INTELIGENCIA ARTIFICIAL LEGAL Y ADMINISTRACIÓN DE JUSTICIA

Directoras
SONIA CALAZA LÓPEZ
Catedrática de Derecho procesal
Universidad Nacional de Educación a Distancia

MERCEDES LLORENTE SÁNCHEZ-ARJONA
Profesora Titular de Derecho procesal
Universidad de Sevilla

INTELIGENCIA ARTIFICIAL LEGAL Y ADMINISTRACIÓN DE JUSTICIA

THOMSON REUTERS
ARANZADI

Primera edición, 2022

THOMSON REUTERS PROVIEW™ eBOOKS
Incluye versión en digital

La obra "Inteligencia artificial legal y Administración de Justicia" se enmarca en el Proyecto I+D+i de generación de conocimiento y fortalecimiento científico y tecnológico, titulado **"Ejes de la Justicia en tiempos de cambio"** (IPs Sonia Calaza y José Carlos Muinelo), del Ministerio de Ciencia e Innovación, con REF PID2020-113083GB-100, en colaboración con el Instituto Andaluz Interuniversitario de Criminología (sección Sevilla) y la Fundación para la Inteligencia Artificial Legal.

Editorial Aranzadi, S.A.U.
Camino de Galar, 15
31190 Cizur Menor (Navarra)
ISBN: 978-84-1124-672-9
DL NA 1075-2022
Printed in Spain. Impreso en España
Fotocomposición: Editorial Aranzadi, S.A.U.
Impresión: Rodona Industria Gráfica, SL
Polígono Agustinos, Calle A, Nave D-11
31013 – Pamplona

Relación de autores

Directoras:

Sonia Calaza López
Catedrática de Derecho procesal
Universidad Nacional de Educación a Distancia

Mercedes Llorente Sánchez-Arjona
Profesora Titular de Derecho procesal
Universidad de Sevilla

Autores:

M.ª Jesús Ariza Colmenarejo
Profesora Titular de Derecho Procesal
Universidad Autónoma de Madrid

Raquel Castillejo Manzanares
Catedrática de Derecho Procesal
Universidad Carlos III de Madrid

José Antonio Colmenero Guerra
Prof. Titular de Derecho Procesal
Universidad Pablo de Olavide

Cristina Domingo Jaramillo
Contratada predoctoral FPU
Departamento de Derecho Penal

José Francisco Etxeberria Guridi
Catedrático de Derecho Procesal
Universidad del País Vasco/Euskal Herriko Unibertsitatea

Iñaki Esparza Leibar
Catedrático de Derecho Procesal, UPV/EHU

Pablo Gallego Rodríguez
Profesor Ayudante Doctor
Universidad de Córdoba

Juan-Luis Gómez Colomer
Catedrático de Derecho Procesal
Universidad Jaime I de Castellón

Vicente C. Guzmán Fluja
Catedrático de Derecho Procesal
Universidad Pablo de Olavide, Sevilla

Inés Celia Iglesias Canle
Catedrática de Derecho Procesal
Universidad de Vigo

Mercedes Llorente Sánchez-Arjona
Profesora Titular de Derecho Procesal
Universidad de Sevilla

Vicente Magro Servet
Magistrado de la Sala de lo Penal del Tribunal Supremo
Doctor en Derecho

Jordi Nieva-Fenoll
Catedrático de Derecho Procesal
Universitat de Barcelona

Joan Picó i Junoy
Catedrático de Derecho Procesal
Universitat Pompeu Fabra (Barcelona)

Irune Suberbiola Garbizu
Profesora de Derecho Financiero
Universidad del País Vasco-Euskal Herriko Unibertsitatea

Rocío Zafra Espinosa de los Monteros
Profesora Titular de Derecho Procesal
Universidad Carlos III de Madrid

Cristina Alonso Salgado
Profesora Ayudante Doctora de Derecho Procesal
Universidade de Santiago de Compostela

Jaime Criado Enguix

Personal Docente e Investigador FPU Departamento de Derecho Procesal
Universidad de Granada

Ana Isabel González Fernández

Doctoranda Derecho Procesal
Universidade de Vigo

Raúl López Martínez

Juez Sustituto adscrito al Tribunal Superior de Justicia de Aragón

Tatiana López Pérez

Abogado

Francisco Vega Agredano

Juez Sustituto y Abogado
Máster ISDE y Máster URJC, Doctorando UMA Derecho Privado Especial

Sumario

Página

Página

Página

Página

Página

Página

Página

Página

Página

Página

DEBATES PROCESALES

Página

Presentación

El nuevo paradigma de la Justicia digital debe sustentarse en dos fases o períodos nucleares: la primera fase, la Justicia extrajudicial digital –con la implementación, vía Apps o programa informático– de todos y cada uno de los medios alternativos de solución de controversias *on line*, ahí dónde puedan implementarse, con asistentes físicos o robots, a elección del justiciable; segunda fase, derivación –ante el resultado infructuoso– al proceso, que debiera digitalizarse en su integridad para aquellos supuestos de escaso valor económico, antes de llegar al Juez.

Las posiciones más avanzadas llegan a considerar la posibilidad de resolución de conflictos –entendemos que para casos sencillos– directamente por exclusivos cauces de IA, sin intervención humana. Pero sin llegar a tan extrema solución –desaconsejada por la UNESCO–, resulta evidente que el trayecto híbrido, entre la IA y la IH, es el más razonable, en un momento –como el actual, de auténtico éxito y empoderamiento de la Justicia predictiva– en el que comienzan a implementarse sistemas automatizados de diagnóstico del conflicto, con exposición –primero– de las técnicas de analítica predictiva, merced a las cuales podrá determinarse, no sólo cuales sean las fórmulas más adecuadas de solución de esa concreta controversia, sino también la expectativa de éxito de cada una de ellas; como paso previo a la implementación, ya en el proceso, de toda suerte de métodos de localización instantánea de documentos, así como la fructífera búsqueda de legislación, doctrina y jurisprudencia en apoyo de la pretensión formulada, las probabilidades de obtención de la resolución favorable –en calculadoras predictivas–, la redacción digital de todo tipo de escritos –declinatoria, petición de diligencias preliminares y/o medidas cautelares, demanda, contestación, reconvención– e, incluso, el acompañamiento tecnológico durante todo el procedimiento, de todas estas posibilidades –en creciente expectativa– que ofrecen las denominadas "machine learning" hasta el término del proceso, dónde, incluso, coadyuvan al éxito no sólo de la prevención –sistema Vio-Gén–, de la evitación del juicio –sistema Veri-pol–; o, llegado el caso, de agilización del procedimiento, sino también de la mayor Justicia de la respuesta, como

acontece –por ejemplo– con la calculadora 988. Fuera de nuestro país existen múltiples mecanismos de IA –softwares predictivos– que favorecen la prevención y represión punitiva como sucede en EE. UU. con PRED-POL, una herramienta informática capaz de detectar, dentro de una ciudad, los denominados "puntos calientes" o zonas dónde, con cierta probabilidad, pueden desarrollarse, en un determinado momento, actuaciones delictivas; o con COMPAS, un software informático que ayuda a los Jueces a tomar la decisión del ingreso en un centro penitenciario o mantenimiento de la libertad en función de la probabilidad de reincidencia del investigado.

En esta monografía –"Inteligencia Artificial Legal y Administración de Justicia"– se analizan todas estas herramientas –y algunas otras– con perspectiva internacional. Esta obra reúne a un destacado número de investigadores y profesionales, que, con las debidas sinergias, en el marco del Proyecto I+D+i de generación de conocimiento y fortalecimiento científico y tecnológico, titulado **"Ejes de la Justicia en tiempos de cambio",** del Ministerio de Ciencia e Innovación, con REF PID2020-113083GB-100, desde el 1 de septiembre de 2021 hasta el 30 de agosto de 2024, hemos logrado afianzar los primeros pasos de esta imprescindible transición digital de la Administración de Justicia hacia la IAL.

Desde trece Universidades públicas españolas –Universidad de Sevilla, Universidad Nacional de Educación a Distancia (UNED), Universidad del País Vasco, Universidad Autónoma de Madrid, Universidad Pompeu Fabra de Barcelona, Universidad de Barcelona, Universidad Carlos III de Madrid, Universidad de Santiago de Compostela, Universidad de Vigo, Universidad Jaume I de Castellón, Universidad Pablo Olavide de Sevilla, Universidad de Córdoba y Universidad de Granada– y en perfecta sintonía con profesionales de la entidad del Ilmo. Ser. D. Vicente Magro (Magistrado de la Sala 2.ª del TS) especialmente comprometidas en implementación de herramientas de Inteligencia Artificial Legal en la Administración de Justicia, aportamos, en el día de hoy, un luminoso estudio sobre ejes tan vertebrales como, por orden alfabético de apellido de los autores, los siguientes: la impugnación de las decisiones judiciales adoptadas con apoyo de la IA [Prof.ª D.ª María Jesús Ariza (Universidad Autónoma de Madrid)]; digitalización o inteligencia artificial [Prof.ª D.ª Raquel Castillejo Manzanares (Universidad de Santiago de Compostela)]; algoritmos y proceso laboral [Prof. D. José Antonio Colmenero Guerra (Universidad Pablo de Olavide)]; reconocimiento facial [(Prof.ª D.ª Cristina Domingo Jaramillo, (Universidad de Granada)]; sistemas biométricos de reconocimiento facial [Prof. D. José Francisco Etxeberría Guridi (Universidad del País Vasco)]; protección de datos e IA [Prof. D. Iñaki Esparza Leibar

(Universidad del País Vasco)]; registros biométricos y aplicación en perspectiva constitucional [Prof. D. Pablo Gallego (Universidad de Córdoba)]; derechos fundamentales e IA [Prof. D. Juan Luis Gómez Colomer (Universidad Jaume I de Castellón)]; predicción del crimen [Prof. D. Vicente Guzmán Fluja (Universidad Pablo de Olavide)]; registros biométricos en España e Italia [Prof.ª D.ª Inés Iglesias Canle (Universidad de Vigo)]; IA y valoración del riesgo [Prof.ª D.ª Mercedes Llorente Sánchez-Arjona (Universidad de Sevilla)]; IA y violencia de género [Ilmo. Sr. D. Vicente Magro (Tribunal Supremo)]; IA y proceso judicial [Prof. D. Jordi Nieva Fenoll (Universidad de Barcelona)]; derecho probatorio ante las nuevas tecnologías [Prof. D. Joan Picó y Junoy (Universidad Pompeu Fabra de Barcelona)]; IA en el ámbito tributario [Prof.ª D.ª Irune Suberbiola (Universidad del País Vasco)]; IA y proceso judicial [Prof.ª D.ª Rocío Zafra (Universidad Carlos III de Madrid)]. A estos estudios dogmáticos, pueden sumarse otras reflexiones finales sobre las siguientes temáticas: riesgos de la aplicación de la IA en la Administración de Justicia; interacción de la IA y la Justicia; predicción del crimen; impulso procesal e IA e IA en la resolución alternativa de conflictos.

A todos ellos, les agradecemos muy sinceramente su valiosa contribución.

La aportación doctrinal que hoy ve la luz es la segunda parte de un estudio dual: su complemento puede encontrarse en la publicación "Digitalización de la Administración de Justicia", también publicado en la Editorial Aranzadi, tanto en formato papel, como *open Access.*

Sonia Calaza López

Catedrática de Derecho procesal
Universidad Nacional de Educación a Distancia

Mercedes Llorente Sánchez-Arjona

Profesora Titular de Derecho procesal
Universidad de Sevilla

Impugnación de las decisiones judiciales dictadas con auxilio de inteligencia artificial[1]

M.ª Jesús Ariza Colmenarejo

Profesora Titular de Derecho Procesal
Universidad Autónoma de Madrid

SUMARIO: I. REALIDAD ACTUAL DE LA INTELIGENCIA ARTIFICIAL EN LA ADMINISTRACIÓN DE JUSTICIA. II. UNA APROXIMACIÓN A LA NATURALEZA JURÍDICA DE LA HERRAMIENTA GUIADA POR IA. 1. *Decisiones judiciales adoptadas exclusivamente de manera automatizada en base a sistemas de IA*. 2. *La IA como auxilio judicial en la toma de decisiones*. III. DECISIONES BASADAS EN INTELIGENCIA ARTIFICIAL Y EL OBJETO DE LA IMPUGNACIÓN. 1. *Recursos y falibilidad humana*. 2. *Inteligencia artificial como medio de solventar la falibilidad humana*. 3. *Impugnación y falibilidad algorítmica*. IV. CONCLUSIONES. V. BIBLIOGRAFÍA.

I. REALIDAD ACTUAL DE LA INTELIGENCIA ARTIFICIAL EN LA ADMINISTRACIÓN DE JUSTICIA

A nadie escapa el hecho de que estamos abocados a emplear los medios tecnológicos que están a nuestro alcance para lograr una Justicia más eficaz, y, sobre todo, más eficiente. En concreto, en materia de resolución de conflictos, ya son muchas las voces que promueven el uso de sistemas desarrollados mediante inteligencia artificial. No obstante, cabe indicar que hablar de ello resulta ser en exceso ambiguo por la multitud de elementos concomitantes que intervienen tanto en la actividad jurisdiccional, como en todo el entramado algorítmico que determina este amplio

1. El presente trabajo ha sido elaborado en el marco del Proyecto I+D "Inteligencia artificial, Justicia y Derecho: ¿irrupción o disrupción tecnológica en el proceso penal?" (PID 2020-119324GB-I00).

concepto llamado inteligencia artificial. La Unión Europea se muestra sensible a la materia, y por ello, ya ha elaborado el Libro Blanco sobre la inteligencia artificial –un enfoque europeo orientado a la excelencia y la confianza de 19-2-2020, donde se comienza a abordar el concepto en sus múltiples posibilidades–. Pero, sobre todo, pone de manifiesto que conlleva riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o incluso riesgos en su uso con fines delictivos. Como vemos, puede traspasar muchos límites de los cuales debemos ser conscientes, y establecer mecanismos regulatorios con ánimo transfronterizo, ya que se corresponde con una materia de eminente carácter global.

Una de las manifestaciones de la inteligencia artificial se plasma en la idea de una Justicia automatizada, o lo que es lo mismo, la posibilidad de que la resolución de la controversia sea obra de un robot o de una máquina, sustituyendo la decisión del juez. La Justicia automatizada se aleja de otras cuestiones como la posibilidad de que existan aplicaciones informáticas que analicen un sinfín de resoluciones judiciales con el objetivo de anticipar cuál será la decisión de un juez en una tipología de controversias concretas. En este último caso estamos en presencia de herramientas que son útiles a las partes, y que facilitan el planteamiento de una estrategia adecuada a su pretensión, y que se viene denominando Justicia predictiva[2].

Además de lo anterior, la inteligencia artificial constituye una vía de mejora en la tramitación del procedimiento ante los tribunales, es decir, permite conseguir un desarrollo de las actuaciones óptimo[3]. En este sentido, muchas de las actuaciones judiciales vienen determinadas por el impulso formal del proceso, lo que supone un alto grado de automatización en la decisión. Como ejemplos están muchas de las providencias de dación de cuenta de escritos de parte, o de traslado de escritos, notificaciones, y un largo etcétera que no requerirían a priori la intervención de ningún profesional. En este punto la inteligencia artificial cuenta con mayor aceptación, habida cuenta de la ausencia de decisión basada en presupuestos de tipo valorativo. Muestra de lo dicho se encuentra en el impulso que se dará con el Anteproyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia de 2021. El art. 56 incorpora el

2. PÉREZ DAUDÍ, V., "El precedente judicial. La previsibilidad de la sentencia y la decisión automatizada del conflicto", *Revista General de Derecho Procesal*, 54, 2021, p. 2, aborda la cuestión desde la perspectiva de la previsibilidad, no de la elaboración de la decisión mediante mecanismos automatizados.

3. NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial*, Madrid, 2018, p. 35, analiza los casos en los que existe una posibilidad de desarrollar automatismos en el proceso judicial.

concepto de "actuaciones automatizadas", referido a "la actuación procesal producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular". Se produce la desconexión entre la máquina y el juez, pero conviene puntualizar que este sistema está dirigido a la automatización de actuaciones de trámite o de resoluciones simples que no requieren interpretación jurídica[4].

En cualquier caso, lo cierto es que herramientas similares a lo que se viene identificando con inteligencia artificial, aparecen en la toma de decisiones, bien de manera directa, o bien de forma indirecta. En función del grado de intervención en la resolución de controversias, puede tener una repercusión a efectos impugnatorios, si bien no podemos eludir el hecho de que la inteligencia artificial es objeto de críticas cuando se pretende suplir la labor del juez en la toma de decisiones, bajo la excusa de la eficiencia, y también en aras de la objetividad que se presupone por esta vía. También habrá que tener en cuenta el tipo de resolución que se adopte cuando señalamos al sistema de IA como autor de la decisión. No será lo mismo que intervenga en decisiones de carácter interlocutorio, como puede suceder con incidentes de recusación, cuestiones de competencia o conflictos jurisdiccionales, o decisiones de admisión de demandas o recursos (por poner algunos ejemplos), y, sobre todo, la adopción de medidas cautelares, como puede ser una sentencia que pone fin al proceso, con todo tipo de expresiones, valoraciones y pretensiones. A efectos de una adecuada sistematización y estudio más extendido, deberían analizarse por separado cada uno de estos grupos, que, sin duda, no agotarían todas las posibilidades y matices que pueden encontrarse.

Si se realiza una descripción de la presencia de la inteligencia artificial en el momento actual, se comprueba ya existe un cierto grado de intervención. Sin ánimo de ser exhaustivos, y con el fin de comprender indiciariamente esta realidad, hay que partir del concepto de esta figura. Para ello, se puede tomar como referencia la definición que realiza la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial), de 21 de abril de 2021. En el art. 3 se entiende por "Sistema de inteligencia artificial: el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que

4. El precepto se encarga de señalar algunas actuaciones de trámite o simples, como es el numerado o paginado de los expedientes, la remisión de asuntos al archivo cuando se den las condiciones procesales para ello, la generación de copias y certificados, generación de libros, comprobación de representaciones, o la declaración de firmeza de acuerdo con la ley procesal.

puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa". Como puede deducirse, se trata de una definición amplia y que preferentemente pone el foco de atención en el programa informático o software. A partir de ahí, es importante tener en cuenta que existen proveedores, que son los que desarrollan el sistema de IA, y usuarios, que se identifican con los que utilizan el sistema.

Otras definiciones apuntan a la capacidad general de la máquina para replicar de forma independiente los procesos intelectuales típicos de la cognición humana, es decir, reproducir comportamientos intelectuales humanos para resolver problemas, tomar decisiones y aprender del entorno[5]. Para ello, la base del funcionamiento está en el suministro de una cantidad ingente de datos y el desarrollo de algoritmos con finalidades concretas. Lejos de concebirlo como un ser superior, en realidad se trata de un sistema que tiene un funcionamiento estadístico, pero que tiene capacidad para procesar millones de datos en función del objetivo que el ser humano quiera[6]. El razonamiento humano realiza procesos lógicos deductivos e inductivos a partir de un número de datos o de información. A mayor información, estará en condiciones de adoptar una decisión más ajustada en términos de justicia. Y esa es la ventaja con la que cuenta la IA, la capacidad a través de las máquinas de acumular mucha más información y lograr los objetivos que se le marquen, ya sea de tipo predictivo-estadístico, ya sea para identificar patrones repetitivos[7].

