680 por ir dirigida exclusivamente al sector público) incluye diversos mecanismos que requieren de la cooperación entre poderes públicos y actores privados para su efectividad, como, por ejemplo, la elaboración de códigos de conducta para el procesamiento de datos (arts. 40 y 41 RGPD) y el desarrollo de mecanismos de certificación (art. 42 RGPD).

2.2. Los límites y deficiencias de las normas en materia de protección de datos

El marco jurídico europeo en materia de protección de datos ofrece una serie de mecanismos que pueden ser útiles para controlar y prevenir algunos de los riesgos generados por el tratamiento automatizado de datos personales y las decisiones y perfiles que pueden derivarse de él. Sin embargo, el RGPD y la Directiva 2016/680 son, al fin y al cabo, instrumentos diseñados para proteger el derecho a la protección de datos, por lo que se quedan cortos a la hora de establecer un sistema de protección eficaz frente a otros riesgos y daños que producen los sistemas automatizados de toma de decisiones. Especialmente cuando se trata de los riesgos para otros derechos fundamentales, en particular los derechos a la igualdad y la no discriminación, el marco de protección de datos no ofrece suficientes salvaguardias, responsabilidad y recursos,

---

de 2018, p. 21: "El artículo 22, apartado 1, establece una prohibición general de las decisiones basadas únicamente en el tratamiento automatizado. Esta prohibición se aplica tanto si el interesado adopta una acción relativa al tratamiento de sus datos personales como si no lo hace".

principalmente porque no se articula como un instrumento de no discriminación, pero también porque muchas de sus disposiciones han resultado ser, en la práctica, instrumentos jurídicos no vinculantes.

2.2.1. Los límites de la protección de datos personales

El marco jurídico europeo en materia de protección de datos se limita a proteger las personas cuyos datos personales sean recogidos y tratados, pero no se ocupa de los datos que hayan sido anonimizados. Esto supone un problema si tenemos en cuenta que, a medida que evoluciona la tecnología, es cada vez más sencillo reidentificar a aquellas personas cuyos datos han sido anonimizados[75].

También cabe destacar la falta de protección ofrecida a los perfiles de grupo. Los perfiles de grupo se desarrollan en relación con individuos que tienen características comunes. Los instrumentos de protección de datos personales no se aplican a los perfiles de grupo puesto que estos no contienen información que permita la identificación de personas concretas[76]. La cantidad de información que se encuentra disponible en la actualidad ofrece la posibilidad de crear perfiles sin emplear datos personales sino a través de la identificación de determinados atributos o acciones que pueden poner sobre la pista de la pertenencia de una persona a un determinado grupo. Los perfiles de grupo, generados sin emplear datos personales, son luego aplicados a personas específicas y pueden provocar daños significativos en caso de haberse construido sobre estereotipos perjudiciales para determinados grupos sociales.

Finalmente, puesto que el ordenamiento jurídico europeo en materia de protección de datos se centra, principalmente, en la protección de los datos de entrada al sistema, no establece normas claras relativas a los datos de salida, esto es, a las inferencias que realiza el sistema y en las que basa sus resultados. El sistema actual no ofrece suficientes mecanismos para detectar y poner en tela de juicio aquellos resultados basados en deducciones inexactas o que, de manera injustificada, perjudiquen a sus destinatarios[77]. Además, no existen normas que determinen la forma en que deben evaluarse los datos de salida ni mecanismos de garantía que encargados y responsables del tratamiento deban aplicar a los datos de salida.

---

[75] Paul Ohm, "Broken promises of privacy: responding to the surprising failure of anonymization", *UCLA Law Review*, vol. 57, 2010, pp. 1701-1777 (p. 1776); Alejandro Huergo Lora, "Una aproximación a los algoritmos desde el Derecho administrativo", en Alejandro Huergo Lora (dir.) y Gustavo Manuel Díaz González (coord.), *La Regulación de los Algoritmos*, Cizur Menor, Aranzadi, 2020, pp. 23-87 (pp. 55-56).

[76] Wim Schreurs *et al.*, "Cogitas, ergo sum. the role of data protection law and non-discrimination law in group profiling in the private sector" en Mireille Hildebrandt y Serge Gutwirth (eds.), *Profiling the European Citizen*, Springer, Berlín, 2008, pp. 241-270 (p. 243).

[77] Sandra Wachter y Brendt Mittelstadt, "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI", *Columbia Business Law Review*, vol. 2019, núm. 2, 2019, pp. 494-620 (p. 499).

2.2.2. Los límites de un sistema basado en el consentimiento y actitudes proactivas de las personas interesadas

El objetivo principal del sistema europeo de protección de datos personales es ofrecer a las personas interesadas información sobre el tratamiento de sus datos personales para que puedan dar (o no) un consentimiento debidamente informado. Así, por ejemplo, una de las excepciones al derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado es el consentimiento explícito otorgado por la persona interesada[78].

Asimismo, se proporciona a las personas interesadas una serie mecanismos de reacción. Todo ello tiene como objetivo dotar a las y los interesados de autonomía en la gestión de su información personal. Este enfoque tiene indudables beneficios en la medida que reconoce la autonomía decisional como expresión de la dignidad que puede ser denegada a las personas sometidas a procesos automatizados de toma de decisiones[79].

Sin embargo, como ya se abordó anteriormente, conceder un amplio margen de autonomía en la gestión de la información personal a cada individuo no es necesariamente garantía de un sistema efectivo de protección[80]. Así, la dificultad para comprender y valorar correctamente la magnitud de los riesgos que se generan cuando compartimos nuestros datos personales hace que, incluso cuando las personas interesadas son informadas sobre los extremos relevantes del procesamiento, estas tomen decisiones que pueden resultar perjudiciales para ellas en el medio o largo plazo[81].

Es más, en muchos casos, no existe una elección real entre compartir o no los datos personales y lo que se ofrece a la ciudadanía es una suerte de "ilusión de control" sobre su información personal. También son comunes los supuestos en que la información sobre el procesamiento ofrecida a las personas interesadas no es clara y comprensible. Cabe además añadir que el actual sistema de garantías basa la efectividad de estas, sobre todo, en actitudes proactivas de las y los interesados que pueden solicitar el acceso a sus datos, impugnar las decisiones automatizadas que se toman con respecto a ellas o solicitar la intervención de un ser humano en el procesamiento automatizado. Así, sitúan una serie de cargas (costes de transacción) sobre las personas que estas no son siempre capaces de asumir, en no pocos casos, por no ser ni siquiera conscientes de las posibilidades de acceso e impugnación al tratamiento automatizado de las que disponen[82].

---

[78] Art. 22.2.c.

[79] Margot Kaminski, "Binary governance…", *cit.*, 2019, pp. 1529-1616 (pp. 1553-1554); Bert-Jaap Koops, "The problem with European data protection law", *cit.*, 2014, pp. 250-261 (p. 251).

[80] Alejandro Huergo Lora, "Una aproximación a los algoritmos desde el Derecho administrativo", *cit.*, 2020, pp. 23-87 (pp. 56-58).

[81] Spyros Kokolakis, "Privacy attitudes and privacy behaviour...", *cit.*, 2017, pp. 122-134 (p. 125).

[82] Margot Kaminski, "Binary governance…", *cit.*, 2019, pp. 1529-1616 (p. 1590).

