EL USO DE ALGORITMOS Y SU IMPACTO EN LOS DATOS PERSONALES

THE USE OF ALGORITHMS AND THEIR IMPACT ON PERSONAL DATA

ALEJANDRO HUERGO LORA[1]

RESUMEN

En el presente artículo se abordan las principales concepciones del término "algoritmo" y cómo el mismo es aplicado en el ámbito jurídico. Asimismo, se explica su relación con las predicciones basadas en datos y con los conceptos de inteligencia artificial digitalización y automatización, explicando sus principales características y diferencias. Posteriormente, se evalúa la aplicación de la inteligencia artificial en la creación y aplicación del Derecho. Después se analiza la injerencia de la regulación de datos personales en la utilización de algoritmos y el rol de la administración pública. Finalmente, se analizan los pormenores del proyecto del Reglamento sobre la Inteligencia Artificial.

PALABRAS CLAVE

Algoritmos | Predicción | Regulación | Datos | Administración

ABSTRACT

This article addresses the main conceptions of the term "algorithm" and how it is applied in the legal field. It also explains its relationship with data-driven predictions and with the concepts of artificial intelligence digitization and automation, explaining their main characteristics and differences. Subsequently, the application of artificial intelligence in the creation and application of the Law is evaluated. Then the interference of the regulation of personal data in the use of algorithms and the role of public administration is analyzed. Finally, the details of the draft Regulation on Artificial Intelligence are analyzed.

KEYWORDS

Algorithms | Prediction | Regulation | Data | Administration

CONTENIDO

1 Licenciado en Derecho por la Universidad de Oviedo y Doctor en Derecho por la Universidad de Bolonia. Ha sido investigador en la Universidad de Múnich tras ser el primer jurista español que obtuvo una beca postdoctoral del programa Marie Curie de la Unión Europea. Actualmente, se desempeña como catedrático de la Universidad de Oviedo desde 2010 y también imparte docencia en múltiples estudios de posgrado de diversas universidades españolas. Sus temas más habituales son las sanciones administrativas, los contratos públicos y el contencioso-administrativo. Ha dirigido el libro La regulación de los algoritmos (2020, con coordinación de Gustavo Manuel Díaz González). Contacto: ahuergo@uniovi.es

sometidas a autorización; **5.3.** Aplicaciones de la IA para las que se establecen reglas concretas de transparencia; **5.4.** Aplicaciones de la IA "de alto riesgo" y sus mecanismos de control; **5.5** Otras previsiones; **5.6.** Lo que regula y lo que no regula el proyecto de Reglamento.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 14 de junio de 2021 y aprobado para su publicación el 16 de agosto de 2021.

1. ALGORITMOS: UN CONCEPTO DEMASIADO AMPLIO

"Algoritmo" es una palabra de uso reciente en español, que parece muy ligada a los problemas y retos que plantea la inteligencia artificial o el *big data*. Sin embargo, no es exactamente así, y por ello creo que no es correcto hablar de un "régimen jurídico" o "naturaleza jurídica" de los algoritmos (o predicados similares), porque el término es demasiado impreciso.[2]

Aunque el uso de la palabra "algoritmo" en español es, como acabo de decir, reciente, y está ligado a la informática, en realidad tiene el mismo origen o raíz que la palabra "guarismo", mucho más antigua y con un significado matemático, pero alejado del mundo de la inteligencia artificial o la informática. En realidad, parece que la palabra viene del nombre del matemático Mohamed ben Musa *al Juarismi* (que se supone que vivió entre 780 y 850, y trabajó fundamentalmente en Bagdad), y, de hecho, Juarismi sería la localidad de la que procedía, situada en el actual Uzbekistán (existe la palabra "Corasmia" para traducir ese toponímico). Al Juarismi ha tenido una gran influencia en la historia de las matemáticas y se le considera el creador del álgebra.[3]

En todo caso, el origen inmediato de la palabra "algoritmo" es la inglesa "algorithm", que hace referencia a cualquier procedimiento formalizado en una serie de pasos para solucionar un problema o conseguir un resultado. Aunque puede haber (y hay) algoritmos al margen de los ordenadores, es decir, algoritmos no gestionados por ordenadores, lo cierto es que la palabra algoritmo se ha desarrollado (y ha llegado a la lengua castellana) en relación con la informática, pues los ordenadores necesitan ser programados y un programa de ordenador consiste, precisamente, en una sucesión ordenada de pasos que el ordenador ha de llevar a cabo. Los seres humanos pueden actuar mediante algoritmos o no; los ordenadores sólo pueden funcionar siguiendo un algoritmo.

Los "procedimientos" administrativos o judiciales son, al menos en cierto modo, algoritmos, en la medida en que se componen de pasos dotados de un contenido determinado, que han de seguirse para llegar a una solución (la resolución o acto final del procedimiento). La semejanza con los programas informáticos es, sin embargo, limitada, porque el tipo de vinculación que lleva al instructor o tramitador del procedimiento a seguir sus fases no tiene el mecanicismo de un programa informático, sino que se trata de una vinculación jurídica. Al tramitar el procedimiento, el instructor sigue, voluntariamente, una norma jurídica. El programa no hace más que "obedecer" inconscientemente las órdenes que aparecen en el programa. Del mismo modo, mientras que en un programa es sencillamente imposible que se llegue al resultado final sin seguir todos los pasos o fases

2 De las cuestiones de que trata este artículo me he ocupado por extenso en "Una aproximación a los algoritmos desde el Derecho administrativo", en Huergo Lora, Alejandro (Dir.) / Díaz González, Gustavo Manuel (Coord.), *La regulación de los algoritmos*, Aranzadi, Cizur Menor, 2020, págs. 23-87, obra a la que remito a los lectores interesados.

3 BREZINA, C., *Al-Khwarizmi: The Inventor of Algebra*, Rosen Central, 2005.

(el programa "se colgaría" y no podría avanzar), en un procedimiento administrativo sí se puede dictar la resolución omitiendo (o ejecutando incorrectamente) alguna de las fases, y los efectos de esa omisión se determinarán con arreglo a una normas jurídicas (valorando, por ejemplo, la indefensión o los efectos de esa omisión sobre el contenido de la resolución final) y no en función de reglas mecánicas o puramente formales.

Si aplicamos este concepto al Derecho, existe una primera manifestación de los algoritmos jurídicos, que es la más sencilla y a la que estamos plenamente acostumbrados, aunque no se le haya dedicado una especial atención. Es frecuente que la Administración utilice programas o aplicaciones para llevar a cabo tareas concretas, es decir, para aplicar normas jurídicas o tramitar procedimientos. Un ejemplo sencillo, que en este caso manejan los ciudadanos y no la Administración, es el programa utilizado para elaborar la declaración del IRPF (durante bastantes años denominado "programa PADRE" y ahora "renta Web"). El contribuyente introduce los datos y el programa rellena las casillas de la declaración y establece el resultado, que el contribuyente firma, dotándolo así de efectos jurídicos. Las normas (en este caso, la Ley y el reglamento del IRPF, así como la legislación autonómica) han sido "volcadas" en un programa informático, algo que en este caso resulta en principio sencillo porque se trata de normas regladas. Las dudas que pueden surgir (por ejemplo, sobre la calificación jurídica de determinados ingresos, si son renta del trabajo o de actividades económicas, o están exentos) las resuelve, bajo su responsabilidad, el contribuyente al introducir los datos (aunque a veces el programa fuerza esas decisiones al admitir sólo una opción).

Este tipo de algoritmos no sustituyen a la norma, obviamente, sino que la traducen para facilitar su aplicación. Cuando un funcionario crea una hoja Excel en la que introduce los datos y efectúa los cálculos necesarios para, por ejemplo, liquidar los intereses de un justiprecio expropiatorio, está utilizando un algoritmo. En este caso, claramente no es necesario que la norma prevea o autorice la creación y aplicación del algoritmo. Por otro lado, sus posibles errores (es decir, la infidelidad en la traducción de la norma, por la eventual falta de incorporación al mismo de algunas de las opciones contempladas por ésta, o porque exista algún defecto que dé lugar a un resultado incorrecto o sesgado) darán lugar a la invalidez de sus resultados, porque lo único que importa y que tiene validez jurídica es la norma, no el algoritmo. Una liquidación tributaria preparada por un algoritmo pero que no se ajusta a la legislación aplicable es, obviamente, contraria a Derecho y así tendrá que declararse en cualquier procedimiento de impugnación, sin que tenga la menor relevancia que el error haya surgido al programar el algoritmo o al introducir los datos (en una operación manual de un funcionario).

En la práctica pueden surgir problemas, en la medida en que, por razones jerárquicas, los funcionarios se vean obligados a utilizar una aplicación que no se ajuste al marco jurídico. Ocurre a veces que el algoritmo está mal diseñado y calcula erróneamente el resultado o que no permite incorporar datos que son jurídicamente relevantes en la aplicación de la norma. Puede suceder que, de hecho, la comodidad del algoritmo induzca a sus usuarios a no comprobar la corrección del resultado, de forma que, aunque el algoritmo no prevalece sobre la norma, y los resultados que no se ajusten a la norma sean ilegales, en muchos casos prevalezca el algoritmo sobre la Ley. Todo indica que en estos casos el problema no es acceder al código del programa, sino conseguir que se aplique la norma por encima del error del algoritmo.

Este tipo de algoritmos se utilizan con frecuencia y a veces han llegado a los tribunales. Ya hace bastantes años se utilizaban programas informáticos para efectuar sorteos, por ejemplo, para determinar los tribunales que habían de juzgar los concursos de acceso a plazas de profesorado universitario. El programa permitía automatizar un proceso

(el sorteo) que es totalmente reglado pero que puede tener cierta complejidad porque los distintos miembros del tribunal proceden de conjuntos o colectivos diferentes. Algo así sucede en el programa utilizado para elegir, de entre los profesores solicitantes, a los miembros de los tribunales de las pruebas de acceso a la universidad, que en Cataluña ha dado lugar a una resolución de la autoridad de transparencia. (Comissió de Garantia del Dret D' Accéss a la Informació Pública [GAIP], 21 de setiembre de 2016). En esta misma línea, en Italia varias sentencias han anulado las resoluciones del concurso de traslados de personal docente, que era decidido en aplicación de un algoritmo que "casaba" las diferentes solicitudes, supuestamente en aplicación de los criterios previstos en las normas.[4] En España, un ejemplo reciente y muy polémico se ha producido en relación con el proceso de elección de plazas de formación como Médicos Internos Residentes (MIR). Estas plazas se asignan en función de la puntuación obtenida en un examen previo, por lo que se trata de un proceso perfectamente reglado. En 2020, se acordó, mediante Orden ministerial, que el proceso de elección no se haría de forma presencial (los aspirantes eligen por orden de puntuación), sino telemática (en años anteriores el aspirante podía optar entre la elección personal o telemática), lo que significa que los aspirantes presentarán una lista de peticiones y el programa hará la asignación en función de su puntuación. Aunque el sistema es, en principio, equivalente, otorga menos capacidad de elección a los aspirantes, que en la vía presencial pueden, por ejemplo, dejar pasar a otros aspirantes para poder elegir a la vez que una persona con quien quieran hacer la residencia, y tienen la garantía de conocer, en el momento de la elección, qué plazas están a su disposición, en lugar de formular al principio una serie de peticiones hipotéticas. Formulado recurso, el Tribunal Supremo concedió, en primer lugar, la suspensión cautelar (por lo que el sistema telemático no se aplicó) y después anuló la Orden, básicamente por razones formales (rango normativo), en sentencia de 13 de abril de 2021 (recurso 150/2020). Otro ejemplo es el programa "Euphemia", con el que, en el mercado eléctrico europeo, se casa la oferta y la demanda y se fijan los intercambios que deben producirse en cada momento entre los distintos sistemas nacionales para que el precio sea óptimo.[5] También en relación con la electricidad, pero ahora no para determinar el precio en un mercado, sino para aplicar la norma que establece los requisitos para disfrutar del bono social, debe mencionarse el programa creado por el Ministerio competente, que en este momento es objeto de un recurso contencioso-administrativo en el que se solicita su difusión pública.[6]

A veces el algoritmo está en la propia norma, cuando ésta especifica la fórmula que debe aplicarse para llegar al resultado final: por ejemplo, en revisiones de precios (contratos), actualizaciones de tarifas (concesiones) o, con frecuencia, para la distribución de recursos escasos (ponderación de notas y otros méritos para la asignación de becas, por ejemplo). En estos casos se trata de algoritmos en el sentido de fórmulas o baremos que establecen la consecuencia jurídica a partir de un determinado supuesto de hecho, y es indiferente el modo técnico en que se aplique la fórmula (elaboración de una aplicación informática, aplicación de la fórmula a cada caso concreto por un funcionario, etc.).

