IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

ARTÍCULO

Inteligencia artificial y Administración de Justicia: ¿*Quo vadis, justitia*?

Pere Simón Castellano
Universidad Internacional de La Rioja

Fecha de presentación: agosto de 2020
Fecha de aceptación: diciembre de 2020
Fecha de publicación: abril de 2021

Resumen

La presencia en nuestra vida cotidiana de las más modernas tecnologías de la información y la comunicación, así como de la llamada inteligencia artificial (IA), es cada vez mayor a la par que más valiosa. Las Administraciones públicas no pueden permanecer inmóviles ante una nueva realidad social que ofrece también una brillante oportunidad para incrementar su eficiencia y eficacia en ámbitos muy concretos como, por ejemplo, la lucha contra el fraude y las irregularidades. Los retos y desafíos jurídicos que presenta la IA, empero, son muchos y muy significativos, cuya afectación se proyecta en ámbitos tan diversos como la protección de datos personales, la igualdad, la seguridad jurídica, la transparencia y la rendición de cuentas, entre otros. Los problemas se multiplican exponencialmente en el ámbito de la Administración de Justicia y, muy especialmente, para determinados usos en el marco del proceso penal. Aunque la justicia no es ni debe convertirse en un mero acto de predicción ni en un modelo matemático que pueda encerrarse en fórmulas, no es menos cierto que el empleo de la IA para fines concretos puede resultar muy útil en todos los órdenes jurisdiccionales. El presente artículo plantea en este complejo entramado los términos del debate analizando el marco legal europeo, los usos de la IA en el ámbito de la justicia penal y su impacto en los derechos fundamentales.

Palabras clave

inteligencia artificial, decisiones automatizadas, Administración de Justicia, proceso penal

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Artificial Intelligence in Judicial Systems. Quo vadis, justitia?

Abstract

The presence in our daily life of information and communication technologies is moving up at the same time as what we call artificial intelligence (AI) is increasing as well as being more valuable. Public administrations cannot remain passive in the face of a new social reality that also offers a brilliant opportunity to grow their efficiency and effectiveness in very specific areas such as, for example, the fight against fraud and irregularities. The legal challenges presented by AI, however, are many and very significant, whose impact is projected in very wide-ranging areas such as the protection of personal data, equality, legal certainty, transparency and accountability, among others. The troubles increase exponentially in the field of justice and, especially, for certain uses in the framework of the criminal proceedings. Although justice is not and should not become a mere act of prediction, nor a mathematical model that can be enclosed in formulas, the truth is that the use of AI in certain contexts can be very useful, in all sorts of proceedings. The article sets out in this complex scenario the terms of the debate, analysing the European legal framework, the uses of AI in the field of criminal justice and its impact on fundamental rights.

Keywords

Artificial Intelligence, Automated Decisions, Judicial Systems, Criminal Proceedings

Introducción: el debate en torno a la inteligencia artificial en las Administraciones públicas

La universalización de internet y el empleo masivo de las más modernas nuevas tecnologías, dentro de las cuales debemos incluir desde los sistemas de procesamiento *big data* hasta la inteligencia artificial (en adelante, IA), pasando por el internet de las cosas (o *Internet of Things,* en adelante, IoT), lo han revolucionado prácticamente todo. La forma como nos comunicamos y relacionamos, la inmediatez en el acceso, la velocidad del mensaje y la importancia que damos a la información que nos trasladan nuestras «amistades». En un mundo inundado de información irrelevante (Noah Harari, 2018), cada vez resulta más fácil descontextualizar lo que leemos y compartimos (Dumortier, 2010), subsumidos en una arquitectura en red, sin jerarquía, que pone en tela de juicio la aplicación de criterios y principios que tradicionalmente han permitido a los operadores jurídicos dar respuesta a aquellos casos difíciles en los que chocan o colisionan distintos bienes jurídico-constitucionales que bien merecen protección[1].

En este complejo escenario, asistimos a la proliferación de nuevas técnicas que permiten la recolección, interpretación y procesamiento masivo de datos (personales o no), y su uso por sistemas expertos que piensan y actúan como humanos, o bien piensan y actúan siguiendo la lógica racional (Kaplan, 2017, pág. 1). La IA se está aplicando hoy en día, fundamentalmente, en los campos del procesamiento del lenguaje natural, la visión computerizada y la robótica (Kaplan, 2017, pág. 53), para fines muy diversos, aunque como patrones o elementos comunes cabe destacar que, en cualquier caso, todos los sistemas de IA encuentran sus cimientos, de un lado, en el procesamiento masivo de datos (personales o no) y, del otro, en el uso de algoritmos que establecen reglas lógicas para establecer una respuesta que emule, como decíamos anteriormente, la forma de pensar o actuar de los humanos (Mayer-Schönberger y Cukier, 2013, pág. 13).

Los algoritmos están muy presentes en nuestra realidad cotidiana: especialmente, han sido empleados con notable fortuna (aunque también con un porcentaje de fallo muy significativo) en procesos de *marketing online* y publicidad comportamental, condicionando de forma considerable las decisiones que acabamos tomando, por ejemplo, en el ámbito del consumo de productos y servicios en línea. Para algunos autores somos ya esclavos de la tiranía de los algoritmos (Edwards y Veale, 2017, págs. 19-20).

En la actualidad, los esfuerzos científicos se centran en aquellos algoritmos que permiten el aprendizaje automático o *machine learning*, ya que tienen un mayor potencial de impacto y también una mayor fiabilidad, por la capacidad de aprender de los datos y la experiencia (Federal Financial Supervisory Authority, 2018, págs. 20, 24). Sin embargo, aún estamos lejos de contar con auténticos sistemas de *deep learning* o aprendizaje profundo, cuya principal arista desde la óptica del derecho público es la falta de transparencia en el algoritmo, que se modifica y perfecciona sin que el usuario sea capaz de descubrir de forma sencilla por qué o cómo el algoritmo ha adoptado una decisión o ha producido un determinado resultado[2].