En la actualidad ya se han desarrollado sistemas que utilizan la IA como herramienta en la toma de decisiones de los distintos operadores jurídicos. Quizá una de las primeras ha sido Jurimetría, encargada de extraer patrones repetitivos en las decisiones de los jueces. Se trata de un sistema que está enfocado a los abogados en orden a establecer estrategias en sus litigios, pero también tiene la virtualidad de que no conlleva toma de decisiones de carácter jurisdiccional, con lo cual simplemente es una herramienta más. Distinto es el caso de sistemas como COMPAS,

5. SIMÓ SOLER, E., y ROSSO, P., "La destrucción algorítmica de la humanidad", *Diario La Ley*, n.° 9982, 4 de enero de 2022.
6. SIMÓ SOLER, E., y ROSSO, P., *op. cit.*
7. Uno de los ejemplos más generalizados es el uso de la Jurimetría, entendida como herramienta de analítica jurisprudencial predictiva, ya que permite anticiparse en términos estadísticos, a la decisión posible y probable que va a adoptar un órgano judicial concreto, lo que constituye un instrumento que facilita la creación de una estrategia procesal, y, sobre todo, analiza la viabilidad de una pretensión. *Vid.* Retana, C., *et al.*, "Diálogos para el futuro judicial XXII. Jurimetría y Justicia predictiva", *Diario La Ley*, n.° 9837, 26 de abril de 2021.

desarrollado por la empresa Northpointe, que consiste en calcular la probabilidad de reincidencia o de comisión delictiva de un sujeto[8]. El sistema se ha caracterizado por no hacer público el algoritmo que emplea, y porque además se ha demostrado que incorpora un sesgo racial. La herramienta era utilizada por los jueces en EE. UU. como soporte para adoptar determinadas decisiones, y, por consiguiente, se comprobó que algunas fueron decisiones sesgadas.

Por su parte, también se cuenta en la actualidad con el sistema VioGén, que se constituye en el sistema de referencia para seguimiento integral en casos de violencia de género, y que se inserta entre las herramientas que el Ministerio del Interior pone a disposición de los ciudadanos[9]. Su origen está en la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, si bien no se pone en funcionamiento hasta 2007. Entre sus funciones, y en lo que a IA se refiere, destaca la posibilidad de realizar una evaluación del riesgo de reincidencia, lo que a su vez permite llevar a cabo un seguimiento y protección de la víctima a lo largo de todo el territorio. Para ello, se establecen niveles de riesgo[10], que la policía evalúa a través de sistemas informáticos, y que parte de la aportación de la información que se obtiene en el caso concreto[11]. Se trata, en definitiva, de una estructura en la que, a partir de la obtención de datos siguiendo una guía de información, se obtiene un resultado estadístico por el que se establece el nivel de riesgo. Al final, son factores que pueden determinar la adopción de medidas cautelares o de órdenes de protección de víctimas[12].

En otro orden de cosas, y como ejemplo de los usos que la IA tiene en el ámbito de la Administración de Justicia en la actualidad, el CGPJ pone a disposición de los jueces y magistrados una tecnología basada en el "machine learning", cuyo objetivo es llevar a cabo la seudonimización automática de un documento y el acceso automático mediante vínculos a la legislación y jurisprudencia. Se trata de una utilidad de gestión en el

8. SIMÓN CASTELLANO, P., *et al.*, "Diálogos para el futuro judicial XXII. Jurimetría y Justicia predictiva", *cit.*, pone de manifiesto que el problema del sesgo se producía en la incorporación de datos, los cuales no tenían una muestra muy variada y, por lo tanto, las variables del algoritmo también eran escasas. De ahí la necesidad de realizar un diseño del algoritmo idóneo y público.
9. Para un análisis más amplio, *vid.* MARTÍNEZ GARCÍA, E., BORGES BLÁZQUEZ, R., y SIMÓ SOLER, E., "Inteligencia artificial y perspectiva de género en la justicia penal", *Diario La Ley*, n.° 47, Sección Ciberderecho, 20-1-2021.
10. Instrucción 4/2019, de la Secretaría de Estado de Seguridad.
11. Como señala la Instrucción 4/2019, el resultado de la valoración policial del riesgo se comunicará al juez y fiscal en forma de informe automatizado que genera el propio sistema.
12. PLANCHADELL-GARGALLO, A., "Inteligencia artificial y medidas cautelares", Barona Vilar, S., (dir.) *Justicia algorítmica y neuroderecho*, Valencia, 2021, pp. 389 ss.

KENDOJ que facilita dicha seudonimización y el acceso a las decisiones judiciales por los usuarios externos del Poder Judicial, con máximo respeto de los derechos fundamentales en materia de protección de datos.

Una de las cuestiones a resolver como premisa básica, que sólo pretende ser apuntada en este momento, es si el sistema de IA es capaz de resolver problemas y adoptar decisiones que también puede tomar el juez, o si, por el contrario, puede ir más allá, dando solución a problemas que el ser humano no puede resolver, lo que supondría un paso más y concebirlo como un ente más inteligente[13]. Mientras estemos en el primer escenario, se podrá dudar de la utilidad de suplir al juez por la máquina, si bien el factor tiempo es el que va a jugar en favor del uso tecnológico. Si la conclusión fuera la otra, es decir, dotar a la máquina de una cualificación superior al juez, entonces habría que replantear un proceso diferente al que tenemos hoy en día. Por ahora, nada parece apuntar a que un robot o sistema de IA pueda suplir al juez, por lo que la posibilidad hay que descartarla. En definitiva, se trata de un problema de eficiencia, en la idea de empleo de menos recursos para lograr una decisión más rápida y con menos coste humano y material[14].

II. UNA APROXIMACIÓN A LA NATURALEZA JURÍDICA DE LA HERRAMIENTA GUIADA POR IA

En función de lo que consideremos que es la inteligencia artificial y el papel que juega, estaremos en presencia de un sistema que participa de la decisión jurisdiccional de diversos modos, en el sentido de formar parte de la decisión como un todo, o bien considerar que estamos en un mecanismo auxiliador a modo de especialización pericial en determinados aspectos. Así pues, cabe establecer una diferenciación tajante entre la toma de decisiones del juez con auxilio de la inteligencia artificial, y el reemplazo o sustitución del juez. A medio camino estaría la decisión automatizada, pero bajo la supervisión del factor humano[15], que ejerce control sobre la misma, en cuyo caso la percepción es similar al primer caso. Se

13. FERNÁNDEZ, C., "Los jueces ante los problemas jurídicos de la inteligencia artificial", *Diario La Ley*, 3-1-2022, quien trae a colación el documento elaborado por James E. Baker, Laurie N. Hobart y Matthew G. Mittelsteadt, titulado *AI for Judges. A Framework*, en el Center for Security and Emerging Technology.

14. Además, en este caso habría que valorar si la puesta en marcha de un sistema de IA abarata costes, y, por lo tanto, resulta ser más eficiente que la provisión de recursos humanos y tecnológicos para que siempre sea el juez el que adopte la decisión. Si le proveemos de bases de datos, acceso a registros, y programas de análisis estadístico, debe mantenerse la idea de mantener al órgano judicial por encima de la máquina.

15. Al respecto, la Propuesta de Reglamento de IA, dedica todo el art. 14 a la vigilancia humana cuando se utilizan sistemas de IA de alto riesgo.

trataría de un supuesto en el que el órgano judicial es el que asume la resolución, incluso a efectos impugnativos ya que recae sobre él la responsabilidad final. Por otro lado, y como venimos señalando, este mismo esquema puede tener distintas consecuencias según estemos bien ante una decisión puramente formal o de impulso formal del proceso, bien ante una resolución interlocutoria, o bien una decisión de fondo que pone término al proceso. El grado de contribución y relevancia para el derecho del justiciable varía en cierto modo.

La cuestión es determinante de cara a la posible impugnación de la decisión, con independencia del contenido de que se trate. En este sentido, las distintas categorías de IA exigen un esfuerzo legislativo en orden a articular vías impugnativas de esta decisión, se trata de regular el uso de sistemas de expertos en el ámbito jurisdiccional que incluso tiene un trasfondo ético[16]. Los denominados sistemas de expertos consisten en "una serie de programas que permiten obtener inferencias válidas a partir de bases de datos estructuradas, siguiendo trayectos que no se prevén en *ex ante*, justificando cada recorrido con la disposición de las reglas aplicadas y poniendo a disposición una interfaz hombre-máquina para facilitar la introducción de reglas nuevas en aquellos puntos en que las bases de conocimiento revelan ser incompletas o no actualizadas"[17]. En este sistema se distinguirían tres componentes, que son la base de conocimientos, el motor de inferencia, y la base de hechos. Con estos mecanismos se intenta obtener verdades mediante la comprobación y generación de la máquina, que iría más allá de las posibilidades de detección del ser humano.

La utilización de herramientas de este tipo puede equipararse al uso de informes periciales, que llegan a sus propias conclusiones aplicando máximas de experiencia específicas de su arte, profesión o ciencia. La diferencia estriba en el factor tecnológico, ya que ahora podríamos afirmar que se trata de un informe o dictamen elaborado por un robot, en cuyo caso la semejanza en cuanto a su uso y protagonismo en el proceso sería similar. Esta circunstancia facilitaría el tratamiento procesal y consiguientemente su impugnación a través de las vías tradicionales. No obstante, el carácter probatorio del dictamen del perito no sería suficiente para concebir la presencia de un sistema de IA en el proceso[18]. De ahí que su función

16. BUENO DE MATA, F., "Macrodatos, inteligencia artificial y proceso: luces y sombras", *Revista General de Derecho Procesal* 51, 2020, p. 13.
17. ROBERTO GRANERO, H., "La inteligencia artificial aplicada al Derecho –El cumplimiento del sueño de Hammurabi–", *Revista Iberoamericana de Derecho Informático*, n.° 5, 2018, p. 123.
18. CORTÉS DOMÍNGUEZ, V., con MORENO CATENA, V., *Derecho Procesal Civil. Parte General*, Valencia, 2021, p. 274, apunta a que la prueba no sólo recae sobre hechos, sino

auxiliadora lo aleje de la estricta prueba pericial, para considerarlo una forma de auxilio judicial informático o estadístico.

1. DECISIONES JUDICIALES ADOPTADAS EXCLUSIVAMENTE DE MANERA AUTOMATIZADA EN BASE A SISTEMAS DE IA

Para el análisis de este aspecto, tomamos como punto de partida la resolución sobre el fondo, sentencia o auto, que, como adelantamos, constituye un ejemplo del ámbito en el que la IA no puede suplantar al juez a la vista de los siguientes argumentos. Así pues, nos hallaríamos en la situación opuesta a lo que entendemos en la actualidad como resolución de controversias a cargo del órgano judicial; es decir, se trata de sustraer la toma de decisiones de la valoración del juez, para trasladarlo totalmente al sistema de IA. No es la referencia a útiles para el procedimiento, ni a ayudas puntuales para que el que juez adopte una resolución, sino que simplemente se incorporarían los datos del caso concreto para que fuera la máquina la que resolviera.

De entrada, cabe rechazar esta posibilidad, habida cuenta de que existen múltiples obstáculos de carácter constitucional que impiden trasladar la toma de decisiones del poder judicial a la máquina. En primer lugar, el art. 117 CE establece que la jurisdicción se ejerce en exclusiva por juzgados y tribunales predeterminados en la ley. Esto nos sitúa en un escenario en el que el ciudadano justiciable acude a jueces y magistrados para encontrar una resolución de su controversia. Articular un mecanismo diferente supondría transformar el propio Estado de Derecho donde el sistema de inteligencia artificial formara parte de alguno de los poderes del Estado a fin de residenciar las decisiones.

En segundo lugar, precisamente las notas de independencia e imparcialidad pueden ser cuestionadas en caso de mecanismos automatizados, ya que, lejos de asumir que existe aprendizaje en la toma de decisiones, es inevitable vislumbrar un conjunto de elementos de carácter humano que se esconde en el diseño del sistema, y que quedaría fuera de cualquier control a efectos de valorar el cumplimiento de las notas esenciales de la jurisdicción[19]. A ello se le añaden los mecanismos de control e impugnación

también sobre juicios o conceptos. La prueba de peritos sirve para obtener el conocimiento sobre elementos del supuesto de hecho de la norma que no son hechos propiamente dicho, sino máximas de experiencia. Es un conocimiento necesario, pero al mismo tiempo complementario.

19. GÓMEZ COLOMER, J. L., "Unas reflexiones sobre el llamado "juez-robot", al hilo del principio de la independencia judicial", *Justicia algorítmica y neuroderecho*, *cit.*, p. 252.

de la falta de independencia e imparcialidad del juez, que entendemos son mucho más asumibles por el justiciable que si se pretendiera poner de manifiesto esa misma falta de imparcialidad de la máquina, buscando sesgos que hayan provocado indefensión.

Además, cuando el nivel o categoría en el uso de la IA llega a la desvinculación del ser humano, es decir, del juez, entonces los requisitos de la decisión deben estar inspirados en el principio de transparencia a fin de que se colmen los derechos y garantías procesales. Nos referimos a dotar de publicidad y transparencia todo el entramado algorítmico de modo tal que se permita identificar el fallo que constituya objeto de impugnación. Se trata de desviar notablemente el objeto de un recurso hacia ámbitos tecnológicamente avanzados.

De entrada, cabe señalar que esta cuestión ya está vedada en el art. 22 del RGPD (Reglamento 2016/679, de 27 de abril), en el que se reconoce el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, cuando produzca efectos jurídicos en él o le afecte significativamente de modo similar[20].

Un paso intermedio se puede encontrar en los casos en que sea el sistema de IA el que adopte decisiones, pero, en aplicación de las prohibiciones establecidas en la Propuesta de Reglamento sobre IA de 2021, las mismas han de estar vigiladas por el ser humano en virtud del art. 14. Tal y como se señala en la propuesta, podemos identificar que se trata de un sistema de IA de alto riesgo al afectar a derechos fundamentales (tutela judicial efectiva, derecho de defensa, principio de igualdad), por lo que queda prohibida la falta de vigilancia humana. Se trataría de ejercer control, si bien la decisión principal se adopta por la máquina. La determinación del sujeto o mecanismo sobre el que recae la responsabilidad en la toma de la decisión se diluye.

Frente a la idea de que puede optimizarse la decisión automatizada o adoptada por un sistema de IA, cabe señalar su inadecuación a los derechos y garantías procesales. En ningún caso se podrá considerar que la decisión del conflicto puede mecanizarse, ya que en la elaboración del juicio jurisdiccional está presente la valoración de material probatorio, la

20. No obstante, se entiende que este precepto se aplica sólo a decisiones automatizadas, y que afectan a los titulares de los datos, y no regula la lógica del algoritmo, tal y como señala COTINO HUESO, L., *et al.*, "Un análisis crítico constructivo de la Propuesta de Reglamento de la UE por el que se establecen normas armonizadas sobre la Inteligencia Artificial (*Artificial Intelligence Act*)", *Diario La Ley*, 2/7/2021. Este tipo de cuestiones puede generar dudas en la identificación del responsable de la decisión cuando hay completa desvinculación entre sistema de IA y juez.

identificación de hechos como probados, y la aplicación de preceptos de carácter general al caso concreto. La doctrina ha señalado que las máquinas no son capaces de interpretar conceptos complejos e introducir variables nuevas, ya que detrás de la toma de decisiones esta su introducción previa por parte de un humano[21]. El establecimiento de un software que pueda ser calificado como más independiente, más imparcial que el juez, parece inalcanzable. Diferente es que nos hallemos en un contexto procedimental automático, como aquel en que se encuentra el impulso formal del proceso. Quizá sólo en este campo pueda generarse un sistema más eficiente en base a decisiones que no requieren valoración particular, sino puro mecanicismo. Así se anticipa en el art. 56 del anteproyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia de 2021. No obstante, el propio precepto se encarga de posibilitar que las actuaciones automatizadas proactivas (es decir, aquellas que se inician sin intervención humana), se puedan también realizar en forma no automatizada, incluso que se puedan deshabilitar, revertir o dejar sin efecto las actuaciones automatizadas ya producidas.

Además, hay que tener en cuenta la perspectiva del justiciable, que generalmente ha puesto su confianza en el juez para la resolución de su controversia. Habría que ver si ante una máquina que resuelve su controversia amplía su confianza. En buena lógica cabe llegar a la conclusión de que cuando el justiciable ve satisfecha su pretensión, muestra plena conformidad con la institución, con el Poder Judicial y con el juez que ha dictado la resolución. Por el contrario, si la petición ha sido desestimada, es probable que se ponga en entredicho la independencia e imparcialidad del órgano judicial.

Con las máquinas nada hace pensar que lleguemos a conclusiones diferentes. La percepción puede ser similar, habida cuenta de que cuando es un programa informático el que decide e impone la decisión, se hace más palpable la falta de conocimiento de un razonamiento adaptado al caso concreto. Y es en este punto donde también se aprecian diferencias en la decisión y en las posibilidades posteriores de impugnación.

En efecto, la cuestión se focaliza ahora en la necesidad de motivación de las decisiones judiciales. Al respecto, se ha llegado a decir que

21. MARTÍNEZ GARCÍA, E., BORGES BLÁZQUEZ, R., y SIMÓ SOLER, E., "Inteligencia artificial y perspectiva de género en la justicia penal", *cit.*, plantean la situación en la que la máquina es capad de tener conciencia y variar sus decisiones como algo utópico. BARONA VILAR, S., "Una justicia digital y algorítmica para una sociedad en estado de mudanza", Barona Vilar, S., (dir.) *Justicia algorítmica y neuroderecho*, *cit.*, p. 46, plantea la imposibilidad de que aún las máquinas piensen como el humano. Su pensar no sería inteligente sino estadístico.

los motivos por los que se resuelve el caso concreto se manifiestan de manera más objetiva cuando se automatizan, especialmente cuando se trata de resolver asuntos con la base fáctica idéntica o similar, por lo que se cumpliría mejor con esta exigencia constitucional. La cuestión ha sido puesta de manifiesto en un ámbito como el de los procesos colectivos, donde se parte de la base de hechos similares a los que le son de aplicación el mismo efecto como consecuencia de la similitud de las particulares situaciones. En la actualidad, ya se cuenta con prácticas en el foro en las que se percibe un comportamiento similar[22]. Es decir, por un lado, y con la creación de juzgados especializados en cláusulas abusivas, se tiende a repetir, cuando no a reproducir, mismos argumentos. Y por otro, consecuencia de que al final el mismo juez asume un volumen ingente de asuntos con prácticamente la misma base fáctica, éste viene a dictar sentencias de forma automatizada.

La pregunta que surge inmediatamente es la siguiente: ¿esta misma forma de decidir también la van a realizar los programas informáticos en los que se basa el sistema de IA? Pero, además, ¿eso favorece una justicia más eficiente? Y, en último término, ¿qué consecuencias puede tener la revocación de una sentencia dictada bajo esta fórmula sobre las demás? Los riesgos de generalizar o reiterar justificaciones o motivaciones estándar son incluso mayores que cuando el juez trae a colación la jurisprudencia habida sobre un caso concreto[23]. El problema no se reduce exclusivamente a identificar el objeto de la impugnación, sino el efecto sobre asuntos particulares similarmente resueltos.