4 Resoluciones del TAR de Lazio, de 10 de septiembre de 2018 (número 9227) y del Consejo de Estado decisión 2270/2019, publicada el 8 de abril de 2019). Serán analizadas *infra*.

5 Una descripción en https://www.n-side.com/pcr-euphemia-algorithm-european-power-exchanges-price-coupling-electricity-market/.

6 Se trata del procedimiento ordinario 18/2019, ante el Juzgado Central de lo Contencioso-Administrativo número 8.

2. CÓMO FUNCIONAN LAS PREDICCIONES BASADAS EN DATOS ("MACHINE LEARNING")

En realidad, el fenómeno realmente novedoso no son los algoritmos, sino las predicciones basadas en datos, que constituyen el producto o resultado de un tipo determinado de algoritmos que podemos denominar algoritmos predictivos.

Es imprescindible una visión, aunque sea sintética, de qué son y cómo funcionan las previsiones basadas en datos[7]. En esencia, se trata de analizar -con la utilización de algoritmos- grandes cantidades de datos relativos a un determinado fenómeno, para extraer correlaciones que nos lleven a producir, como resultado final, predicciones de hechos futuros.

Pensemos en el ejemplo del crédito, de la actividad de otorgamiento de préstamos. Toda entidad financiera intenta evitar la morosidad, porque cada préstamo no devuelto reduce sus beneficios. En el modelo tradicional, la decisión de conceder -o no- financiación se basa en múltiples criterios, algunos de los cuales están establecidos formalmente (por ejemplo, no estar incluido en una lista de morosos, o disponer de una garantía inmobiliaria o de un contrato de trabajo) mientras que otros son informales, puesto que la decisión final queda en manos de empleados que tendrán en cuenta todo tipo de "impresiones". En definitiva, se trata de una mezcla entre criterios "razonados" (es decir, explicables racionalmente) y criterios subjetivos (el "ojo clínico" del empleado, que puede perder su prestigio dentro de la empresa si una operación importante resulta fallida).

El nuevo enfoque basado en los algoritmos parte de analizar una gran cantidad de datos (=*big data*) sobre operaciones anteriores (fallidas y exitosas). Datos relativos a los prestatarios (edad, profesión, titulación académica, domicilio, nivel de renta, hábitos de consumo, historial crediticio, etc.) y a las operaciones realizadas (capital, plazo, canal de comunicación con el cliente, tiempo dedicado a la negociación…). A veces los datos proceden del propio banco o son suministrados por el cliente al solicitar el préstamo, pero también pueden proceder de terceros (aseguradoras, empresas energéticas, de telecomunicaciones, redes sociales, etc.). Cada dato está "etiquetado", es decir, sabemos qué personas han pagado sus créditos y cuáles otras no lo han hecho, de modo que cada dato personal (haber visitado determinada página, haber terminado el doctorado) se corresponde con haber demostrado solvencia o no haberlo hecho. Dicho de otro modo: tenemos miles de datos de las operaciones que han salido bien y de las que han salido mal. A partir de aquí, el algoritmo "remueve" esos datos, cruzándolos una y otra vez en todas las direcciones posibles, para establecer correlaciones. Algunas pueden ser más o menos obvias (a mayor nivel de renta del prestatario, más probabilidad de que se devuelva el préstamo), pero otras no tanto (por ejemplo, puede existir una correlación entre haber tenido muchos siniestros de tráfico comunicados a la aseguradora, y no pagar un crédito).

Otro ejemplo muy gráfico es el aprendizaje de idiomas. En el sistema tradicional, se aprenden las reglas de la gramática y de la pronunciación (previamente inducidas por expertos filólogos a partir del uso hablado y escrito del idioma), así como una cantidad suficiente de vocabulario, y de ese modo se aprende a formular frases correctas. Con

7 De entre los múltiples textos no jurídicos que pueden servir para obtener esa introducción, cabe citar MAYER-SCHÖNBERGER, V.; CUKIER, K., *Big data. La revolución de los datos masivos*, Turner, Madrid, 2013 (el libro original también se publicó en 2013) y LEE, K. F., *AI Superpowers. China, Silicon Valley and the New World Order*, Houghton Mifflin Harcourt, Boston-New York, 2018.

algoritmos predictivos se puede crear un traductor de un idioma a otro por una vía distinta. Se le proporciona al sistema un *corpus* enorme de textos escritos en los dos idiomas (por ejemplo, todos los textos normativos de la UE, que están publicados en todos los idiomas oficiales y se sabe que son equivalentes), de forma que, tras cruzar todos esos textos con la ayuda de algoritmos, el ordenador descubre, por ejemplo, a qué palabra inglesa equivale cada palabra española cuando aparece en un contexto determinado, y así puede ofrecer la correspondiente traducción. Como vemos, es el mismo método que permitió descifrar el lenguaje jeroglífico egipcio a partir de la piedra Rosetta, pero a una escala enorme, de modo que tanto la gran cantidad de datos utilizados como la entrada en juego de algoritmos nos permiten prescindir (hasta cierto punto) de Champollion.

Estos modelos son muy complejos y lo normal es que tengan en cuenta muchas variables, no sólo una. El resultado final es que, combinando todos los factores que se ha observado que tienen una correlación con la solvencia o, dicho de otro modo, que ayudan a predecir si el crédito será devuelto o no, y combinándolos entre sí en la proporción que resulta del modelo, obtenemos una "fórmula" que se puede aplicar a quien solicita un préstamo. Así, introduciendo los datos relevantes de esa persona (su titulación académica, su historial asegurador, etc.), obtendremos un resultado que nos indicará su propensión a ser buen o mal pagador, y ese dato podrá ser tenido en cuenta para conceder o denegar el crédito.

En unos casos, la decisión será automática (es decir, sin intervención humana) a la vista del resultado que proporciona el algoritmo, mientras que en otros ese resultado será una especie de "informe" que un humano (el encargado de tomar la decisión) tendrá en su mano y al que dará la importancia que considere adecuada.

Lógicamente, la predicción está sujeta a error, puesto que se basa en un modelo matemático que puede estar mal construido y que además depende de unos datos que pueden no predecir adecuadamente el futuro, como sucede, por ejemplo, si se producen cambios importantes desde el momento del que proceden los datos al momento en que hay que aplicar la predicción (por ejemplo, si intentamos predecir la evolución del PIB de 2020 con un modelo que funcionó en años anteriores pero que no tiene en cuenta el COVID-19). En el mundo real eso no es un problema: sencillamente, si las predicciones no funcionan dejan de ser usadas y se les hace el mismo caso que a los horóscopos publicados en los periódicos o a los sesudos gráficos que intentan predecir las cotizaciones bursátiles, que con frecuencia tienen el mismo grado de fiabilidad. El problema surge con las predicciones que no pueden ser verificadas. Por ejemplo: si el algoritmo recomienda otorgar un préstamo a una empresa y ésta no lo devuelve, queda claro que el algoritmo falla, y si los fallos abundan, dejará de utilizarse. Pero si el algoritmo recomienda no conceder un préstamo a una persona, y efectivamente no se le concede, es más difícil saber si el algoritmo ha fallado o no, porque no podemos saber si esa persona habría devuelto el crédito. Esto puede producir situaciones de indefensión (para quienes, por seguir el ejemplo, no reciben préstamos pese a que podrían haberlos devuelto). A la vez, como hay situaciones excepcionales que, precisamente por su excepcionalidad, no se tienen en cuenta en los cálculos, y con las que no se cuenta porque no suceden casi nunca y llegan a ser olvidadas, parece que el algoritmo es infalible y que se puede confiar ciegamente en él, lo que puede llevar a un exceso de confianza injustificada que a veces produce resultados catastróficos.[8]

8 En general, sobre la confianza en modelos matemáticos no comprobables que se utilizan para ganar seguridad en la toma de decisiones de riesgo, y los peligros a que puede llevar esa confianza (verificados, sin ir más lejos, en la crisis económica de 2008 y ahora en el caso del coronavirus), es fundamental la referencia a TALEB y su tetralogía *Incerto*, de entre la que

Podemos poner algunos ejemplos jurídicos. El programa COMPAS es uno de los más utilizados en Estados Unidos por los tribunales para determinar si se concede o no la libertad provisional (bien en la propia sentencia, o después). El programa analiza múltiples criterios que se supone que ayudan a predecir si un sujeto va a ser reincidente o no. No se trata de un "baremo" al uso, porque no son criterios establecidos en una norma, sino que han sido deducidos por un algoritmo a partir de experiencias anteriores, y están sujetos a modificación en función de los nuevos datos que se suministren. Una conocida sentencia del Tribunal Supremo de Wisconsin (asunto Loomis) acepta que los tribunales utilicen el informe suministrado por este programa para determinar sus sentencias, siempre que lo hagan junto con otros criterios. (Tribunal Supremo de Wisconsin, 13 de julio de 2016). En la Administración penitenciaria autonómica catalana se utiliza un programa muy parecido, denominado RISCANVI, para otorgar o denegar permisos penitenciarios, y existe una abundante jurisprudencia que, en sentido muy similar a la sentencia de Wisconsin, 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.[9] Es muy frecuente que las Administraciones encargadas de perseguir el fraude o el incumplimiento de normas, utilicen, incluso sin que una norma lo prevea o autorice, aplicaciones que, analizando datos, ayuden a descubrir casos en los que se pueda estar cometiendo un fraude y sea conveniente iniciar un procedimiento.[10] No sólo eso, sino que hay Leyes que prevén la utilización de ese tipo de sistemas para detectar casos en los que pueda ser procedente la iniciación de un procedimiento.[11] Recientemente, el Tribunal de Distrito de

---

cabe destacar *El cisne negro* (el libro original es de 2007, la traducción española se publicó en Paidos, 2008) y la última parte, *Skin in the game*, Random House, New York, 2018.

9 Sobre el programa RISCANVI, FÉREZ-MANGAS, D.; ANDRÉS-PUEYO, A., "Eficacia predictiva en la valoración del riesgo del quebrantamiento de permisos penitenciarios", *La Ley Penal*, 1342 (2018), así como la entrevista http://www.fbg.ub.edu/es/actualidad/antonio-andres-pueyo-reto-riscanvi-detectar-que-interno-tiene-alto-riesgo-reincidencia/ (20 de enero de 2020). Como ejemplos de aplicación jurisprudencial pueden citarse los autos de la AP de Girona de 16 de noviembre de 2018 (recurso 890/2018) y 20 de diciembre de 2018 (recurso 974/2018). En ambas se lee: "ya hemos dicho en otras ocasiones que la forma que creemos más oportuna para valorar el RISCANVI no es la consistente en enmascarar los resultados ofrecidos por el algoritmo de manera automática tras la introducción de los datos de los que el test se compone, sino la de proporcionar posteriormente una explicación acerca de la fiabilidad de dichos datos, que creemos que se produce aludiendo a los meritados factores estáticos que no varían pese al transcurso del tiempo, por lo que las tendencias serán siempre medias o altas. Así ocurre en este caso por cuestiones relativas a los numerosos delitos cometidos de la misma tipología y por la existencia de una causa fundada en la drogadicción".

10 De este tipo de aplicaciones nos enteramos con noticias como https://www.lne.es/noticias-suscriptor/economia/2018/08/26/arsenal-algoritmos-fraude/2338570.html (26 de agosto de 2018), https://blogs.elconfidencial.com/economia/big-data/2018-07-14/patrones-comportamiento-voracidad-fiscal_1592433/ (14 de julio de 2018), entre otras.