Sea como fuere, lo cierto es que la IA está de moda[3], lo que se acredita fácilmente con la atención que los mercados le están prestando últimamente, así como con los informes de prestigiosas firmas que le auguran un crecimiento imparable a lo largo de la próxima década[4]. De la IA se dice que transformará de forma definitiva la forma como vivimos, proyectando sus efectos sobre las relaciones del trabajo y la producción, automatizando tareas manuales o

1. Buena muestra de ello es el arduo debate en torno al nacimiento y configuración legal del llamado «derecho al olvido digital», un asunto al que la doctrina nacional ha prestado especial atención. Véase en este sentido Simón Castellano (2012 y 2015), Berrocal Lanzarot (2017) y Cobacho López (2019). Otro ámbito paradigmático, por lo que se refiere a la proyección de nuevos problemas por la aplicación de los criterios y principios jurídicos tradicionales al ámbito de internet y a las redes sociales, es el de los llamados «delitos de odio». Véase al respecto Cabellos Espiérrez (2018).
2. La doctrina se refiere tradicionalmente a ello como la *black box* o caja negra del algoritmo, que despliega numerosos rompecabezas desde la óptica jurídica. Véase Cerrillo i Martínez (2019).
3. En esta misma dirección véase Asís Roig (2018, pág. 28); Barocas y Selbst (2016, pág. 672); Cerrillo i Martínez (2019); Cerrillo i Martínez y Peguera Poch (2020).
4. Para muestra un botón. Se estima que la IA puede incrementar el producto interior bruto en 15,7 trillones (PriceWaterhouseCoopers, 2017, pág. 1) y puede suponer un ahorro anual para el Gobierno estadounidense de 1.200 millones de horas y 41.000 millones de dólares (Eggers, Schatsky y Viechnicki, 2018, pág. 3).

rutinarias, en el marco de una nueva revolución industrial, la cuarta o 4.0, que vendrá de la mano de un nuevo paradigma en el que el aprendizaje constante y la especialización no serán una opción[5].

No es de extrañar entonces que la IA cuente ya con numerosas manifestaciones en las Administraciones públicas[6], que la doctrina la haya estudiado con profundidad[7], que el legislador se haya posicionado abrazando tal posibilidad incluso con demasiada premura y sin suficientes cautelas[8], y que dispongamos de la primera resolución judicial que ha declarado ilegal un algoritmo sobre evaluación de características personales de los ciudadanos[9].

En este estado de cosas, las Administraciones públicas utilizan la IA para distintos fines legítimos, entre los que destacan la prevención de riesgos, la detección de irregularidades, fraudes y casos de corrupción, o el apoyo o asesoramiento en la toma de decisiones, por ejemplo, mediante sistemas de predicción policial, de asistencia a médicos para el tratamiento de enfermedades, para asignar subvenciones o evaluar profesores, de alerta de abandono escolar, etc. No se trata ni mucho menos de un listado exhaustivo de fines, puesto que la IA también es utilizada para la prestación de servicios públicos, para responder de forma automática a las cuestiones más frecuentes de los administrados mediante *chatbots* o incluso para la resolución de conflictos entre las Administraciones públicas y la ciudadanía, en cuyo caso la aplicación del algoritmo despliega plenos efectos jurídicos sobre los administrados y, paralelamente, incrementa exponencialmente los retos jurídicos.

En las próximas páginas nos proponemos compartir el marco legal y los fundamentos tecnológicos de la IA, a fin de abordar a continuación el análisis de los usos de esta en el ámbito de la Administración de Justicia y, posteriormente, estudiar su impacto sobre los derechos fundamentales de las partes en el proceso. Es un tema al que la doctrina nacional, hasta la fecha, ha prestado poca atención, si bien ya contamos con una obra de referencia al respecto, más concretamente, el trabajo de Nieva Fenoll (2018).

1. Marco legal europeo

En la actualidad existen muchos instrumentos legales que pueden considerarse directa o indirectamente aplicables en relación con la IA. En este ámbito, y antes de empezar con los instrumentos legales de la Unión Europea, conviene hacer mención del Convenio 108 del Consejo de Europa de 1981, que en 2018 se ha renombrado como Convenio 108+, incorporando como elementos clave los principios de transparencia y proporcionalidad en el tratamiento de datos e incrementando las garantías que han de adoptarse junto a las adecuadas medidas técnicas y organizativas de salvaguarda.

5. Diversos estudios señalan que el 47% de los trabajos actuales están en alto riesgo de desaparecer, por el mero hecho de que serán automatizados o desarrollados por robots en las próximas dos décadas. Véase Frey y Osborne (2017, pág. 38).
6. Atlanta predice el riesgo de incendio de los edificios, Hampton el riesgo de riadas y Chicago y Las Vegas identifican los locales que serán objeto de inspección. Son solo algunos ejemplos; véase más al detalle el Informe IBM Center for The Business of Government (2018).
7. Más concretamente, se ha señalado con acierto que los algoritmos empleados por parte de las Administraciones públicas para la adopción efectiva de decisiones han de ser considerados reglamentos por cumplir una función material estrictamente equivalente a la de las normas jurídicas, al reglar y predeterminar la actuación de los poderes públicos. Véase Boix Palop (2020). Más en general, sobre los efectos y retos jurídicos de la IA, véase Cotino Hueso (2019) y Cerrillo i Martínez y Peguera Poch (2020). Resultan de indudable interés también los documentos de la Red DAIA, más concretamente la conclusión y la declaración final del I y II Seminario Internacional en Derecho Administrativo e Inteligencia Artificial, adoptadas en Toledo y Valencia, respectivamente [en línea] https://www.dropbox.com/s/5px5jkvauiz06vu/CONCLUSIONES_toledoDAIAvfinal.pdf?dl=0 y https://www.dropbox.com/s/zIth1wq0n2z8c0b/declaracionDAIA_Valencia.pdf?dl=0 [Fecha de consulta: 9 de enero de 2021].
8. Es el caso de la Ley 22/2018, de 6 de noviembre, de la Generalitat Valencia, que prevé un sistema de alertas tempranas anticorrupción (SATAN), basado en los criterios de Falciani, respecto del que no tenemos constancia alguna de que se esté utilizando. La Agencia Española de Protección de Datos (en adelante, AEPD), en el Informe 385661/2017, y la doctrina (Cotino Hueso, 2020) han valorado de forma crítica la citada Ley, que consideran restringe de forma inadmisible los derechos al no cumplir los requisitos constitucionales de los límites a los derechos ni los requisitos del artículo 23 del Reglamento General (EU) de Protección de Datos (en adelante, RGPD).
9. Nos referimos a la Sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya, asunto C/09/550982/HA ZA 18-388 [en línea] https://gdprhub.eu/index.php?title=Rb._Den_Haag_-_C/09/550982/HA_ZA_18/388 [Fecha de consulta: 9 de enero de 2021]. Véase al respecto Fernández Hernández (2020a) y Cotino Hueso (2020).

Para lo que aquí interesa, en relación con la IA, el Consejo Consultivo del Convenio 108 ha aprobado como herramientas de derecho dúctil o *soft law* dos guías, una en 2018, dedicada a esclarecer cómo pueden utilizarse las más modernas TIC para prevenir y combatir el crimen[10]; otra en enero de 2019, sobre el uso de la IA y sus implicaciones para la protección de datos[11].