En cualquier caso, si pensamos en una posible impugnación de la decisión que adopta el sistema de IA, el esquema clásico de recursos cae, ya que éste está construido sobre la base de la falibilidad humana, y, por lo tanto, habría que atribuir este carácter también a la máquina, como veremos más adelante. A ello se añade el hecho de que la aplicación de la norma al caso concreto se convierte en una generalización análoga a la actividad legislativa, entendida como regulación de situaciones en abstracto, frente a la función jurisdiccional, que busca la decisión de asuntos concretos. Con ello se destruiría el sistema de separación de poderes y nos situaría ante un juez legislador, en línea con ordenamientos de corte anglosajón. El *common law* precisamente espera del juez la vinculación al precedente, que se construye sobre la base de la eficiencia, la continuidad del derecho, la justicia o equidad, la legitimidad y la mejora de las

22. PÉREZ DAUDÍ, V., "El precedente judicial. La previsibilidad de la sentencia y la decisión automatizada del conflicto", *cit.*, p. 15.

23. NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial*, *cit.*, p. 24, quien trae a colación el corta-pega tan accesible para todos los que consultan textos.

decisiones de los tribunales[24]. Bien es cierto que la necesidad de dotar de seguridad jurídica a la actividad jurisdiccional hace que casos concretos se resuelvan de forma similar, o al menos con una aplicación uniforme de la norma, pero eso no supone una exactitud o identidad absoluta entre las motivaciones. Sobre todo, porque es más que probable que la actividad probatoria difiera y su resultado también.

2. LA IA COMO AUXILIO JUDICIAL EN LA TOMA DE DECISIONES

Mucho se está hablando de la posibilidad de que la IA ayude al juez en la toma de decisiones, bien como vía para reforzar la motivación, o como incorporación al juicio jurisdiccional de máximas de experiencia elevadas a la máxima potencia, o como control a la parcialidad o sesgo del juez. La realidad, así como el principio de exclusividad jurisdiccional residencia el juicio en el juez, entendido como persona que, a través de la sentencia, realiza un acto de voluntad y de pensamiento[25]. La cuestión no tendría más trascendencia si no fuera porque se intenta incorporar una herramienta en forma de algoritmos, que coadyuva en la decisión judicial. El problema fundamental es dilucidar cómo y cuándo contribuye en la decisión del juez.

Cuando se presenta la controversia ante el juez, éste se encuentra en la necesidad de identificar qué hechos quedan probados a partir de la actividad probatoria que desarrollan las partes. En este sentido, los sistemas de IA pueden desplegar su utilidad en múltiples vertientes. Por ejemplo, pensemos en una fórmula para identificar la credibilidad de un testigo, en la que se incorpore información y datos al sistema que concluya con porcentajes de credibilidad del testigo, o incluso de la parte. Algo similar puede desarrollarse cuando nos referimos a la prueba pericial, tan determinante en la mayor parte de procesos y sustento básico en la decisión del juez. Establecer parámetros o algoritmos que permitan predecir el resultado o viabilidad del informe, también constituye una herramienta que facilita la conclusión del juez.

La focalización de los sistemas de IA en la actividad probatoria facilita la labor del razonamiento probatorio del juez, con el fin de declarar la existencia de hechos probados. Al mismo tiempo, el auxilio se puede tener

24. BRENNER, S. y SPAETH, H. J., *Stares indecisis. Las alteraciones del precedente en la Corte Suprema de Estados Unidos*, Madrid, 2017, p. 17, donde se vienen a analizar los problemas y ventajas del uso de precedente, cuestión que puede ser aplicable y predicable de las decisiones adoptadas bajo un sistema de IA.

25. CORTÉS DOMÍNGUEZ, V., con Moreno Catena, V., *Derecho Procesal Civil. Parte General*, *cit.*, p. 314.

incorporando todas estas variantes probatorias, para lograr un resultado de certeza de hechos, lo que conseguiría lograr una aplicación más ajustada del derecho.

Si la aplicación de la IA en la actividad probatoria resulta ambiciosa, no lo es menos cuando puede contribuir a establecer líneas jurisprudenciales, sus manifestaciones, existencia de jurisprudencia contradictoria, mayoritaria, etc. Se trataría de sistemas similares a los que ya utilizan los abogados con el fin de plantear una estrategia de demanda y de defensa[26]. Al fin y al cabo, la idea es encontrar en tiempo record las líneas jurisprudenciales, o como sucede en otros ordenamientos, el precedente sobre el que se construye la nueva decisión. En este caso, nos movemos en el mundo de la motivación del derecho, es decir, la labor de subsumir un hecho en la norma jurídica correspondiente, lo que deriva en una determinada consecuencia jurídica.

En definitiva, cabría traer a colación en este punto las preguntas que Cortés Domínguez prevé como sucesión de problemas metodológicos del juez[27]. Al respecto se plantea cómo puede conocerse si una consecuencia jurídica se presenta como exigida en un determinado momento y lugar. Pero también, y más identificable en el problema de la IA, cómo llega a conocer el juez el hecho y cómo la regla jurídica. Por último, habría que identificar los actos de pensamiento que son necesarios para realizar la subsunción.

La complejidad del juicio jurisdiccional realizado por el juez se fracciona en varios hitos, como se ha señalado, hitos relativos a la actividad probatoria, y a la labor de subsunción, para finalizar en la consecuencia jurídica pedida por las partes. El recurso a sistemas de IA puede ser considerado como un complemento de la actividad probatoria. Así pues, si, por ejemplo, se ha utilizado un programa para identificar el grado de credibilidad de un testigo, en el que se incluye información que detecte contradicciones en su declaración, con análisis facial, gestual, de voz, o incluso incluyendo parámetros que tienen que ver con su lugar de nacimiento, filiación, estudios, actividad laboral, gustos (perfectamente extraíbles del uso de telefonía móvil), etc., podemos concluir que la herramienta aporta máximas de experiencia para que el juez pueda valorar con mayor acierto una prueba testifical. Viene a constituir un elemento análogo a la práctica en la que el juez rescata de su experiencia casos en los que discrimina

26. El mecanismo es el desarrollado por empresas privadas, tales como Jurimetría, que sirve de apoyo a los juristas en la toma de decisiones porque se basa en la creación de patrones repetitivos a partir de resoluciones judiciales.
27. CORTÉS DOMÍNGUEZ, V., *op. cit.*, p. 318.

sobre la certeza o mayor incerteza de una declaración. Lo importante en este caso es que el juez manifieste los elementos que le han llevado a dotar de credibilidad un testimonio, en virtud de la necesidad de razonar su resolución.

En la actualidad, sobre el juez recae una exigencia argumentativa basada en criterios de sana crítica y de la lógica racional, pero si incorporamos el sistema algorítmico que coadyuva para dar la explicación, la obligación puede tener una doble lectura. O bien entendemos que aportaría un plus de explicación y justificación, o, por el contrario, la remisión a la máquina puede provocar el efecto inverso, es decir, un automatismo en el juez relajando la necesidad de motivación porque ya lo hace la IA y su criterio goza de una presunción de objetividad, imparcialidad, y eficiencia. Esta cuestión es determinante para futuros recursos, en los que se plantee una revisión de la motivación, y en concreto del razonamiento probatorio seguido por el órgano judicial.

La necesidad de que el juez asuma, en última instancia, la responsabilidad de su decisión, se anticipa en el Anteproyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia, por la que se transpone al ordenamiento jurídico español la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades. La propia Exposición de Motivos establece la posibilidad de que el juez se haga asistir de sistemas de IA que elaboren borradores o propuestas de textos, pero manteniendo siempre el control sobre éste, y sin que el borrador se constituya en una decisión sin la intervención del operador. Por su parte, el art. 35 del anteproyecto regula los principios generadores del dato, materia especialmente sensible cuando se habla de inteligencia artificial, con el fin de posibilitar el uso de la IA para un conjunto de funciones relacionadas con la Administración de Justicia, incluyendo la tramitación y la conclusión, pero sobre todo con el fin de promover políticas públicas.

Con carácter más general, el art. 57 del anteproyecto regula las que denomina "actuaciones asistidas", que vienen posibilitadas cuando el "sistema de información de la Administración de Justicia genera un borrador total o parcial de documento complejo en base a datos, que puede ser producido por algoritmos, y puede constituir fundamento o apoyo de una resolución judicial o procesal". Por lo tanto, la materia se va a focalizar en el fundamento y apoyo de la resolución judicial o procesal. El borrador que se genere puede ser modificado a voluntad del usuario, que es el juez, por lo que la autoría le va a ser atribuida en exclusiva.

Resulta especialmente relevante la regulación que se hace de las actuaciones automatizadas, ya que se diferencia entre el carácter de asistida o proactiva, si bien en ambos casos la figura del Comité Técnico Estatal de la Administración Judicial Electrónica se encargará de describir las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, la auditoría del sistema de información y de su código fuente. Con el fin de evitar zonas de penumbra en el funcionamiento de estos programas, los criterios de decisión automatizada han de ser públicos y objetivos. Con ello se pretende salvaguardar el conocimiento por terceros, y no sólo por parte de los jueces, de los datos y criterios que se han seguido para establecer los algoritmos que asisten o promueven decisiones. El riesgo de algoritmos sesgados se minimiza, aunque el control al respecto parece tener un carácter público y administrativo.

III. DECISIONES BASADAS EN INTELIGENCIA ARTIFICIAL Y EL OBJETO DE LA IMPUGNACIÓN

Si bien se están planteando cuestiones y problemas que pertenecen al campo de la justicia-ficción, no se puede evitar pensar en los riesgos y en el cambio de paradigma, a la vista de distintas fórmulas de adopción de decisiones. En este sentido, es determinante conocer el papel que puede jugar la IA en decisiones jurisdiccionales, aunque adelantamos que ha de excluirse cualquier posibilidad de que la lógica judicial sea suplantada por la lógica algorítmica. Todo lo más puede ayudar en la toma de decisiones como lo que es, es decir, una herramienta capaz de procesar ingente información en la idea de llegar a conclusiones estadísticas.

La referencia al ordenamiento procesal pasa inevitablemente por el establecimiento de un sistema de recursos que permita la revisión de la decisión emitida en primera instancia, sobre la base del hipotético error del juez en la toma de la decisión. Los problemas que suscita el nuevo elemento están referidos al grado de intervención en la resolución, y a la forma de justificar tanto el auxilio al mismo como todo lo que se esconde tras el producto del que el juez es usuario.

1. RECURSOS Y FALIBILIDAD HUMANA

Las sentencias en general nacen con vocación de permanecer en el tiempo, ya que es consustancial a la jurisdicción el hecho de que se creen y reconozcan situaciones jurídicas y se decida sobre ellas de forma

irrevocable. Ello es quizá más importante cuando nos referimos al proceso penal. Por ello, el ordenamiento procesal incorpora herramientas mediante las que se impugna una decisión del juez. Como señalara Calamandrei, el enjuiciamiento realizado en primera instancia puede adolecer de defectos en la actividad procedimental, lo que determina una irregularidad formal durante el proceso decisorio, y de defectos en la actividad de enjuiciamiento, que conduce a una aplicación de la norma al caso concreto poco satisfactoria para alguna de las partes[28].

En la actualidad, el derecho a los recursos se encuentra regulado tanto a nivel internacional como a nivel interno, por lo que cualquier decisión que provenga del órgano judicial debe insertarse en una estructura en la que se permite la revisión por otro órgano judicial. No obstante, no merece la misma consideración una resolución de carácter interlocutorio que aquella que pone fin a la controversia, también a efectos de valorar la incursión de un sistema de IA en el resultado, ya que el derecho al recurso también tiene una distinta graduación.

El Pacto Internacional de Derechos Civiles y Políticos de 1950 dispone en el art. 14.5 que "toda persona declarada culpable de un delito tendrá derecho a que el fallo condenatorio y la pena que se le hayan impuesto sean sometidos a un tribunal superior, conforme a lo prescrito por la ley". Dentro del ámbito de la Unión Europea, y siguiendo con la línea marcada en el Pacto de Nueva York, el Convenio Europeo de Derechos Humanos introduce en el año 1984 una regulación más prolija (Protocolo 7, art. 2), en el sentido de reconocer el derecho a que la "declaración de culpabilidad o la condena sea examinada por un tribunal superior. El ejercicio de este derecho, incluidos los motivos por los cuales pueda ser ejercitado, se regularán por ley".

Como puede comprobarse, desde el ámbito internacional, la existencia de un reconocimiento al derecho a los recursos en determinados ámbitos plantea de por sí algunos debates, pero si introducimos el elemento tecnológico, el planteamiento debe revisarse, y, sobre todo, identificar el punto en que la decisión del juez puede ser revisada, y qué aspectos de la misma pueden también ser objeto de impugnación. En todo caso, la jurisdicción ha de mantener sistemas de depuración de determinados errores del juez, al tiempo que se configure un espectro de decisión para el órgano superior. Nos referimos al hecho de que, incluso el órgano superior puede hacerse asistir de sistemas de IA para resolver el recurso planteado.

28. CALAMANDREI, P., "Vicios de la sentencia y medios de gravamen", en *Estudios sobre el proceso civil*, trad. Sentís Melendo, S., Buenos Aires, 1961, p. 445.

2. INTELIGENCIA ARTIFICIAL COMO MEDIO DE SOLVENTAR LA FALIBILIDAD HUMANA

El esquema propio del sistema de recursos parte de la premisa que señala al juez como persona que puede cometer errores, y, por lo tanto, dictar resoluciones o sentencias erróneas. Como se viene señalando, la multitud de resoluciones es muy amplia, con lo que habría que realizar un ejercicio pormenorizado para determinar en qué casos, la irrupción de la IA puede atenuar la posibilidad de error judicial, y cuándo podría ser objeto de impugnación.

Cuando los mecanismos de IA coadyuvan a dictar la sentencia del juez, especialmente en cuestiones más puntuales como la determinación de la credibilidad de un testigo, o en el ámbito de medidas cautelares, debe quedar claro cuál es el campo de decisión del juez y cuál el de la máquina. En este sentido, no cabe duda de que la decisión que acude a la ayuda debe integrar el resultado automatizado. En este punto se despliega una serie de cuestiones complejas a dilucidar en cada caso concreto.

Reconocer que el juez puede errar en el fallo es algo comúnmente aceptado, y, por ende, se regulan mecanismos impugnatorios para solventar posibles errores que se cometen durante el proceso jurisdiccional. De ahí que, la incorporación de sistemas de IA atenúen o minimicen el error como aspiración última[29]. No se trata sólo de potenciar una justicia eficiente por ser más rápida e inmediata, sino que se eliminen aquellos aspectos que pueden dar lugar a los recursos porque la IA supere las dificultades que el juez tiene para identificar ciertas cuestiones por sí solo. Por ejemplo, una valoración más exhaustiva de cualquier prueba evitaría recursos basados en la errónea valoración de la prueba (art. 849.2.° LECrim), o una mejor identificación de criterios jurisprudenciales uniformes o contradictorios, o la interpretación de infracciones de derechos o garantías procesales que provocan indefensión.

Ahora bien, no cabe duda de que estaríamos ante una composición dual de la decisión. Juez y máquina interactúan, pero es el juez el que debe asumir en última instancia la decisión. Entre las cuestiones a resolver está el hecho de establecer si el juez estaría obligado a acudir a un sistema de IA para completar o complementar su decisión, o si puede prescindir, o si viene obligado (pensemos en el programa COMPAS o VIOGEN); por otro lado, hasta qué punto es suficiente señalar en una sentencia o auto que se decide en función de lo que dice la máquina; además, cuando se habla de

29. Se llega a señalar que la aplicación de IA lleva a una menor parcialidad que las personas, ya que los datos son objetivos, neutros y racionales. *Vid.* SIMÓ SOLER, E., y ROSSO, P., *op. cit.*

la vigilancia del humano sobre la máquina, tendríamos que formar tecnológicamente a los jueces no sólo para saber utilizar la herramienta, sino para comprenderla y cohonestar las decisiones que se adopten.

Todas estas cuestiones repercuten en el objeto de una impugnación, ya que el justiciable debe conocer en cada momento de las razones que han llevado al juez a decidir su asunto, para así, recurrir la decisión en base a una errónea valoración de la prueba por parte del juez, una errónea apreciación de la prueba por parte del sistema de IA, una falta de uso de la misma, o una toma de decisión en exclusiva por parte de la máquina sin ningún tipo de vigilancia, control, o comprobación, por no hablar de la ampliación de motivos que pueden dar lugar a un recurso.

En la medida en la que el proceso o el recurso alegue la vulneración de una cuestión más automatizable, como puede ser el caso de una sentencia que tienen defectos formales, o un procedimiento dictado sin el correcto emplazamiento del demandado, entonces el sistema puede ser útil. Ahora bien, esta misma automatización puede realizarla el juez sin necesidad de la máquina. La incorporación de la IA lo que hace es multiplicar las posibilidades de encontrar motivos para recurrir la decisión.

A la vista de futuras regulaciones, para la consideración de sistemas automatizados enfocados a las actuaciones judiciales, el análisis debe centrarse en su repercusión en el derecho a un proceso con todos los derechos y garantías procesales, sin que provoque indefensión. Este ha sido el argumento que se ha utilizado para impugnar las decisiones adoptadas en Estados Unidos con el soporte de COMPAS[30]. El famoso "caso Loomis" dio lugar a recurrir la sentencia que había condenado al señor Loomis sobre la base del resultado del programa que decidía que existía un algo riesgo para la comunidad. El recurso alega la vulneración del derecho a un proceso con todas las garantías porque no se podía conocer cuál había sido el algoritmo que había utilizado el programa para llegar a tal conclusión, habiendo sido asumida la decisión íntegramente por el juez sin mayor discusión. El recurso fue rechazado por la Corte Suprema de Wisconsin porque consideraron que el programa informático se había basado en factores habituales, como huir de la policía y el historial delictivo. Se dotaba al programa de presunción de objetividad, y, por lo tanto, se superaban los sesgos que el ser humano podía tener en la decisión.

Dicho lo anterior, como vemos, si su uso se considera como un derecho o garantía procesal, entonces habrá que estipular en qué términos, lo cual puede quedar a criterio constitucional por cuanto cada caso concreto

30. PINTO PALACIOS, F., "¿Pueden los robots administrar justicia?", *Diario La Ley*, n.° 9808, 11-3-2021.

puede diferir. Por supuesto, si partimos de la concepción de su uso con el fin de garantizar una decisión objetiva e imparcial, entonces la decisión del juez prescindiendo del programa informático puede generar una decisión contraria a las garantías procesales que causa indefensión. De ahí la necesaria articulación del auxilio de sistemas automatizados, auxilio que no imposición, en términos similares a lo que establece el art. 56.4 del anteproyecto de Ley de Eficiencia Digital, que previene la posibilidad de realizar las actuaciones de forma no automatizada. El recurso al sistema debe quedar, en todo caso, bajo la decisión del juez a la vista del caso concreto.