11 Un ejemplo es la Ley de la Comunidad Valenciana 22/2018, de 6 de noviembre, de Inspección General de Servicios y del sistema de alertas para la prevención de malas prácticas en la Administración de la Generalitat y su sector público instrumental. Se regula un sistema de alertas (artículo 17) que básicamente analiza la información que tiene la propia Administración autonómica, y la que sus titulares hayan proporcionado libremente en internet (por ejemplo, mediante su participación en redes sociales), y suministra datos que pueden servir para la iniciación de una actuación de investigación (artículo 30). Sobre esta Ley, pronosticando su posible inconstitucionalidad a partir de la sentencia holandesa que se cita en la nota siguiente, COTINO, L., "«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*, Wolters Kluwer, 4 (2020).

La Haya ha decidido que un sistema similar (denominado SYRI) es contrario al derecho a la intimidad reconocido en el artículo 8 del CEDH.[12]

Veíamos antes cómo, en la forma "tradicional" de tomar decisiones, los criterios son, o bien racionales (es decir, criterios basados en algún razonamiento, algún principio) o bien irracionales, subjetivos (el "ojo crítico", la "sana crítica", etc.), a los que se recurre cuando se considera que hay factores imposibles de racionalizar, y que normalmente tienen como consecuencia que la decisión se encomienda a personas muy concretas que tienen la formación y/o la experiencia que supuestamente las convierte en idóneas para tomar esa clase de decisiones.[13]

En el mundo de los algoritmos predictivos y las predicciones basadas en datos, esto cambia por completo. Desaparecen las decisiones subjetivas o irracionales, siendo sustituidas por predicciones basada en correlaciones descubiertas analizando gran cantidad de datos referidos a operaciones anteriores. Pero también son desplazados los criterios "racionales", derivados de principios o argumentos, porque las predicciones algorítmicas sustituyen la causalidad por la correlación.[14]

Este es un punto fundamental al que es imprescindible prestar más atención. Estamos acostumbrados a que las decisiones se tomen en función de criterios razonados, explicables, lo que nos remite a juicios de causalidad o de tipo normativo. Se opta por un determinado camino porque nos llevará al objetivo al ser el más coherente con los principios que se aplican en esa actividad, el recomendado por "la doctrina", el que resulta de "la teoría", etc. En cambio, los algoritmos predictivos suponen una nueva perspectiva. Simplemente se analiza el pasado (gran cantidad de datos referidos a experiencias anteriores, de las que sabemos qué resultado produjeron) y se extraen correlaciones, es decir, se identifica (automáticamente) qué características o grupos de características han llevado a los mejores resultados, y se toman esos criterios como base para las decisiones.[15] Un ejemplo de aplicación de esta técnica es la creación de *tests* "baratos" o "sucios" para la detección de enfermedades o de otro tipo de situaciones, que, en lugar de identificar el patógeno o el hecho en sí que se está buscando (lo que puede ser caro), buscan otros datos que "normalmente" coinciden con aquel.[16]

---

12 Sentencia de 5 de febrero de 2020 del Tribunal de Distrito de La Haya (ECLI:NL:RBDHA:2020:1878). El texto, con enlace a la versión en inglés, es accesible en https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865.

13 Para una revisión crítica de esa confianza en "el sentido común", el "ojo clínico" y otras expresiones con las que se proporciona cobertura o justificación a la confianza en la decisión no objetivable de los expertos, KAHNEMAN, D., *Thinking, fast and slow*, Penguin, 2012 (el libro se publicó originalmente en 2011; hay traducción española: *Pensar rápido, pensar despacio*, Debate, 2012), especialmente, capítulos 18 y 22.

14 Como explican en detalle MAYER-SCHÖNBERGER, V./CUKIER, K., *Big data*, *cit*., págs. 69-94.

15 Por lo demás, *nihil novum sub sole*. En cierto modo, triunfa la tesis del filósofo escocés David HUME (1711-1776), que consideraba que la causalidad no existe, sino que es una ilusión creada a partir de las correlaciones, que son lo único realmente observable. "Según él, la conexión causal no significa sino una relación de *coexistencia* y *sucesión*. Cuando un fenómeno coincide repetidas veces con otro o lo sucede en el tiempo, llamamos, en virtud de una *asociación de ideas*, al primero, *causa*, y al segundo, *efecto*, y decimos que este acontece *porque* se da el primero. La sucesión, por muchas veces que se repita, no nos da la seguridad de su indefinida reiteración, y no nos permite afirmar un vínculo de causalidad en el sentido de una *conexión necesaria*" (MARÍAS, J., *Historia de la Filosofía*, Alianza, Madrid, 1993, 3ª ed., págs. 250-251).

16 Como se hizo por distintos grupos de investigación en relación con el Covid-19, sobre todo cuando los tests eran muy caros y escasos: https://www.elcomercio.es/sociedad/disenan-modelo-

Este nuevo camino puede llevar -y lleva- a que aparezcan nuevas opciones en las que nadie había pensado o en las que nadie *habría* pensado, porque las ocultaba inconscientemente el modo de pensar tradicional o el "marco" conceptual comúnmente aceptado. Un ejemplo frecuentemente mencionado es el algoritmo "AlphaGo" (creado por Deepmind, una compañía crucial en el desarrollo de los algoritmos predictivos que ahora pertenece a Google), que en 2017 venció al considerado mejor jugador de go del mundo (el go es un juego oriental, que hace algunos años se popularizó en occidente en una versión simplificada con el nombre comercial de Othello). A este programa no se le "enseñó" a jugar al go, al modo de los programas que juegan al ajedrez desde los años 80 (y que también han ganado a grandes jugadores). A "AlphaGo" se le suministraron millones de partidas (de las que se sabe, obviamente, quién ganó), para que, "revolviendo" esos datos con algoritmos, detectase cuáles eran o podían ser las opciones que llevan al triunfo con mayor probabilidad. El programa opera -no hace falta decirlo- sin prejuicios, y utilizaba jugadas por las que era muy poco probable que un jugador usual hubiese optado.[17] Por eso se habla de "aprendizaje supervisado" *(supervised learning)* en el caso de los antiguos programas que jugaban al ajedrez (a los que no sólo se les programaban las reglas del juego, sino que se les indicaba cuáles eran las mejores jugadas ante los distintos escenarios posibles), frente al "aprendizaje no supervisado" *(unsupervised learning)* de los actuales algoritmos predictivos, porque (tomando una vez más el ejemplo de "AlphaGo") es "el ordenador" el que, aplicando el algoritmo, consigue, a partir del análisis de millones de partidas, identificar las mejores jugadas, es decir, aquellas que ofrecen más probabilidades de llevar a la victoria. De aquí la expresión *machine learning* (aprendizaje "mecánico", es decir, "no humano"), porque, una vez puesto en marcha el mecanismo, el sistema "aprende solo", sin necesidad de guía.[18]

---

inteligencia-artificial-coronavirus-rafiografia-torax-20200415135337-nt.html, https://comunicacion.jcyl.es/web/jcyl/Comunicacion/es/Plantilla100Detalle/1284877983892/NotaPrensa/1284946083306/Comunicacion. Un ejemplo reciente es la divulgación por la empresa Deep Mind de un "mapa" de las proteínas humanas (https://elpais.com/ciencia/2021-07-22/la-forma-de-los-ladrillos-basicos-de-la-vida-abre-una-nueva-era-en-la-ciencia.html) o la puesta a disposición de la comunidad científica, por un equipo liderado por Nuria López-Bigas, de la Universidad de Barcelona, de otro "mapa" de las mutaciones causantes de los distintos tipos de cáncer (https://elpais.com/ciencia/2021-07-28/un-sistema-de-inteligencia-artificial-identifica-las-mutaciones-causantes-del-cancer-para-cada-tipo-de-tumor.html). En ambos casos, la inteligencia artificial ha permitido llegar a esas conclusiones de forma mucho más rápida que por los procedimientos experimentales habituales.

17 En el mundo del deporte real también se producen cambios cualitativos de este tipo, que suponen una ruptura con la *lex artis* (aplicado este concepto con un significado diferente al habitual en responsabilidad civil médica). Como ocurrió, por ejemplo, cuando en los Juegos Olímpicos de México de 1968 Dick Fosbury saltó de espaldas en la prueba de salto de altura. Hasta ese momento todos los saltadores lo hacían hacia delante (utilizando la técnica del "rodillo ventral"), y se iban produciendo variantes o mejoras en el salto, pero siempre dentro del "marco conceptual" de hacerlo hacia delante. A quien comenzaba a practicar ese deporte se le enseñaba a saltar así. Una vez que Fosbury abrió ese nuevo camino, todos los siguieron porque se vio que permitía saltar más alto. Otro ejemplo (en este caso es un ejemplo de experimento innovador, aunque no es un cambio que se haya impuesto triunfalmente): en 2015, el tenista Roger Federer comenzó a restar a media pista, en lugar de hacerlo desde el fondo, que es lo habitual. No es algo que se haya universalizado (de hecho, el interés del movimiento radica en que se realiza por sorpresa, cuando el contrario está mirando hacia arriba para sacar), pero también es un ejemplo de movimiento que puede ser eficaz, pero en el que normalmente ni siquiera se pensaría porque se sale de lo usual.

18 En estos momentos existe una "nueva frontera" que es el *reinforcement learning*, que no deja de ser una aplicación del conductismo al *machine learning*, en el que se combina el "aprendizaje automático" a partir del análisis de un altísimo número de experiencias, con la introducción

Podría discutirse si este cambio (de causalidad a correlación) es tan radical. En la mayoría de actividades ya se opera de forma empírica o experimental. La medicina moderna, por ejemplo, no prescribe diagnósticos o remedios en función de una visión filosófica del cuerpo humano, sino en función de la observación de los síntomas, que ha llevado a identificar y describir enfermedades y sus correspondientes tratamientos (basados también en la observación de su eficacia).[19] De todas formas, la aplicación de algoritmos predictivos introduce cambios importantes incluso en estos casos, porque se tiene en cuenta una cantidad de datos superior a la que puede procesar un analista humano y, además, el análisis de esos datos se realiza por un procedimiento "automático" (es decir, por un ordenador), lo que elimina los sesgos o prejuicios que podría tener un analista humano.[20]

Precisamente en el Derecho son mayores las posibilidades de los algoritmos (o, dicho de otro modo, su aplicación supone un cambio mayor), en la medida en que las decisiones no suelen tomarse en función de criterios empíricos (derivados de correlaciones), sino normativos.[21]

3. INTELIGENCIA ARTIFICIAL

Inteligencia artificial, digitalización y automatización son etiquetas diferentes, aunque frecuentemente se confunden. A grandes rasgos, la digitalización supone la utilización de tecnologías de la información y las comunicaciones (TIC) para los procesos administrativos, sustituyendo al papel. Afecta, en primer lugar, a la comunicación entre la Administración

---

de incentivos para los resultados más acertados. Con ello se intenta reducir el tiempo de aprendizaje, es decir, evitar que el sistema tenga que probar todas las combinaciones posibles y se encamine con más rapidez al territorio en que se manifiestan resultados prometedores.

19 Con independencia de la inteligencia artificial, existe una tendencia conocida como "medicina basada en la evidencia" (*evidence-based medicine*, EBM), que supone, básicamente, que la prescripción de remedios o tratamientos se basa en un análisis estadístico de los resultados, que lleva a marginar algunos tratamientos o a privilegiar otros, con independencia de su mayor o menor justificación teórica o fisiológica, únicamente en función de su eficacia para la curación o mejora del paciente, medida con procedimientos estadísticos.

20 Se ha destacado que las predicciones basadas en *big data* suponen un cambio importante frente a los procedimientos estadísticos usuales porque éstos se basan en "muestras", es decir, en una selección de entre los datos disponibles, debido a que con los métodos tradicionales era imposible manejar todos los datos. La superación del muestreo reduce las posibilidades de error o de distorsión de los resultados. *Vid.* MAYER-SCHÖNBERGER, V.; CUKIER; K., *Big data*, *cit.*, págs. 49-68.