Cabe añadir también que esta clase de sistemas, basados en la protección individual, benefician a los segmentos sociales en posiciones socioeconómicas acomodadas, ya que disponen de más recursos para conocer y actuar en defensa de sus datos personales[83]. Es más probable que quienes gozan de mejores circunstancias económicas ejerzan los derechos que les ofrece el marco jurídico en materia de protección de datos y que tengan más posibilidades reales de elegir si prestan o no el consentimiento al procesamiento de sus datos. Esto, a su vez, implica que los sistemas automatizados contendrán más información sobre las personas con menos recursos, dando lugar a un mayor control sobre sus vidas, así como a la construcción de perfiles sesgados. Así, las diferencias entre aquellas personas que pueden elegir no ser sometidas al procesamiento y aquellas que, a efectos prácticos, no tienen esa libertad de decisión, contribuirá a reforzar las estructuras preexistentes de desigualdad[84].

Finalmente, un sistema construido sobre nociones de autonomía e individualidad dificulta la detección de errores sistémicos, que son los que se hallan en el origen de la discriminación algorítmica. Si no se dispone de acceso y control sobre la totalidad del sistema y de información comparada sobre los resultados obtenidos para diferentes personas, será muy difícil determinar si el algoritmo discrimina contra personas pertenecientes a un grupo vulnerable o desaventajado. Así, si se trata de un supuesto de discriminación directa, en que la pertenencia al grupo se considera de manera explícita, será suficiente con que una persona interesada solicite una explicación acerca de la lógica que subyace al sistema para que se pueda detectar la existencia de dicho trato discriminatorio. Sin embargo, en los supuestos de discriminación indirecta, no será posible detectar la existencia de un caso de discriminación si no se tiene acceso al propio sistema o a los resultados para otras personas sometidas al procesamiento.

Lo mismo sucede con otra clase de sesgos o errores contenidos en el sistema que no podrán ser detectados únicamente mediante el ejercicio de derechos subjetivos conferidos a las personas interesadas en el procesamiento. Además, los derechos derivados del marco jurídico en materia de protección de datos no están diseñados para ejercer un control *ex ante* sobre el sistema por lo que no dan la posibilidad de prevenir daños que, en ocasiones, pueden ser difíciles o imposibles de reparar una vez producidos.

2.2.3. Los límites de la intervención humana

Una de las herramientas de control y salvaguardia de los derechos de las personas interesadas es el derecho que tienen a obtener la intervención humana por parte del responsable en los procesos de toma de decisiones basados en procesamientos

---

[83] Bert-Jaap Koops, "The problem with European data protection law", *cit.*, 2014, pp. 250-261 (p. 252); Cass Sunstein, "Sludge and ordeals", *Duke Law Review*, vol. 68, núm. 8, 2018, pp. 1843-1883 (p. 1859).

[84] Margot Kaminski, "Binary governance…", *cit.*, 2019, pp. 1529-1616 (pp. 1590).

puramente automatizados (art. 22.3 RGPD). El reconocimiento de este derecho es relevante por cuanto que introduce un componente humano en el procedimiento, restaurando así algunos de los posibles daños causados a la dignidad de las personas y también aumentando la posibilidad de que se detecten aquellos elementos intangibles que el sistema no capta. Sin embargo, los seres humanos tenemos un sesgo que nos hace confiar en exceso en los resultados obtenidos por programas informáticos[85]. Por lo que, salvo que las personas encargadas de realizar esa intervención humana estén correctamente formadas para supervisar el sistema[86], su intervención no será más que simbólica.

2.2.4. Ineficacia en el control de la toma de decisiones automatizadas por las Administraciones públicas

Los problemas principales que, hasta la fecha, se han detectado en relación con los procesos de toma de decisiones públicas en los que se emplean sistemas algorítmicos se han ubicado, sobre todo, en el ámbito de la transparencia. Resulta especialmente preocupante que las Administraciones públicas parezcan denegar, de manera sistemática, el acceso al código fuente e información general del sistema incluso en los procesos de toma de decisiones que no deberían ser especialmente problemáticos[87]. Dos ejemplos especialmente significativos que se han dado en España en relación con el ejercicio del derecho de acceso son los casos del sistema utilizado por la Generalitat de Catalunya para la selección del profesorado integrante de los tribunales de corrección de las pruebas de acceso a la universidad (PAU)[88] y del sistema empleado en la concesión del bono social energético[89].

Con respecto al primer caso, las personas interesadas solicitaron acceso al contenido del algoritmo empleado por el Consejo Interuniversitario de Cataluña, habiendo este desestimado la solicitud al considerar que proporcionar el contenido del algoritmo perjudicaría el buen funcionamiento del sistema y que la opacidad de dicho procedimiento se encontraba justificada por el límite de la confidencialidad del procedimiento (art. 14.1.k Ley de Transparencia y Buen Gobierno). Este acceso fue posteriormente concedido por la Comisión Catalana para la Garantía del Derecho de Acceso por considerar que no operaba tal límite[90]. También en parecido sentido, en el ámbito comparado, vamos viendo supuestos en que tribunales y órganos admi-

---

[85] Danielle Citron, "Technological due process", *cit.*, 2008, pp. 1249-1313 (pp. 1271-1272).

[86] Juli Ponce Solé, "El derecho a una buena administración y la personalización de los servicios públicos", *cit.*, 2019, pp. 51-71 (pp. 59-62).

[87] Andrés Boix Palop, "Los algoritmos son reglamentos…", *cit.*, 2020, pp. 223-270 (p. 243).

[88] Comisión Catalana para la Garantía del Derecho de Acceso a la Información Pública, Resolución a las reclamaciones 123/2016 y 124/2016 (acumuladas), de 21 de septiembre.

[89] Javier De La Cueva, "Código fuente, algoritmos y fuentes del derecho", *El Notario del Siglo XXI*, núm. 77, 2018; "El derecho a no ser gobernados mediante algoritmos secretos", *El Notario del Siglo XXI*, núm. 87, 2019.

[90] *Ibidem*.

nistrativos de control van progresivamente reconociendo el derecho de acceso a los algoritmos empleados en los procesos de toma de decisiones de las Administraciones públicas[91].

Sin embargo, no deja de llamar la atención que las Administraciones públicas rechacen, por defecto, el acceso a los sistemas algorítmicos que estas emplean. En este sentido, resulta sobre todo llamativo y preocupante el segundo supuesto citado, esto es, el del algoritmo empleado en la concesión del bono social eléctrico, el acceso al cual no solo fue denegado por el Ministerio para la Transición Ecológica, sino también por el Consejo estatal de Transparencia y Buen Gobierno[92], que, amparándose en la protección de la propiedad intelectual del sistema, consideró que el derecho de acceso de los recurrentes debía verse limitado en este supuesto.

El hecho de que las Administraciones públicas parezcan apostar por mantener la opacidad de los algoritmos que utilizan es, en parte, el resultado de que el uso de programas informáticos que no son, de por sí, transparentes ni accesibles permite a las Administraciones ocultar, por defecto, la forma en que se tramitan los procedimientos. Esta situación es también el resultado de la confianza que se ha depositado en el RGPD como principal instrumento para combatir los diferentes problemas surgidos del creciente uso de sistemas automatizados. Puesto que esta norma no se encuentra específicamente diseñada para lidiar con las particularidades propias de la actividad de los poderes públicos, a pesar de aplicarse a estos, no llega abordar cuestiones como las especiales exigencias en materia de transparencia y motivación que deberían ser siempre de aplicación a aquellos.

Esta realidad se conjuga con la dudosa naturaleza jurídica de los algoritmos empleados por las Administraciones públicas[93], que propicia que estas eludan las normas de transparencia propias y específicamente aplicables a las Administraciones públicas, al defender, por ejemplo, que el derecho de acceso de la ciudadanía debe verse limitado por la protección de la propiedad intelectual cuando se empleen algoritmos[94].

Debemos recordar que la Ley de Propiedad Intelectual excluye de su ámbito de aplicación "las disposiciones legales o reglamentarias y sus correspondientes proyec-

---

[91] Tribunal Regional Administrativo del Lazio-Roma, Sección III bis, Sentencias núm. 3769, de 22 de marzo de 2017 y núm. 10964, de 13 de septiembre de 2019; Comisión Francesa de Acceso a los Documentos Administrativos, Decisiones núm. 20144578, de 8 de enero de 2015 y núm. 20180276, de 19 de abril de 2018.