Por lo que se refiere a los instrumentos de la Unión Europea, y más allá del reconocimiento de derechos ya conocidos en el Tratado de Lisboa y en la Carta de los Derechos Fundamentales de la Unión Europea, la normativa más relevante en este ámbito procede, de un lado, del Reglamento 2019/881, de 18 de abril de 2019, relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) (en adelante, Reglamento sobre la Ciberseguridad), si bien no se trata de una normativa *ad hoc* de la IA (Fernández Hernández, 2020c); del otro, de la normativa europea en protección de datos, encabezada por el Reglamento 2016/679, de 27 de abril de 2016 (en adelante, RGPD), y en especial, el artículo 22, que recoge el derecho a no ser objeto de decisiones basadas únicamente en un tratamiento automatizado, cuando estas produzcan efectos jurídicos en el titular de los datos. Un derecho que, a su vez, el apartado segundo del citado artículo excepciona en determinadas circunstancias siempre y cuando se establezcan medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

El principal problema es que el RGPD no cubre ni ofrece una visión homogénea para todos los supuestos. Hay que tener en cuenta, no solo las normativas nacionales, sino muy especialmente la Directiva 2016/680, de 27 de abril de 2016, relativa a la protección de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales (en adelante, Directiva LED), que aplica solo en aquellos casos en los que las autoridades tratan datos personales para los fines citados, pero que en cambio no aplica a las instituciones, órganos y agencias europeas. Para estas últimas debemos estar a lo que regula el Reglamento 2018/1725 relativo a la protección de datos por las instituciones, órganos y organismos de la Unión Europea. Mención especial merece el Reglamento 2017/1939, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea, que tiene su propia regulación y previsión normativa en relación con la protección de datos.

Como se observa, el hecho de contar con un marco jurídico complejo atomizado en distintas directivas y reglamentos, más las normativas nacionales de referencia[12], incrementa la dificultad para establecer criterios comunes para la aplicación de sistemas expertos de IA en el ámbito de la justicia, y evidentemente esta situación redunda en diferentes estándares que en la práctica afectan a los individuos en relación con el procesamiento de sus datos (Belfiore, 2013, pág. 367). La Directiva LED es la normativa de referencia por tratarse de una ley especial que se refiere precisamente al tratamiento de datos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.

Con todo, el principal problema es que el marco jurídico actual europeo no ofrece necesariamente una protección suficiente[13] para el derecho a la protección de datos y el

10. Consejo Consultivo del Convenio 108. Practical guide on the use of personal data in the police sector [en línea] https://rm.coe.int/practical-guide-on-the-use-of-personal-data-in-the-police-sector-couv-/16807913b4 [Fecha de consulta: 9 de enero de 2021].
11. Consejo Consultivo del Convenio 108. New guidelines on artificial intelligence and data protection [en línea] https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 [Fecha de consulta: 9 de enero de 2021].
12. En España debemos hacer referencia necesariamente a la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, y a la mención expresa en relación con las actuaciones automatizadas. En caso de actuación automatizada, deberá establecerse previamente por el Comité técnico estatal de la Administración judicial electrónica la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, la auditoría del sistema de información y de su código fuente. La Ley define las actuaciones automatizadas en su anexo, y en el articulado solo se refiere a los sistemas de firma electrónica, a las copias electrónicas, y a un sistema automatizado de remisión y gestión telemática que garantizará la celeridad en la publicación de los edictos.
13. Como reacción a esta marcada insuficiencia, el Parlamento Europeo aprobó con holgadas mayorías el 20 de octubre de 2020 tres informes que estudian cómo regular la IA para impulsar la innovación, el respeto de estándares éticos y la confianza en la tecnología, en el que anuncia, además, que prepara una batería de medidas para abordar las oportunidades y desafíos de la IA, centradas en la confianza en la tecnología y en su potencial impacto tanto en los ciudadanos a nivel individual como en la sociedad y la economía. Los eurodiputados quieren que

respeto de la vida privada de las personas a la vista del aumento de la utilización de los sistemas automatizados de toma de decisiones y de elaboración de perfiles por las fuerzas policiales y la jurisdicción penal[14] (González Fuster, 2020). Y ello, como consecuencia de que las cautelas y garantías que contiene el RGPD no se aplican necesariamente cuando el tratamiento se realiza con esos fines y porque es el ámbito cubierto por la Directiva LED, que es el verdadero instrumento jurídico aplicable que, si bien es cierto que prevé salvaguardias similares a las del RGPD, no son exactamente equivalentes en todos los casos, además de incluir restricciones, excepciones y derogaciones parciales.

2. Usos de la IA en la Administración de Justicia

El empleo de los sistemas expertos de IA en la Administración de Justicia, en general, puede tener mucha lógica y sentido, por ejemplo, para la propia gestión del seguimiento de archivos, con indiferencia de la naturaleza del proceso o del orden jurisdiccional. La creación de alertas tempranas por parte del algoritmo en función de la inmensa cantidad de datos procesados y la experiencia previa que este haya acumulado puede contribuir a simplificar su gestión y aumentar la eficiencia (CEPEJ, 2018, pág. 63).

Siguiendo en el plano general, las técnicas de IA pueden mejorar el acceso a la jurisprudencia en base al aprendizaje automático y son un activo considerable para complementar búsquedas o vincular varias fuentes legales y jurisprudenciales, incluso mediante técnicas de visualización de datos (CEPEJ, 2018, pág. 63). También la IA puede contribuir a fortalecer la relación entre la justicia y los ciudadanos, haciendo a la primera más transparente, gracias a los *chatbots*, que podrían configurarse para facilitar el acceso a las diversas fuentes de información existentes utilizando lenguaje natural, compartiendo información (plantillas de documentos, solicitudes o modelos contractuales básicos) o incluso generándola en línea (CEPEJ, 2018, pág. 63).

Por su parte, la aplicación de técnicas de IA sobre los datos de la actividad judicial puede arrojar una información clave para realizar evaluaciones cuantitativas y cualitativas, cuyas conclusiones deberían contribuir a mejorar la eficiencia de la justicia, haciendo proyecciones relativas a la carga de trabajo, los recursos humanos y el presupuesto necesario para hacer frente a lo anterior (CEPEJ, 2018, pág. 63).

La IA, en la jurisdicción civil y social, debe tener mucho recorrido en la llamada resolución extrajudicial de conflictos y controversias, ámbito en el que el empleo de sistemas expertos solo puede redundar en beneficios para todas las partes, así como en el ámbito del llamado *Online Dispute Resolution* (ODR). Sirva como ejemplo el uso de técnicas de justicia predictiva por parte de las compañías aseguradoras, que calculan y evalúan las posibilidades de éxito de acudir a los tribunales y, en el caso de que este resulte inferior a un determinado porcentaje, prefieren acudir a sistemas de resolución extrajudicial de conflictos, evitando los costes del proceso judicial.