21 Pensemos en un ejemplo concreto: la acreditación de profesores universitarios. El sistema actual utiliza un baremo (como forma de reducir la discrecionalidad y sustituir los juicios de valor acerca de la "calidad" de los aspirantes), establecido en una norma (o, actualmente, *en virtud de una norma*, concretamente del Real Decreto 1312/2007, de 5 de octubre, por el que se establece la acreditación nacional para el acceso a los cuerpos docentes universitarios). El autor de la norma ha decidido (juicio de valor) cuáles son las características de un profesor ideal y puntúa a los aspirantes en función del grado en que las posean. Un algoritmo no predictivo sería una aplicación que calculase las puntuaciones a partir de los datos brutos curriculares (publicaciones, docencia, etc.). Ese algoritmo podría perfeccionarse de modo que pudiera importar los datos automáticamente de bases de datos sin necesidad de que el aspirante los introdujera en la aplicación. Un algoritmo predictivo creado para desarrollar esta misma función: *(1)* analizaría los datos de los profesores *senior* (es decir, los considerados mejores o más productivos de acuerdo con criterios previamente establecidos), *(2)* establecería qué características formativas o curriculares están asociadas a ese nivel de excelencia, y *(3)* identificaría, de entre los aspirantes, a los que reúnen esas características y por lo tanto es de prever que alcanzarán ese nivel.

y otros sujetos, pero también al archivo de los procedimientos. Provoca que quede un registro de toda la actuación administrativa en forma de datos estructurados que son la base para la posterior aplicación de inteligencia artificial. Anteriormente, ese registro quedaba en papel y no estaba estructurado, por lo que cualquier trabajo estadístico requería un esfuerzo adicional.

La automatización va más allá de la digitalización y sustituye al operador humano. Es un paso mucho menos frecuente, que de momento se limita, por razones comprensibles, a actos completamente reglados, que la Administración está obligada a dictar cuando se cumplan una serie de requisitos, y también, muy recientemente, a la iniciación de procedimientos sancionadores (Real Decreto-ley 2/2021, de 26 de enero, que modifica el texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre y texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, aprobado por Real Decreto Legislativo 5/2000, de 4 de agosto). La actuación administrativa automatizada requiere una previsión normativa previa, de conformidad con el artículo 41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. No podría ser de otro modo, porque las Leyes atribuyen la potestad para dictar los distintos actos administrativos a órganos administrativos, cuyos titulares son personas físicas.

La inteligencia artificial suele entenderse, en este contexto, en el sentido de que las TIC llevan a cabo tareas que antes requerían la intervención humana, incluida la elaboración de todo o parte del contenido de una decisión administrativa. Normalmente se habla de inteligencia artificial cuando, a partir del análisis algorítmico de gran cantidad de datos, se puede ir más allá de la aplicación de las reglas que el programador ha fijado, y el programa crea nuevas reglas a partir de las correlaciones que descubre en los datos que se le suministran. Por ejemplo, los programas que, a partir del análisis de las infracciones detectadas en el pasado en un sector, predicen dónde es más probable que se estén produciendo infracciones, para que la Administración concentre allí el esfuerzo inspector.

La digitalización es condición necesaria de la automatización y la inteligencia artificial, pero no es condición suficiente. La "Administración electrónica", tal como se regula en las Leyes 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, suele quedarse en digitalización. Por otro lado, automatización e inteligencia artificial son independientes entre sí: puede haber automatización sin inteligencia artificial (programas que realizan liquidaciones tributarias o que notifican denuncias por infracciones de tráfico detectadas con radar) e inteligencia artificial sin automatización (predicciones que sirven para que un inspector decida dónde acudir a inspeccionar, o que sirven para motivar la clasificación de un espacio como suelo no urbanizable debido a un riesgo de inundaciones establecido con un algoritmo).

Es obvio que el Derecho tiene que reaccionar ante la inteligencia artificial porque cambia algunos de sus presupuestos básicos, pero no es tan evidente cómo debe hacerlo.

La Administración y la jurisdicción, ahora o en el futuro próximo, tendrán diferentes relaciones con la inteligencia artificial: *utilizarla* en sistemas que faciliten sus procedimientos y la elaboración de sus decisiones (así como también el análisis de eficacia y eficiencia sobre las políticas públicas y las normas jurídicas), *controlar* su uso por la Administración (jurisdicción contencioso-administrativa) o por el sector privado (jurisdicción civil, autoridades de protección de datos), *contratarla* a través de distintas figuras de la legislación de contratos públicos (y con la importante discusión acerca del grado de transparencia que se exige a los productos que vaya a utilizar la Administración, que influye sobre los modelos de negocio) y *padecerla*, en la medida en que se utilizará

la IA para tratar de predecir el comportamiento de Administraciones y órganos judiciales y adelantarse a él, produciendo posibles distorsiones que obligarán a reformular los criterios o programas normativos de actuación administrativa o judicial.

A veces parece que los riesgos y los problemas sólo surgen cuando se sustituye al operador humano por una aplicación informática, y que la solución consiste en rechazar la sustitución y exigir la presencia humana. Pero la historia demuestra que la garantía para los ciudadanos nunca ha estado en la intervención de un humano, sino en el establecimiento de reglas que le vinculen. El Derecho ha servido siempre para controlar la actuación de los humanos, precisamente porque esa actuación humana es peligrosa. Lo más relevante no es quién actúe. Lo importante es cómo actúe y, sobre todo, que se pueda controlar esa actuación y garantizar que respete el programa normativo previamente establecido.

Tampoco podemos exigir a un algoritmo lo que no le pedimos a un humano. Por ejemplo, las decisiones de iniciación de procedimientos sancionadores, o, más aún, la decisión de inspeccionar (que para muchos ni siquiera supone iniciar un procedimiento administrativo), están sometidas a un control jurídico mínimo. El inicio de un procedimiento es un acto de trámite no recurrible, que puede basarse en causas muy variadas (empezando por la "propia iniciativa" del titular del órgano) y que, de hecho, no requiere ninguna justificación. En realidad, los tribunales relativizan el peso de los instrumentos que pretenden racionalizarlas (planes de inspección).[22] No parece correcto que sólo se vean riesgos en ese tipo de decisiones cuando se utilizan algoritmos para intentar objetivarlas. El algoritmo puede tener sesgos (no por el propio algoritmo, sino por su programación o por los datos que se le suministran), pero al menos esos sesgos dejan huellas, mientras que los sesgos de los operadores humanos que deciden dónde inspeccionar o en qué casos iniciar un procedimiento, que también existen y son casi inevitables, no son tan fácilmente detectables o demostrables.

Como ya he explicado por extenso en otro lugar, el esquema básico para analizar jurídicamente el uso de la inteligencia artificial ha de ser detectar la función que cumple un determinado algoritmo o aplicación en el proceso de creación y aplicación del Derecho. Ese análisis sería similar a la "naturaleza jurídica" o a la calificación jurídica. Y en ese sentido (y dejando a un lado la aplicación ineludible de la normativa de protección de datos, en la que no puedo detenerme por falta de espacio), pueden avanzarse tres situaciones básicas:

- Algoritmos que traducen un régimen jurídico para facilitar la toma de decisiones por la Administración. Por ejemplo, programas que ayudan a liquidar un tributo, a calcular la subvención que le corresponde a una empresa en un determinado

22 Un buen ejemplo lo encontramos en la sentencia del Tribunal Supremo de 19 de febrero de 2020 (recurso de casación 240/2018). Un contribuyente impugnaba el resultado de una inspección tributaria alegando que el suyo no era uno de los supuestos en los que debía centrarse la actividad inspectora de la Administración según los programas oficiales aprobados y publicados: "La introducción de los planes de actuación, de Control, parciales, pueden tener la finalidad de facilitar a la Administración Tributaria su funcionamiento, especialmente mediante la aplicación de programas informáticos que permitan un tratamiento más ágil de la fiscalización de un determinado sector de contribuyentes, pero su previsión, quizá no muy acertada, en normas legales y reglamentarias, no puede traducirse sin más en un derecho subjetivo del contribuyente a no ser investigado si no se encuentra incluido en dichos planes y programas, pues ello supondría el incumplimiento por parte de la Administración del deber de fiscalización de que todos los ciudadanos cumplan con el deber de contribuir, previsto en el artículo 31.1de nuestra norma constitucional".

régimen de ayudas, la pensión de jubilación o la carga docente que tiene que asumir un profesor. Facilitan la actuación administrativa (ahorro de horas de trabajo humano, reducción de errores) pero no influyen en su contenido. Son programas que equivalen a una fórmula que traduce el contenido de la norma o de las bases que ha de aplicar la Administración (de hecho, algunas normas jurídicas o bases de licitaciones o de procedimientos selectivos ya describen su supuesto de hecho con una fórmula matemática). Lo más importante es que se puede (a efectos del control de lo que ha hecho la Administración) aplicar la norma "a mano", *sin el algoritmo*, y comprobar si la aplicación algorítmica es correcta o no. El algoritmo no cambia el marco jurídico ni contribuye por sí mismo a determinar el contenido de la actuación administrativa, sino que es neutro. Si como consecuencia de un error en su configuración o aplicación, no lo es, el resultado será contrario a Derecho y será relativamente fácil detectarlo.

- Algoritmos que, como los anteriores, sirven para mecanizar o automatizar procesos reglados, sin cambiar su marco normativo, pero en los que el proceso es tan complejo que no se puede replicar sin el algoritmo, por lo que, en el momento de controlar la actuación administrativa, no se puede prescindir de él y es necesario verificar cómo ha funcionado. Es el caso de procesos complejos de asignación de recursos escasos (por ejemplo, concursos de traslados con un alto número de funcionarios, como ocurrió en Italia, o la asignación de plazas MIR, que ya hemos visto que suspendida cautelarmente y después anulada por la Sala de lo Contencioso-Administrativo del Tribunal Supremo), en los que los resultados individuales están interconectados. El control jurídico de estas decisiones tomadas con ayuda de algoritmos no puede consistir en aplicar la norma "con lápiz y papel" para ver si coincide con la actuación realizada con ayuda algorítmica, sino que es necesario revisar el funcionamiento del algoritmo, lo que exigirá conocer todos los factores que contribuyen a determinar su resultado.

- Algoritmos de tipo predictivo, que contribuyen a orientar en una determinada dirección la actuación administrativa y que, a diferencia de los anteriores, aportan elementos decisionales propios. Esto sería inteligencia artificial en sentido estricto. Normalmente, su efecto es equiparable al de un baremo, que es una de las formas típicas de dirigir la acción administrativa, pero con la peculiaridad de que en este caso el baremo no lo fija una norma o una decisión administrativa de tipo no normativo (como un pliego de cláusulas administrativas particulares o las bases de un concurso), sino que lo determina el propio algoritmo a partir del análisis de casos precedentes. El algoritmo intenta conseguir un objetivo fijado por la norma (identificar a los estudiantes que se encuentren en riesgo de fracaso escolar, por ejemplo) y para ello crea una especie de retrato robot a partir del análisis de los datos de años anteriores. Las características concretas de ese retrato robot no las ha dibujado nadie, sino que las produce el modelo algorítmico. A día de hoy, ese tipo de modelos se aplican (sin habilitación normativa) como apoyo a decisiones de iniciación de procedimientos o, en un escalón inferior de formalización jurídica, para orientar el uso de los recursos públicos de bienestar o de inspección (por ejemplo, para identificar a personas a las que puede ser necesario seguir porque pueden estar en una situación de riesgo no detectada).[23] En la medida en que, en ausencia

23 El Ministerio de Trabajo ha adjudicado sucesivos contratos de servicios para dotarse de un servicio de "consultoría estratégica" que consiste, básicamente, en un modelo predictivo que apunte a empresas o supuestos en los que sea, en principio, más probable detectar infracciones

de algoritmo, esas decisiones carecerían, en la práctica, de control jurídico (no son actos administrativos discrecionales, sino actuaciones informales o actos de trámite), el peligro que se asume con la utilización de modelos algorítmicos es limitado, y también lo es la necesidad de regulación.

Una regulación es necesaria (y ya se está intentando a nivel europeo), y debería partir de las diferentes funciones jurídicas que puede desempeñar la inteligencia artificial.