En este sentido, dejar a la discrecionalidad del juez el uso o no de tales sistemas, puede llegar a ser interpretado como una decisión que también debe estar justificada. Ahora bien, podría regularse en términos de opción para las partes, e incluso para el juez; es decir, que fueran las partes las que, mediante solicitud razonada, pudieran pedir al juez hacerse auxiliar de un sistema de IA a fin de dotar de seguridad y mayor certeza la decisión. En este caso situaríamos la herramienta al mismo nivel que una prueba pericial tecnológica, de la cual el juez puede hacer uso o no, y en su caso, tomar en cuenta en su decisión. Pongamos el caso de un sistema para arrojar más luz sobre la credibilidad de un testigo, o una fórmula para establecer el mayor peso probatorio entre varios dictámenes periciales, o en su aplicación para determinar el riesgo por la mora procesal para la adopción de medidas cautelares.

La situación mencionada, en la que son las partes las que instan el uso y auxilio de sistemas de IA, facilitaría, por un lado, la confianza en la máquina, y por otro, la aceptación de las decisiones que se adoptan con el sistema, lo que revierte en menor tasa en el planteamiento de recursos. Quedarían alejados los problemas que suscita la decisión unilateral del juez, y la integración del resultado en su decisión. No obstante, esto puede dar lugar a nuevos interrogantes, como el proveedor del sistema de IA, los controles por parte de órganos judiciales, Administración de Justicia, y ciudadanos, o su integración cual peritos judiciales. A medida que se avanza en las hipótesis, surgen nuevos inconvenientes.

Por otro lado, si nos centramos en el sistema de IA, el justiciable tendrá que conocer en qué términos se ha generado el programa, con el fin de que pueda valorar la idoneidad de la contribución. Nos referimos a la publicidad y transparencia que debe tener el sistema a fin de poder identificar motivos de recurribilidad. En línea con lo señalado anteriormente, ha de resultar imprescindible acceder a los entresijos del programa que genera el sistema, con el fin de controlar los términos de la decisión. Así pues, cuestiones como los datos que se incorporan, la tipología de datos,

la recopilación de datos, debe poder ser objeto de conocimiento por los justiciables, y, por ende, objeto de impugnación cuando se dé la sospecha de una resolución no ajustada a Derecho en base a la intervención automatizada, y con independencia de que se haya adoptado la resolución exclusivamente por este conducto, o constituya elemento de auxilio judicial, pero base de su decisión.

No obstante, además de los datos, también debe ser accesible y público el algoritmo empleado, es decir, la fórmula de la que se extrae el resultado o conclusión a partir de los datos suministrados. Para el análisis y control de estos aspectos, es imprescindible contar con expertos que informen sobre la idoneidad y funcionamiento del sistema de IA, lo que nos lleva a la existencia de peritos. De este modo, es bastante probable que la impugnación de la herramienta requiera de peritos informáticos especializados en la materia, lo que supone un coste adicional importante para la parte que quiera impugnar estos extremos.

3. IMPUGNACIÓN Y FALIBILIDAD ALGORÍTMICA

Al igual que el juez emplea la lógica de la razón en la valoración de la prueba y en la decisión, podemos entender que la IA acude a la lógica del algoritmo para llegar a encontrar patrones repetitivos que ayudan a tomar una decisión. Como se ha señalado, la precisión del algoritmo copia la lógica humana en el ámbito del lenguaje computacional[31]. Además, como ha señalado ARMENTA DEU[32], existe una falsa apreciación de la infalibilidad de la máquina, por lo que cabría poner de manifiesto la falta de objetividad e imparcialidad, lejos de la confianza que en la actualidad se fomenta respecto a la tecnología. Ahora bien, detrás del programa que establece el sistema de IA, está la intervención humana, que se encarga de introducir los datos y generar los algoritmos que sirven para el fin concreto para el que se destina. En este sentido, aparece como un primer avance en materia de IA y Administración de Justicia, lo previsto en el Anteproyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia de 2021. El art. 58 otorga el carácter de público y objetivo a los criterios de decisión automatizada. Precisamente se pretende establecer una vía de control a todo el entramado que se forma para la toma de decisiones judiciales.

En cualquier caso, son múltiples los documentos que, desde organismos públicos, se están generando en colaboración con entidades

31. SIMÓN CASTELLANO, P., *Justicia cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos judiciales*, 2021, p. 48.

32. ARMENTA DEU, T., *Derivas de la justicia*, Madrid, 2021, p. 305.

especializadas, y que parten de los riesgos consustanciales al uso de la tecnología. Así, la Carta de Derechos Digitales presentada en julio de 2021 (CDD), si bien muy general y sin carácter vinculante, pretende ser el marco global de múltiples cuestiones que afectan a los ciudadanos en la vertiente digital. En esta línea, la CDD dedica algunas líneas a los derechos en materia de inteligencia artificial. Entiende que la inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad, perseguirá el bien común y asegurará cumplir con el principio de no maleficencia. Especialmente preocupa la no discriminación en las decisiones, el uso de sus datos y el proceso de IA. Como gran enseña, se reconoce el derecho a establecer condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible.

En especial, y relacionado con el control de estos sistemas, la CDD establece que "las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial". Si bien esta proclamación en forma de derecho tiene un carácter general, llevado a su aplicabilidad a las decisiones adoptadas en el seno del proceso jurisdiccional, alcanza una dimensión mayor, habida cuenta que va a convivir con un sistema previo de impugnaciones como institución procesal, dentro del cual debe tener acogida la posibilidad de impugnar en sus diversas formulaciones, las distintas decisiones automatizadas.

Por ello, la accesibilidad a la información y el procedimiento del sistema de IA, así como el empleo de un lenguaje comprensible, se erigen en derechos del ciudadano. En otro momento de la Carta se recalca la idea de "transparencia sobre el uso de instrumentos de inteligencia artificial y sobre su funcionamiento y alcance en cada procedimiento concreto y, en particular, acerca de los datos utilizados, su margen de error, su ámbito de aplicación y su carácter decisorio o no decisorio. La ley podrá regular las condiciones de transparencia y el acceso al código fuente, especialmente con objeto de verificar que no produce resultados discriminatorios".

De manera más específica se reconoce el derecho a "obtener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes, tecnología empleada, así como de los criterios de aplicación de las mismas al caso. El interesado tendrá derecho a que se motive o se explique la decisión administrativa cuando esta se separe del criterio propuesto por

un sistema automatizado o inteligente". Aunque en este caso la Carta se refiere a las decisiones adoptadas en el ámbito administrativo, es perfectamente extrapolable al ámbito de la Administración de Justicia, donde se refuerzan algunos elementos relacionados como el lenguaje, la motivación, y la explicación de decisiones.

Las conclusiones que pueden extraerse son múltiples, pero, sobre todo, es preciso recalcar los riesgos inherentes al uso de sistemas de IA en la toma de decisiones, ya que, al igual que los jueces pueden errar, la máquina también, debido fundamentalmente a que no es infalible ni quien genera el programa, ni el propio algoritmo. Y es una cuestión que se reconoce por las instituciones cuando buscan regular y garantizar los derechos de los ciudadanos. Así se recoge en el Libro Blanco sobre la inteligencia artificial de 2020 que señala que "los prejuicios y la discriminación son riesgos inherentes a toda actividad social o económica. La toma de decisiones de las personas no es ajena al error ni a la subjetividad. No obstante, en el caso de la IA, esta misma subjetividad puede tener efectos mucho más amplios, y afectar y discriminar a numerosas personas sin que existan mecanismos como los de control social que rigen el comportamiento humano".

En esta línea, el riesgo fundamental reside en la existencia de sesgos en la inteligencia artificial[33]. Éstos han sido definidos como el error sistemático en que incurre el entorno estadístico al realizar muestreos o ensayos, de tal modo que se favorecen o promueven ciertas respuestas, constituyendo la principal amenaza en este entorno[34]. Además, el sesgo puede proceder de los datos, que no abarcan el muestreo completo que se pretende, o puede residir de los algoritmos aplicados, lo cual resultaría todavía más difícil de demostrar por parte de quien pretende destruir una resolución basada en este programa. A tal efecto, se ha señalado por los expertos la necesidad de adoptar estrategias de prueba, evaluación y mitigación para minimizar los casos de sesgos. Fernández señala mecanismos consistentes en reforzar el conocimiento de la IA por

33. TAPIA HERMIDA, A. J., "Decálogo de la inteligencia artificial ética y responsable en la Unión Europea", *Diario La Ley*, n.° 9749, 4-12-2020, señala la idea del mito de los algoritmos neutrales, si bien referidos a su uso en las finanzas. Se pone de manifiesto igualmente la necesidad de establecer seguros obligatorios de responsabilidad civil para los operadores de sistemas de IA de alto riesgo, lo que minimizaría los riesgos derivados de su uso indebido. Lógicamente, entendemos que si en el ámbito de la Administración de Justicia esto sería deseable cuando el sistema fuera creado y gestionado por instituciones privadas, cuando pasa a titularidad estatal, la cuestión se desplaza al ámbito de la responsabilidad del Estado, extremo sobre el que sería conveniente un análisis pormenorizado.

34. FERNÁNDEZ, C., "¿Se pueden evitar los sesgos en la Inteligencia Artificial?", *Diario La Ley*, 25-6-2021.

la sociedad, exigir evaluaciones y pruebas para sistemas de IA de alto riesgo, exigir transparencia en su uso, y, sobre todo, establecer limitaciones universales.

En este punto surge la duda respecto de quién debe asumir la creación y puesta a disposición de sistemas de IA que decidan en lugar de los jueces. Si desde opciones de política legislativa se integra el sistema en las instituciones públicas, debe ser exigible pasar los correspondientes controles *ex ante*, y que el justiciable conozca el funcionamiento de dichas tecnologías para poder realizar un control con carácter previo al planteamiento de su pretensión ante los tribunales. Las dificultades son evidentes, así como los costes, por lo que, en última instancia, serán los poderes públicos los que deban garantizar y asumir la implantación de sistemas que no atenten contra los derechos fundamentales, y aseguren un proceso con todos los derechos y garantías sin que produzca indefensión. Parece que cualquier otra opción que permita que sean las empresas privadas las que gestionen un sistema de IA debe quedar vedado en aras de los intereses y derechos generales que están en juego.

El Libro Blanco sobre la IA señala la necesidad de que las personas afectadas tengan medios para comprobar cómo se ha tomado una decisión determinada con ayuda de la IA, y si se han respetado las normas pertinentes. De ahí que, a efectos del establecimiento de recursos, se debe facilitar la información y herramientas tecnológicas de manera gratuita, sin necesidad de que los costes derivados de informes periciales sean asumidos por el justiciable.

IV. CONCLUSIONES

A la vista de lo analizado, podemos extraer diversas conclusiones. De entrada, la aplicación de sistemas de IA al ámbito de la Administración de Justicia no puede aceptarse o rechazarse sin más, ya que el concepto es suficientemente amplio, y los campos en los que puede ser útil también. De ahí que sea preciso establecer dos cuestiones como punto de partida. La primera está relacionada con el tipo de resoluciones judiciales en las que puede ser de aplicación la IA; y la segunda está referida al grado de intervención o auxilio que la IA puede prestar a la decisión judicial.

Respecto de lo primero, podemos sentar tres niveles de aplicabilidad; a saber, la tramitación judicial, lo que entraña un automatismo básico en aras del impulso formal, y ámbito en el que parece más viable y eficiente implantar sistemas de IA; las decisiones de carácter interlocutorio, donde

tendría cabida un conjunto heterogéneo de resoluciones judiciales en las que es necesario realizar una labor intelectual de razonamiento, deducción o interpretación, y que se correspondería básicamente con incidentes y adopción de medidas cautelares; y por último, las resoluciones que ponen fin a la controversia y al proceso, es decir, sentencias y algunos autos donde se decide la cuestión de fondo.

Respecto de estas últimas decisiones, el grado de intervención de sistemas de IA parece tener mayores dificultades de implementación, por no decir ninguna en caso de considerar que hay una suplantación total de la máquina respecto del juez.

Por ello, el núcleo fundamental y problemático lo constituye el conjunto de decisiones, bien sobre medidas cautelares, bien decisiones de fondo, que se adoptan por el juez, pero con auxilio o apoyo de la IA. En estos casos, identificar el sistema de IA como carácter autónomo o integrado en la decisión del juez, nos hace pensar en distintas formas de impugnación de resoluciones. Así pues, si consideramos que la IA ayuda al juez como si de un perito experto en la materia se tratara, el recurso debe ir dirigido a cuestionar el soporte o motivación del juez, es decir, a impugnar a la máquina, en todas sus manifestaciones algorítmicas o de datos. Por el contrario, si concebimos a la IA como algo que le sirve al juez para motivar mejor, entonces el recurso se deberá plantear en términos de motivación o razonamiento de la decisión.

En cualquier caso, se abren interrogantes sobre el papel que ocupan los sistemas de IA, como es la obligatoriedad de su uso o no, las consecuencias de su uso indebido por el juez, el apartamiento de la decisión respecto de lo dicho por la máquina, etc. Todas ellas son cuestiones que pueden generar un campo más amplio a efectos de establecer motivos tasados o no para recurrir ante órganos superiores.

V. BIBLIOGRAFÍA

ARMENTA DEU, T., Derivas de la justicia, Madrid, 2021.

BARONA VILAR, S., "Una justicia digital y algorítmica para una sociedad en estado de mudanza", Barona Vilar, S., (dir.) *Justicia algorítmica y neuroderecho*, Valencia, 2021.

BRENNER, S. y SPAETH, H. J., *Stares indecisis. Las alteraciones del precedente en la Corte Suprema de Estados Unidos,* Madrid, 2017.

BUENO DE MATA, F., "Macrodatos, inteligencia artificial y proceso: luces y sombras", *Revista General de Derecho Procesal* 51, 2020.

CALAMANDREI, P., "Vicios de la sentencia y medios de gravamen", *Estudios sobre el proceso civil*, trad. Sentís Melendo, S., Buenos Aires, 1961.

CORTÉS DOMÍNGUEZ, V., con Moreno Catena, V., *Derecho Procesal Civil. Parte General,* Valencia, 2021.

COTINO HUESO, L., *et al.*, "Un análisis crítico constructivo de la Propuesta de Reglamento de la UE por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Artificial Intelligence Act)", *Diario La Ley*, 2-7-2021.

FERNÁNDEZ, C., "¿Se pueden evitar los sesgos en la Inteligencia Artificial?", *Diario La Ley*, 25-6-2021.

FERNÁNDEZ, C., "Los jueces ante los problemas jurídicos de la inteligencia artificial", *Diario La Ley*, 3-1-2022.

GÓMEZ COLOMER, J. L., "Unas reflexiones sobre el llamado "juez-robot", al hilo del principio de la independencia judicial", Barona Vilar, S., (dir.) *Justicia algorítmica y neuroderecho,* Valencia, 2021.

MARTÍNEZ GARCÍA, E., BORGES BLÁZQUEZ, R., y SIMÓ SOLER, E., "Inteligencia artificial y perspectiva de género en la justicia penal", *Diario La Ley*, n.° 47, Sección Ciberderecho, 20-1-2021.

NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial*, Madrid, 2018.

PÉREZ DAUDÍ, V., "El precedente judicial. La previsibilidad de la sentencia y la decisión automatizada del conflicto", *Revista General de Derecho Procesal*, 54, 2021.

PINTO PALACIOS, F., "¿Pueden los robots administrar justicia?", *Diario La Ley*, n.° 9808, 11-3-2021.

PLANCHADELL-GARGALLO, A., "Inteligencia artificial y medidas cautelares", Barona Vilar, S., (dir.) *Justicia algorítmica y neuroderecho,* Valencia, 2021.

RETANA, C., *et al.*, "Diálogos para el futuro judicial XXII. Jurimetría y Justicia predictiva", *Diario La Ley*, n.° 9837, 26 de abril de 2021.

ROBERTO GRANERO, H., "La inteligencia artificial aplicada al Derecho –El cumplimiento del sueño de Hammurabi–", *Revista Iberoamericana de Derecho Informático*, n.° 5, 2018.

SIMÓ SOLER, E., y ROSSO, P., "La destrucción algorítmica de la humanidad", *Diario La Ley*, n.° 9982, 4 de enero de 2022.

SIMÓN CASTELLANO, P., *et al.*, "Diálogos para el futuro judicial XXII. Jurimetría y Justicia predictiva", *Diario La Ley*, n.° 9837, 26 de abril de 2021.

SIMÓN CASTELLANO, P., *Justicia cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos judiciales*, Barcelona, 2021.

TAPIA HERMIDA, A. J., "Decálogo de la inteligencia artificial ética y responsable en la Unión Europea", *Diario La Ley*, n.° 9749, 4-12-2020.

Digitalización y/o Inteligencia Artificial

Raquel Castillejo Manzanares

Catedrática de Derecho Procesal
Universidad Carlos III de Madrid

SUMARIO: I. DIGITALIZACIÓN DE LA JUSTICIA. 1. *La ciberjusticia*. 2. *El expediente judicial electrónico y LexNET*. 3. *Los juicios telemáticos*. 4. *Las ODR*. II. ALGORITMOS. III. INTELIGENCIA ARTIFICIAL. 1. *Historia*. 2. *Concepto*. IV. MACHINE LEARNING. V. BIG DATA. VI. PROBLEMAS QUE PRESENTA. VII. INTELIGENCIA ARTIFICIAL EN EL PROCESO. VIII. AFECCIÓN DE DERECHOS FUNDAMENTALES AL INTRODUCIR LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL.

I. DIGITALIZACIÓN DE LA JUSTICIA

1. LA CIBERJUSTICIA

Se pueden destacar dos tendencias hacia las que se encaminan los cambios en el proceso judicial con la extensión de la digitalización y de la aplicación en el mismo de las tecnologías de la Inteligencia Artificial: una es la tendencia hacia la Ciberjusticia, la otra es la referente a la desjudicialización[1].

Con el término "Ciberjusticia" se hace referencia a la nueva forma de estructurar y organizar los procedimientos del proceso judicial debido a la aplicación de estas Tecnologías 4.0. Por su parte, la tendencia a la desjudicialización no viene sólo del impulso de los legisladores de reducir la carga del sistema judicial, sino que la propia Tecnología 4.0, junto con la

1. DE LA QUADRA SALCEDO, T/PIÑAR, J., *Sociedad digital y Derecho,* Madrid, 2018, p. 795.

globalización y la liberalización del mercado jurídico, es un acicate natural para esta descarga.

Caben destacar tres niveles jurídicos de la actividad del tribunal en los que podían clasificarse los desarrollos en las Tecnologías de la Comunicación y de la información: En primer lugar "la trastienda de la oficina judicial", en la que se incluyen las tecnologías de bases de datos jurídicas y los procesadores de texto, que suponen un progreso en las labores documentales, de despacho de asuntos y de gestión de tribunal. En según lugar, las salas de audiencias, que agrupa a aquellas tecnologías que están siendo aplicadas en las vistas de los juzgados, como cámaras de alta resolución o amplificadores de sonido. El último nivel, "comunicación externa del tribunal", engloba tecnologías como el correo electrónico o las videoconferencias, que afectan a la manera en que los tribunales interactúan con las partes de puertas afuera[2].