Otros usos, ya más cuestionables de la IA, antes de entrar a analizar en concreto su empleo para fines propios de la jurisdicción penal, son los relativos al perfilado de jueces y magistrados y los destinados a anticipar, en sentido literal, el sentido de las resoluciones judiciales. Cuantificar y analizar exhaustivamente la actividad de un juez contribuiría a disponer de unos resultados que en el mejor de los casos podría considerarse un asesoramiento cuantitativo y cualitativo para los propios jueces, con fines puramente informativos y de asistencia en la toma de decisiones (CEPEJ,

la futura legislación sobre IA en la UE promueva la innovación, garantice la seguridad y proteja los derechos humanos. Véase la nota de prensa de la sesión plenaria [en línea] https://www.europarl.europa.eu/news/es/press-room/20201016IPR89544/el-parlamento-muestra-el-camino-para-la-normativa-sobre-inteligencia-artificial [Fecha de consulta: 9 de enero de 2021].

14. La Comisión Europea es plenamente consciente de esta debilidad y, en el Libro Blanco sobre la IA señala que el nuevo marco regulador en materia de IA debe ser eficaz para alcanzar sus objetivos sin ser excesivamente prescriptivo, y debe construirse siguiendo un enfoque basado en el riesgo, para así garantizar que la intervención reguladora sea proporcionada. No obstante, requiere de criterios claros para establecer diferencias entre las distintas aplicaciones de IA, en especial para determinar si entrañan un riesgo elevado o no. En el propio Libro Blanco se señalan sectores en los que el uso de la IA debe siempre considerarse de riesgo, como la sanidad, la energía y determinados ámbitos del sector público, como la Administración de Justicia. Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, adoptado en Bruselas, 19.2.2020. COM (2020) 65 final.

2018, pág. 66). Así, el análisis por parte de sistemas expertos de la predictibilidad y previsibilidad de las decisiones judiciales estaría orientada exclusivamente a reducir el margen de discrecionalidad de los jueces, considerado en ocasiones excesivo (Fernández Hernández, 2020b). Estas herramientas, empero, podrían estar abiertas al abuso si se emplean no solo para gestionar los asuntos judiciales de manera más eficiente, sino también para evaluar el grado de desempeño de los jueces, incluido el análisis de supuestos sesgos ideológicos en sus patrones de comportamiento.

En resumen y en términos generales, la IA se utiliza o se está estudiando utilizarla en los sistemas jurídicos europeos con diversos fines: entre otros, para facilitar el acceso a la Justicia (por ejemplo, mediante los *chatbots*), apoyar medidas alternativas de solución de conflictos en el ámbito civil o para el perfilado de jueces (CCBE, 2020).

Un bloque más concreto de usos son los relativos a la sustitución o apoyo por parte de los sistemas de IA aplicados al proceso de determinación judicial de la responsabilidad por la perpetración de un delito, esto es, al *sentencing* o proceso de decisión, hasta la fecha propio de jueces humanos que parten de los heurísticos o atajos intuitivos (Kahneman, Slovic y Tversky, 1982; Nieva Fenoll, 2018, págs. 44-60). Es lo que algunos autores han denominado «inteligencia artificial judicial», que ha centrado el interés dogmático-jurídico en España por las potenciales implicaciones para los derechos fundamentales derivadas de un mal uso de estos sistemas (Miró Llinares, 2018, págs. 97-98).

Los esfuerzos, en cambio, en el marco del ámbito de la jurisdicción penal se pueden englobar básicamente en dos grandes bloques: la actividad predictiva (*predictive policing*) y el reconocimiento facial (González Fuster, 2020).

Respecto a la actividad predictiva, cabe señalar que esta se basa en la consideración de que el procesamiento algorítmico de grandes conjuntos de datos permite revelar patrones de probable comisión de actos delictivos o la identificación de posibles víctimas de futuros delitos, permitiendo su interceptación antes de que ocurran. La predicción *ad hoc* de la prevención del crimen es una tendencia imparable cuya *vis expansiva* ha marcado notablemente los avances en materia de seguridad a nivel mundial y en Europa desde los atentados del 11 de septiembre de 2001, lo que típicamente se ha asociado a la prevención de la delincuencia (Menezes y Agustina, 2020).

Dentro de la actividad predictiva, podemos desglosar cuatro grandes categorías de técnicas utilizadas con tal fin: los métodos destinados a predecir delitos, o a prever lugares y momentos con mayor riesgo de que se produzca un delito[15]; los métodos destinados a identificar a las personas que corren el riesgo de cometer un delito (o de reincidir en él) en el futuro; los métodos destinados a predecir, o a crear perfiles similares a los de los delincuentes anteriores; finalmente, los métodos destinados a predecir a las víctimas de delitos, utilizados para identificar a grupos o personas que tienen probabilidades de convertirse en víctimas (González Fuster, 2020; y Fernández Hernández, 2020b). Los datos que nutren estos sistemas expertos destinados a la actividad predictiva no deben ser necesariamente datos personales (aunque estos siempre aportan un mayor valor), ni estar inextricablemente vinculados a una actividad delictiva; de hecho, sucede exactamente lo opuesto: se trata de información muy diversa que procede en su mayor parte de empresas privadas en el contexto de su actividad ordinaria, y muy especialmente de empresas del sector de la banca, salud, telecomunicaciones y turismo, que también son las más interesadas en sistemas de procesamiento *big data,* junto al sector asegurador o actuarial.

La actividad predictiva permite realizar también un primer cálculo o aproximación al riesgo de que un sujeto incurra en conducta descrita por un tipo penal, en supuestos en los que se debate acordar medidas cautelares (como la prisión provisional) o en los que se enjuicia la concesión de la libertad condicional. Se trataría de que el juez y el ministerio público en su caso se apoyaran en los datos y la técnica algorítmica. El uso de estos instrumentos de predicción por parte de los jueces de la jurisdicción penal en Europa es muy escaso (González Fuster, 2020); no obstante, ya disponemos de resultados de experiencias significativas en modelos en perspectiva comparada, y más concreta-

15. Véase al respecto Valls Prieto (2017) y Miró Llinares (2020).

mente en Estados Unidos y el Reino Unido. Me refiero a los programas COMPAS[16] y HART[17], respectivamente, que calculan el riesgo de reincidencia de una persona que ha sido anteriormente condenada, si bien ambos proyectos han sido duramente criticados por organizaciones no gubernamentales (ProPublica en el caso de COMPAS y Big Brother Watch en el caso de HART).