4. PARÁMETROS JURÍDICOS DERIVADOS DE LA PROTECCIÓN DE DATOS

4.1 Pluralidad de perspectivas jurídicas sobre los algoritmos predictivos.

Los datos son uno de los tres elementos necesarios para la utilización de algoritmos predictivos, junto con los propios algoritmos y la capacidad de computación. No es sorprendente que las normas sobre protección de datos sean la primera respuesta jurídica al fenómeno.

No se trata, sin embargo, de la única. También existen otros títulos de intervención, que van desde el Derecho de la competencia (o de la competencia desleal), el del consumo o -por centrarnos en el uso que de estos algoritmos hacen las Administraciones Públicas- la regulación del procedimiento administrativo. El derecho fundamental a la protección de datos es sólo uno de los derechos del ciudadano que entran en juego en este campo, pero el particular también debe ser protegido en su condición de interesado en un procedimiento administrativo, lo que afecta a otros derechos (fundamentales o no) y a otros títulos de intervención del legislador, desde el derecho a la buena administración, el derecho a la tutela judicial efectiva y el mandato constitucional al legislador para la regulación del procedimiento administrativo (artículo 105).[24]

En este sentido, es muy probable que se esté desplazando el centro de gravedad de algunas instituciones. Ciertas reglas o derechos pueden estar perdiendo importancia porque las nuevas técnicas de análisis de datos abren nuevas posibilidades de actuación para las Administraciones Públicas que les permiten eludir esas garantías. Pensemos en el derecho a no declarar contra uno mismo (o derecho a la no autoincriminación), recogido en el artículo 24.2 CE y aplicable tanto al proceso penal como a los procedimientos sancionadores, según una jurisprudencia constitucional y ordinaria bien conocida. La importancia práctica de esa regla disminuye a medida que aumenta la cantidad de datos libremente accesibles por la Administración que pueden servir para probar la comisión de infracciones o delitos. El "deber de colaboración" pierde relevancia cuando la Administración tiene a su disposición datos que no aporta el ciudadano en cumplimiento de ese deber, sino que voluntariamente va produciendo y "liberando" y que llegan a manos de la Administración.[25]

(https://www.eldiario.es/economia/inspectores-trabajo-denuncian-externalizacion-empresa-privada-lucha-fraude_1_6304432.html).

24 En este sentido, CIVITARESE MATTEUCCI, S., "«Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità", *Diritto pubblico*, 2019, págs. 5-41, pág. 23, que subraya que el RGPD sólo se ocupa del derecho a la protección de datos, pero no de otras perspectivas jurídicamente relevantes como el fundamento normativo necesario para que la Administración pueda actuar de forma automatizada.

25 Todo ello con independencia de los problemas prácticos que puedan surgir para que tales datos (por ejemplo, videos colocados por el presunto infractor -o por terceros- en redes sociales) produzcan efectos probatorios. Un análisis de estos problemas en la sentencia del Juzgado Central de lo Contencioso-Administrativo número 1 de 7 de julio de 2017 (recurso contencioso-administrativo 167/2016).

4.2 Los algoritmos funcionan, sobre todo, con datos anonimizados.

Otra advertencia importante, en la línea de relativizar la importancia del Derecho de protección de datos dentro del abordaje jurídico de los algoritmos, es que la normativa de protección de datos (fundamentalmente, el RGPD y la LO 3/2018) establece normas dirigidas a la utilización de datos *personales*, es decir, "información sobre una persona física identificada o identificable" (artículo 4), mientras que las predicciones algorítmicas se realizan, sobre todo, a partir de datos no personales.[26] Así, por ejemplo, para "entrenar" a un algoritmo que sirva para determinar la solvencia de potenciales solicitantes de préstamos sólo se necesita información sobre la ejecución de préstamos anteriores, pero se trata de información no personal porque no es necesario conocer el nombre y apellidos del prestatario, sólo aquellas notas de esa persona que puedan ser relevantes y, en particular, los datos relativos a si ha cumplido, o no, el contrato de préstamo. A partir de esos datos no personales (anonimizados) se hallarán correlaciones y se elaborarán perfiles que servirán para ayudar a decidir la concesión o denegación de una nueva petición de crédito. Por tanto, el peticionario de crédito sí aporta sus datos personales, que son analizados por la entidad financiera mediante un modelo algorítmico, pero esa aportación de datos no plantea problemas desde el punto de vista de la normativa de protección de datos, porque es una aportación consciente, consentida y legitimada por ese consentimiento y además por su necesidad para la celebración del contrato (artículo 6 RGPD). Pero el tratamiento de los datos anteriores queda al margen de la normativa de protección de datos porque no son datos personales. Es verdad que, como se ha observado reiteradamente, la anonimización puede fallar en casos concretos, en los que, por el escaso número de personas que se encuentren en una determinada situación, sea fácil identificar al sujeto que reúne esas condiciones. Pero se trata de excepciones y no podemos ignorar que la legislación de protección de datos acepta la anonimización como un procedimiento para eliminar el carácter personal de los datos y levantar algunas barreras a su tratamiento.[27]

4.3 El consentimiento del interesado y sus debilidades.

En la práctica, la aplicación de las normas de protección de datos se ha traducido en la solicitud al interesado del consentimiento al tratamiento de sus datos, con carácter previo a la celebración de cualquier contrato o incluso a cualquier contacto comercial con una empresa, y, en especial, cuando se accede a cualquier página web o se utiliza cualquier aplicación. De hecho, también se exige ese consentimiento en los impresos de solicitud de participación en numerosos procedimientos administrativos, aunque se trata de un consentimiento "obligatorio" y, por tanto, no es un verdadero consentimiento.[28]

---

26 Insiste en este argumento HOFFMANN-RIEM, W., *Big data. Desafíos también para el Derecho*, Civitas, Cizur Menor, 2018 (el original alemán también se publicó en 2018), pág. 107.

27 Apartado 26 del preámbulo del RGPD: "los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo".

28 O se establece, en la convocatoria de que se trate, que la presentación de la solicitud "conlleva el *consentimiento* para la comunicación a otras administraciones públicas de los datos", o "conlleva la *autorización* de la entidad solicitante para tratar dichos datos de manera automatizada y cederlos a los órganos de instrucción, evaluación, resolución, seguimiento y control competentes (…)" (artículo 15.13 de la Resolución de la Secretaría de Estado de Universidades, Investigación, Desarrollo e Innovación y de la Presidencia de la Agencia Estatal de Investigación de 13 de agosto de 2018, por la que se aprueba la convocatoria de tramitación anticipada para el año 2018 del procedimiento de concesión de ayudas a Proyectos de I+D+i «Retos investigación»

Las cláusulas de prestación del consentimiento (política de privacidad y protección de datos), no se leen por casi nadie, entre otras cosas porque se plantean como un paso previo a la utilización de una aplicación o a la obtención de una información en una página web, que son procesos a los que es inherente la celeridad. Dicho de otro modo: si los consumidores no siempre leen todas las cláusulas de los contratos que firman (a veces ni siquiera en el caso de los contratos firmados ante notario), aunque se les suministren con días de antelación a la firma, es ilusorio pensar que vayan a leer las cláusulas que actúan como paso previo al acceso a una página web o a la utilización de una aplicación, cuando la razón por la que se acude a la página o a la aplicación es precisamente por la rapidez con que pueden ser utilizadas, desde cualquier soporte (especialmente, el teléfono móvil) y sin más dilación. No digamos cuando se trata de aplicaciones que se descargan para solucionar una necesidad inmediata (pagar el aparcamiento, buscar rápidamente un hotel o restaurante, etc.).

Esta legislación de protección de datos que resulta desactivada por el consentimiento del interesado (es decir, que sólo obliga a pedir y obtener el consentimiento), además de resultar poco útil, utiliza una técnica que, en sectores similares como el Derecho de consumo, fue superada hace décadas. Tanto en el Derecho de los consumidores como en la protección de datos se parte del presupuesto de que existe una parte débil, que en el primer caso es el consumidor y en el segundo es el titular de los datos cuando se enfrenta a peticiones de consentimiento que son difíciles de gestionar (por su prolijidad) y que, si se le plantean como una condición necesaria para utilizar aplicaciones, pueden llegar a ser casi obligatorias, si la negativa le conduce a una especie de aislamiento o de renuncia a la tecnología. La respuesta del Derecho de consumo a esta situación ha sido, como es sabido, prescindir del dogma del consentimiento, es decir, afirmar que el hecho de que el consumidor haya firmado un contrato no es suficiente para que el mismo le vincule en su integridad, porque, si hay cláusulas abusivas, éstas son nulas a pesar del consentimiento del consumidor. Por eso, los *disclaimers* y los consentimientos que se aceptan antes de cualquier contrato electrónico tienen una importancia muy limitada *en lo relativo a las cláusulas contractuales* (dejamos a un lado en este momento la protección de datos, donde el consentimiento sí tiene una importancia decisiva) porque se aplica un control material, que expulsa las cláusulas abusivas.

El Derecho de la protección de datos camina en esta dirección, pero todavía lo hace muy lentamente. No existen apenas normas imperativas que prohíban determinados tratamientos de los datos *a pesar del consentimiento del interesado*. Y, aunque existen reglas para la prestación del consentimiento, que intentan evitar cesiones en blanco o una prestación del consentimiento que sea sólo una apariencia, la realidad muestra que ese consentimiento se sigue prestando de forma irreflexiva y en un contexto (el acceso a páginas o a aplicaciones) en el que priman la urgencia o la celeridad. Por lo tanto, en la práctica, buena parte de los límites legales se superan con facilidad gracias al consentimiento de los afectados.

Por otro lado, la tecnología ha facilitado a los usuarios la posibilidad de registrar todas sus actividades, lo que tiene muchas ventajas (pensemos en las pulseras de actividad que registran la práctica deportiva o la actividad física en general, las tarjetas y en general los pagos electrónicos, que permiten el control del gasto y evitan tener que archivar miles de documentos en papel, o la geolocalización y sus múltiples utilidades, etc.). Salvo excepciones, el ciudadano colabora voluntariamente y crea grandes cantidades de datos. Y se ha asentado un modelo económico en el que esos datos no tienen utilidad sólo para

correspondientes al Programa Estatal de I+D+i Orientada a los Retos de la Sociedad, en el marco del Plan Estatal de Investigación Científica y Técnica y de Innovación 2017-2020).

el ciudadano, sino también para las empresas, y con frecuencia es el potencial de esos datos lo que ha llevado a empresas a crear las aplicaciones que utilizan los usuarios.[29] La evolución de la tecnología no ayuda a la restricción en los consentimientos al tratamiento de datos, sino al revés.

4.4 Peculiaridades en el uso de datos por Administraciones Públicas.

Ya hemos visto, como un ejemplo de la aplicación de la normativa de protección de datos por las Administraciones, que hay convocatorias (por ejemplo, de becas o subvenciones) en las que se exige al peticionario que acepte expresamente el tratamiento de sus datos (sin opción de no hacerlo) o se establece en la propia convocatoria que la presentación de la solicitud conlleva la autorización o consentimiento para dicho tratamiento. El consentimiento del interesado es necesario para que la solicitud sea tramitada y se convierte, por tanto, en uno de los requisitos necesarios para obtener una resolución favorable. Esta técnica es inadecuada porque un consentimiento "obligatorio" es una contradicción. El consentimiento es innecesario porque el tratamiento de los datos se justifica en virtud de otros títulos jurídicos [una misión realizada en interés público por la Administración, artículo 6.1.e) RGPD].

Más allá de este ejemplo, es necesario tener en cuenta las peculiaridades del tratamiento de los datos cuando quien pone en marcha una aplicación es una Administración Pública o, en general, un ente que opera en régimen de Derecho administrativo (lo que incluye a los concesionarios y contratistas cuando lo hagan para gestionar una actividad pública que les haya sido encomendada). Incluso en el caso de que estemos hablando de actividades prestacionales y no de policía, y se trate de prestaciones de recepción voluntaria por el interesado, no podemos considerar libre el consentimiento cuando la negativa a prestarlo impide al ciudadano acceder a una prestación o supone renunciar a las ventajas derivadas de utilizar una aplicación en línea, y condenarse a utilizar formas de relación no electrónica. Por eso, en estos casos el tratamiento de datos que lleva a cabo la Administración ha de justificarse en normas que legitimen ese tratamiento en algún título distinto del consentimiento, y no (o no sólo) en el consentimiento de los afectados, y han de cumplirse, además, los límites y garantías específico (empezando por el principio de proporcionalidad).