El primer hito en la gestión pública española del sector justicia fue el Plan Estratégico de Modernización de la Justicia 2009-2012, que en sus programas de actuación introdujo una referencia a la automatización en cuanto a la gestión procesal, en la puesta en marcha e integración de los Registros administrativos de apoyo a la actividad judicial, en el proceso de generación de informes estadísticos del Registro Civil, en la gestión de identidades digitales, en la reingeniería de las TIC, entendida como el objetivo de transformar integralmente los sistemas, procesos automatizados para generar avances en su eficiencia, eficacia y tiempos de respuesta, como elemento de la interoperabilidad de sistemas para el traslado de información entre los mismos.

El Protocolo marco de actuación de la Oficina Judicial dentro de las normas para estandarizar taras procesales, definía de este modo los sistemas de gestión procesal como sistemas de tramitación guiada.

El primer reto tecnológico para el funcionamiento de la Administración de Justicia española consistirá en trascender esa tramitación guiada hacia la implantación y generalización de la tramitación automatizada, entendiendo por la misma aquella que se produce sin intervención humana. 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, otorga habilitación específica para introducir la tramitación automatizada en el sector justicia. Definiendo la actuación judicial automatizada como *"Actuación judicial producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso*

2. DE ASIS PULIDO, M., *Derecho al debido proceso e inteligencia artificial*, en "Inteligencia artificial y derecho. El jurista ante los retos de la era digital, Aranzadi, 2021, p. 70.

singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de los meros actos de comunicación".

En esta norma se establecen algunas previsiones como la implantación de sistemas de firma electrónica para la actuación judicial automatizada, obtención automatizada de copias electrónicas digitalizadas de documentos privados aportados al proceso, o la emisión e justificantes por registros judiciales electrónicos.

Uno de los más importantes avances en la modernización de la justicia española vino como consecuencia de la reforma procesal de la legislación procesal para la implantación de la Oficina Judicial, ley 13/2009, comenzando a celebrarse legalmente vistas de juicios orales sin la presencia física de un fedatario público documentadas por medios audiovisuales y autentificadas mediante firma electrónica posterior. Pero a raíz de ellos hacen precisos más avances tecnológicos, así:

A. La implantación de un sistema de textualización de las declaraciones grabadas por medios audiovisuales.

B. Procesamiento del lenguaje natural generado en diferentes idiomas.

C. Tratamiento de metadatos en archivos audiovisuales[3]. La principal herramienta tecnológica aplicable a los metadatos de las grabaciones y registros audiovisuales es la de reconocimiento facial, cuya incorporación a los sistemas judiciales no resulta difícil imaginar en la exclusiva medida del uso para contribuir a la acreditación de identidad de declarantes que previamente constasen en una base de datos en el ámbito judicial, o para una eventual interconexión entre bases de datos policiales y judiciales en la gestión de requisitorias penales[4].

---

3. Según apunta la página web de SEDIC (Sociedad Española de Documentación e Información Científica) metadato es "*toda información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación y/o interoperabilidad*".

   En lo que respecta a los archivos audiovisuales la digitalización y la grabación en formato digital han permitido que se creen entornos con distintos tipos de documentos (sonoros, imágenes físicas, imágenes en movimiento…) y que el acceso a estos se amplie a todo tipo de usuarios (por ejemplo, en una cadena de TV una periodista puede recuperar unas imágenes que le interesen sin necesidad de pedírselas a la Unidad de documentación de la cadena).

4. Experiencias tecnológicas operativas con tecnología de reconocimiento facial e incidencia en el sector justicia lo tenemos en el sistema público de gafas con software de reconocimiento facial implantado en la policía de la República Popular China, primero para el control de pasajeros de tren en Zhengzhou y posteriormente desplegada en la periferia de Beijing. En el mismo país también se ha incorporado el sistema combinado de identificación biométrica a las propias redes de transporte público de

En este marco el 28 de abril se publicó el Real Decreto-ley 16/2020, con la finalidad de agilizar los procesos. A tal fin, en su artículo 19 manifiesta expresamente su apertura a una mayor digitalización de la justicia, con la celebración de juicios por vía 100% telemática.

Con posterioridad, la Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente a la covid-19 en el ámbito de la Administración de Justicia, ha concretado las previsiones del Real Decreto. Así en los artículos 1 y 2 sobre medidas procesales: tramitación de la impugnación de ERES, expedientes de JV y otros.

En el Capítulo III de medidas organizativas y tecnológicas: celebración de actos procesales mediante presencia telemáticas, acceso a las salas de vista, atención al público mediante videoconferencia, por vía telemática o a través de correo electrónico en las condiciones previstas en el art. 18, dedicado a la "atención al público", previendo los casos excepcionales en que resulte imprescindible acudir a la sede judicial o de la fiscalía, mediante cita previa. En efecto, se concreta en:

a. Celebrar actos procesales mediante presencia telemática, a excepción de la necesaria presencia del acusado en los juicios por delitos graves, así como de su letrado cuando lo solicite aquel o este último, garantizándose el derecho a la asistencia letrada efectiva, a la interpretación, la traducción, a la información y al acceso a los expedientes judiciales –art. 14–.

b. Emisión de vistas mediante sistemas de difusión telemática de la imagen y el sonido –art. 14.6–.

c. Remisión por vía telemática del expediente médico para la realización de las exploraciones médico-forenses y de los equipos psicosociales, siempre que sea posible y cualquier de las partes o el facultativo encargado o el juez no solicite o acuerde la exploración presencial –art. 15–.

d. La atención al público será a través de videoconferencia, vía telemática o correo electrónico, siempre que sea posible en función de la naturaleza de la información requerida y respetando en todo caso

Beijing y Shanghai. Se trata del sistema Bio-ID que combina y coteja con bases de datos estatales el reconocimiento facial con huellas de la palma de la mano de los usuarios.

También el sistema de reconocimiento facial de prófugos de la República Argentina, que comenzó a operar en abril de 2019. Utiliza unas 300 cámaras rotativas en la Ciudad de Buenos Aires y está interconectado con una aplicación judicial, la Consulta Nacional de Rebeldías y Capturas, que registra las más de 46.000 personas objeto de requisitoria judicial.

> lo dispuesto en la ley de protección de datos personales y garantía de los derechos digitales y salvo que resulte imprescindible acudir a la sede judicial o fiscalía –art. 18–.
>
> Pero cabe ir más allá y utilizar un software dotado con capacidad de aprendizaje automático que interactúe con humanos. Así, gran parte de la relación de la justicia con la ciudadanía consiste en intercambio de información, de una información cambiante y personalizada, pero en gran parte homogeneizable y apta para su tratamiento a través de *software* conversacional o *chatbots* integrados en las sedes electrónicas o bien mediante otro tipo de *interficies* o medios que faciliten la accesibilidad ciudadana en aquellos supuestos en que la misma se vea a priori limitada.

A efectos de comunicación, se contempla la comunicación edictal electrónica, a través del Tablón Edictal único, como medio de publicación y consulta de las resoluciones y comunicaciones, modificándose además, la Ley reguladora del uso de las tecnologías de la información y la comunicación en la Administración de justicia, autorizándose el uso de los sistemas de identificación y firma electrónicos, siempre que dicho sistema identifique de forma unívoca como profesional para el trámite –Disposición final 4.ª–.

La Disposición transitoria 2.ª donde se contempla la aplicación de estas medidas hasta el 20 de junio de 2021, siempre y cuando la situación sanitaria no obligue a extender las organizativas y tecnológicas previo informe del Centro de Coordinación y Emergencias Sanitarias hasta el fin de la situación de fin de crisis sanitaria.

Y, por último, la Disposición Adicional 5.ª contempla la dotación de medios e instrumentos electrónicos y sistemas de información, formando a los integrantes de órganos, oficinas, o fiscalías en el uso y utilización en el uso y utilización de dichos medios e instrumentos.

Al mismo tiempo, en línea con la digitalización, surge la Ley de Servicios Electrónicos, Ley 6/2020, de 11 de noviembre, por la que se deroga la Ley 59/2003, de Firma Electrónica.

2. EL EXPEDIENTE JUDICIAL ELECTRÓNICO Y LEXNET

Actualmente y sin ánimo de ser exhaustiva, se hallan vigentes, entre otros, el expediente judicial electrónico, el cual, ya en la disposición adicional 2.ª de la Ley 18/2011, reguladora del Uso de las Tecnologías de la Información y la Comunicación en la Administración de Justicia, se hacía

alusión a él, otorgándose un plazo de cinco años para que la Administración de Justicia se dotara de sistemas que permitieran la tramitación electrónica de los procedimientos, debiendo garantizarse la interoperabilidad en los sistemas de gestión procesal.

Se implementó mediante al Plan de Modernización del Sistema de Justicia 2009-2012, en noviembre de 2010 en la Audiencia Nacional, aunque con varios problemas de incompatibilidad entre los sistemas de las sedes judiciales y los equipos de teletrabajo, así como entre las diferentes aplicaciones informáticas de las distintas Comunidades Autónomas.

También entra en juego LexNET, creado a tenor de los arts. 135.5, 6 y 162 LEC y regulada su implementación por el Real Decreto 84/2007, de 26 de enero, para completar el marco del proceso de informatización de la Ley 18/2011, de 5 de julio y el RD 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el territorio Ministerio de Justicia. Se trata de una plataforma tecnológica que permite el intercambio seguro de documentos y escritos procesales entre la Administración de Justicia y los sujetos que interactúan con ella.

Su funcionamiento no es todo lo bueno que se espera debido a la falta de formación del personal, de inversión material, así como a las limitaciones técnicas, como las disfunciones del navegador y de la firma electrónica, el escaso ancho de banda que limita el envío de datos, la caída del sistema…

3. LOS JUICIOS TELEMÁTICOS

Por último, cabría hacer referencia los juicios telemáticos y a las ODR. En lo relativo a los juicios telemáticos, son algunas las normas que hacen referencia los mismos. Ya hicimos mención a la Ley 3/2020, de 18 de septiembre de medidas procesales y organizativas para hacer frente a la covid-19.

Así la Guía para la celebración de actuaciones judiciales telemáticas aprobada por la Comisión Permanente del CGPJ el 11 de febrero de 2021, en la que se ofrecen pautas y recomendaciones para conciliar la aplicación preferente de estos medios tecnológicos al proceso con el pleno respeto a los principios y garantías que establecen las leyes. El documento señala que aunque el art. 299 LOPJ ya prevé la posibilidad de realización telemática de determinadas actuaciones procesales y el RD 16/2020 ha establecido que la forma telemática sea el modo preferente de celebración de las actuaciones judiciales durante la vigencia del estado de alarma y los

tres meses posteriores a su levantamiento, estas normas no precisan los criterios para la aplicación de estos medios tecnológicos ni los requerimientos técnicos que la hagan conciliable con el principio de publicidad de las actuaciones judiciales, la confidencialidad exigida por las normas procesales y de protección de datos, la mayor amplitud de los derechos de defensa; la validez, integridad y calidad epistémica de la prueba o la garantía que aporta la inmediación.

La Guía entiende que *"la aplicación de las tecnologías al proceso ha de ser una forma de avanzar, no de retroceder, e implicaría un retroceso limitar las garantías procesales al servicio de la tecnología, cuando ha de ser la tecnología la que se adapte y permita la plena satisfacción de esas garantías*".

La Guía advierte asimismo de que las experiencias en el uso de tecnologías telemáticas en actuaciones judiciales son limitadas, básicamente se han constreñido a la conexión telemática de algunos de los participantes en actos procesales presenciales, y que su aplicación para la práctica de actuaciones más complejas, como el desarrollo de un juicio íntegro, precisan de un marco normativo más completo que el vigente, de una mayor inversión económica y de una apuesta decidida por las tecnologías por parte de las Administraciones prestacionales.

Por otra parte, y de conformidad con el art. 230 LOPJ, la Guía identifica los requisitos técnicos mínimos que, para establecer un marco común homogéneo, han de ser considerados para asegurar que los actos procesales se desarrollen con las debidas garantías. Con arreglo a ese precepto, a las Administraciones prestacionales les corresponde la implementación de los sistemas tecnológicos teniendo en cuenta los requerimientos mínimos establecidos por el CGPJ para que puedan considerarse de uso obligatorio para jueces y magistrados en caso de que estos opten por celebrar actos de forma telemática.

La Guía aborda, en cuatro apartados, los aspectos relacionados con la preferencia para empleo de medios telemáticos, la forma de celebración, el lugar y los requisitos técnicos mínimos que deban tenerse en cuenta para realizar telemáticamente los distintos actos procesales.

En el primero se distingue entre actuaciones internas, tales como deliberaciones, reuniones de los órganos de gobierno, juntas de jueces, etc., y externas y, dentro de estas, aquellas en las que solo intervienen operadores jurídicos (Ministerio Fiscal, abogados, procuradores y graduados sociales) y otras en las que participan los ciudadanos. Dentro de esta última categoría se incluiría la celebración de juicios en los que deban practicarse pruebas con intervención personal, como interrogatorios de parte, testificales o periciales.

El segundo apartado aborda la forma de celebración de cada tipo de actuación en función de si son internas o externas, y de las prevenciones que deben adoptarse para garantizar su confidencialidad y reserva cuando así lo exijan las normas, el ejercicio del derecho de defensa, la publicidad y la intangibilidad de los medios de prueba.

En el tercero se indica qué lugares pueden ser los más adecuados para la conexión de cada uno de los intervinientes en actos telemáticos, subrayando que en el caso de actuaciones externas el juez o los miembros del tribunal se constituirán siempre en la seda del Juzgado o Tribunal.

Por último, el apartado dedicado a los requisitos técnicos mínimos señala que los servicios técnicos del CGPJ verificarán su cumplimiento y subraya la conveniencia de que las Salas de Gobierno de los distintos órganos jurisdiccionales establezcan los protocolos correspondientes con las Administraciones prestacionales, Fiscalías y corporaciones profesionales afectadas para adaptar la aplicación de las pautas ofrecidas en la Guía a las peculiaridades que puedan concurrir en su territorio.

También cabe destacar el artículo 14 y ss. de la Ley 3/2020, de medidas procesales y organizativas para hacer frente a la covid-19 en el ámbito de la Administración de Justicia se extiende a los procesos civil y penal, cuando señalan que los actos de juicios, comparecencias, declaraciones y vistas, y en general todos los actos procesales, se realizarán, hasta el 21 de junio, preferentemente de manera telemáticas. Se exceptúan, únicamente, la presencia física del acusado en el orden jurisdiccional penal cuando se trate de delitos graves. Al igual que en la audiencia previa prevista en el art. 505 LECr, para adoptar la prisión provisional, o en los juicios cuando alguna de las acusaciones solicite pena de prisión superior a los dos años, salvo que concurran causas justificadas o de fuerza mayor que lo impidan.

4. LAS ODR

En lo relativo a las ODR, el Anteproyecto de Ley de Eficiencia Digital de la Justicia regula las actuaciones negociales desarrolladas por medios telemáticos. De hecho, en su artículo 5 prevé que las partes podrán acordar que todas o alguna de las actuaciones de negociación en el marco de un medio adecuado de solución de controversias, se lleven a cabo por medios telemáticos, por videoconferencia u otro medio análogo de transmisión de la voz o la imagen, siempre que queda garantizado el respeto de las normas previstas en este título y, en su caso, a la normativa de desarrollo específicamente contemplada para la mediación.

Asimismo, exige que cuando el objeto de controversia sea una reclamación de cantidad que no exceda de 600 euros, se desarrollará preferentemente por medios telemáticos, salvo que el empleo de éstos no sea posible para alguna de las partes.

Toda esta normativa se ha hecho precisa a la vista de la situación actual, avivada por la pandemia. Coincidiendo con ALZATE SÁEZ DE HEREDIA[5], estimo que este fenómeno es parte de la pujanza económica y de todo tipo que Internet está teniendo en los últimos años. Para entender dicha pujanza debemos tener en cuenta dos elementos fundamentales:

El primero de ellos es la naturaleza descentralizada de la información en línea y la velocidad con la que se distribuye por todo el mundo. El acceso universal a la información en línea 24 horas al día, siete días a la semana, ha cambiado de forma fundamental muchos elementos en la comunidad mundial.

El segundo elemento a considerar es el papel predominante que Internet está adaptando en las transacciones comerciales y financieras. El comercio electrónico se está convirtiendo en la vía fundamental para muchos servicios electrónicos bancarios, la aparición y desarrollo de empresas cuyo flujo comercial es a través de internet, no son más que una señal de este cambio en el panorama comercial de la última década.

A la vista de todo ello, han emergido diferentes tipos de resolución de disputas en el ciberespacio. En la vida cotidiana, los procedimientos a los que se acude con normalidad son los judiciales o asimilados, como antes mencionamos, el proceso judicial o el arbitraje, junto a los actualmente denominados adecuados. En el marco virtual no han existido procedimientos que sirvieran a lo que se viene requiriendo, es por ello que se han buscado procedimientos relacionados con la Resolución de Disputas en Línea, los que se adaptan mejor por reconocer el entorno fluido y transterritorial de las nuevas tectologías de comunicación.

Es así que desde finales de la década de los 90, varias entidades buscaron y propusieron esquemas de resolución de disputas en línea (*Online Dispute Resolution –ODR–).*

En España fuimos conscientes de ello y ya con la Ley de mediación en asuntos civiles y mercantiles, en su artículo 24.2 se dispone la preferencia de un procedimiento de mediación por medios electrónicos para aquellos casos de reclamaciones de cantidad que no sobrepasen los 600 euros, siempre y cuando sea factible para ambas partes.

5. ALZATE SÁEZ DE HEREDIA, R., "Mediación en línea", *Revista de Mediación. ADR, Análisis y Resolución de Conflictos*, núm. 1, p. 1.

II. ALGORITMOS

La inteligencia artificial se distingue de una apuesta clara y actual de la justicia española en el proceso de modernización de la Administración de Justicia, se trata de la automatización masiva de procesos. La automatización está referida a procedimientos o series de acciones relacionadas entre sí de modo que una conduce necesariamente a la otra, conducción que se delega total o parcialmente en el uso de un intermediario tecnológico no humano. Sin embargo, como vemos, la inteligencia artificial va más allá e implica que ese elemento tecnológico no humano puede trascender total o parcialmente la condición de intermediario y convertirse en agente activo, además de tener capacidad de aprendizaje y de toma de decisiones.

De hecho, según la define la Comisión Europea en el *White Paper On Artificial Inteligence-A European approach to excellence and trust* de febrero de 2020, es una colección de tecnologías que combina datos, algoritmos y capacidad de computación. O como también la define el Grupo de Expertos de Alto Nivel de la Comisión Europea sobre Inteligencia Artificial de 9 de abril de 2019 "… los sistemas que muestran un comportamiento inteligente al analizar su entorno y tomar acciones, con cierto grado de autonomía, para alcanzar objetivos específicos. Los sistemas basados en IA pueden basarse exclusivamente en software, actuando en el mundo virtual (por ejemplo, asistentes de voz, análisis de imágenes), software, motores de búsqueda, sistemas de reconocimiento de voz y de rostro) o IA pueden integrarse en dispositivos de hardware (por ejemplo, Robots avanzados, autos autónomos, drones o aplicaciones de Internet de las Cosas".