Lo cierto es que las principales conclusiones o propuestas formuladas por los citados algoritmos mostraron un preocupante sesgo; por ejemplo, en el caso de COMPAS, se demostró la existencia de un sesgo racial indirecto en los modelos que predicen el riesgo de reincidencia mediante el uso de variables sustitutivas que no son neutrales. Aunque la doctrina no es pacífica, diversos estudios afirman que aplicando el citado algoritmo los acusados negros tenían casi el doble de probabilidades en relación con los blancos de ser considerados en situación de alto riesgo de reiteración delictiva (Babuta, Oswald y Rinik, 2018, pág. 7). Tanto el proyecto COMPAS como HART muestran los problemas de un enfoque discriminatorio o determinista, el cual debería basarse más bien en los sistemas europeos, civilistas, que abrazan la reinserción social.

En cuanto a las tecnologías de reconocimiento facial, estas están siendo objeto de notable controversia y limitaciones por lo que se refiere a su utilización, especialmente por parte de empresas privadas. Lo cierto es que se han implementado hasta la fecha muchas iniciativas de reconocimiento facial[18], tanto por parte de autoridades como por parte de empresas privadas; el último caso, muy sonado en España, es el de las cámaras de videovigilancia de Mercadona, que han sido utilizadas para detectar a personas con una orden de alejamiento que les prohíbe entrar a las tiendas, cuestión sobre la que la AEPD ha abierto una investigación[19].

La idea es prevenir el delito o dar cumplimiento a prohibiciones emitidas por sujetos de derecho público o privado mediante la identificación con reconocimiento facial del infractor. Muchos de estos proyectos están paralizados o en moratoria por las cautelas en el tratamiento y las dudas en relación con la normativa de protección de datos. Sin embargo, ciertas iniciativas han obtenido un beneplácito expreso por parte de las autoridades nacionales de protección de datos, como es el caso de la autoridad de protección de datos danesa, que autorizó el empleo de sistemas de reconocimiento facial por parte de un club de futbol para evitar la entrada en el estadio de personas que tenían el acceso prohibido (IT-Pol, 2019).

3. Impacto en los derechos fundamentales y retos jurídicos de la IA en la Administración de Justicia

Los usos de la IA que acabamos de exponer plantean notables retos para la Administración de Justicia desde el punto de vista jurídico, así como amenazas significativas a la calidad de nuestros sistemas de justicia, a la protección de los derechos fundamentales y al Estado de derecho, en general. Los riesgos se multiplican en relación con los usos que facilitan, ayudan o implican la toma de decisiones que despliegan plenos efectos jurídicos sobre los ciudadanos, como por ejemplo los derivados de la actividad preventiva y del reconocimiento facial. Y es en este ámbito en el que procede recordar que los derechos fundamentales de las personas no pueden subordinarse a criterios como la mera mejora de la eficiencia o el ahorro de costes, ya sea para los ciudadanos o para las propias autoridades judiciales (CCBE, 2020).

Por ello resulta fundamental separar los distintos usos de la IA en el ámbito de la justicia, puesto que unos generan muchos más dilemas que otros, por su grado de afectación a los derechos fundamentales (CEPEJ, 2018, pág. 66). De un lado, encontramos un primer bloque de usos de la IA vinculados a los fines relativos a mantener una comunicación activa con los ciudadanos, a reforzar la transparencia del Poder Judicial, a limitar el ámbito de discrecionalidad judicial mediante el perfilado de jueces y magistrados, a

16. Correctional Offender Management Profiling for Alternative Sanctions.
17. The Harm Assessment Risk Tool.
18. En China, Rusia, Estados Unidos, Suecia, etc. Véase al respecto González Fuster (2020, págs. 24-25).
19. Véase la noticia publicada en el diario *El País* al respecto [en línea] https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html [Fecha de consulta: 5 de agosto de 2020].

anticipar el sentido de las resoluciones judiciales y asistir a las partes hacia otras fórmulas como la mediación o la resolución extrajudicial de conflictos, a evaluar el funcionamiento de los tribunales y los jueces o para garantizar el seguimiento de la ejecución de las resoluciones judiciales. Este bloque plantea básicamente problemas en relación con dos derechos o principios fundamentales de alcance constitucional: las cautelas y salvaguardas propias de la normativa en protección de datos personales y el principio de transparencia.

El empleo de sistemas expertos basados en IA en el ámbito de las Administraciones públicas plantea siempre problemas desde la óptica del derecho a la protección de datos, debido a la naturaleza misma de la IA y a su funcionamiento a partir de la recogida, el tratamiento y la combinación de datos. Los algoritmos pueden afectar así, negativamente, a la vida privada de las personas (Crawford y Schultz, 2014, pág. 96), y muy especialmente si se adoptan técnicas basadas en el perfilado y la toma de decisiones automatizadas (Citron y Pasquale, 2014, pág. 3). A través de la elaboración de perfiles, la Administración de Justicia podrá evaluar aspectos de la vida privada de las personas y sus circunstancias personales (familiares, hábitos, etc.) y profesionales, y, en consecuencia, predecir su comportamiento, con un margen de error aún significativo.

Por su parte, la transparencia es uno de los principios de actuación de las Administraciones públicas que ha adquirido sin lugar a duda un mayor reconocimiento y que está teniendo un significativo impacto en el proceso de transformación de la Administración de Justicia en los últimos años (Gómez Manresa y Fernández Salmerón, 2019). Lo anterior exige poner límites a las cajas negras del algoritmo (Cerrillo Martínez, 2019 y Ponce Solé, 2019).

Un segundo bloque de usos de la IA en el ámbito de la justicia penal lo integran los fines susceptibles de transformar nuestro modelo a mejor, pero que a la par despliegan reforzadas amenazas que van más allá del principio de transparencia y del derecho a la protección de datos. En este segundo bloque incluimos el empleo de los sistemas expertos durante las audiencias, ya sea en la fase de juicio o antes del juicio, para fines tan diversos como, por ejemplo, acordar la prisión provisional o la concesión del tercer grado o, en otros modelos judiciales más propios del *common law*, negociar y llegar a acuerdos con la fiscalía sobre los cargos de la acusación en caso de colaboración y aportación de pruebas, o bien para acordar la libertad condicional o calcular la probabilidad de reincidencia de un acusado.

El primer aspecto u óbice que cabe señalar desde la óptica constitucional para este segundo bloque de usos es el contenido del artículo 117.3 de la Constitución y el principio de exclusividad jurisdiccional: únicamente jueces y magistrados pueden juzgar y hacer ejecutar lo juzgado. La función jurisdiccional, que no incluye solo el acto de juzgar, sino también el de hacer ejecutar lo juzgado, corresponde en exclusiva a jueces y magistrados por expreso mandato constitucional.