4.5 Ambigüedad y casuismo.

La normativa sobre protección de datos tiene, por otro lado, debilidades evidentes. Una de ellas es la constante utilización de conceptos legales indeterminados, entre los que destacan los de "proporcionalidad" y "adecuación": en numerosos supuestos, la norma

29 Como explica ZUBOFF, S., *The age of surveillance capitalism*, Profile Books, London, 2019, pág. 5, la aparición de esta economía de los datos no era previsible (o al menos no fue prevista) cuando, hacia el año 2000, y ya en pleno auge de internet, comenzó a avanzarse en lo que sería el internet de las cosas, es decir, la domótica y demás posibilidades de manejar aparatos online. Los primeros proyectos suponían el control centralizado a distancia de múltiples mecanismos, pero sin que los datos fueran manejados o aprovechados por alguien distinto de su titular. Es lo mismo que sigue sucediendo, por ejemplo, con el control de grandes instalaciones (centrales energéticas, etc.), que también son manejadas por medios electrónicos y digitales, pero bajo el control del titular de la instalación. El gran cambio vino cuando, debido en buena medida a los avances de los algoritmos, se vio la utilidad económica de los datos agregados generados por millones de usuarios, y eso impulsó a muchas empresas a invertir y a generar aplicaciones gratuitas que han ganado el interés de los usuarios y son masivamente utilizadas por ellos, a cambio del "único" precio (que en buena medida es invisible o percibido como inocuo) de entregar sus datos.

permite una determinada conducta, siempre que sea proporcional y se apliquen garantías adecuadas (o bien, la prohíbe, salvo que concurra uno de los presupuestos habilitantes y se cumplan esos conceptos indeterminados). Esa forma de legislar produce inseguridad jurídica y supone que el autor de la norma abdica parcialmente de su labor, porque deja en manos del aplicador la tarea de ponderar distintos intereses o principios en juego, en lugar de tomar la decisión y establecer preferencias dentro de ciertos ámbitos o cuando se respeten algunos requisitos. El resultado final es, como he dicho, inseguridad jurídica y dificultad para predecir las decisiones que se tomen en los casos concretos.[30]

Todo ello se une a los déficits de aplicación que se producen en esta materia, derivados de que con frecuencia el tratamiento de datos resulta invisible. Podemos discutir si las cláusulas con las que se solicita el tratamiento de los datos son adecuadas o no[31], pero es mucho más difícil reaccionar cuando se produce una cesión de datos no autorizada, entre otras cosas porque muchas veces no es detectable: el ciudadano que resulta destinatario de una decisión tomada a partir de esa cesión de datos (con resultados favorables o desfavorables para él, según los casos), puede no enterarse de que la decisión ha sido tomada sobre la base de un previo análisis de datos.

Por otro lado, en éste como en otros sectores, parece bastante claro que las autoridades de protección de datos no tienen medios suficientes para imponer la aplicación de las normas por vía sancionadora, sobre todo en un contexto de innovación tecnológica.

30 Un ejemplo reciente lo encontramos en la sentencia del TJUE de 11 de diciembre de 2019 (asunto C-708/18, TK), que resuelve una cuestión prejudicial en un pleito iniciado por un vecino de un bloque de viviendas que se oponía a que la comunidad de propietarios instalara cámaras en el portal como medida de seguridad ante los robos que se habían producido. La sentencia rechaza la aplicación de algunas reglas que podrían haber resuelto con claridad el caso (por ejemplo, normas nacionales que prohíben sin excepciones el tratamiento de ciertos tipos de datos, o, en sentido contrario, que considerar que la comunidad, como gestora de las zonas comunes, pueda disponer sobre la instalación de cámaras), y opta por un modelo de ponderación en cuya virtud la conformidad a derecho de la decisión va a depender en cada caso de conceptos cuya aplicación última corresponde al juez, como la proporcionalidad, o de si existen otros medios menos invasivos para la intimidad que puedan conseguir la misma finalidad (algo similar al *favor libertatis*). El resultado es que se produce un brusco salto entre la enunciación de esos principios generales y la decisión concreta (que podía haber sido ésa u otra diferente, a partir de los mismos principios) y que ésta ni siquiera la toma el TJUE, sino que se remite al órgano que había planteado la cuestión: "Habida cuenta de las consideraciones anteriores, procede responder a las cuestiones prejudiciales planteadas que los artículos 6, apartado 1, letra c), y 7, letra f), de la Directiva 95/46, deben interpretarse, a la luz de los artículos 7 y 8 de la Carta, en el sentido de que no se oponen a disposiciones nacionales que autorizan la instalación de un sistema de videovigilancia como el controvertido en el litigio principal, colocado en las zonas comunes de un edificio de uso residencial sin el consentimiento de los interesados, con el fin de satisfacer intereses legítimos consistentes en garantizar el cuidado y la protección de las personas y de los bienes, si el tratamiento de datos personales mediante el sistema de videovigilancia de que se trata reúne los requisitos impuestos en dicho artículo 7, letra f) [es decir, "interés legítimo" perseguido por el responsable del tratamiento, que prevalezca sobre "el interés o los derechos y libertades fundamentales del interesado"], circunstancia que corresponde verificar al órgano jurisdiccional remitente".

31 La discusión sobre la conformidad a la normativa de protección de datos de las cláusulas de solicitud del consentimiento sí está presente en la jurisprudencia del TJUE. Un ejemplo reciente en la sentencia de 1 de octubre de 2019 en el asunto C-673/17 (Planet 49): "el consentimiento (…) no se presta de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de *cookies* se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento".

Seguramente serán necesarios más mecanismos de aplicación de las normas, incluido el de contar con la colaboración de otros agentes, privados, que se especialicen en la detección de conductas infractoras y que las denuncien o ayuden a los perjudicados a ejercitar acciones civiles.[32]

4.6 Reglas concretas sobre el uso de algoritmos: decisiones automatizadas.

A la luz de estas consideraciones, que ayudan a relativizar la importancia de la legislación de protección de datos en este contexto, vamos a analizar brevemente algunas de las normas más relevantes para la utilización de predicciones algorítmicas. Ya se ha indicado que lo más habitual es que se utilicen datos anonimizados para "entrenar" algoritmos, es decir, para poder elaborar perfiles o modelos y que, posteriormente, esos modelos se utilicen con los datos personales (éstos sí son personales, no están anonimizados) del interesado, para realizar alguna predicción respecto a él. En otros casos, los datos anonimizados con los que trabaja el algoritmo elaboran predicciones generales que no están dirigidas a ningún interesado en concreto, sino que sirven a la Administración para tomar medidas de organización (como ocurre con los datos generales anonimizados sobre movilidad de la población, que la Administración compra para poder obtener conclusiones que le sirvan para planificar sus políticas).

Como los datos con los que se elabora el modelo algorítmico están anonimizados, las previsiones de la legislación de protección de datos no les afectan o sólo de manera muy ligera. En cuanto a los datos del interesado respecto al que se va a tomar una decisión con apoyo en las conclusiones del modelo algorítmico, tampoco plantea demasiados problemas su tratamiento, porque los suministra él mismo y la legitimidad del tratamiento deriva de la función pública que desempeña la Administración [letras e), y, en su caso, c) y f) del artículo 6.1 del RGPD]. Por tanto, los problemas o los límites se van a plantear desde otros sectores del ordenamiento jurídico, más que desde el flanco de la protección de datos. Concretamente, una vez que el modelo algorítmico descubre una serie de correlaciones que permiten predecir un determinado resultado con cierta probabilidad, el problema es saber qué relevancia jurídica puede darse a esa predicción, y también si determinados factores, por mucho que se muestren relevantes en la práctica (es decir, aunque puedan ser indicativos de una correlación), pueden ser tenidos en cuenta o están vetados por ser discriminatorios. Pero son problemas distintos de la protección de datos, que se abordarán más adelante.

Mención aparte merece la regulación de las decisiones individuales automatizadas en el artículo 22 RGPD.[33] Comencemos por el ámbito de aplicación. La norma sólo se aplica a "una decisión basada *únicamente* en el tratamiento automatizado, incluida la elaboración de perfiles". Ya sabemos que las predicciones algorítmicas son eso,

32 Sobre esta cuestión, HUERGO, A., "Las sanciones administrativas en el marco del *law enforcement*", en ZEGARRA VALDIVIA, D. (Coord.), *La proyección del Derecho Administrativo Peruano. Estudios por el Centenario de la Facultad de Derecho de la PUCP*, Palestra, Lima 2019, págs. 515-539 (esp., págs. 532-538).

33 El artículo 22 ("Decisiones individuales automatizadas, incluida la elaboración de perfiles") dispone:

"1. 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.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

predicciones, que pueden ser seguidas o no por quien ha de tomar la decisión. Por tanto, esta regulación no afecta a todas las predicciones algorítmicas, sino que sólo opera en aquellos casos en que la predicción se integra en un sistema automatizado de toma de decisiones.[34] En la práctica, lo normal es que, si la decisión tiene una entidad económica suficiente, no se tome de modo puramente automático, sino que la predicción se integre como un elemento más de juicio. Pierde relevancia, por consiguiente, el artículo 22. Éste no aborda la esencia de los algoritmos predictivos, sino una de sus posibles formas de utilización.

En segundo lugar, el artículo 22 sólo se refiere a una decisión "que produzca efectos jurídicos en él [el interesado] o le afecte significativamente de modo similar". De nuevo se restringe el ámbito de aplicación, porque lo normal (lo veremos más adelante) es que las predicciones algorítmicas sirvan para seleccionar objetivos a la Administración, para indicarle dónde puede ser necesario actuar (tanto en caso de actuaciones de gravamen, por ejemplo, sancionadoras, como favorables, por ejemplo, en servicios sociales), más que para determinar el contenido de la decisión. Es dudoso que esta clase de decisiones (que a veces ni siquiera se refieren a personas concretas, sino a grupos o a zonas), produzcan "efectos jurídicos en el interesado" en el sentido del artículo 22.[35] Sin embargo, la conocida sentencia SYRI del Tribunal de Distrito de La Haya, de 5 de febrero

---

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado".

34 Sobre la relación entre decisiones automatizadas y uso de algoritmos, VAN ECK, M., "Algorithms in Public Administration", entrada de blog publicada el 31 de enero de 2017 (https://marliesvaneck.wordpress.com/2017/01/31/algorithms-in-public-administration/).