La representación informática por excelencia de los procesos automatizados es el algoritmo. El concepto de algoritmo, que es asimilable al de un conjunto de instrucciones que puedan seguirse sin ningún tipo de ambigüedad para resolver un problema, se remonta a la matemática de la antigua Grecia, con el algoritmo de Euclides. Siendo éste una serie de ecuaciones matemáticas que se entrelazan para proporcionar un resultado. Esto es como lavar un cesto que contiene ropa de tejidos sintéticos. Hay que introducirla en el bombo de lavado y cerrarlo. Poner el detergente en uno de los huecos y el suavizante en otro. Girar el indicador de temperatura al programa número 3 de ropa sintética (prelavado-lavado-enfriamiento-4 enjuagues y parada de enjuague). Cuando la máquina se haya parado y se haya apagado la luz indicadora y suene el pitido, se abre la lavadora y se saca la ropa limpia y mojada. Esto es un algoritmo.

Así bien, al conjunto de instrucciones se le conoce como algoritmo y está basado en la existencia de determinadas variables que implican

datos. Luego, para ser ejecutado, el algoritmo debe pasar a cierto lenguaje de programación que permitirá al computador entender e interpretar en lenguaje de máquina las instrucciones.

Las tres partes de un algoritmo son: input (entrada), esto es, información que damos al algoritmo con la que va a trabajar para ofrecer la solución esperada. La segunda es el proceso, o conjunto de pasos para que, a partir de los datos de entrada, llegue a la solución de la situación. Para terminar con el output o salida.

¿Qué diferencia hay entre un algoritmo y un conjunto de instrucciones para realizar una tarea? En principio ninguna. Cuando sumamos dos números, hacemos lo que nos enseñaron en el colegio, sólo ponemos en práctica el algoritmo de la suma, es decir, realizando una serie de operaciones mecánicas sin tener que pensar si son o no teóricamente correctas. Realizar un algoritmo no requiere de ninguna inteligencia, en todo caso de cierta destreza, ya que toda la inteligencia necesaria para realizar la operación está contenida en el algoritmo.

Un algoritmo es, pues, una secuencia finita de instrucciones que deben ser realizables, que no plantean ningún tipo de ambigüedad y que nos permiten resolver, de manera genérica, algún tipo de problema.

A un dispositivo capaz de materializar un algoritmo se le puede dar el nombre genérico de "máquina algorítmica".

Lo que actualmente se halla generalizado son los sistemas automatizados de toma de decisiones basados en algoritmos. En efecto, en el contexto de la inteligencia artificial, muchos sistemas en uso actualmente contienen algoritmos "entrenados" a partir de ingentes cantidades de datos, en parte disponibles por la expansión de los servicios de internet en los móviles, que permiten automatizar cada vez más infinidad de decisiones que afectan a los ciudadanos. Según DE MIGUEL BERIAIN y PÉREZ ESTRADA[6], se trata de "series de ecuaciones matemáticas que se entrelazan para proporcionar un resultado, una instrucción concreta, que sirva para solucionar el problema planteado, gracias a la consideración de un número de variables que varía sustancialmente de un caso a otro". El algoritmo se construye gracias a la utilización de una gran base de datos ordenados de manera comprensible (Smart data), que un modelo matemático va utilizando de manera aleatoria, hasta establecer patrones de correlación determinista entre ellos. Según COTINO HUESO, la finalidad

6. DE MIGUEL BERIAIN, I./PÉREZ ESTRADA, M. J., *La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados*, Revista de Derecho UNED, núm. 25, 2019.

del algoritmo no es certificar la veracidad de una hipótesis planteada, sino la búsqueda de correlaciones deterministas entre unos datos y otros[7].

La representación gráfica del algoritmo se suele expresar convencionalmente mediante un gráfico dinámico característico o "diagrama de flujo" en el que se incluye los pasos consecutivos, las diferentes posibilidades y sus consecuencias asociadas, y donde, en definitiva, toda la secuencia y sus posibles resultados están predeterminados.

III. INTELIGENCIA ARTIFICIAL

1. HISTORIA

Todo lo que está aconteciendo actualmente con relación a la irrupción de la inteligencia artificial nos parece de película. Pero a lo largo de los siglos se han desarrollado inventos que nos han cambiado la vida. Hace 5.500 años la rueda, hace 2300 el martillo, hace 1000 la brújula, la imprenta hace 600, el motor hace 200, el teléfono hace 120 e Internet a finales de los años 60 en el contexto de la guerra fría, como una herramienta que garantizase las comunicaciones estatales en caso de amenaza nuclear[8].

La inteligencia artificial se inicia en la década de 1950. Ya será en 1996, un 10 de febrero, cuando en Filadelfia, el supeordenador de IBM Deep Blue se impuso al entonces campeón de ajedrez, Garry Kaspárov, en la primera partida de un encuentro pactado a seis. Tras el susto inicial, el gran maestro ruso dominó con tres victorias, y dejó el marcador final en 4 a 2 a su favor. La revancha se celebró en Nueva York, en mayo de 1997. En aquel duelo ganó la máquina por un 3,5 a 2,5.

Han pasado poco más de 20 años y la tecnología de Deep Blue se aplica hoy a campos como la creación de nuevos fármacos, el diseño de aviones, el control del tráfico o el ámbito financiero. La vieja Deep Blue pesaba casi dos toneladas, mientras que hoy en día, cualquier smartphone rinde al nivel de un gran maestro en ajedrez.

---

7. COTINO HUESO, L., *Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales*, Madrid, Dilemata, 2017, pp. 24, 131-150.

8. Su creación fue obra de ARPA, la Red de la Agencia de Proyectos de Investigación Avanzada a cargo del Departamento de Defensa de Norteamérica. La función de ARPA, nacida en 1958, era y continúa siendo acompañar el desarrollo de las nuevas tecnologías con fines militares.

   En 1969 es el año en que nació Internet. Fue entonces cuando se creó ARPAnet (*Advanced Research Projects Agency Network*), una red informática que permitió conectar a diversas Universidades norteamericanas.

En 2016, en marzo, se celebra otra partida, pero con un juego más intuitivo. Se enfrenta Lee Sedol, jugador profesional de Go y campeón del mundo en varias ocasiones contra AlphaGo, el programa desarrollado por Google DeepMind. Este último ha vuelto a ganar la partida y ha cerrado el encuentro con un resultado final de 4 victorias y una derrota. AlphaGo contaba con importantes avances en inteligencia artificial, destacando su capacidad de aprender y mejorar sus propias estrategias y movimientos en el transcurso del juego, a diferencia de la antigua Deep Blue.

El Go es un antiquísimo juego, bastante más que el ajedrez, originado en China hace unos 2.500 años. El juego consiste en "capturar" terreno a lo largo del tablero, pudiendo eliminar las fichas del contrario hasta el final de la partida. También tiene unas 10 elevado a 100 veces el número de posiciones que se pueden hacer en ajedrez. Con semejante complejidad, podemos comprender lo difícil que es para un ordenador aprender a jugar. La computación que hace falta para poder manejar semejante tamaño de operaciones ha de ser muy avanzada. No basta con un ordenador capaz de calcular, por fuerza bruta, todos los movimientos. Es necesario "aprender" y actuar en consecuencia para poder tener la más mínima oportunidad en el Go. Hasta esa fecha, se decía que el Go era una de esas razones por las que las máquinas nunca superarían al hombre.

A través de estas máquinas y estos juegos podemos concluir que hubo una primera generación de la IA, fue la "analítica descriptiva" basada en la pregunta ¿qué pasó? El segundo "análisis de diagnóstico" aborda ¿por qué sucedió? La tercera y actual generación es "análisis predictivo", que responde a la pregunta "basado en lo que ya sucedió, ¿Qué podría suceder en el futuro?

Se pasa de la programación tradicional con Algoritmos deterministas, basados en datos que se introducen en el programa de un ordenador y la salida de los mismos, a la gran evolución del software. En los años 70, el software comercial comienza con la fundación de Microsoft, Oracle y SAP. En los 80, la programación orientada a objetos hizo que *sotfware* fuera reutilizable y aumentó su escala y capacidad de manera espectacular. En la década de 2000, Internet democratizó el software, haciendo crecer el mercado de millones a miles de millones de personas. En 2012, las redes neuronales profundas ganaron el desafío *ImageNet*, lo que marcó el comienzo de la era del aprendizaje profundo o software 2.0. En 2020, el aprendizaje profundo impulsó casi todos los servicios de Internet a gran escala, incluidas las recomendaciones de búsqueda, redes sociales y videos. Durante la próxima década, creemos que el software más importante se creará mediante el aprendizaje profundo que permitirá la conducción autónoma de automóviles, el descubrimiento acelerado de fármacos y más.

Si bien el análisis predictivo puede ser muy útil y ahorrar tiempo para los científicos de datos, aún depende completamente de los datos históricos. Por lo tanto, los científicos de datos quedan indefensos cuando se enfrentan a escenarios nuevos y desconocidos. Para tener una verdadera inteligencia artificial, se necesitan máquinas que puedan "pensar" por sí mismas, especialmente cuando se enfrenta a una situación desconocida. Se necesita una IA que no solo pueda analizar los datos que se muestran, sino que exprese un presentimiento cuando algo no cuadre. En resumen, necesitamos una IA que pueda imitar la intuición humana.

Actualmente faltan a la Inteligencia Artificial tres cualidades propias del ser humanos, a saber: la curiosidad, el pensamiento crítico y la creatividad.

Precisamente la cuarta generación de la IA es la intuición artificial, que permite a las computadoras identificar amenazas y oportunidades sin que se les diga qué buscar, al igual que la intuición humana nos permite tomar decisiones sin que se nos instruya específicamente sobre cómo hacerlo.

Así bien, los sistemas computacionales, en la inteligencia artificial, deben ser capaces de simular características que son comúnmente asociadas con la inteligencia de la conducta humana. Un sistema inteligente es aquel que exhibe un comportamiento similar al humano cuando se enfrenta a un problema idéntico.

Los sistemas expertos son programas que imitan el comportamiento de un humano. Utilizan la información que el usuario les proporciona para emitir un resultado sobre cierta materia. Por tanto, se considera un sistema experto aquel sistema computacional capaz de proporcionar respuestas que, atribuidas a los humanos, presuponen procesos inteligentes de carácter heurístico. Los sistemas expertos tratan de emular la toma de decisiones de un experto humano en dominios de conocimiento bien definidos. El término "pensar" denota una serie de fenómenos neurofisiológicos que no podemos encontrar en las máquinas, pero si se puede hacer que una máquina simule algunos procesos de pensamiento[9].

Los sistemas expertos tienen ventajas sobre los expertos humanos. Por una parte, el conocimiento contenido en los sistemas expertos es más fácil de documentar y de transferir que el de los expertos humanos. Por otra, dicho conocimiento es remanente, es decir, permanece tras la desaparición de los expertos, por lo que constituye lo que se ha dado en llamar la memoria institucional del organismo o empresa que lo ha desarrollado.

9. MARTÍNEZ BAHENA, G. C., *La inteligencia artificial y su aplicación al campo del Derecho, alegatos*, núm. 82, México, septiembre/diciembre, 2020, p. 829.

Asimismo, resulta fácilmente transportable dando lugar a una especie de "experto ubicuo" que, por añadidura, no se cansa ni está sujeto a presiones. Por todo esto los sistemas expertos resultan más económicos para cualquier organización que los expertos humanos. Ahora bien, presentan claras limitaciones al compararlos con los expertos humanos. Ante todo, carecen pro completo de creatividad y de sentido común. Además, sólo sirven para parcelas bien acotadas del conocimiento frente a la mayor universalidad del saber humano, han de recibir sus entradas de forma simbólica en tanto que el hombre utiliza sus sentidos, y por tanto, todavía tienen serias dificultades para adquirir nuevos conocimientos por sí mismos[10].

2. CONCEPTO

Según la *Comisión* Europea en el documento sobre "Inteligencia artificial para Europa"[11], "*El término "inteligencia artificial" se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos*".

La *Encyclopedia Of Artificial Intelligence* la devine como "*un campo de la ciencia y la ingeniería que se ocupa de la comprensión, desde el punto de vista informático, de lo que denomina comúnmente comportamiento inteligente. También se ocupa de la creación de artefactos que exhiben este comportamiento*".

Según McCarthy, cofundador con Minsky del Laboratorio de Inteligencia Artificial del MIT (Instituto Tecnológico de Massachusetts) "*es la ciencia e ingenio de hacer máquinas inteligentes especialmente programas de cómputo inteligentes*"[12]. Por su parte Minsky la entiende como "*la ciencia de hacer que las máquinas hagan cosas que requerirían inteligencia si las hicieran las personas*"[13].

Actualmente la inteligencia artificial tiene autonomía en entornos dinámicos y complejos, capacidad de aprender y capacidad de resolver problemas en campos de expertos.

10. PINO DIEZ, R./GÓMEZ GÓMEZ, A./DE ABAJO MARTÍNEZ, N., *Introducción a la inteligencia artificial: sistemas expertos, redes neuronales artificiales y computación evolutiva,* Servicio de Publicaciones Universidad de Oviedo, marzo 2001, p. 10.
11. Comunicación de la Comisión, Bruselas, 25.4.2018 COM (2018) 237 final, p. 1.
12. HUALPA TAPIA, M. L., *Aplicación de la inteligencia artificial en solución de problemas empresariales*, Arequipa, p. 1.
13. DELGADO, M., *La inteligencia artificial. Realidad de un mito moderno*, Granada, Servicio de Publicaciones de la Universidad de Granada, 1996, p. 18.

Según Barona[14], siguiendo a Stuart Russel y Peter Norvig, hay cuatro tipos de inteligencia artificial: Los sistemas que imitan como piensan los humanos, que son capaces de tomar decisiones autónomas y resolver problemas y también tienen capacidad de aprendizaje; los sistemas que actúan como humanos e imitan su comportamiento; los que utilizan el pensamiento lógico racional humano, capaces de inferir una solución a un caso a partir de una información sobre un contexto dado; y, por último, los sistemas que emulan la forma racional del comportamiento humano, como los sistemas inteligentes o expertos.

Arend Hintze[15], diferencia entre otros cuatro tipos en los que se pueden clasificar los sistemas dotados de inteligencia artificial:

a. Las máquinas reactivas, no tienen memoria y no pueden utilizar experiencias pasadas para la toma de decisiones. Así bien, actúan en función de lo que ocurre en cada momento, siendo adecuadas para realizar determinadas tareas. Un ejemplo claro es jugar al ajedrez, actúan basándose en la disposición de las fichas en el tablero, pero no recuerdan partidas anteriores.

b. Máquinas con memoria limitada, tampoco son capaces de aprender, pero sí son capaces de almacenar datos pasados. Un ejemplo son los coches autónomos, capaces de conducir solos.

c. Máquinas con una teoría de la mente: son capaces de entender y expresar emociones e ideas, así como también pueden trabajar en equipo y adaptar su comportamiento a lo que ocurre a su alrededor.

d. Máquinas con una conciencia propia que, a partir de sus estados internos, pueden predecir comportamientos y sentimientos ajenos.

Un primer ámbito de aplicación de la IA en el Derecho son los programas expertos a los que ya hemos hecho referencia. Los ámbitos jurídicos en los que esta tecnología de sistemas expertos o inteligentes pueden tener aplicación en la automatización de tareas serían: Análisis, extracción de información relevante, predicción, generación de argumentos, redacción de documentos contractuales, informes o memoranda, planificación de tareas en los despachos y juzgados, redacción de normas, resolución de demandas mediante técnicas automatizadas de solución alternativa de conflictos, negociación de contratos y contratación mediante programas informáticos *(bots)* inteligentes.

14. BARONA VILAR, S., *Reflexiones en torno al 4.0 y la inteligencia artificial en el proceso penal,* Ius Puniendi, vol. 7, 2018, pp. 313-336.
15. HINZE, A., *Understanding the four types of AI, from reactive robots to self-aware beings*, The Conversation, 2016.

IV. MACHINE LEARNING

Dentro de la Inteligencia Artificial encontramos el *machine learning* que busca dotar a las computadoras con la capacidad de aprender, tal y como lo hace una persona. Se trata de una tecnología mediante la cual el sistema informático es capaz de aprender de sus propias experiencias y resolver problemas complejos. En ella, existe un algoritmo que está instruido para crear nuevos modelos matemáticos que permitan hacer predicciones o tomar decisiones en base a datos de muestra, conocidos como datos de entrenamiento. En otras palabras, cuando hablamos de *machine learning*, es el propio algoritmo el que crea nuevos algoritmos mediante la identificación de patrones o similitudes existentes en la base de datos de entrenamiento. Así, cuando se procesan nuevos datos, el sistema es capaz de reconocer los nuevos patrones en base al algoritmo creado por él mismo, lo que está vinculado a la cualidad de aprendizaje. Como resultado, los sistemas que incorporan este tipo de tecnología pueden percibir y relacionarse con el entorno, resolviendo problemas y generando respuestas en relación con un fin específico. En este sentido, un algoritmo de *machine learning* desarrolla la capacidad de modificarse a sí mismo con el fin de adaptarse a los datos que está procesando. El objetivo de ello es poder resolver un problema computacional por su propia cuenta. Dicho "problema" puede consistir en encontrar patrones ocultos de comportamiento o en ejecutar tareas complejas de forma automática. Así, un sistema con *big data* y *machine learning* puede captar problemas con los datos y al mismo tiempo resolverlos.

Uno de los subcampos del *machine learning* es el de las redes neuronales artificiales (RNA), también conocidas como sistemas conexionistas, y que implican un modelo computacional evolucionado a partir de diversas aportaciones científicas que están registradas en la historia. Consiste en un conjunto de unidades, llamadas neuronas artificiales, conectadas entre sí para transmitirse señales. La información de entrada atraviesa la red neuronal, donde se somete a diversas operaciones, produciendo unos valores de salida. Estos sistemas aprenden y se forman a sí mismos, en lugar de ser programados de forma explícita, y sobresalen en áreas donde la detección de soluciones o características es difícil de expresar con la programación convencional. El objetivo de la red neuronal es resolver los problemas de la misma manera que el cerebro humano, aunque las redes neuronales son más abstractas.

La palabra red en el término red neuronal artificial se refiere a las interconexiones entre las neuronas en las diferentes capas de cada sistema. Un sistema ejemplar tiene tres capas. La primera capa tiene neuronas de

entrada que envían datos a través de la sinapsis[16] a la segunda capa de neuronas, y luego a través de más sinapsis a la tercera capa de neuronas de salida. Los sistemas más complejos tendrán más capas.

Las redes neuronales tienen la posibilidad de aprendizaje. Lo que implica definir lo que es una función de coste, esto es, ninguna solución tiene un costo menor que el costo de la solución óptima. La función de coste es un concepto importante en el aprendizaje, ya que representa lo lejos que una solución particular se encuentra de la solución óptima al problema a resolver. Los algoritmos de aprendizaje buscan a través del espacio de soluciones para encontrar una función que tiene el menor costo posible.

Dentro del subcampos de las redes neuronales artificiales se halla el llamado *Deep learning* o aprendizaje profundo, que se genera cuando en un sistema hay redes neuronales con grandes cantidades de capas de nodos. A mayor cantidad de capas, mayor profundidad de la red neuronal. Así, para que el sistema sea capaz de procesar esas redes tan profundas, se deben implementar técnicas de *Deep learning*. De esta manera, gracias al aprendizaje profundo, un sistema informático puede ser capaz de predecir tendencias, fenómenos o circunstancias. Así como también de aprender a mejorar procesos sin asistencia humana. Así, mediante algoritmos basados en lo que se conoce como computación cognitiva, con la que se trata de emular la forma de aprender y razonar del cerebro humanos construyendo simulaciones más o menos complejas en forma de redes neuronales.