Algo muy distinto es el empleo de los sistemas de IA como un apoyo para los operadores jurídicos (especialmente, jueces, magistrados y fiscales) que les asista en determinados procesos y les ayude a formar una opinión formada, valga la redundancia, sobre un asunto, con los resultados de los estudios en los que se haya aplicado la técnica algorítmica, ya sea a nivel estadístico, de mera probabilidad o como actividad preventiva.

Anteriormente hemos alertado de las muchas cautelas que hay que predefinir y evaluar *ex ante* en relación con el principio de transparencia y el derecho fundamental a la protección de datos. A la ecuación, ahora, hay que sumar además el derecho a un juicio justo, el derecho de defensa y el principio de igualdad, todos ellos de naturaleza y alcance constitucional. En el caso del derecho de defensa y del derecho a un juicio justo, las alertas se corresponden con la inherente falta de transparencia en la forma en que opera la IA y con la necesidad de garantizar que las partes procesales puedan discutir e impugnar, también, los resultados de la IA. El derecho de defensa exige en este campo permitir que todas las partes involucradas identifiquen el uso de la IA en el caso concreto, pudiendo verificar los datos de entrada de los que se nutre el sistema y los criterios de toma de decisión o razonamiento de la herramienta, porque solo así podrá impugnar en su caso la decisión o resultado que esta propone. La neutralidad y la objetividad de los instrumentos de IA utilizados por el sistema judicial deben estar en cualquier caso garantizadas y ser verificables (CCBE, 2020).

En el caso del principio de igualdad, los problemas aumentan exponencialmente. Buena muestra de ello son las experiencias fallidas de los programas COMPAS y HART,

empleados en Estados Unidos y el Reino Unido, que ya han sido citados más arriba, y que han puesto de manifiesto que los mismos algoritmos que pueden promover la eficiencia, la consistencia y la justicia, también pueden reforzar discriminaciones históricas u obscurecer comportamientos indeseables (Ponce Solé, 2019).

Como indicamos *supra*, los clasificadores algorítmicos de riesgo usados en el sistema COMPAS doblaban la clasificación de personas negras como futuros criminales en relación con las personas blancas, y lo hacían de forma incorrecta (Babuta, Oswald y Rinik, 2018, pág. 7) por varias razones: no había sido testado ni entrenado el algoritmo de forma suficiente (*training data*); no tenía suficiente bagaje en la identificación de patrones y reglas estadísticas; no disponía de suficientes datos o estos eran poco representativos, afectando como resultado la lógica algorítmica a las minorías o a los colectivos poco representados y estableciendo correlaciones sin causaciones.

En consecuencia, desde la perspectiva de la regulación, debería exigirse explícitamente que en el diseño de los algoritmos se respete el principio de igualdad y que se articulen las medidas técnicas, disponibles, para evitar las discriminaciones y los sesgos (Calders, Kamiran y Pechenizkiy, 2009, págs. 13-18). Para ello resulta capital incorporar en el equipo técnico la participación de juristas que garanticen que las reglas de clasificación y las correlaciones siguen también la lógica jurídica y que los datos son suficientes para no aplicar conclusiones sin sustento contra minorías o colectivos poco representativos.

Además, el uso de algoritmos podría limitar el ámbito de discrecionalidad judicial evitando que estos dicten resoluciones que contengan sesgos que generen discriminaciones a una persona o a un colectivo de personas (Zarsky, 2016, pág. 122), empero no podemos desconocer que estamos muy lejos de una técnica tan refinada y que los experimentos, hasta la fecha, han ido más bien en el sentido contrario, con casos de discriminación causados por el uso de algoritmos fallidos.

Conclusiones

A lo largo de este trabajo hemos planteado los términos del debate acerca del empleo de la IA en la Administración de Justicia. Una Administración que, como tercer poder, se encuentra ante la oportunidad o el precipicio, más aún si tenemos en cuenta los efectos que sobre ella se han proyectado en el marco de la crisis del coronavirus. Los desfases de la Administración de Justicia, que presentan diferente naturaleza (estructurales, personales y de interconexión), nos abocan a la digitalización, a las comunicaciones telemáticas y a un apoyo reforzado, mediante sistemas tecnológicos, incluida la IA, a los jueces y magistrados, con el fin de colocar a nuestro tercer poder en el rango público y posición que como tal le corresponde (Perea González, 2020).

El uso de la IA en la justicia, sin embargo, entraña tantos o más riesgos que oportunidades, tanto para la seguridad jurídica como para los principios procesales, en la medida que esta puede verse afectada por la evolución que experimente el algoritmo, basado en un sistema de aprendizaje autónomo. La pérdida del control sobre el algoritmo puede derivar en una afectación de derechos fundamentales de la ciudadanía como la igualdad, el derecho de defensa, la intimidad, la protección de los datos personales o el principio de publicidad y transparencia de las actuaciones judiciales.

A lo largo de este trabajo hemos analizado que los usos de la IA hasta la fecha en la justicia han sido, en perspectiva comparada, muy limitados y para fines muy concretos, si bien las previsiones indican un avance tecnológico notable durante los próximos años en el campo del aprendizaje autónomo. En este escenario que combina, de un lado, la necesidad de la Administración de Justicia de modernizarse y dar respuesta a las crecientes exigencias cívicas, y, del otro, las proyecciones del imparable avance técnico en el campo de la IA, lo más preocupante es, sin lugar a duda, la falta de una regulación y gobierno marco para su uso por parte de las Administraciones públicas, en general, y por parte de la Administración de Justicia, en particular. El marco jurídico aplicable es incipiente y no cubre en esencia la granularidad de supuestos en los que el empleo de la IA puede conllevar un menoscabo de derechos.

En sintonía con todo lo anterior, existe a nuestro humilde entender un único límite infranqueable que opera como óbice a determinados usos de la IA en la justicia penal. Nos referimos a la imposibilidad de que el juez delegue su poder de decisión en un sistema de IA; lo que es de aplicación, además, a cualquier orden jurisdiccional, porque como hemos señalado a lo largo del trabajo la Constitu-

ción es prístina por lo que se refiere al ejercicio de la función jurisdiccional. Este impedimento sería a todas luces insalvable. Cualquier proyecto encaminado a implementar sistemas de IA en la justicia penal debería, además, respetar los principios y derechos de la normativa de protección de datos y superar una evaluación de impacto que en ese ámbito debería esclarecer los riesgos concretos del sistema en el supuesto de hecho en cuestión. Una evaluación sometida a los criterios habituales de los sistemas de cumplimiento normativo, es decir, al principio de mejora continua y revisión, comunicación y consulta, que además admite segundas y terceras opiniones de expertos internos o externos.