35 Un documento relevante para la interpretación de este concepto podrían ser las "Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2017/679" adoptadas por el "Grupo de Trabajo sobre Protección de Datos del artículo 29" el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053). Aunque se analiza expresamente este concepto legal (páginas 23-25), parece claro que una decisión de inicio de un procedimiento no es una decisión "que produzca efectos jurídicos" para el afectado, y, en su caso, podrá entrar en la categoría de una decisión que "le afecte significativamente de modo similar", aunque los ejemplos que se analizan se refieren todos al tráfico privado (publicidad online, aplicación de condiciones contractuales diferentes, denegación de crédito). Se detiene en esta cuestión HERNÁNDEZ, J. C., "Decisiones algorítmicas de perfilado: régimen y garantías jurídicas", *RED*A, 203 (2020), págs. 281-322, esp. págs. 293-295. Los ejemplos que menciona, basándose en el documento que se acaba de citar, parecen corresponder a resoluciones, no a actos de trámite (ni "preparatorios de actos de trámite"): "la cancelación de un contrato, la denegación de entrada a un país, o la concesión o denegación de una prestación por una administración pública". Parece considerar las circunstancias personales del destinatario de la decisión como un criterio para determinar si la decisión afecta a los derechos o no, lo que puede introducir una importante dosis de inseguridad.

de 2020, se basa, para declarar que dicho sistema de selección de posibles casos de fraude es ilegal, justamente en que los informes de riesgo "afectan significativamente" a los ciudadanos "de modo similar" a una decisión que produzca efectos jurídicos.[36]

Al margen de estos problemas y dudas sobre el ámbito de aplicación, el artículo 22 constituye una buena muestra de las limitaciones de las normas de protección de datos. Establece, en resumen, una prohibición con excepciones. De las tres excepciones, dos tienen escaso desarrollo en Derecho público: el consentimiento (por lo que ya he dicho, es decir, porque aquí no debería considerarse suficiente en la mayoría de los casos) y el supuesto de que la decisión automatizada "es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento", pensado más para el Derecho privado (y este supuesto plantea, además, muchas dudas, porque no está claro cuándo "es necesaria" una decisión de este tipo para la celebración o ejecución de un contrato, pues normalmente es la conveniencia de una de las partes, no la necesidad, lo que impulsa la utilización de algoritmos). La otra excepción es una autorización normativa. Es decir: hace falta una habilitación normativa (no necesariamente legal) para que puedan adoptarse decisiones "basadas únicamente en el tratamiento *automatizado*" de datos personales, si se quiere que la decisión "produzca efectos jurídicos en él [el interesado] o le afecte significativamente de modo similar". A su vez, y como se adelantó hace un momento, no basta la habilitación normativa, sino que es preciso que se cumpla un requisito adicional que consiste en la adopción de "las medidas adecuadas para salvaguardar los derechos y libertades y los derechos y los intereses legítimos del interesado". Aunque esas "medidas adecuadas" son indeterminadas, su mínimo queda, sin embargo, perfectamente explicitado: "el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión".[37]

Además, se establecen dos precisiones. La primera, que la decisión automatizada no puede basarse en las categorías de datos especialmente protegidos del artículo 9.1, de nuevo salvo excepciones entre las que se incluyen "razones de un interés público esencial".

La segunda, que, mediante Ley, se pueden establecer excepciones en los supuestos del artículo 23, que son muy amplios, y que incluyen algunos que parecen muy relacionados con algunas actividades típicamente administrativas, como "objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbito fiscal, presupuestario y monetario, la sanidad pública y la seguridad social", "la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas

36 Sentencia de 5 de febrero de 2020, apartado 6.59: "El hecho de un informe de riesgo no necesariamente lleve a posteriores investigaciones, ni a una sanción administrativa o penal, y que no puede ser utilizado como único fundamento jurídico de una decisión dirigida a hacer cumplir una norma *[enforcement decision]* no significa que no produzca efectos significativos en la vida privada del titular de los datos". Sobre esta sentencia, *vid.* el comentario muy favorable de COTINO, L., "«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*, Wolters Kluwer, 4 (2020).

37 Se trata de la "reserva de humanidad" que ha destacado la doctrina, pudiendo citarse, por todos, PONCE, J., "Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", *Revista General de Derecho Administrativo*, 50 (2019). Desde otra perspectiva, OSWALD, M., "Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power", *Philosophical Transactions of the Royal Society*, A, 2018, 376:20170359 (17).

deontológicas en las profesiones reguladas", o "una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública (…)".

El RGPD establece, así, que la actuación administrativa automatizada requiere una habilitación normativa, algo que el artículo 41 LRJSP no expresa con la misma claridad.[38] En Alemania, se exige una habilitación normativa para que puedan adoptarse actos administrativos de forma automatizada, con independencia de que se basen, o no, en predicciones basadas en datos.[39] En cambio, en Francia se exige que, cuando una decisión administrativa se tome sobre el fundamento de un "tratamiento algorítmico", se informe de ello al ciudadano.[40] No importa si la decisión se adopta de forma automática o no; lo que es relevante es el uso de un "tratamiento algorítmico". Y no se exige una base normativa para dicho tratamiento, pero sí se exige que se informe al ciudadano. Me parece una opción normativa más adaptada a la realidad.

5. EL PROYECTO DE REGLAMENTO SOBRE LA INTELIGENCIA ARTIFICIAL

Después de una consulta previa, un Libro Blanco y peticiones de otras instituciones como el Parlamento o el Consejo, la Comisión acaba de ejercer su competencia de iniciativa legislativa y ha formulado proyecto de Reglamento sobre "un enfoque europeo de la inteligencia artificial".[41]

El proyecto define la IA como un software que, a partir del uso de técnicas matemáticas y de programación que se enumeran en el Anexo I (y que son lo que vulgarmente se entiende por "algoritmos", aunque esta palabra tenga un significado más amplio, como ya sabemos), produce resultados que sirven para realizar predicciones, recomendaciones de decisiones futuras, etc.

El punto de partida de este futuro Reglamento es ya conocido: la IA es una oportunidad a la que no se puede renunciar porque permite ganar en eficiencia y porque *si no lo hacemos nosotros, lo harán otros,* y a la vez supone riesgos importantes, que van desde la posibilidad de que un sistema "inteligente" que controle una central energética o una máquina de tratamiento médico comience a funcionar mal y cause daños graves, a

38 Una cuestión en la que CIVITARESE MATEUCCI, S., "«Umano troppo umano»", *cit.*, págs. 34 y sigs., es partidario de exigir no sólo habilitación normativa, sino una habilitación normativa específica para la adopción de un tipo concreto de decisiones automatizadas, no una habilitación general para la toma de decisiones automatizadas.

39 Mediante una Ley de 18 de julio de 2016, de modernización de los procedimientos tributarios, se introdujeron reformas en distintas Leyes y, concretamente, en la Ley de Procedimiento Administrativo *(Verwaltungsverfahrensgesetz -VwVfG-)* se introdujo un nuevo parágrafo, el 35 a, que dispone: "Se puede dictar un acto administrativo por medios totalmente automáticos, siempre que haya sido admitido por una norma y no exista discrecionalidad ni margen de apreciación". Cuando el precepto habla de norma jurídica *(Rechtsvorschrift)*, emplea una expresión técnica que incluye leyes y reglamentos, pero excluye lo que en Alemania se llaman reglamentos administrativos *(Verwaltungsvorschrift)*, similares a circulares o instrucciones.

40 La norma se encuentra en la Ley de República Digital (Ley 2016-1321, de 7 de octubre), en su artículo 4 (que modifica el Código relaciones con la Administración, artículo L311-3-1): "Sous réserve de l'application du 2° de l'article L. 311-5, une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande".

41 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

que se discrimine a personas en función de los "informes" que produzca un sistema de análisis inteligente de datos, o que se establezcan sistemas de vigilancia omnipresente de tipo "Gran Hermano". El riesgo consiste, en definitiva, en la posibilidad de que se causen daños que pueden afectar a la integridad o vida de las personas, daños materiales, impactos graves para la sociedad en su conjunto, o para actividades económicas de gran importancia, o distorsión en la prestación de servicios esenciales, o impactos negativos en los derechos fundamentales (incluido el derecho a no ser discriminado o el derecho a la intimidad). La utilización de IA supone un riesgo de que se vulneren derechos o bienes jurídicos que ya están protegidos a nivel legal y, en algunos casos, constitucional.

Este punto de partida (necesidad de minimizar los riesgos que produce una actividad a la que no se puede o quiere renunciar) es el mismo de casi cualquier otra regulación de actividades de riesgo, por ejemplo, las industriales.

A partir de aquí, se pueden utilizar varios instrumentos o técnicas de intervención: la prohibición total o parcial de ciertas actividades para evitar los riesgos (siguiendo el principio de precaución), un régimen autorizatorio (control preventivo), otras formas de control preventivo (declaraciones responsables, por ejemplo), un control exclusivamente posterior (responsabilidad civil y, en su caso, penal de quien causa daños utilizando esa técnica creadora de riesgos), todo ello acompañado de un aparato inspector, que actúa, normalmente, a instancia de los perjudicados, y que ayuda a éstos y a los tribunales a descubrir y acreditar las conductas infractoras.

En este proyecto de Reglamento se combinan esos enfoques, que además se adaptan a la especialidad y complejidad del objeto de regulación.

5.1 Aplicaciones de la IA prohibidas

De entrada, se prohíben algunos usos de la IA (artículo 5): cualquier sistema "que se sirva de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra", o que "aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra", o bien el uso de "sistemas de IA por *parte de las autoridades públicas* [significativa restricción] o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas, de forma que la clasificación social resultante" produzca resultados perjudiciales "en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente" o bien provoque un trato perjudicial o desfavorable "que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este". También se prohíben los sistemas de vigilancia indiscriminada y general ("gran hermano").

La verdad es que los tres primeros son supuestos que representan versiones extremas de algunos usos habituales de la IA y, precisamente por estar descritos en términos tan extremos y con tal acumulación de adjetivos, es muy difícil que se apliquen, por lo que la prohibición tiene una utilidad pequeña.

Decir que una aplicación de IA manipula el comportamiento humano, provocando que una persona se comporte, asuma una opinión o tome una decisión en su propio perjuicio, es decir todo y nada. Gran parte de la publicidad podría entrar en esa definición, pero a

la vez el comportamiento humano sigue siendo voluntario (esa es al menos la creencia que sustenta todo el ordenamiento jurídico), por lo que difícilmente podemos decir que una aplicación tiene esa fuerza "obligatoria" que "fuerce" a los ciudadanos a comportarse de una determinada manera. Por lo demás, no hace falta usar la IA para manipular ni para intentar llevar a las personas a tomar decisiones que son más favorables al interés de quienes les mueven en esa dirección que al interés de quienes las toman.

Lo mismo podemos decir de las aplicaciones que explotan información o predicciones sobre una persona o grupo de personas para atacar sus debilidades o circunstancias especiales, llevando a una persona a comportarse, formar una opinión o tomar una decisión en su propio perjuicio.

En cuanto a las aplicaciones que "clasifican" a las personas en función de datos obtenidos a partir de su comportamiento o de sus características personales (o de predicciones acerca de ellas), y que llevan a tratar de forma discriminatoria a determinadas personas o grupos, en contextos que nada tienen que ver con los datos en los que se basa la clasificación, o de forma desproporcionada, es uno de los escenarios de mal uso de la IA más frecuentemente descritos. Por ejemplo, un sistema que calcule la prima del seguro de automóvil en función de distintas circunstancias que puedan "predecir" la mayor o menor probabilidad de que un conductor provoque un accidente, y que acabe encareciendo la prima, por ejemplo, a quienes tengan menos estudios, o carezcan de un empleo indefinido, o se vean obligados a recorrer largas distancias en coche para ir a trabajar todos los días. Sólo se restringe su uso por poderes públicos. No se está eliminando completamente la posibilidad de utilizar el análisis de datos para que las empresas adapten su esfuerzo publicitario, sus ofertas o sus condiciones contractuales a las características de distintos clientes, que es una de las utilizaciones más habituales de la IA.

Alguna de estas conductas prohibidas (la vigilancia biométrica en tiempo real) puede ser llevada a cabo, de forma excepcional, por una autoridad pública cuando lo autorice una norma y para fines de seguridad pública.

5.2 Aplicaciones de la IA sometidas a autorización.

La identificación biométrica remota en lugares públicos (videovigilancia en calles, por ejemplo) se somete a autorización administrativa, que sólo se concederá cuando exista una norma habilitante, para la lucha contra delitos graves (incluido el terrorismo) y sometida a límites y garantías (artículo 5.3). Como es sabido, no se trata de la instalación de cámaras que simplemente graben lo que pasa en la calle, y ayuden posteriormente a saber qué pasó y a buscar a posibles responsables, sino de sistemas que comparan las imágenes percibidas con bases de datos, lo que les permite identificar automáticamente a una persona (el proyecto no dice que esta exigencia de autorización se aplique sólo a las aplicaciones en las que la identificación es inmediata o en tiempo real).

5.3 Aplicaciones de la IA para las que se establecen reglas concretas de transparencia.

En el artículo 52.1 se obliga a que, cuando se utilice un *chatbot* u otro mecanismo automatizado que interactúe con los usuarios, se advierta a éstos de que no están hablando o mensajeándose con una persona real, sino con una aplicación, salvo que esto sea obvio en vista de las circunstancias.