[92] Resolución 701/2018 de 18 de febrero de 2019.

[93] En relación con la discusión doctrinal acerca de la naturaleza jurídica de los algoritmos ver, en general: Luís Arroyo Jiménez, "Algoritmos y reglamentos", *Almacén de Derecho*, 25 de febrero de 2020, disponible el 1 de diciembre de 2020 en *https://almacendederecho.org/*; Andrés Boix Palop, "Los algoritmos son reglamentos…", *cit.*, 2020, pp. 223-270; Alejandro Huergo Lora, "Una aproximación a los algoritmos desde el Derecho administrativo", *cit.*, 2020, pp. 23-87 (pp. 66-69); Juli Ponce Solé, "Inteligencia artificial, Derecho administrativo y reserva de humanidad…", *cit.*, 2019, pp. 1-52 (p. 35).

[94] Art. 14.1.j) Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

tos, las resoluciones de los órganos jurisdiccionales y los actos, acuerdos, deliberaciones y dictámenes de los organismos públicos, así como las traducciones oficiales de todos los textos anteriores"[95]. Procedemos pues, a determinar si los algoritmos empleados en los procedimientos administrativos tienen la naturaleza jurídica correspondiente a alguno de los instrumentos mencionados en el citado precepto.

Como puntualización inicial, resulta necesario determinar si los sistemas automatizados empleados en el contexto de procedimientos administrativos producen efectos jurídicos o constituyen meros elementos accesorios o de apoyo al procedimiento que carecen de relevancia jurídica y no inciden en la esfera jurídica de las personas interesadas. Conviene recordar que el Grupo de Trabajo del Artículo 29 ya determinó que para considerar que una decisión tiene efectos jurídicos debe afectar a los derechos, el estatuto jurídico de una persona o sus derechos derivados de un contrato[96]. En la medida en que las decisiones tomadas por algoritmos en el sector público influyen o incluso, en ocasiones, determinan el resultado final de un procedimiento, estos sistemas tienen efectos jurídicos sobre las personas interesadas y, por tanto, no pueden ser tratados como meros instrumentos de apoyo a las decisiones tomadas por los poderes públicos.

Una vez determinada esta primera cuestión, resulta necesario atender a la clase de instrumento jurídico que constituyen los algoritmos empleados en la toma de decisiones públicas. Así, en función de si consideramos que los sistemas automatizados constituyen reglamentos, actos administrativos o un instrumento completamente diferente, determinaremos también cuáles son las exigencias, por ejemplo, de transparencia y justificación, que son aplicables a los sistemas automatizados empleados por la Administración pública.

Cuando se diseñan los algoritmos, se crean como conjuntos de instrucciones que se aplican a casos específicos. Estas instrucciones establecen cómo procesar los datos que se introducen en el sistema. Los sistemas de aprendizaje autónomo evolucionan, aprenden de los datos que procesan y cambian continuamente sus parámetros en consecuencia, lo que significa que el conjunto de instrucciones varía con el paso del tiempo. Sin embargo, estas modificaciones no cambian la realidad intrínseca del sistema como un conjunto de reglas, una abstracción de la realidad en la que se introducen los datos a fin de obtener resoluciones para casos particulares. Por consiguiente, mientras que la decisión específica que resulta del tratamiento automatizado de los datos equivale a un acto administrativo, el sistema algorítmico constituye los parámetros generales que deben seguirse y aplicarse a cada supuesto de hecho, es decir, constituye un instrumento regulador. Por consiguiente, si bien el resultado de la decisión algorítmica en casos concretos puede clasificarse y tratarse como acto

---

[95] Art. 13 Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[96] Grupo de Trabajo del Artículo 29, "Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679", *cit.*, 2018, p. 23.

administrativo, el algoritmo que se utiliza y su código fuente deben tratarse como un instrumento regulador y, concretamente, como reglamento.

En algunos casos, los sistemas automatizados se utilizan en procedimientos administrativos en los que hay alguna forma de intervención humana en el proceso de adopción de decisiones o en los que los resultados generados por el programa no son vinculantes[97]. Las Administraciones públicas pueden utilizar sistemas de predicción para fundamentar las decisiones o producir resultados no vinculantes, en lugar de utilizarlos como sistemas totalmente automatizados de adopción de decisiones[98]. Podría entonces argumentarse que el efecto que tendrían los algoritmos en estos casos es similar al de los dictámenes o informes de expertos emitidos en el marco de los procedimientos administrativos[99].

Sin embargo, aun cuando un sistema automatizado no se utilice para proporcionar decisiones vinculantes sino solo como instrumento de asesoramiento o apoyo, también debe tratarse, en cierta medida, como un instrumento regulador. En este sentido, es conveniente establecer una analogía con la forma en que se regula la actividad de los órganos consultivos de la Administración pública. Los órganos consultivos elaboran sus informes y desarrollan su actividad basándose en los instrumentos jurídicos que los regulan. Un algoritmo utilizado con fines similares a los ejercidos por los órganos consultivos abarca tanto las normas en que se basa el dictamen que emite (equivalente a los instrumentos jurídicos que regulan los órganos consultivos) como el procedimiento que conduce al dictamen que emite (equivalente a las actividades y procedimientos que llevan a cabo los órganos consultivos al emitir un dictamen). Por consiguiente, aunque los efectos que el algoritmo tiene en el procedimiento no son tan relevantes como cuando la decisión se toma de manera totalmente automatizada, también deben tratarse como reglamentos en la medida en que deciden la forma en que se emite la opinión.

No debemos olvidar las diferencias entre los instrumentos tradicionales de regulación y los sistemas automatizados. Estas diferencias indudablemente generarán tensiones si pretendemos aplicar exactamente las mismas normas a ambos tipos de instrumentos. Por ejemplo, no parece realista obligar a publicar el código fuente y otras especificaciones de los algoritmos empleados por el sector público en el diario oficial correspondiente. Sin embargo, mientras continuemos con debates teóricos acerca de la naturaleza de estos sistemas y la posible creación de una categoría jurídica

---

[97] Andrés Boix Palop, "Los algoritmos son reglamentos…", *cit.*, 2020, pp. 223-270 (p. 237).

[98] Marion Oswald, "Algorithm-assisted decision-making in the public sector…", *cit.*, 2018, pp. 1-20 (pp. 2-3).

[99] Aunque en el contexto específico de la Administración penitenciaria, cabe destacar, en este sentido, el papel que tiene el programa RISCANVI en el otorgamiento o denegación de permisos penitenciarios en Cataluña. Ver, en este sentido, Alejandro Huergo Lora, "Una aproximación a los algoritmos desde el Derecho administrativo", *cit.*, 2020, pp. 23-87 (p. 36): "[…] existe una abundante jurisprudencia que […] considera que se puede utilizar el resultado que arroja el programa RISCANVI para motivar la resolución (aunque no se conozca su contenido exacto), siempre que se puedan utilizar también otros factores y someter a crítica ese resultado".

completamente nueva que les sea de aplicación, existirá una laguna jurídica plagada de algoritmos utilizados por el sector público con efectos nada despreciables sobre las vidas de las personas. Es por ello que resulta necesario que consideremos la naturaleza reglamentaria de estos sistemas y que, en aquellos supuestos en los que proceda, adaptemos las exigencias y requisitos que son de aplicación a dichas normas a los sistemas algorítmicos. Así, a modo de ejemplo, en lugar de exigir la publicación de los sistemas automatizados en los diarios oficiales, debería crearse un registro público de algoritmos, como ya existe en la ciudad de Ámsterdam [100], en el que se contengan todos los datos relativos a cada sistema empleado.