Para garantizar la transparencia y el derecho de defensa, así como la igualdad de armas procesales, deberíamos contar con mecanismos *ex lege* que a su vez permitan un control efectivo de la actividad realizada por los equipos técnicos. Para dar respuesta a estas dificultades, los órganos de gobierno de los jueces podrían impulsar la creación de agencias independientes que asumiesen la función de supervisión de los algoritmos utilizados en la Administración de Justicia, siendo más que positivo el establecimiento de la obligación legal periódica de auditar los algoritmos con la publicación de las conclusiones de esta. En consecuencia, desde la perspectiva de la regulación, debería exigirse explícitamente que en el diseño de los algoritmos se respete el principio de igualdad y que se articulen las medidas técnicas, disponibles, para evitar las discriminaciones y los sesgos, así como el control del algoritmo por parte de agencias independientes.

Aunque hoy los usos de la IA estén limitados, es evidente que el futuro, por razones de eficacia, eficiencia y economía procesal, pasa por su empleo como apoyo y asistencia en la Administración de Justicia. El problema estriba en cómo determinar con seguridad jurídica las garantías, cautelas y salvaguardas concretas para cada uso o finalidad específica.

Es trabajo del legislador europeo adaptar el marco normativo incluyendo medidas como las mencionadas con el fin de que los operadores jurídicos puedan, en la práctica, garantizar el empleo de la IA y aprovechar la oportunidad que esta brinda, también, a la Administración de justicia, sin descuidar obviamente los demás derechos y garantías jurídico-constitucionales que se reúnen en las salas de justicia.

20. Aplicando aquí por analogía lo que la doctrina ya ha tenido ocasión de indicar para las Administraciones públicas, en general. Véase Edwards y Veale (2017, págs. 76). Los autores proponen crear un árbitro de datos neutral o *neutral data arbiter*.

Referencias bibliográficas

ASÍS ROIG, R. F. DE (2018). «Robótica, inteligencia artificial y derecho». *Revista de privacidad y derecho digital*, vol. 3, núm. 10, págs. 27-77.

BABUTA, A.; OSWALD, M.; RINIK, C. (2018). «Machine learning algorithms and police decision-making: legal, ethical and regulatory challenges». *Whitehall Report*, núm. 3. Royal United Services Institute for Defense and Security Studies.

BAROCAS, S.; SELBST, A. D. (2016). «Big data's disparate impact». *California Law Review,* núm. 104, págs. 671-732 [en línea] DOI: https://doi.org/10.2139/ssrn.2477899 [Fecha de consulta: 9 de enero de 2021].

BELFIORE, R. (2013). «The protection of personal data processed within the framework of police and judicial cooperation in criminal matters». En: RUGGERI, S. (ed.). *Transnational inquiries and the protection of fundamental rights in criminal proceedings*. Berlín: Springer, págs. 355-370.

BERROCAL LANZAROT, A. I. (2017). *Derecho de supresión de datos o derecho al olvido*. Madrid: Reus.

BOIX PALOP, A. (2020). «Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones». *Revista de Derecho Público. Teoría y Método*, núm. 1, págs. 223-269 [en línea] DOI: https://doi.org/10.37417/RPD/vol_1_2020_33 [Fecha de consulta: 9 de enero de 2021].

CABELLOS ESPIÉRREZ, M. A. (2018). «Opinar, enaltecer, humillar: respuesta penal e interpretación constitucionalmente adecuada en el tiempo de las redes sociales». *Revista Española de Derecho Constitucional*, núm. 112, págs. 45-86 [en línea] DOI: https://doi.org/10.18042/cepc/redc.112.02 [Fecha de consulta: 9 de enero de 2021].

CALDERS, T.; KAMIRAN, F.; PECHENIZKIY, M. (2009). «Building classifiers with independency constraints». En: *IEEE International Conference on Data Mining Workshops*, págs. 13-18 [en línea] DOI: https://doi.org/10.1109/ICDMW.2009.83 [Fecha de consulta: 9 de enero de 2021].

CCBE-COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE (2020). *Considerations on the legal aspects of Artificial Intelligence*. Bruselas: CCBE [en línea] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf [Fecha de consulta: 9 de enero de 2021].

CEPEJ-EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (2018). *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment.* Adoptada en el Pleno del CEPEJ (31.ª sesión), en Estrasburgo, el 3-4 de diciembre de 2018 [en línea] https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment [Fecha de consulta: 9 de enero de 2021].

CERRILLO I MARTÍNEZ, A. (2019). «El impacto de la inteligencia artificial en el derecho administrativo: ¿nuevos conceptos para nuevas realidades técnicas?». *Revista General de Derecho Administrativo,* núm. 50.

CERRILLO I MARTÍNEZ, A.; PEGUERA POCH, M. (2020). *Retos jurídicos de la inteligencia artificial*. Pamplona: Aranzadi.

CITRON, D. K.; PASQUALE, F. (2014). «The scored society: due process for automated predictions». *Washington Law Review,* núm. 89, págs. 1-33.

COBACHO LÓPEZ, A. (2019). «Reflexiones en torno a la última actualización del derecho al olvido digital». *Revista de Derecho Político*, núm. 104, págs. 198-227 [en línea] DOI: https://doi.org/10.5944/rdp.104.2019.24313 [Fecha de consulta: 9 de enero de 2021].

COTINO HUESO, L. (2019). «Riesgos e impactos del Big Data, la inteligencia artificial y la robótica: enfoques, modelos y principios de la respuesta del derecho». *Revista General de Derecho Administrativo*, núm. 50.

COTINO HUESO, L. (2020). «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, núm. 4.

CRAWFORD, K.; SCHULTZ, J. (2014). «Big data and due process: Toward a framework to redress predictive privacy harms». *Boston College Law Review*, núm. 55, págs. 93-128.

DUMORTIER, F. (2010). «Facebook and risks of "de-contextualization" of information». En: GUTWIRTH, S.; POULLET, Y.; DE HERT, P. (eds.). *Data protection in a profiled world*. Londres: Springer, págs. 119-138.

EDWARDS, L.; VEALE, M. (2017). «Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for». *Duke Law & Technology Review,* núm. 16, págs. 18-84 [en línea] DOI: https://doi.org/10.31228/osf.io/97upg [Fecha de consulta: 9 de enero de 2021].

EGGERS, W. D.; SCHATSKY, D.; VIECHNICKI, P. (2018). *AI-augmented government. Using cognitive technologies to redesign public sector work*. Dallas: Deloitte University Press.