Otra regla importante (artículo 52.3) es que la obliga a que los sistemas conocidos como *deep fake*, que generan imágenes y/o sonido que pueden engañar y hacer creer que son imágenes reales de personas concretas (por ejemplo, personajes famosos o políticos, que pueden verse comprometidos por vídeos en los que parece que hacen o dicen cosas totalmente contrarias a sus ideas o imagen público) adviertan de que se trata de una ficción, aunque se admiten excepciones basadas, por ejemplo, en la libertad de expresión (lo que puede legitimar el uso de estas técnicas en obras de ficción como películas o series).

Menos clara me parece la obligación de advertir de la utilización de sistemas de reconocimiento de emociones a partir de datos, aunque parece hacer referencia a supuestos en que el reconocimiento se produce "en directo", es decir, a partir de datos obtenidos en ese momento (artículo 52.2).

5.4 Aplicaciones de la IA "de alto riesgo" y sus mecanismos de control.

Pero el núcleo del proyecto de Reglamento no son las aplicaciones prohibidas o las que se someten a autorización o a reglas concretas, sino el régimen de las aplicaciones "de alto riesgo", que se enumeran en el Anexo III y se regulan en los artículos 6-51.

Un primer grupo de aplicaciones de alto riesgo (para las que se exige, como veremos, su verificación previa por un tercero independiente) son las que se utilizan en productos que, por los riesgos que producen, están sometidos a alguna de las normas europeas enumeradas en el Anexo II, y ésta exige que el producto en cuestión se someta a una evaluación de conformidad realizada por un organismo independiente. La explicación es clara: si el sistema de IA se inserta en un producto sometido a un determinado mecanismo de control dirigido a reducir riesgos, el propio sistema de IA deberá someterse a ese mismo control.

El otro grupo (que no requiere esa verificación independiente, sino que estará sometido a una especie de declaración responsable) incluye las aplicaciones típicas de la IA "predictiva", como las que sirven para determinar la admisión (o no) de estudiantes a centros educativos, la contratación de trabajadores o su promoción dentro de la empresa, la concesión -o denegación- de créditos, la concesión de prestaciones sociales (y la vigilancia sobre el cumplimiento de sus condiciones), la "policía predictiva" y la evaluación de riesgos que se utiliza para distribuir los recursos policiales o, en fin, las aplicaciones de IA dirigidas a su uso por jueces y tribunales. Puede comprobarse que la creación de perfiles o la utilización de IA para determinar las condiciones contractuales o el trato a un sujeto no están completamente prohibidas por el artículo 5, sino que, salvo casos extremos, son simplemente "aplicaciones de IA de alto riesgo".

Para este tipo de aplicaciones entra en juego otra forma de tratamiento jurídico, que no es la prohibición sino el establecimiento de unos requisitos que deben cumplir. A diferencia de lo que sucede en otros ámbitos tradicionalmente considerados "de riesgo", como el industrial, donde la regulación acaba, a nivel reglamentario, con la aprobación de normas que establecen condiciones concretas de seguridad, aquí se enuncian unos requisitos tan generales que recuerdan al artículo 6 de la Constitución de 1812 ("El amor a la Patria es una de las principales obligaciones de todos los españoles, y asimismo el ser justos y benéficos"). Así, las aplicaciones de alto riesgo deben estar basadas en datos "pertinentes y representativos, [que] carecerán de errores y estarán completos" (artículo 10.3). Es preciso documentar y archivar los datos generados en la creación y utilización de la aplicación (artículo 11). Los registros "garantizarán un nivel de trazabilidad del funcionamiento del sistema de IA durante su ciclo de vida que resulte adecuado para la

finalidad prevista del sistema" (artículo 12.2). Además, los sistemas de IA de alto riesgo "se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de una herramienta de interfaz humano-máquina adecuada" (artículo 14.1).

No se exige una transparencia total, sino "suficiente para que los usuarios interpreten y usen correctamente su información de salida" (artículo 13.1). El artículo 70.1.a) dice que las obligaciones de información serán compatibles con "los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo en los casos contemplados en el artículo 5 de la Directiva 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas".

Estos requisitos son, en cierto modo, "objetivos" máximos a los que se debe tender, pero que pueden conseguirse de muchas maneras y también con niveles de intensidad diferentes. Pensemos en la transparencia, la solidez o la documentación o archivo de los datos generados en el funcionamiento de la aplicación: habrá que buscar en cada caso concreto cuál es el modo de cumplir esos objetivos, y no hay una única forma de hacerlo, puesto que, entre otras cosas, se puede aspirar a un nivel máximo, medio o mínimo de calidad o de seguridad. Podemos decir, por ejemplo, que los coches deben ser "seguros", pero no hay una única forma de conseguirlo y, por otro lado, no todos los modelos y marcas aspiran al mismo nivel de seguridad. Queda, por tanto, mucho que concretar.

En las aplicaciones de alto riesgo, y dejando a un lado las de identificación biométrica, las de manejo de infraestructuras críticas, así como aquellas que se instalan en productos que están sometidos a una regulación de seguridad (maquinaria industrial, juguetes, ascensores, explosivos, etc.) es el propio "proveedor" o "fabricante" quien controla el cumplimiento de esos requisitos de forma responsable (artículo 43). Por eso digo que el mecanismo es similar al de una declaración responsable (Anexo II, apartado 3).

Esto supone aplicar la técnica del *compliance* o "cumplimiento normativo". Cada fabricante o diseñador tendrá que establecer, en cada producto de IA y en su proceso de creación y aplicación, una serie de medidas dirigidas a cumplir suficientemente los requisitos establecidos en los artículos 10-14 del proyecto de Reglamento, y documentarlo. Esas medidas no serán las mismas en todos los casos, sino que tendrán que ser proporcionales al tipo de aplicación, a su complejidad, a los daños que pueda causar, al riesgo de que tales daños se produzcan, etc.

Hay algunos casos en los que sí se establecen normas que traducen los requisitos generales en estándares concretos, y el proyecto hace referencia a ellas. Esto sucede cuando la IA se aplique en productos que tienen normas de seguridad que se extiendan también a aquélla (por ejemplo, vehículos de transporte, sometidos a una normativa de seguridad estricta) o cuando la UE apruebe estándares técnicos sobre algún aspecto de la IA.

Para aquellos supuestos en que el proyecto exige que la conformidad sea certificada por un tercero (que son, fundamentalmente, las aplicaciones de IA que se utilizan en productos sometidos a normativa de seguridad, así como también las de identificación biométrica y las de manejo y control de infraestructuras críticas), se regulan las entidades de verificación en términos similares a otros sectores (como la auditoría o la inspección técnica de vehículos, por mencionar sólo dos campos muy diferentes entre sí): entidades que son independientes de las empresas cuyos productos verifican, y que están sometidas

a regulación administrativa, además de tener un seguro de responsabilidad y disponer de competencias técnicas suficientes. Sus decisiones deberán estar sujetas a recurso (artículo 37).

5.5 Otras previsiones.

Las aplicaciones que no estén calificadas como "de alto riesgo" (lo que significa que las probabilidades de que con ellas se causen daños a derechos o bienes protegidos son menores) podrán asumir códigos de conducta voluntarios para dar cumplimiento a los requisitos establecidos para las aplicaciones de alto riesgo (artículo 69).

Los Estados miembros deben establecer mecanismos de supervisión y también de sanción. Las multas tendrán un tope máximo de 30 millones de euros o del 6% de la cifra de negocios mundial (si es superior a aquella cantidad), para infracciones que consistan en la utilización de las aplicaciones prohibidas de la IA, el suministro de información falsa a las entidades de verificación o el incumplimiento de los requerimientos de las autoridades (artículo 71).

También se regulan cuestiones como el establecimiento de *sandboxes* o espacios controlados de pruebas (artículo 53).

5.6 Lo que regula y lo que no regula el proyecto de Reglamento.

Este proyecto de Reglamento establece unos requisitos para que se puedan utilizar aplicaciones de IA tanto por operadores públicos como privados. Son requisitos generales y adicionales, porque ahora no existen expresamente, con los que se quiere prevenir daños a bienes y derechos dotados de protección al máximo nivel jurídico. Dicho de otro modo: no es que el Reglamento prohíba cosas que ahora están permitidas, sino que intenta prevenir que se produzcan esos resultados lesivos o dañinos.

El cumplimiento de los requisitos establecidos por el Reglamento (que es un cumplimiento relativo, como estamos viendo, sobre todo en el caso de las aplicaciones de alto riesgo, porque los requisitos son más bien objetivos máximos más que reglas concretas) no agota los problemas jurídicos de la IA. Queda en pie, de entrada, el control posterior que veíamos al principio. Si se producen daños a pesar de, por ejemplo, las medidas preventivas especificadas en el documento de *compliance* elaborado por el productor de la aplicación de IA o aprobado por la entidad certificadora, podrá haber responsabilidad civil o, en su caso, penal, aunque será necesario valorar en qué medida la responsabilidad queda excluida como consecuencia de la aplicación de esas medidas, que en principio suponen una actuación diligente dirigida a minimizar los riesgos. Es lo mismo que sucede con la ITV, que es un sistema dirigido a reducir los riesgos en la circulación de vehículos a motor, pero el hecho haber superado la ITV no excluye que se produzcan daños ni que el conductor y/o propietario del vehículo sean responsables de ellos.

Por otro lado, el cumplimiento de los requisitos establecidos en el Reglamento no significa que las aplicaciones de IA se puedan utilizar sin más y para cualquier cosa. Es necesario también cumplir la normativa sobre protección de datos y, además, habrá que estar atentos a la normativa aplicable, en su caso, al concreto sector en el que se aplique la IA. Así, por ejemplo, en su uso por Administraciones Públicas habrá que tener en cuenta qué se quiere hacer con esa aplicación: no es lo mismo utilizarla para automatizar procesos, de forma puramente instrumental (como en las aplicaciones que facilitan las declaraciones tributarias, que son jurídicamente irrelevantes), que usarlas como una ayuda para decidir cuándo se inicia un procedimiento administrativo (un paso más) o para determinar el contenido de una resolución administrativa, lo que exigirá

normalmente una habilitación normativa y no sólo el cumplimiento de los requisitos generales que establece este proyecto de Reglamento.

REFERENCIAS BIBLIOGRÁFICAS

Brezina, C. (2005). *Al-Khwarizmi: The Inventor of Algebra*. Rosen Central.

Civitarese, S. (2019). ¨Umano troppo umano¨. Decisioni amministrative automatizzate e principio di legalità". *Diritto pubblico*, 1, 5-41.

Díaz, G. (Coord.) (2020). *La regulación de los algoritmos*. Aranzadi.

Hernández, J. (2020). Decisiones algorítmicas de perfilado: régimen y garantías jurídicas. *REDA*, (203), 281-322.

Hoffman-Riem, W. (2018). *Big data. Desafíos también para el Derecho*. Civitas.

Huergo, A. (2019). Las sanciones administrativas en el marco del *law enforcement*. En D. Zegarra, (Coord.), *La proyección del Derecho Administrativo Peruano. Estudios por el Centenario de la Facultad de Derecho de la PUCP*, (pp. 515-539). Palestra.

Kahneman, D. (2012). *Thinking, fast and slow*. Penguin.

Lee, K. F. (2018). *AI Superpowers. China, Silicon Valley and the New World Order*. Houghton Mifflin Harcourt.

Mayer-Schönberger, V. y Cukier, K. (2013). *Big data. The massive data revolution*.

Resolución de estimación de las reclamaciones 123/2016 y 124/2016. (2016, 21 de septiembre). *Comissió de Garantia del Dret d'Accés a la Informació Pública* (Oriol Mir Puigpelat). http://www.gaip.cat/es/inici/

Sentencia 2015AP157-CR. (2016, 13 de julio). *Tribunal Supremo de Wisconsin, State v. Loomis* (Ann Walsh Bradley, J.). https://casetext.com/case/state-v-loomis-22

Van Eck, M. (31 de enero de 2017). Algorithms in Public Administration. *Marlies van Eck*.https://marliesvaneck.wordpress.com/2017/01/31/algorithms-in-public-administration/).

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.