Dentro del *Deep learning* encontramos, a lo largo del tiempo, las tecnologías digitales del lenguaje, entendidas como aquellas capacidades, herramientas informáticas y algoritmos que hacen posible que las máquinas puedan entender y generar expresiones en lenguaje humano en múltiples idiomas.

Los algoritmos de NLP son grandes consumidores de datos que sirven de entrada para el entrenamiento de los modelos de inteligencia artificial

16. El concepto de sinapsis hace referencia a la existencia de una conexión entre dos neuronas, caracterizada por la presencia de un pequeño espacio que sirve de vía de transmisión de la información. Es decir, la existencia de la sinapsis nos muestra que las neuronas no forman un tejido celular compacto, sino que se interconectan entre sí de maneras complejas y manteniendo una cierta independencia las unas de las otras. La función principal de esta conexión es la de permitir la transmisión de la información entre las diferentes neuronas.

    En definitiva, básicamente la sinapsis se reduce a un impulso nervioso que se produce a través de las neuronas y posibilita su comunicación. Consiste, en esencia, en una descarga química traducida en una señal eléctrica que viaja a través de las redes neuronales de nuestro encéfalo a una velocidad vertiginosa.

que hacen posible el entendimiento del lenguaje humano por parte de las máquinas[17].

Alan Turing, conocido como uno de los padres de la Inteligencia Artificial y de los antepasados de los ordenadores, publicó en 1950 un artículo titulado *"Computing Machinery and intelligence"*, que puede considerarse el texto que inaugura la historia del NLP. Hasta la década de 1980, la mayoría de los sistemas de procesamiento de lenguaje natural se basan en conjuntos complejos de reglas pre-definidas o fijas (*Hard-Rules*). A partir de 1980 se produce una revolución en el campo del NLP, gracias a la potencia de cálculo de los ordenadores y a la mayor cantidad de textos digitalizados, se empiezan a aplicar técnicas estadísticas basadas en modelo de *machine learning* sencillos. En 1990 con el boom de los ordenadores personales y la Ley de Moore cumpliéndose, el volumen de datos de entrenamiento aumenta exponencialmente trayendo consigo cada vez mejores resultados.

Es en 2013 cuando investigadores de un equipo de Google inventaron un nuevo modelo para la representación de texto llamado *word2vec*, un modelo de *Deep Learning* capaz de representar el significado semántico.

Ya en la siguiente década la existencia de algoritmos pre-entrenados como *word2vec, Glove, fastText*, acelera y democratiza el desarrollo de soluciones para NLP. Se van añadiendo cada vez más lenguajes diferentes al inglés.

Ejemplos donde se puede adoptar PLN es como resumidor de documentos; como identificador de palabras y frases en lenguaje hablado por los humanos y transformarlas en un formato legible para el sistema informático; generando textos naturales; detectando diferentes idiomas y agilizando procesos en entornos multilingües; autocompletando tanto en buscadores como en herramientas para la escritura de texto; analizando el sentimiento y la intencionalidad de los mensajes en redes sociales; y extrayendo información clave.

El sistema de *machine learning* provoca problemas acentuados:

En primer lugar, que el coste marginal que tiende a cero. Para fabricar un producto se necesita hacer un desembolso; el costo marginal es la inversión requerida para crear un producto o servicio adicional. De ahí que la producción en serie es un método para disminuir el costo marginal.

17. Un ordenador convencional basado en tecnología del silicio es una máquina, que, a pesar de su complejidad, se basa en el simple principio de codificar y decodificar información digital binaria basada en ceros y unos. Por lo tanto, parece lógico pensar que, para hacer que una máquina entienda nuestro lenguaje, debemos de convertir el texto en códigos binario. Esto se conoce como codificación de texto o *text encoding*.

Con la llegada de internet de alta velocidad y tecnologías como el cómputo en la nube con las que podemos tener acceso a servidores y almacenamiento sin tener que adquirir el equipo; nos ha permitido que prácticamente cualquier persona pueda hacer alguna actividad profesional y venderla con un coste marginal muy cercana a O.

Con los avances tecnológicos que existen y las constantes innovaciones que salen hacia el mercado, puede ser muy fácil creer que la tecnología, en especial la inteligencia artificial, se vuelve cada vez más sencilla de producir y sobre todo costeable, pero esto no necesariamente es cierto.

Según el postulado de la Ley de Moore, el número de componentes en un circuito integrado se duplica cada año y el costo de producción permanece relativamente igual o que incluyo disminuye. Pero está ley tiene detractores, de hecho, en Febrero de 2021 el *MIT Technology Review* habló sobre la muerte paulatina de esta norma por la dificultad para fabricar nueva tecnología.

Un factor que dificulta el entrenamiento de los sistemas de IA es la dificultad en la incorporación de datos, de hecho, normalmente hay insuficiencia de datos. Así en el sistema BERT, un modelo de procesamiento de lenguaje que funciona por medio de IA creado en 2018 para implementarse en el motor de búsqueda de Google. Para alimentar el algoritmo de este sistema y entrenarlo se utilizaron 3.300 millones de palabras, seleccionadas principalmente de Wikipedia. Sin embargo, se podría entrenar con más palabras y, sin duda, funcionaría mejor.

Otro factor lo constituye los altos costos de la implementación de los sistemas de IA. Por eso sólo las compañías que son gigantes tecnológicos podrán hacerlo.

En segundo lugar, la polarización. Uno de los grandes retos que nos trae la Inteligencia Artificial en la actualidad es la generación de corrientes de pensamiento que se antojaban impensables hace pocos años. Hay que tener en cuenta que, en sólo un minuto, circulan por internet 187 millones de emails, 38 millones de mensajes de WhatsApp, se hacen casi 4 millones de búsquedas en Google y algo más de un millón de *swipes* en Tinder. La información que se mueve de un lugar para otro es tan abrumadora que es difícil imaginarla. Si de todas esas millones de comunicaciones, sólo un 0,01% de ellas fueran informaciones falsas, querría decir que en un solo minuto se estarían transmitiendo 10.000 *fake news* por minuto en todo el planeta.

En tercer lugar, las recomendaciones. Es común encontrarnos con escenas en las que buscamos cierta información, un libro, un artículo…, y de

manera automática nuestras redes y buscadores se alinean para arrojarnos toda una estampida de recomendaciones según nuestras búsquedas recientes. Y es que la IA se nutre de nuestro comportamiento en redes –sociales o no– aprende y crece con nosotros, nos observa, nos agrupa y en las redes sociales adapta el lenguaje, recomendaciones y contenidos a cada usuario, es algo así como un moderno "gran hermano".

En cuarto lugar, los sesgos de confirmación. Unido a lo anterior, la IA al estudiarnos, podría arrastrarnos por una corriente de sesgos confirmatorios que pueden ser buenos o malos, pero usualmente muy subjetivos, lo cual puede representar ciertos peligros si no contamos con criterios centrados, objetivos y múltiples fuentes de información y confirmación, o peor aún, podrían ser manipulados por quienes controlan la información recaudada.

En quinto lugar, las cámaras de eco. La inteligencia artificial ha hecho que sea aún más fácil crear y difundir información falsa o engañosa. Este problema es exacerbado por el hecho de que cada vez más consumimos más información en cámaras de eco digitales, provocando que acceder a información imparcial sea cada vez más difícil.

Por último, la suplantación de identidad. Un *Deep Fake* es cualquier video en el que la imagen o la voz de la persona han sido manipuladas utilizando software de inteligencia artificial para hacer que aquel vídeo modificado parezca real. Se basa en la suplantación de identidades mediante técnicas de *Machine Learning*.

V. BIG DATA

El desarrollo de la inteligencia artificial está íntimamente relacionado con el uso o con la disponibilidad de una gran cantidad de datos que son procesados por algoritmos. Nos estamos refiriendo al Big Data o, "macrodatos", que define el Parlamento Europeo como "la recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personas, procedentes de diferentes fuentes y objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones (analítica de macrodatos)"[18].

18. Resolución de 14 de marzo de 2017, sobre las implicaciones de los "macrodatos" en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley [2016/2225 (INI)].

Por lo tanto, dicho procesamiento solo se puede hacer mediante técnicas y sistemas especiales para el big data. Esta complejidad se debe a las tres principales características de este tipo de datos, las cuales se conocen como las 4 V del big data:

a. Volumen, pues la cantidad de datos es enorme, una empresa puede llegar a recolectar de petabytes (1 millos de GB) o exabytes (1 mil millones de GB) de información.

b. Velocidad, en cuanto los datos se producen de manera extremadamente rápida, a cada segundo se están generando grandes cantidades de estos.

c. Variedad, dado que los datos son complejamente heterogéneos, tienen distintos formatos, tamaños, tipologías, estructuras y provienen de múltiples fuentes.

d. Y veracidad, refiriéndonos a la incertidumbre de los datos, es decir al grado de fiabilidad de la información recibida. Es necesario invertir tiempo para conseguir datos de calidad, aplicando soluciones y métodos que puedan eliminar datos imprevisibles que puedan surgir.

Teniendo en cuenta los tres últimos conceptos, las principales diferencias son que, por un lado, el big data extrae y procesa grandes cantidades de datos muy complejos para luego organizarlos, con la finalidad de facilitar su consulta por parte de personas y programas. Sin embargo, el big data no realiza ningún tipo de análisis inteligente sobre ellos.

El *machine learning* ejecuta análisis inteligentes sobre grandes cantidades de datos para encontrar patrones y tendencias, con la finalidad de apoyar las decisiones de negocio. Sin embargo, el *machine learning* no extrae ni procesa los datos para aplicarles orden.

El *Deep learning* utiliza los datos para aprender de ellos sin intervención humana, con la finalidad de automejorar el sistema y el algoritmo. Sin embargo, el *Deep learning* tampoco extrae ni procesa los datos para disponibilizar su consulta.

En síntesis, mientras el big data se preocupa por las fuentes de datos y la naturaleza de estos, el aprendizaje automático y el profundo se ocupan de los análisis y del aprendizaje computacional.

La relación del big data con *machine learning* y *Deep learning* se produce a raíz de sus mismas diferencias. Se trata de que el big data extrae y procesa los datos para disponbilizarlos ante los algoritmos de *machine learning*. Se puede decir que el big data es la fuente de ingesta de datos

para el ML y DL. El *machine learning* toma los datos procesados por el big data y los analiza para genera *insights* de negocio o aprender a realizar ciertas tareas automáticamente. Por último, el *Deep learning* ingiere los datos más importantes del *big data* para aprender sobre ellos a niveles mucho más profundos y para realizar tareas más complejas.

VI. PROBLEMAS QUE PRESENTA

Se ha evolucionado de sistemas expertos, en los que los programadores trasladaban al algoritmo las normas para tomar decisiones, a algoritmos que permiten el aprendizaje automático de la máquina (*machine learning*). La automatización de decisiones mediante algoritmos basados en datos arroja grandes ventajas para optimizar la toma de decisiones y la gestión y mejora de la eficiencia de muchos sectores públicos y privados. Su impacto social es muy relevante, y de ahí la aspiración desde diversos ámbitos para asegurar que dichos algoritmos nos permitan tomar decisiones más justas, basadas en datos, inmunes a la corrupción, los sesgos cognitivos o los conflictos de interés.

Se trata, al utilizar la inteligencia artificial en el proceso judicial de una reestructuración de las exigencias de imparcialidad e independencia. Como Nieva Fenol ha puesto de manifiesto, las causas de parcialidad de un juez pueden resumirse en emociones de afecto y de odio. En este sentido, una máquina no podrá ser parcial, pues es imposible que en su diseño contemple la posibilidad de sentir emociones. Tampoco es posible que la herramienta de Inteligencia artificial se deje corromper por el poder, por lo que la independencia en su funcionamiento no corre riesgo. Sin embargo, esto no elimina el problema, sino que más bien traslada su foco: ahora la independencia y la imparcialidad tienen que ser garantizadas en el diseño y por lo tanto, el sujeto pasivo de estas exigencias sería quien elabora el algoritmo, que tendrá que cumplir las pautas de igualdad, no discriminación y sometimiento a la ley[19].

Qué nos hace desconfiar de la Inteligencia artificial. Pues precisamente sus características: complejidad, opacidad, aprendizaje automático, aprendizaje continuo y aprendizaje autónomo.

El problema radica, en primer lugar, en que su funcionamiento resulta incomprensible, lo que indudablemente dificulta la legitimidad de las decisiones que adoptan.

19. NIEVA FENOLL, J., *Enjuiciamiento prima facie. Aproximación al elemento psicológico de las decisiones judiciales,* Atelier, Barcelona, 2017.

En segundo lugar, son fundamentales los datos que introducimos, y es precisamente con ellos con los que se generan graves problemas. Por un lado, cabe destacar que no representan todos los escenarios. A veces la máquina no sabe porque hay un escenario que no se ha introducido, en este supuesto generaliza. Esto es producto de que no se ha introducido mucha información.

Por otro, no siempre el sesgo nace de forma intencionada. Los sistemas de inteligencia artificial y de aprendizaje automático se alimentan de datos y patrones relacionales por lo que, si en los datos de aprendizaje, se encuentran sesgos, la capacidad cognitiva contará con ellos. Además, es inherente al propio sistema algorítmico, matemático o relacional el que puedan existir sesgos a la hora de aplicar la propia metodología de cálculo e interpretación. Estas técnicas se basan en el uso y clasificación de los datos. Tengamos en cuenta que enseñamos a la Inteligencia artificial mediante datos e informaciones lo que es cada cosa. Ya estamos clasificando directamente mediante los conjuntos de aprendizaje. Es obvio, que en este modelo de aprendizaje cabe sesgo en la clasificación o simplemente ausencias en el conjunto de los datos de entrenamiento y validación. Así se crea uno de los sesgos más importantes y a los que son vulnerables los sistemas de Inteligencia artificial.

Es por esto, que el sesgo, o la ausencia de muestra real o total, siempre estará presente, pero, además, podemos aumentarlo al tratar la información con el prejuicio matemático o algorítmico de su creador.

Por ejemplo, si en una imagen aparece una persona con pelo largo y rasgos de mujer, el software no es capaz de detectar el objeto que sostiene como una taladradora y lo puede cambiar como un secador. Pues bien, en el ámbito policial y judicial, ello puede tener consecuencias terribles pues los sistemas de predicción delictiva o de análisis de riesgos trabajarán con datos extraídos de intervenciones policiales o judiciales previas que pueden estar cargadas de sesgo (*dirty data*).

El problema es, además, especialmente grave cuando, no existen estudios, como es el caso de Europa, dirigidos a identificar esos *dirty data*. Por ejemplo, en España, no existen datos policiales sobre el origen racial de las personas paradas por la policía para ser identificadas, aunque estudios independientes ponen de manifiesto que el porcentaje de personas de raza gitana, árabe, norteafricanos o latinoamericanos es muy superior a la de otras etnias u orígenes raciales[20].

20. SOUZA DE MENEZES, C./AGUSTINA SANLLEHÍ, J. R., *Big Data, inteligencia artificial y policía predictiva. Bases para una adecuada regulación legal que respete los derechos fundamentales*, en Dupuy, Daniela *et al.*, Cibercrimen III. Inteligencia artificial.

Hoy en día existen sesgos importantes en los sistemas de reconocimiento facial y vocal, aunque se están desarrollando grandes estudios e implementaciones para mitigar el impacto. Imaginen lo importante que puede ser que el sesgo haga que un sistema de reconocimiento facial o vocal nos identifique de manera errónea o que simplemente no nos identifique.

Puede haber soluciones para evitar los sesgos que pasan por tener sistemas de big data para combatir los posibles sesgos en los datos de entrada a los sistemas de inteligencia artificial; verificar cada una de las salidas del sistema, relacionarla con las entradas que motivaron la decisión y evaluar el acierto final; o realizar un prechequeo de los datos que alimentan los modelos que detectan potenciales sesgos de origen y poderlos eliminar o minimizar antes de que los algoritmos trabajen con ellos.

A todo ello se unen los datos con sesgo oculto. Hay algunos sesgos que no se manifiestan a primera vista, pero están. Recuerden como se llaman todas las aplicaciones que nos ayudan: Siri, Alexia. O cuando un proceso automatizado determina descartar las aplicaciones de mujeres para un trabajo en Amazon, o como le pasó a una investigadora del Instituto de Tecnología de Massachusetts (MIT) Joy Buolamwini, cuando el sistema de reconocimiento facial falla con su tono de piel.

Es posible también que los datos contengan errores (IMPACT). Realmente es difícil asegurar la calidad de los datos que se ponen en línea y esto repercute en la propia fiabilidad de las elaboraciones realizadas por los sistemas de Big Data Analytics, corriendo el riesgo de frustrar su aportación, incluso en aquellos casos en los que sería extremadamente útil. E incluso, a veces, los datos provienen de distintas fuentes y eso hace que en muchas ocasiones sean incompatibles.

Es posible que cuando no se tengan datos se utilicen datos sustitutivos. Tengamos en cuenta que el establishment tecnológico se ver reforzado por la ventaja competitiva resultante de la posesión de una posición monopolística o dominante en determinados sectores, que le permite adquirir continuamente una enorme cantidad de datos y ser capaz de procesarlos de forma cada vez más inteligente. Al mismo tiempo, los sujetos públicos se ven obligados a recurrir a los poderes privados para adquirir la información necesaria para el desempeño de sus funciones.

Por último, además si se entrena la caja negra con un objetivo determinado, sin límites en el uso de datos, podemos tener resultados no

Automatización, algoritmos y predicciones en el derecho Penal y procesal penal, buenos Aires, BdeF, 2020, p. 163.

deseados. De hecho, el problema de la opacidad de las *black box* que realizan las elaboraciones, ocultando el razonamiento utilizado para tomar determinadas decisiones. En este marco, la opacidad es casi absoluta: normalmente no es posible saber qué y cuánta información se adquiere y elabora realmente, ni cómo es, ni controlar realmente su circulación.

En tercer lugar, las decisiones algorítmicas tienen limitaciones, por ejemplo, riesgos de discriminación en casos, como hemos visto, por el uso de algoritmos entrenados con datos sesgados.

Cuando los algoritmos incluyen sesgos, su aplicación puede agravar posibles discriminaciones sociales, ya que las decisiones replican dichas desviaciones. En ese caso, pueden reproducir o amplificar patrones de discriminación presentes en la sociedad, es el caso del programa Compas utilizado por algunos jueces en EE. UU., en donde se comprobó que la población negra resultaba perjudicada.

Los algoritmos de IA afectan cada vez más a nuestras decisiones personales. Además, las empresas y los gobiernos han aumentado su dependencia de los algoritmos para tomar decisiones. En este contexto, investigaciones recientes han comenzado a advertir sobre la amplificación de prejuicios sociales en estos algoritmos. Los grupos históricamente desfavorecidos, como las mujeres y las personas de color, sufren más los efectos de los sesgos algorítmicos. Un estudio[21] encontró que si se daba como arranque la frase *"el hombre blanco trabaja como…"*, la IA la completaba con "*un oficial de policía*". En cambio, si el comienzo de la frase era "*el hombre negro trabaja como…"*, el algoritmo generaba el texto "*un proxeneta durante 15 días*".