2.3.4 Ineficacia de los mecanismos generales de control

Tal como se ha indicado anteriormente, el marco jurídico europeo en materia de protección de datos incorpora una serie de mecanismos generales de control, como las evaluaciones de impacto o certificación de los sistemas de tratamiento de datos. El objetivo de estos es asegurar los sistemas algorítmicos funcionan correctamente y respetan las normas jurídicas que les son de aplicación según el contexto en el que vayan a ser utilizados. En principio, estos mecanismos deberían salvar algunas de las deficiencias derivadas de centrar el sistema de protección de datos en la autonomía de las y los interesados. Sin embargo, hasta el momento, la efectividad de los instrumentos a los que nos referimos en este epígrafe ha demostrado ser muy limitada.

En primer lugar, la implementación de códigos de conducta y mecanismos de certificación es voluntaria [101]. Asimismo, incluso cuando se decide adoptar uno de estos instrumentos, únicamente se prevé la participación de autoridades públicas, responsables y encargados del tratamiento en su elaboración y diseño, y no de organizaciones o asociaciones representativas de intereses que se puedan ver afectados por el tratamiento de datos [102]. Esta falta de previsión genera un evidente riesgo de construir instrumentos de supervisión sesgados a favor de los intereses de los responsables y encargados del tratamiento.

En segundo lugar, aunque sea obligatorio realizar evaluaciones de impacto cuando el tratamiento entrañe un riesgo elevado para los derechos y libertades de las personas físicas [103], lo cierto es que las autoridades de protección de datos no disponen de recursos suficientes para controlar que todas estas evaluaciones de impacto se estén llevando a cabo. Es más, el propio concepto de "alto riesgo" proporciona a responsables y encargados del tratamiento cierto margen de discrecionalidad para decidir en qué casos deben llevarse a cabo las evaluaciones de impacto.

---

[100] Algorithm Register, 2020. Disponible el 9 de diciembre de 2020 en *https://algoritmeregister.amsterdam.nl/*.

[101] Arts. 40 y 42 RGPD.

[102] Art. 40.2 RGPD.

[103] Art. 35 RGPD.

Como muestra de la ineficacia de la obligación de realizar evaluaciones de impacto cabe mencionar la sentencia dictada en relación con el programa "SyRI", empleado por la Inspección de Trabajo y Seguridad Social holandesa para detectar y prevenir casos de fraude cometidos por personas receptoras de prestaciones de la seguridad social[104]. Dicha sentencia, que prohibió la utilización del sistema, se pronunció, entre otros extremos, sobre el incumplimiento por la Inspección de Trabajo y Seguridad Social holandesa de la obligación de someter el programa a todas las evaluaciones de impacto requeridas[105]. Considerando que dicho sistema era empleado por una Administración pública, y que las Administraciones públicas en teoría se someten a unas condiciones de actuación y supervisión más estrictas que los actores privados, cabe preguntarse hasta qué punto se está cumpliendo, tanto en el sector público como en el privado, con las obligaciones derivadas de los mecanismos de control general regulados en el RGPD.

2.3.5. Límites de la protección frente a la discriminación

Por último, cabe destacar que la normativa en materia de protección de datos también pretende articularse como instrumento de protección de la igualdad y la no discriminación. Así, al prohibir el procesamiento de categorías especiales de datos (arts. 9 RGPD y 11 Directiva 2016/680)[106], las cuales coinciden en gran medida con las categorías sospechosas de discriminación contenidas en los instrumentos de protección de derechos fundamentales, se pretende precisamente evitar que puedan darse situaciones en las que se trate de manera diferente (perjudicial) a un sujeto por su pertenencia a un determinado grupo, generalmente desaventajado.

La voluntad del marco europeo en materia de protección de datos de tratar de prevenir las posibles situaciones de discriminación derivadas del tratamiento de datos personales debe, sin duda, valorarse de manera positiva. Sin embargo, no debe confiarse en exceso en la efectividad de la prohibición de procesar categorías especiales de datos ya que, incluso si no se procesa directamente la pertenencia de una persona a un grupo desaventajado, el algoritmo puede, con todo, inferir dicha pertenencia de otros datos. Así, aunque la prohibición se refiera al "tratamiento de datos personales que *revelen* el origen étnico o racial, las opiniones políticas, etc.", lo cierto es que,

---

[104] Sobre el caso SyRI, *vid.* Lorenzo Cotino Hueso, "«SyRI, ¿a quién sanciono?» Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", *La Ley Privacidad*, núm. 4, 2020 y Adrián Todolí Signes, "Retos legales del uso del *big data* en la selección de sujetos a investigar por la Inspección de Trabajo y de la Seguridad Social", *Revista Galega de Administración Pública*, núm. 59, 2020, pp. 313-337.

[105] Sentencia del Tribunal de distrito de La Haya, de 5 de febrero de 2020, Asunto C / 09/550982 / HA ZA 18-388, párrafos 6.104-6.105.

[106] "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".

como han demostrado múltiples estudios, resulta prácticamente imposible eliminar todos aquellos datos que revelen la pertenencia a un grupo especialmente protegido sin hacer que el algoritmo sea inservible[107].

Asimismo, la no inclusión de la pertenencia a grupos desaventajados en el sistema puede dificultar la detección de casos de discriminación pues será más fácil que los responsables y encargados del tratamiento tomen decisiones basándose en características aparentemente inocuas que, en realidad, oculten un ánimo discriminatorio. En este sentido, Žliobaitė y Custers proponen incluir una exención en el marco jurídico europeo que permita el tratamiento de categorías especiales de datos personales cuando dicho tratamiento se lleve a cabo mediante algoritmos diseñados y dirigidos a detectar y reducir situaciones de discriminación[108].

3. PROPUESTAS PARA UN MARCO JURÍDICO DE CONTROL DE LOS ALGORITMOS

Las limitaciones del marco jurídico en materia de protección de datos para enfrentarse a los problemas derivados del creciente uso de algoritmos generan una ineludible necesidad de adoptar nuevos instrumentos jurídicos que hagan frente a esta nueva realidad. Esta situación es ampliamente reconocida por la Unión Europea y sus Estados miembros, que en los últimos años han coincidido en la necesidad crear un sistema normativo que aborde, de manera global, los diferentes problemas derivados del uso de la inteligencia artificial[109]. Esta sección pretende realizar un esbozo general de algunas posibles medidas que podrían adoptarse con este objetivo y que, consideramos, contribuirían a reducir algunas de las principales deficiencias del actual marco normativo en la protección de los derechos fundamentales y otros valores democráticos que pueden ser dañados por el uso de sistemas automatizados de toma decisiones, incluyendo la creación de perfiles.

3.1. Red de autoridades de control algorítmico

La creación de una red de autoridades que, de manera específica, se ocupen de controlar el uso de sistemas algorítmicos resulta recomendable, no solo por los crecientes riesgos que generan los procesos automatizados de toma de decisiones, sino también por la complejidad y especialidad de dichos riesgos. Desde diferentes secto-

---

[107] Bryce W. Goodman, "A step towards accountable algorithms?: Algorithmic discrimination and the European Union general data protection", *29th Conference on Neural Information Processing Systems*, 2016. Disponible el 9 de diciembre de 2020 en: http://www.mlandthelaw.org/ .

[108] Indrė Žliobaitė y Bart Custers, "Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models", *Artificial Intelligence & Law*, vol. 24, núm. 2, 2016, pp. 183-201.

[109] Ver, por ejemplo, Comisión Europea, "Libro blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza", COM(2020) 65 final, 19 de febrero de 2020.

res doctrinales y también la propia Comisión Europea recogen esta propuesta como la más adecuada de cara a controlar el uso de estos sistemas tanto en el sector público como en el sector privado [110].