EXECUTIVE OFFICE OF THE PRESIDENT NATIONAL SCIENCE & TECHNOLOGY COUNCIL COMMITTEE ON TECHNOLOGY (2016). *Preparing for the future of Artificial Intelligence* [en línea] https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf [Fecha de consulta: 9 de enero de 2021].

FEDERAL FINANCIAL SUPERVISORY AUTHORITY (2018). *Big data meets artificial intelligence. Challenges and implications for the supervision and regulation of financial services* [en línea] https://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.html [Fecha de consulta: 9 de enero de 2021].

FERNÁNDEZ HERNÁNDEZ, CARLOS B. (2020a). «Primera sentencia europea que declara ilegal un algoritmo de evaluación de características personales de los ciudadanos». *Diario La Ley Ciberderecho*, núm. 37.

FERNÁNDEZ HERNÁNDEZ, CARLOS B. (2020b). «Informe para el Parlamento Europeo sobre el uso de la inteligencia artificial en los ámbitos policial y judicial». *Diario La Ley,* 24-7-2020.

FERNÁNDEZ HERNÁNDEZ, CARLOS B. (2020c). «El Consejo de la Abogacía Europea analiza los efectos de la aplicación de la Inteligencia Artificial en el ámbito jurídico». *Diario La Ley Ciberderecho*, núm. 39.

FREY, C. B.; OSBORNE, M. A. (2017). «The future of employment: how susceptible are jobs to computerisation?». *Technological forecasting and social change,* núm. 114, págs. 254-280 [en línea] DOI: https://doi.org/10.1016/j.techfore.2016.08.019 [Fecha de consulta: 9 de enero de 2021].

GÓMEZ MANRESA, F.; FERNÁNDEZ SALMERÓN, M. (2019). *Modernización digital en la administración de la justicia.* Pamplona: Aranzadi.

GONZÁLEZ FUSTER, G. (2020). «Artificial Intelligence and law enforcement-impact on fundamental rights». *European Parliament Think Tank Study* [en línea] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf [Fecha de consulta: 9 de enero de 2021]

IBM (2018). *Delivering Artificial Intelligence in Government: Challenges and Opportunities.* IBM Center

for The Business of Government [en línea] http://www.businessofgovernment.org/report/delivering-artificial-intelligence-government-challenges-and-opportunities [Fecha de consulta: 9 de enero de 2021].

IT-POL (2019). «Danish DPA approves Automated Facial Recognition». *European Digital Rights Initiative* [en línea] https://edri.org/danish-dpa-approves-automated-facial-recognition/ [Fecha de consulta: 9 de enero de 2021].

KAHNEMAN, D.; SLOVIC, P.; TVERSKY, A. (1982). *Judgment under Uncertainty: Heuristics and Biases*. Cambridge: Cambridge University Press.

KAPLAN, J. (2017). *Inteligencia artificial. Lo que todo el mundo debe saber.* Zaragoza: Teell Editorial.

MAYER-SCHÖNBERGER, V.; CUKIER, K. (2013). *Big data. La revolución de los datos masivos*. Madrid: Turner.

MENEZES, C.; AGUSTINA, J. (2020). «Big Data, Inteligencia Artificial y policía predictiva. Bases para una adecuada regulación legal que respete los derechos fundamentales» [en línea] https://www.researchgate.net/publication/341791776_Big_Data_Inteligencia_Artificial_y_policia_predictiva_Bases_para_una_adecuada_regulacion_legal_que_respete_los_derechos_fundamentales [Fecha de consulta: 9 de enero de 2021].

MIRÓ LLINARES, F. (2018). «Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots». *Revista de Derecho Penal y Criminología,* núm. 20, 2018, págs. 87-130.

MIRÓ LLINARES, F. (2020). «Policía predictiva: ¿utopía o distopía? Sobre las actitudes hacia el uso de algoritmos de big data para la aplicación de la ley». *IDP. Revista de Internet, Derecho y Política,* núm. 30 [en línea] https://www.raco.cat/index.php/IDP/article/view/373608 [Fecha de consulta: 9 de enero de 2021].

NIEVA FENOLL, J. (2018). *Inteligencia artificial y proceso judicial*. Madrid: Marcial Pons.

NOAH HARARI, Y. (2018). *21 lecciones para el siglo XXI*. Madrid: Debate.

PEREA GONZÁLEZ, A. (2020). «Tercer poder: la oportunidad o el precipicio». *El Mundo,* 24-6-2020.

PONCE SOLÉ, J. (2019). «Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico». *Revista General de Derecho Administrativo,* núm. 50.

PRICEWATERHOUSECOOPERS (2017). *Sizing the prize: What's the real value of AI for your business and how can you capitalise?* [en línea] https://www.pwc.dk/da/publikationer/2017/pwc-ai-analysis-sizing-the-prize-report.pdf [Fecha de consulta: 9 de enero de 2021].

SIERRA, S. (2020). «Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la Administración Pública». *Revista General de Derecho Administrativo*, núm. 53.

SIMÓN CASTELLANO, P. (2012). *El régimen constitucional del derecho al olvido digital*. Valencia: Tirant lo Blanch.

SIMÓN CASTELLANO, P. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE*. Barcelona: Wolters Kluwer-Bosch.

VALLS PRIETO, J. (2017). *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial.* Madrid: Dykinson.

ZARSKY, T. (2016). «The trouble with algorithmic decisions: an analytic road map to examine efficiency and fairness in automated and opaque decision making». *Science, Technology & Human Values,* vol. 41, núm. 1, págs. 118-132 [en línea] DOI: https://doi.org/10.1177/0162243915605575 [Fecha de consulta: 9 de enero de 2021].

Cita recomendada

SIMÓN CASTELLANO, Pere (2021). «Inteligencia artificial y Administración de Justicia: Quo vadis, justitia?». *IDP. Revista de Internet, Derecho y Política*, núm. 33. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i33.373817

Sobre el autor

Pere Simón Castellano
peresimon@icab.cat
Universidad Internacional de La Rioja

Profesor contratado doctor (acreditado ANECA desde 2015) en la Universidad Internacional de La Rioja (UNIR). Docente en asignaturas de grado y posgrado en distintas universidades (UNIR, Universitat de Girona, UOC, ESERP Business School) y en colegios y asociaciones profesionales (Ilustre Colegio de Abogados de Barcelona, APEP, WCA). Abogado of counsel en Font Advocats. Premio de la Agencia Española de Protección de Datos (2011) y de la Agencia Vasca de Protección de Datos (2015). Investigador del Grupo de Investigación «PENALCRIM» UNIR. Investigador principal del proyecto sobre prisión provisional RETOS UNIR. Contacto con el autor: pere.simon@unir.net