Dichas instituciones deberían estar integradas por personal procedente de diferentes disciplinas. Resulta, sobre todo, de vital importancia que expertas y expertos en la protección de los derechos fundamentales y en el campo de la ética algorítmica integren estas instituciones ya que, por el momento, como norma general, estos sistemas no están siendo diseñados desde la perspectiva de la protección de la igualdad y otros valores y principios democráticos.

Asimismo, con el objetivo de limitar los costes y aprovechar sinergias ya existentes, facilitando la puesta en marcha de estas instituciones, cabría considerar la posibilidad de emplear la red de instituciones ya existente en la Unión Europea en materia de protección de datos. Estas autoridades independientes podrían ir, paulatinamente, asumiendo más competencias hasta lograr prevenir y controlar los problemas generados por el uso de algoritmos de manera lo suficientemente efectiva.

3.2. Control de los algoritmos en función del nivel de riesgo

Dado que los sistemas automatizados se emplean en toda clase de contextos y procesos de toma de decisiones, no resulta lógico establecer un criterio único para la supervisión y control de algoritmos. Además, también debemos tener en cuenta que existen muchas clases de programas empleados en el tratamiento automatizado de datos, por lo que los requisitos con los que los sistemas deberían cumplir variarán en función de la complejidad, opacidad, capacidad de autoaprendizaje y otros criterios a tener en cuenta y que pueden influir en el nivel y clase de riesgos generados.

En los últimos años, tanto la Comisión Europea como la Comisión Alemana de Ética de los Datos han lanzado sendas propuestas de sistemas regulación y control de los algoritmos basadas en el riesgo [111] y el Gobierno Canadiense ha establecido un sistema de esta clase para el control de los algoritmos empleados en el sector público [112].

---

[110] Comisión Europea, "Libro blanco sobre la inteligencia artificial…", *cit.*, 2020, pp. 24-25; Matthew Scherer, "Regulating artificial intelligence systems: risks, challenges, competencies, and strategies", *Harvard Law & Technology Journal*, vol. 29, núm. 2, 2016, pp. 353-400; Ben Shneiderman, "Algorithmic Accountability: Designing for safety through human-centered independent oversight", *Turing Lecture (The Alan Turing Institute)* 31 de marzo de 2017. Disponible el 26 de noviembre de 2020 en: https://www.youtube.com/watch?v=UWuDgY8aHmU&t=2245s/; Andrew Tutt, "An FDA for algorithms", *Administrative Law Review*, vol. 69, núm. 1, 2017, pp. 83-123; Clara Velasco Rico, "Vigilando al algoritmo. Propuestas organizativas para garantizar la transparencia", *cit.*, 2019, pp. 73-89 (pp. 81-82).

[111] Datenethikkommission, "Gutachten der Datenethikkommission", 2019; Datenethikkommission, "Opinion of the Data Ethics Commission: Executive Summary", 2019; Comisión Europea, "Libro blanco sobre la inteligencia artificial…", *cit.*, 2020.

[112] Canadian Directive on Automated Decision-Making, 1 de abril de 2019.

Sería posible, por ejemplo, establecer un sistema de control que tuviese en cuenta el tipo de algoritmo empleado, así como los objetivos para los que se utiliza. Por una parte, deberían identificarse aquellos sistemas que generan riesgos inasumibles y que, por tanto, deben quedar completamente prohibidos. En esta categoría deberían entrar, por ejemplo, las armas autónomas (no automáticas). Por otra parte, los restantes sistemas deberían clasificarse en función del nivel de riesgo generado, estableciendo controles *ex ante* y *ex post* más intensos y mayores requisitos cuanto más riesgo genere el sistema. Entre los posibles mecanismos de control cabría valorar la posibilidad de incluir evaluaciones de impacto previas llevadas a cabo por la autoridad pública de control algorítmico, certificaciones previas y posteriores a la puesta en marcha del sistema realizadas por entidades privadas acreditadas por la autoridad pública y la puesta en marcha de un registro público de algoritmos, entre otras posibles medidas y requisitos que se deberían ajustar al riesgo generado por cada clase de sistema.

Se propone el establecimiento de cinco categorías en función del nivel de riesgo generado por el sistema automatizado:

En primer lugar, nos encontraríamos con el nivel más elevado de riesgo. Como ya se ha indicado anteriormente, ubicar un sistema automatizado en este nivel de riesgo comportaría su prohibición total.

En segundo lugar, aquellos sistemas que generen riesgos más elevados, pero asumibles, deberían someterse a evaluaciones de impacto llevadas a cabo por la autoridad algorítmica competente en el ámbito territorial en el que se pretenda emplear o distribuir dicho sistema. Dicha evaluación inicial determinaría, en función del grado de complejidad y posibilidad de aprendizaje autónomo del sistema, la necesidad de someterse a evaluaciones periódicas posteriores también llevadas a cabo por la autoridad independiente. Solo en aquellos casos en los que un sistema no tenga apenas capacidad de autoaprendizaje, podrían las evaluaciones posteriores ser realizadas por entidades externas de certificación reconocidas por las autoridades de control algorítmico. Los sistemas que entren dentro de la categoría de más elevado riesgo y sean empleados por Administraciones públicas deberían también ser sometidos a más elevados requisitos de transparencia y otras garantías adicionales por su carácter normativo[113]. Es también así recomendable que, igual que lo ha hecho la ciudad de Ámsterdam, se establezca un registro público de algoritmos en el que aparezcan publicados todos los sistemas automatizados empleados por el sector público[114], sin perjuicio de los posibles límites.

En tercer lugar, los algoritmos que generen riesgos de nivel "medio" deberían, de manera previa a su entrada en el mercado, ser certificados por las autoridades de

---

[113] En este sentido, debe tenerse en cuenta que los sistemas algorítmicos empleados por el sector público deberían ser considerados y tratados, en casi todos los casos, como normas reglamentarias, trasladando por ello a estos y a su regulación las garantías (en su elaboración, publicidad y control de su aplicación) que nuestros ordenamientos ya han decantado durante décadas para aquéllas. Andrés Boix Palop, "Los algoritmos son reglamentos…", *cit.*, 2020, pp. 223-270.

[114] Algorithm Register, *cit.*, 2020.

control algorítmico. Este proceso de certificación examinaría menos extremos que los comprobados con la realización de las evaluaciones de impacto y los plazos deberían ser más breves. Además, los responsables y encargados del tratamiento deberían entregar la información del sistema a la autoridad correspondiente. Los procesos de recertificación podrían realizarse por entidades externas de certificación reconocidas por las autoridades de control algorítmico. La documentación que se debería aportar para la realización del primer proceso de certificación contendría toda la información relativa al *software*, que la autoridad debería conservar.

En cuarto lugar, cabe destacar que aquellos sistemas que generen un nivel de riesgo bajo deberían someterse a procesos de certificación sencillos que podrían llevarse a cabo incluso cuando el sistema ya haya accedido al mercado. Asimismo, también se deberían realizar procesos de recertificación posteriores más espaciados en el tiempo que los aplicables a los sistemas que generen un nivel de riesgo "medio".

Por último, los sistemas que tengan una nula capacidad de autoaprendizaje, es decir, que sean puramente automáticos, y que además se empleen en contextos y para objetivos que no generen prácticamente ninguna clase de riesgo únicamente deberán superar los controles a los que se deban someter los productos en los que se incorporan.

3.3. Establecimiento de un sistema de "mejores técnicas disponibles"

El creciente uso de sistemas algorítmicos puede contribuir a perpetuar determinadas estructuras históricas de desigualdad, dañar los derechos fundamentales de las personas y a quebrar algunos principios básicos de las relaciones de la ciudadanía con los poderes públicos, entre otras cuestiones. Es por ello que se ha desarrollado un campo de estudio dedicado a la "ética algorítmica" que pretende crear algoritmos comprensibles, no discriminatorios y que aseguren la protección de los derechos de la ciudadanía, sin reducir la eficiencia y precisión de estos sistemas. También en este contexto se vienen diseñando sistemas o técnicas dirigidos a detectar algoritmos discriminatorios[115].

Esta rama de investigación todavía se encuentra en sus inicios y, por consiguiente, en ocasiones resulta muy costoso recurrir a esta clase de técnicas. El establecimiento de un sistema europeo de mejores técnicas disponibles, parecido al que existe en Derecho ambiental, permitiría determinar qué algoritmos deben y pueden utilizarse en función del contexto, objetivos y tamaño de la entidad que los utilice, así como si se trata de una organización pública o privada y de los costes y beneficios de la utilización de un sistema tanto para la entidad que lo emplea como para otros intereses en juego. El establecimiento de un sistema de mejores técnicas disponibles también faci-

[115] Michael Feldman, *et al.*, "Certifying and removing disparate impact", *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2015, pp. 259-268.

litaría el enjuiciamiento de decisiones mediadas por algoritmos ya que, por ejemplo, en supuestos de discriminación algorítmica, el tribunal tendría la posibilidad de determinar si existe otro sistema algorítmico que, no siendo excesivamente más costoso ni menos preciso, produce resultados menos discriminatorios en el mismo contexto.

3.4. La contratación pública como mecanismo para prevenir los riesgos en el uso de algoritmos por los sectores público y privado

Cuando las Administraciones públicas emplean sistemas automatizados generalmente los adquieren de empresas privadas o los desarrollan junto a ellas. Es por ello que resulta conveniente que se empleen las técnicas disponibles en materia de contratación pública dirigidas a perseguir objetivos sociales. Así, por ejemplo, se deberían establecer una serie de requisitos relativos al funcionamiento de los sistemas creados por las empresas licitadoras y a la propia organización interna de dichas entidades, asegurando, por ejemplo, que las personas encargadas de desarrollar sistemas algorítmicos cuentan con formación en materia de igualdad. El establecimiento de esta clase de medidas incentivaría a estas empresas a implementar dichos requisitos de manera general, de forma que sus efectos trascenderían a los algoritmos empleados por el sector público para darse también en los sistemas empleados por entidades privadas[116].

3.5. Empoderar a las personas en la gestión de sus datos y modificación de las arquitecturas del diseño

Es necesario fomentar la educación en materia de protección de datos personales y la concienciación con respecto a los riesgos generados por las nuevas tecnologías de procesamiento de datos. Además, se debería fomentar la adopción de estrategias similares a las incorporadas en el ámbito de la protección de personas consumidoras y usuarias con el objetivo de colectivizar la protección frente a los riesgos derivados del uso de sistemas automatizados. En este sentido, se puede tomar también como punto de partida la posibilidad que ofrece el artículo 80 RGPD de que las asociaciones relevantes en materia de protección de datos puedan representar a las personas interesadas en los procedimientos ante autoridades administrativas y judiciales para proteger los derechos reconocidos en el Reglamento.

---

[116] En relación con el papel de la contratación pública en el uso de inteligencia artificial por las Administraciones públicas ver, por ejemplo, Javier Miranzo Díaz, "Inteligencia artificial y contratación pública", en Isaac Martín Delgado y Jose Antonio Moreno Molina (dirs.), *Administración electrónica, transparencia y contratación pública*, Madrid, Iustel, 2020, pp. 105-142 y Julián Valero Torrijos, "Inteligencia artificial y contratación del sector público", *Observatorio de Contratación Pública*, 27 de enero de 2020.

Asimismo, debe obligarse a las empresas privadas e instituciones públicas a establecer arquitecturas del diseño proprivacidad en sus plataformas digitales de manera que, por defecto, no se recojan los datos de las personas que las utilizan y, únicamente si estas dan su consentimiento específico a los diferentes campos, puedan recogerse y procesarse sus datos. Por ejemplo, no podría darse la opción de "aceptar todas las *cookies*".

3.6. Comunicación y cooperación entre disciplinas

Como ya se ha indicado en el apartado en el que se realiza la propuesta relativa a la constitución de autoridades de control algorítmico, es esencial que la experiencia de profesionales procedentes de diferentes disciplinas académicas se integre en dichas instituciones. En este sentido, de manera más general, también debe extrapolarse esta colaboración a otros ámbitos para asegurar que estos sistemas, cuya incidencia en la vida de la ciudadanía es cada vez mayor, se desarrollan teniendo en cuenta las normas que les son de aplicación[117]. También resulta de gran relevancia que se introduzcan cursos sobre ética algorítmica y Derecho en todos los programas de formación universitaria y no universitaria en los que se estudie programación con el objetivo de informar y formar a las y los futuros programadores de aquellos problemas, como los estudiados en este trabajo, que pueden producir los sistemas algorítmicos, así como sus posibles soluciones. Si bien es cierto que algunos programas formativos en estas ramas comienzan a introducir materias jurídicas, no se puede decir lo mismo con respecto a formación específica, por ejemplo, en materia de igualdad y con respecto a los riesgos para los derechos a la igualdad y a la no discriminación que pueden generar los sistemas algorítmicos.

CONCLUSIONES

La creciente capacidad computacional de los sistemas automatizados de procesamiento de datos ha provocado que su uso se extienda a toda clase de procesos decisorios, tanto en el sector público como en el sector privado. El aumento de la eficiencia y precisión que conlleva el uso de estos sistemas no deben hacernos perder de vista muchos de los problemas que se derivan de su utilización, sobre todo si tenemos en cuenta que los mecanismos jurídicos de los que disponemos en la actualidad no están adaptados ni preparados para enfrentarse a las particularidades propias de estas nuevas formas de llevar a cabo actividades tradicionalmente realizadas por seres humanos.

---

[117] Susana De La Sierra Morón, "Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la Administración pública", *Revista General de Derecho Administrativo*, núm. 53, 2020, pp. 1-19 (pp. 11-12).

Las instituciones y la doctrina han confiado en el marco jurídico en materia de protección de datos, al ser el único existente hasta la fecha, para hacerse cargo de los muchos riesgos y daños derivados del uso de algoritmos. La protección de datos ofrece herramientas que pueden resultar útiles para enfrentarse, principalmente, a los riesgos generados en la esfera de la intimidad de las personas por el uso de sistemas automatizados. Sin embargo, no puede pretenderse hacer frente a los muchos y diversos riesgos generados por los sistemas algorítmicos con unas herramientas jurídicas cuyo objetivo principal es la protección de datos, tanto en contextos mediados por herramientas tecnológicas como en tratamientos más tradicionales.

Este trabajo ha pretendido, de manera muy sintética, aportar algunas posibles soluciones a los problemas actuales derivados del creciente uso de sistemas algorítmicos, que son enumeradas a continuación.

— Establecimiento de una red de autoridades de control algorítmico.

— Regulación y control de los algoritmos mediante un sistema basado en el riesgo.

— Establecimiento de un sistema de "mejores técnicas disponibles".

— La contratación pública como mecanismo para prevenir los riesgos en el uso de algoritmos por los sectores público y privado.

— Detección de la discriminación y la desigualdad mediante algoritmos.

— Empoderar a las personas en la gestión de sus datos.

— Comunicación y cooperación entre disciplinas.

Como última puntualización, consideramos conveniente señalar la importancia de no adoptar actitudes tecnófobas. Los programas de automatización del procesamiento de datos y la toma de decisiones generan muchos efectos positivos al producir resultados más precisos y personalizados que los seres humanos en diferentes ámbitos como la medicina o la educación que derivan en importantes beneficios para las personas que, en esos contextos, interactúan con los sistemas algorítmicos. Sin embargo, como pretende apuntar este trabajo, no podemos obviar los perjuicios que pueden llegar a generarse, y ya se están generando, como consecuencia del creciente uso de estos sistemas. El ordenamiento jurídico debe actualizarse, no ya solo en su contenido, sino también en la forma y velocidad con la que responde a los problemas que se dan en la sociedad. De lo contrario, los niveles actuales de evolución tecnológica terminarán por erosionar los principios, valores y estructuras sobre los que se asientan las democracias occidentales.

BIBLIOGRAFÍA

Algorithm Register, 2020. Disponible el 9 de diciembre de 2020 en *https://algoritmeregister.amsterdam.nl/*.

Philip ALSTON, "Digital welfare states and human rights", UN Special Rapporteur on extreme poverty and human rights, informe A/74/493, 11 de octubre de 2019.

Doris ALLHUTTER *et al.*, "Algorithmic profiling of job seekers in Austria: how austerity politics are made effective", *Frontiers in Big Data*, vol. 3, 2020, pp. 1-17.

Mike ANNANY y Kate CRAWFORD, "Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability", *New Media & Society*, vol. 20, núm. 3, 2018, pp. 973-989.

Luís ARROYO JIMÉNEZ, "Algoritmos y reglamentos", *Almacén de Derecho*, 25 de febrero de 2020. Disponible el 1 de diciembre de 2020 en *https://almacendederecho.org*.

Solon BAROCAS, "Data mining and the discourse on discrimination", *Proceedings of the Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining (KDD)*, 2014, pp. 1-4.

Solon BAROCAS y Andrew SELBST, "Big data's disparate impact", *California Law Review*, vol. 104, núm. 3, 2016, pp. 671-732.

— "The intuitive appeal of explainable machines", *Fordham Law Review*, vol. 87, núm. 3, 2018, pp. 1085-1139.

Yochai BENKLER, Robert FARIS y Hal ROBERTS, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford University Press, Oxford, 2018.

Omri BEN-SHAHAR, "Data pollution", *Journal of Legal Analysis*, vol. 11, 2019, pp. 104-159.

Andrés BOIX PALOP, "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones", *Revista de Derecho Público: Teoría y Método*, vol. 1, 2020, pp. 223-270.

Stephanie BORNSTEIN, "Antidiscriminatory algorithms", *Alabama Law Review*, vol. 70, núm. 2, 2019, pp. 519-572.

Kriel BRENNAN-MARQUEZ, "'Plausible cause': explanatory standards in the age of powerful machines", *Vanderbilt Law Review*, vol. 17, núm. 4, 2017, pp. 1249-1301.

Jenna BURRELL, "How the machine 'thinks': understanding opacity in machine learning algorithms", *Big Data & Society*, vol. 3, núm. 1, 2016, pp. 1-12.

Agustí CERRILLO I MARTÍNEZ, "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", *Revista General de Derecho Administrativo*, núm. 50, 2019, pp. 1-38.

— "¿Son fiables las decisiones de las Administraciones públicas adoptadas por algoritmos?", *European Review of Digital Administration & Law*, vol. 1, núm. 1-2, 2020, pp. 18-36.

Alexandra CHOULDECHOVA, "Fair prediction with disparate impact: a study of bias in recidivism prediction instruments", 2016, pp. 1-17. Disponible el 6 de diciembre de 2020 en *https://arxiv.org*.

Danielle CITRON, "Technological due process", *Washington University Law Review*, vol. 85, núm. 6, 2008, pp. 1249-1313.

Cary COGLIANESE y David LEHR, "Regulating by robot: administrative decision making in the machine-learning era", *The Georgetown Law Journal*, vol. 105, núm. 5, 2017, pp. 1147-1223.

Comisión Europea, "Comunicación de la Comisión sobre el recurso al principio de precaución", COM/2000/0001 final, 1 de febrero de 2000.

— "Defensa de la competencia: la Comisión impone una multa a Google de 1,49 miles de millones de euros por prácticas abusivas en la publicidad en línea", 20 de marzo de 2019. Disponible el 8 de diciembre de 2020 en *https://ec.europa.eu.*

— "Libro blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza", COM (2020) 65 final, 19 de febrero de 2020.

Josh CONSTINE, "Facebook is shutting down its API for giving your friends' data to apps", *TechCrunch*, 28 de abril de 2015. Disponible el 8 de diciembre de 2020 en *https://techcrunch.com*.

Lorenzo COTINO HUESO, "«SyRI, ¿a quién sanciono?» Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", *La Ley Privacidad*, núm. 4, 2020.

Datenethikkommission, "Gutachten der Datenethikkommission", 2019.

—"Opinion of the Data Ethics Commission: Executive Summary", 2019.

Javier DE LA CUEVA, "Código fuente, algoritmos y fuentes del derecho", *El Notario del Siglo XXI*, núm. 77, 2018.

—"El derecho a no ser gobernados mediante algoritmos secretos", *El Notario del Siglo XXI*, núm. 87, 2019.

Susana de la SIERRA MORÓN, "Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la Administración pública", *Revista General de Derecho Administrativo*, núm. 53, 2020, pp. 1-19.

Gabriel DOMÉNECH PASCUAL, *Derechos Fundamentales y Riesgos Tecnológicos*, Centro de Estudios Políticos y Constitucionales, Madrid, 2006.

José ESTEVE PARDO, *Lecciones de Derecho Administrativo*, 6.ª ed. Marcial Pons, Barcelona, 2016.

Virginia EUBANKS, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St Martin's Press, Nueva York, 2017.

Michael FELDMAN *et al.*, "Certifying and removing disparate impact", *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2015, pp. 259-268.

Eduardo GARCÍA DE ENTERRÍA y Tomás-Ramón FERNÁNDEZ RODRÍGUEZ, *Curso de Derecho Administrativo I*, Thomson Reuters–Aranzadi, Cizur Menor (Navarra), 2020, pp. 496-500.

Janneke GERARDS, "The discrimination grounds of article 14 of the European Convention on Human Rights", *Human Rights Law Review*, vol. 13, núm. 1, 2013, pp. 99-124.

Grupo de Trabajo del Artículo 29, "Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679", 17/ES, WP 251rev.01, 6 de febrero de 2018.

Bryce W. GOODMAN, "A step towards accountable algorithms?: Algorithmic discrimination and the European Union general data protection", *29th Conference on Neural Information Processing Systems*, 2016. Disponible el 9 de diciembre de 2020 en *http://www.mlandthelaw.org.*

Alejandro HUERGO LORA, "Una aproximación a los algoritmos desde el Derecho administrativo", en Alejandro Huergo Lora (dir.) y Gustavo Manuel Díaz González (coord.), *La Regulación de los Algoritmos*, Pamplona, Aranzadi, 2020, pp. 23-87.

Margot KAMINSKI, "Binary governance: Lessons from the GDPR's approach to algorithmic accountability", *Southern California Law Review*, vol. 92, núm. 6, 2019, pp. 1529-1616.

Cecilia KANG y Mike ISAAC, "U.S. and States Say Facebook Illegally Crushed Competition", *New York Times*, 9 de diciembre de 2020. Disponible el 10 de diciembre de 2020 en *https://www.nytimes.com.*

Nancy KIM y Jeremy TELMAN, "Internet giants as quasi-governmental actors and the limits of contractual consent", *Missouri Law Review*, vol. 80, núm. 3, 2015, pp. 723-770.

Spyros KOKOLAKIS, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", *Computers & Security*, vol. 107, 2017, pp. 122-134.

Bert-Jaap KOOPS, "The problem with European data protection law", *International Data Privacy Law*, vol. 4, núm. 4, 2014, pp. 250-261.

Lawrence LESSIG, *Code: Version 2.0*, Basic books, Nueva York, 2006.

Steve LOHR, "Sizing up big data, broadening beyond the Internet", *The New York Times BITS Blog*, 29 de junio de 2013. Disponible el 6 de diciembre de 2020 en *https://bits.blogs.nytimes.com.*

Stella LOWRY y Gordon MACPHERSON, "A blot on the profession", *British Medical Journal*, 5 de marzo de 1988, pp. 657-658.

Isaac MARTÍN DELGADO, "Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada", *Revista de Administración Pública*, núm. 180, 2009, pp. 353-386.

M.ª Dolores MAS BADÍA, "Credit-based insurance scores: some observations in the light of the european general data protection regulation", *Cuadernos Europeos de Deusto*, núm. 62, 2020, pp. 155-186.

Juan Francisco MESTRE DELGADO, "Una reflexión sobre la regulación constitucional del Derecho administrativo", *Corts: Anuario de Derecho Parlamentario,* núm. extra 31, 2018, pp. 367-386.

Javier MIRANZO DÍAZ, "Inteligencia artificial y contratación pública", en Isaac Martín Delgado y Jose Antonio Moreno Molina (dirs.), A*dministración electrónica, transparencia y contratación pública*, Madrid, Iustel, 2020, pp. 105-142.

Alex MILLER, "Want less-biased decisions? Use algorithms", *Harvard Business Review*, 26 de Julio de 2018. Disponible el 6 de diciembre de 2020 en *https://hbr.org.*

Brendt MITTELSTADT *et al.*, "The ethics of algorithms: mapping the debate", *Big Data & Society*, julio-diciembre 2016, pp. 1-21.

Jerrold NADLER y David CICILLINE, "Investigation of competition in digital markets", Subcommittee on antitrust, commercial and administrative law of the Committee on the judiciary, octubre 2020.

Safiya NOBLE, *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York University Press, New York, 2018.

Cathy O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin Books, Londres, 2017.

Paul OHM, "Broken promises of privacy: responding to the surprising failure of anonymization", *UCLA Law Review*, vol. 57, 2010, pp. 1701-1777.

Angelo Giuseppe OROFINO, "The Implementation of the Transparency Principle in the Development of Electronic Administration", *European Review of Digital Administration & Law*, vol. 1, No. 1-2, 2020, pp. 123-142.

Marion OSWALD, "Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power", *Philosophical Transactions of the Royal Society of London, Series A: Mathematical and Physical Sciences*, vol. 376, núm. 2128, 2018, pp. 1-20.

Adrián PALMA ORTIGOSA, "Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos", *Revista General de Derecho Administrativo*, núm. 50, 2019.

Roger PARLOFF, "Why deep learning is suddenly changing your life", *Fortune*, 28 de septiembre 2016. Disponible el 2 de diciembre de 2020 en *http://fortune.com.*

Julio PASCUAL Y VICENTE, "Prohibiciones del abuso de posición dominante" en *Tratado de Derecho de la competencia*, José María Beneyto Pérez (dir.) y Jerónimo Maillo González (coord.), Bosch, Barcelona, 2005, pp. 455-511.

Juli PONCE SOLÉ, "El derecho a una buena administración y la personalización de los servicios públicos" en Beltrán Puentes Cociña y Andrei Quintiá Pastrana, (dirs.), *El Derecho ante la Transformación Digital*, Barcelona, Atelier, 2019, pp. 51-71.

— "Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", *Revista General de Derecho Administrativo*, núm. 50, 2019, pp. 1-52.

Sofia RANCHORDÁS y Ymre SCHUURMANS, "Outsourcing the welfare state: the role of private actors in welfare fraud investigations", *European Journal of Comparative Law and Governance*, vol. 7, núm. 2, 2020, pp. 5-42.

Ariel RUBINSTEIN, "Dilemmas of an economic theorist", *Econometrica*, vol. 74, núm. 4, 2006, pp. 865-883.

Matthew SCHERER, "Regulating artificial intelligence systems: risks, challenges, competencies, and strategies", *Harvard Law & Technology Journal*, vol. 29, núm. 2, 2016, pp. 353-400

Bart SCHERMER, "The limits of privacy in automated profiling and data mining", *Computer Law & Security Review*, vol. 27, No. 1, 2011, pp. 45-52.

Wim SCHREURS *et al.*, "Cogitas, ergo sum. the role of data protection law and non-discrimination law in group profiling in the private sector" en Mireille Hildebrandt y Serge Gutwirth, *Profiling the European Citizen*, Springer, Berlín, 2008, pp. 241-270.

Sam SHEAD, "Google DeepMind is giving the NHS free access to its patient monitoring app", *Business Insider*, 24 de junio de 2017. Disponible el 10 de diciembre 2020 de *https://www.businessinsider.de.*

Ben SHNEIDERMAN, "Algorithmic Accountability: Designing for safety through human-centered independent oversight", *Turing Lecture (The Alan Turing Institute)* 31 de marzo de 2017. Disponible el 26 de noviembre de 2020 en *https://www.youtube.com.*

Alba SORIANO ARNANZ, "Decisiones automatizadas y discriminación: aproximación y propuestas generales", *Revista General de Derecho Administrativo*, núm. 56, 2021.

Cass SUNSTEIN, "Sludge and ordeals", *Duke Law Review*, vol. 68, núm. 8, 2018, pp. 1843-1883.

Adrián TODOLÍ SIGNES, "Retos legales del uso del *big data* en la selección de sujetos a investigar por la Inspección de Trabajo y de la Seguridad Social", *Revista Galega de Administración Pública*, núm. 59, 2020, pp. 313-337.

Andrew TUTT, "An FDA for algorithms", *Administrative Law Review*, vol. 69, núm. 1, 2017, pp. 83-123.

Amos TVERSKY y Daniel KAHNEMAN, "Judgment under uncertainty: heuristics and biases", *Science*, vol. 147, núm. 4157, 1974, pp. 1124-1131.

Karen YEUNG, "'Hypernudge': Big data as a mode of regulation by design", *Information, Communication & Society*, vol. 20, núm. 1, 2017, pp. 118-136.

Karen YEUNG y Martin LODGE, "Algorithmic regulation: an introduction", en Karen Yeung y Martin Lodge (eds.), *Algorithmic regulation*, Oxford University Press, Oxford 2019, pp. 1-18.

Julián VALERO TORRIJOS, "Inteligencia artificial y contratación del sector público", *Observatorio de Contratación Pública*, 27 de enero de 2020.

— "The legal guarantees of artificial intelligence in administrative activity: reflections and contributions from the viewpoint of Spanish administrative law and good administration requirements", *European Review of Digital Administration & Law*, vol. 1, No. 1-2, 2020, pp. 55-62.

Marlies VAN ECK, "Algorithms in public administration", 31st January 2017. Disponible el 17 de julio de 2019 en *https://marliesvaneck.wordpress.com.*

Clara VELASCO RICO, "Vigilando al algoritmo. Propuestas organizativas para garantizar la transparencia", en Beltrán Puentes Cociña y Andrei Quintiá Pastrana (dirs.), *El Derecho ante la Transformación Digital*, Barcelona, Atelier, 2019, pp. 73-89.

Sandra WACHTER y Brendt MITTELSTADT, "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI", *Columbia Business Law Review*, vol. 2019, núm. 2, 2019, pp. 494-620 (p. 499).

Tal ZARSKY, "Transparent predictions", *University of Illinois Law Review*, vol. 2013, núm. 4, 2013, pp. 1503-1570.

Indrė ŽLIOBAITĖ y Bart CUSTERS, "Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models", *Artificial Intelligence & Law*, vol. 24, núm. 2, 2016, pp. 183-201.