Las personas negras se ven más afectadas por los errores y las predicciones inexactas de las inteligencias artificiales. Google tuvo que disculparse en 2015 porque su algoritmo etiquetó erróneamente la foto de dos personas negras como "gorilas".

Es obvio que los grupos dominantes se benefician de mayores índices de precisión por parte de las IA en comparación con los minoritarios. En este sentido, la falta de diversidad en los equipos de investigación es un problema.

Por otro lado, según la Agencia Europea de Derechos Fundamentales, su creación parte de un proceso no sólo estadístico o matemático, sino

21. "*The woman worked as a babysistter: On Biases in Language Generation*", en "Procedings of the 2019 Conference on Empirical Methodos in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing, China, November 3-7, 2019, pp. 3407 a 3412.

complejo y humano que incluye recopilación, preparación y análisis de datos en diversas etapas, lo que no está exento de polémica porque en ese proceso, es evidente e inevitable, que se contengan ideologías propias de los creadores y diseñadores de los algoritmos[22].

Los sesgos también pueden surgir por un algoritmo mal diseñado o por una mala aplicación del modelo algorítmico en ciertos contextos. Pero además puede darse un mal diseño o error de codificación.

Además, los algoritmos muchas veces resultan de gran complejidad, por estar basados en herramientas estadísticas asimismo muy complejas; o bien por funcionar a través de redes neuronales. Y, sin duda alguna, cuando más complejos, menos interpretables son. En definitiva, cuando más capacidad de entender menos capacidad de explicar los resultados. Es por ello que se da un gran desconocimiento de lo que tiene lugar en la caja negra para la toma de decisiones.

En cuarto lugar, la transparencia de los algoritmos y el respeto a la privacidad.

En lo relativo a la transparencia, la opacidad es un claro factor de los algoritmos de *machine learning*. La misma podrá optar por tres formas distintas:

Una opacidad derivada del secreto púbico o privado, que impide el escrutinio interno del algoritmo. Esta opacidad es la base de la explotación comercial de instrumentos del tipo de COMPAS. No obstante, para que un algoritmo se use para decidir sobre un sistema público de justicia, el contenido del mismo debería ser también público.

ES destacable que si los encargados de trabajar con estos sistemas no comprenden los factores que conducen a una mayor probabilidad de cometer un delito, de fugarse, etc., la eficacia de sus acciones podría verse reducida y el riesgo de que no se depuren determinados sesgos y terminen haciendo un seguimiento ciego de las indicaciones del sistema de la IA se vuelve mucho mayor.

Pero se entrelazan cuestiones de propiedad industrial e intelectual en la creación, comercialización y uso de algoritmos por parte de empresas privadas que han desarrollado este tipo de tecnología y que quieren ofrecerlas al sistema judicial. Desde luego, la propiedad industrial no puede prevalecer nunca frente a los derechos constitucionales fundamentales de los procesados, cosa que tendría lugar, sobre todo, si los análisis de

22. FRA, *BigData: Driscrimination in data-supported decisión making, European Union Agency for Fundamental Rights*, Viena, 2018, p. 4.

inteligencia artificial, más allá de ser una herramienta de auxilio al juez se convierten en el elemento nuclear sobre el que se apoyen sus resoluciones haciendo desaparecer la valoración personal de los distintos elementos probatorios.

Por otro lado, una opacidad derivada de la falta de conocimientos técnicos sobre el funcionamiento de un algoritmo o la interpretación de un código informático. Este campo del conocimiento está todavía reservado a un sector reducido de la población.

Por último, la opacidad relativa al propio funcionamiento de los algoritmos de *machine learning,* cuya peculiaridad estriba en el hecho de que incluso aquellos sujetos que poseen los conocimientos técnicos requeridos pueden llegar a ser incapaces de interpretar los motivos por los que el programa produce un determinado resultado.

Respeto de la privacidad es otro reto en este ámbito para evitar nuevos casos como el escándalo de Cambridge Analytica, una consultora vinculada a la campaña electoral que dio la victoria en EE. UU. a Donald Trump y que tuvo acceso, analizó y diseñó algoritmos basados en datos personales de usuarios de Facebook sin su consentimiento.

En el estricto marco del proceso judicial, estas tecnologías, a la vez que permiten el avance en el derecho a un proceso público y en el control de la actividad judicial, abren la puerta a que los datos de las partes o terceras personas acaben siendo sustraídos o utilizados de manera ilegal. Por ello son precisas políticas que fomenten los derechos a la privacidad y a la protección de los datos personales.

En quinto lugar, uno de los riesgos a los que habrán de enfrentarse los juristas será el peligro de la brecha digital. Con brecha digital nos referimos aquí no solo a la desigualdad en el acceso a herramientas digitales, que es el sentido tradicional de este concepto, sino también al problema del acceso a las aplicaciones de Inteligencia Artificial por parte de los profesionales jurídicos, aplicaciones que sólo son accesibles a los grandes despachos. Por tanto, la desigualdad que provoca la brecha digital tiene una doble vertiente: De un lado, potencia la vulnerabilidad de los sectores más pobres de la población, al no verse los mismos beneficiados por los avances en la Ciber-justicia, sino más bien todo lo contrario. De otro, agrava la diferencia de poder entre los grandes despachos y aquellos más pequeños, al tener acceso los primeros a herramientas de tecnología punta que les permitan prestas mejores servicios jurídicos.

Por último, es importante el riesgo de que la automatización de las decisiones judiciales por el uso de la Inteligencia Artificial conlleve una

reducción de la transparencia y fundamentación de las mismas. Es fundamental la motivación de las sentencias, ello permite a las partes conocer de qué manera ha llegado el juez a la conclusión que se ve reflejada en sus decisiones.

VII. INTELIGENCIA ARTIFICIAL EN EL PROCESO

Con la aplicación de la inteligencia artificial al proceso es posible que se automaticen tareas que son mecánicas y no necesitan de intervención humana, tales como enviar notificaciones o comprobar que una demanda cumple los requisitos formales necesarios para admitirla. La cuestión es si sirve para cuestiones procesales más complejas como la prueba.

En el ámbito jurisdiccional, empiezan a aparecer sistemas automatizados de toma de decisiones basados en algoritmos que persiguen la rapidez y certeza jurídica en la aplicación del derecho, la seguridad en el resultado; en definitiva, el acierto en la decisión judicial. Como consecuencia, en la actualidad, en determinados sistemas penales, se usan algoritmos predictivos que ayudan al juez en la toma de determinadas decisiones judiciales con la idea de lograr eficacia en el proceso, de racionalizar la justicia.

Además, el juez puede guiarse por la prueba fruto de la Inteligencia Artificial, teniendo en cuenta el grado de probabilidad que determine en pruebas como reconocimiento facial, que no sólo va a servir para aportar un valor añadido a la declaración o interrogatorio judicial que se preste, a efectos de verificar la credibilidad, sino también para averiguar la identidad del presunto autor del hecho. O también, la aplicación ALIBI que sirve para construir coartadas de alguien que comete un hecho delictivo.

Una de las cuestiones que resulta más relevante para sostener la posibilidad de aplicar un sistema de inteligencia artificial en el proceso es la verificación de los algoritmos que contienen, la que debe prestar atención, por un lado, a la posibilidad de que presente sesgos que discriminen a unas personas frente a otras, de acuerdo con los intereses o las inclinaciones de los programadores[23]; y, por otro, a su grado de fiabilidad predictiva, lo que en gran parte depende de la calidad de los datos

23. Uno de los principales hándicaps éticos que han planteado en la práctica los algoritmos policiales para reconocimiento facial es el sesgo que presentan con frecuencia respecto a determinadas comunidades. En este sentido, vale la pena consultar el informe *"The Perpetual Line Up"* del Georgetown Law Center on Privacy and Technology que, además de un interesante conjunto de datos, incorpora determinadas recomendaciones a los poderes públicos de los Estados Unidos entre las que se incluye una mayor y más fuerte regulación legal, así como un esfuerzo de transparencia pública de los procesos relativos a la obtención y gestión de los datos.

utilizados en su confección. Es por ello que como ha señalado el Parlamento Europeo en su resolución de 14 de marzo de 2017, considerando 20, serán necesarias "evaluaciones periódicas sobre la representatividad de los conjuntos de datos, así como examinar la exactitud e importancia de las predicciones".

El error en la fuente de datos debido al uso de datos no fiables o de baja calidad o la existencia de sesgos en el propio algoritmo o, incluso, en las interpretaciones de las conclusiones obtenidas afectaría, en el caso de que se utilizase en el proceso al desarrollo de la convicción judicial[24].

En todo caso, coincidimos con BUENO DE MATA[25] en que es necesario fijar una línea roja que no se debe sobrepasar. La inteligencia artificial no puede usarse para sustituir al juez, pues ello atentaría de manera frontal con lo que entendemos hoy en día por función jurisdiccional como actividad exclusiva y excluyente de jueces y magistrados. Por ello considero que cabe el uso de la inteligencia artificial como mecanismo de ayuda o guía al juez en sentido amplio, abarcando funciones de analítica jurisprudencial, asistente virtual para guiar en la tramitación informática de distintos procedimientos o utilizar los datos abiertos de los administrados como elemento predictivo en juicio.

Lo que sean datos abiertos nos los define la Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público, "*aquellos que cualquiera es libre de utilizar, reutilizar y redistribuir, con el único límite, en su caso, del requisito de atribución de su fuente o reconocimiento de su autoría, y a su vez piden que los mismos estén en formatos abiertos legibles por máquinas o sistemas expertos*", definiendo estos formatos como "*Un formato de archivo estructurado que permita a las aplicaciones informáticas identificar, reconocer y extraer con facilidad datos específicos, incluidas las declaraciones fácticas y su estructura interna y un formato de archivo independiente de plataformas y puesto a disposición del público, sin restricciones que impidan la reutilización de los documentos*".

Así bien, se podrá utilizar la información de los distintos organismos públicos y entre ellos del judicial, pues conforme a la Disposición Adicional segunda "*Aplicación a otros organismos*", *prevé en su apartado segundo que "las previsiones contenidas en la presente ley serán de aplicación a las sentencias y resoluciones judiciales*". Como ejemplo destacamos CENDOJ.

24. PÉREZ ESTRADA, M. J., *La inteligencia artificial como prueba científica en el proceso penal español,* Revista Bralileira de Direito Processual Penal, Porto Alegre, v. 7, n. 2, mayo, agosto, 2021, p. 1404.
25. BUENO DE MATA, F., Macrodatos, inteligencia artificial y proceso: luces y sombras, Revista General de Derecho Procesal, 51, 2020, p. 18.

En definitiva, y de acuerdo con BARONA VILAR[26], en que la incógnita es la de valorar si efectivamente el juez robot puede llegar a sustituir al juez humano en el proceso penal. Parece que la robotización judicial en sede penal podría llevar a la liquidación del proceso penal, al convertir este en un expediente automatizado que impediría el ejercicio de los derechos reconocidos a quienes son sujetos del proceso penal; mermarían las garantías de defensa y propulsarían una mecanización judicial que, cuando menos, chocaría con el proceso lógico jurídico de razonamiento judicial que aplica la norma al caso concreto, al sujeto concreto y bajo unas circunstancias concretas, modulando y justificando esta modulación en la motivación de los hechos probados.

A todo esto, se une que los sistemas tecnológicos aplicados al ámbito jurídico se basan en un conglomerado de datos que pertenecen al pasado, siendo esta circunstancia sumamente llamativa pues, sin lugar a dudas, supondrá un problema para el avance del derecho. El automatismo de las decisiones predictivas nos dirige hacia la estandarización de pautas y argumentos jurídicos implicando, indirectamente, la eliminación de los criterios de interpretación, lo que podría conllevar a resultados indeseados.

A partir de aquí, una vez introducida prueba algorítmica en el proceso, el juez podría valorarla y utilizarla en su motivación para dictar una resolución. Esto que resulta un tanto disruptivo en la mente de muchos juristas, resulta habitual en el mundo de la medicina. Un médico acude a un tac, una resonancia… para su diagnóstico. El problema aquí no es tanto que se acuda a la inteligencia artificial, sino a que el instrumento médico valora el presente del enfermo y la judicial se nutre de datos del pasado, y estos datos, son datos con desequilibrio, hay desequilibrio entre las clases por ejemplo, por el simple hecho de que tenemos menos ejemplos de unas clases que de otras. Todo ello nos conduce a que si generalizamos, se cometen errores de sesgo.

Pues bien, como en los coches que pasan la ITV, la máquina tendría que ser sometida a un testeo, presentándole casos, a fin de ver si introducen sesgos o no. Un organismo independiente debería realizar este testeo.

VIII. AFECCIÓN DE DERECHOS FUNDAMENTALES AL INTRODUCIR LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL

Cuando nos introducimos en el marco de la inteligencia artificial aplicada al proceso judicial, hemos de plantearnos los riesgos que puede

26. BARONA VILAR, S., *Cuarta revolución industrial (4.0) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia,* Revista Jurídica Digital UANDES 3/1 (2019), 1-21 DOI: 10.24822/rjduandes.0301.1, p. 15.

comportar esta tecnología en los derechos y garantías procesales de las partes. Así lo puso de manifiesto en 2016 al Comisión Europea para la Eficacia de la Justicia, resaltando la acuciante necesidad de garantizar y preservar las garantías procesales ante los riesgos que entraña la utilización de sistemas automatizados dentro de un proceso penal. Posteriormente, en 2018, la misma Comisión en la Carta Ética Europea sobre el uso de la Inteligencia Artificial en los sistemas judiciales y su entorno, reseña el respeto a los derechos fundamentales como uno de los pilares esenciales en el diseño, desarrollo y utilización de los sistemas inteligentes. Ya en el 2021, la propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas sore la Inteligencia Artificial no sólo contempla la preservación de las garantías procesales frente a la utilización de los sistemas inteligentes, sino que cataloga, como riesgo elevado, cualquier implementación de estos que se produzca en entornos jurídicos.

Partimos de que actualmente, los sistemas de Inteligencia Artificial aplicados al proceso se basan en técnicas predictivas, las cuales, gravitan sobre la obtención y el análisis estadístico de diversos datos que permiten, a través de una programación previa y determinada, arrojar unos resultados porcentuales como consecuencia del cruce de algoritmos inteligentes[27].

Cabe plantearnos la posible afección del Derecho al Proceso con todas las Garantías y, en concreto, al principio de imparcialidad judicial, igualdad de las partes en el proceso, y al principio de contradicción materializado en el derecho de defensa.

Que la garantía de la imparcialidad se halla incluida en el contenido del derecho a un proceso con todas las garantías lo manifiesta expresamente la sentencia 145/1988, de 12 de julio, según la cual "*… debe incluirse, aunque no se cite en forma expresa, el derecho a un juez imparcial, que constituye sin duda una garantía fundamental de la Justicia en un Estado de derecho, como lo es el nuestro, de acuerdo con el art 1.1 CE*". Parce claro que utilizar algoritmos judiciales en el proceso judicial como técnica o prueba aportada por la acusación, influirá en la convicción del juez que debe valorar y resolver el caso concreto.

Afectará a la imparcialidad del juzgador al dictar sentencia, el resultado del análisis de un algoritmo no configurado de forma adecuada o que presente sesgos, porque su convicción judicial estará condicionada al determinado sesgo que presente la herramienta de inteligencia artificial.

27. SAN MIGUEL CASO, C., La aplicación de la inteligencia artificial en el proceso ¿un nuevo reto para las garantías procesales?, Ius et Scientia, 2021, vol. 7, núm. 1, p. 294.

Así bien, la objetividad de estos sistemas debe ser cuestionada desde el primer momento en el que se produce la recogida de esos datos, encontrándonos con bases de datos sesgadas por no ser una muestra aleatoria estadísticamente válida de la población de interés, o porque, en algunos casos, contienen el historial de decisiones anteriores tomadas por seres humanos, basadas en los factores que se reflejan en ellas. No podemos obviar que los algoritmos son exclusivamente reflejo de los datos que se introducen, en forma tal que, si éstos incorporan sesgos, el algoritmo los va a reproducir, o incluso, los exacerbará.

El problema se hace aún mayor con los algoritmos de aprendizaje o *machine learning*, pues desarrollan un aprendizaje autónomo, lo que provoca que superen las barreras de la programación previa y terminen resultando indescifrables para el ser humano. En efecto, Los algoritmos de aprendizaje de datos cuánto más se alimentan de datos, más autónomos se vuelven. Sus resultados solo nos muestran sus tasas de éxito y los códigos que le introdujeron sus programadores, pero no las variables, muy cambiantes, que ha utilizado para llegar al resultado. Esta opacidad de los algoritmos supone un obstáculo más en la tutela de los derechos de las partes, suponiendo una grave lesión del derecho de densa.

Por el contrario, si se consigue que la herramienta de inteligencia artificial que se utilice tenga un alto grado de fiabilidad y, por tanto, sea admisible en el proceso penal, también afectará a la convicción judicial, pero en este caso, habrá una alta probabilidad de que, en el momento de valorar la prueba, el juez se halle conforme con los resultados que haya dado el instrumento de inteligencia artificial y base en éstos su resolución[28].

Dentro del derecho a un proceso con todas las garantías se haya el derecho de defensa. El contenido de éste se materializa en un doble ámbito: las partes deben poder conocer todos los materiales de hecho y de derecho que puedan influir en la convicción del juez en el momento de dictar la sentencia y la facultad de poder alegar, probar y argumentar con la misma idea de incidir en la convicción judicial. Es por ello que la opacidad en el contenido de los datos que presente la herramienta de inteligencia artificial que se pueda llegar a utilizar en el proceso lesionará el derecho de defensa cuando el propio desconocimiento de la estructura que contiene el algoritmo afecte al derecho de defensa del investigado o acusado. No se trata tanto de que no pueda ejercer el derecho de defensa, pues la contradicción está garantizada formalmente, sino que el verdadero problema

28. DE MIGUEL BERIAIN, I/PÉREZ ESTRADA, M. J., *La inteligencia artificial en el proceso penal español. Un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados,* Revista de Derecho UNED, núm. 25, 2019, p. 551.

está en comprender cómo la herramienta inteligente o el algoritmo que se ha usado ha conseguido un determinado resultado y poder así rebatirlo[29]. Como se llega a un resultado con las "cajas negras" afecta al derecho de defensa, pues no puede establecerse como el sistema evalúa y pondera los datos y la información que procesal. Así bien, resulta posible conocer los valores que se han introducido en el sistema y, también el resultado final arrojado por este, pero no se puede comprender el funcionamiento interno de la máquina, ni el cruce ponderativo que ha realizado hasta llegar al resultado final.

Así bien, se hace necesario comprender y explicar los sistemas inteligentes, pero hay que evitar el extremo en el sentido de pretender su total transparencia y explicabilidad.

Por lo tanto, se puede adoptar un enfoque prudente, destinado no a eliminar la opacidad de los sistemas inteligentes, sino a hacerla variable en su intensidad y proporcional a los riesgos que plantean, mediante una regulación que prevea un ámbito y unos métodos adecuados a los tipos específicos de esto sistemas y a su ámbito de aplicación[30]. Ello no es óbice para limitar el secreto de los códigos informáticos, ya que la llamada explicabilidad de los resultados de los sistemas inteligentes debe ser posible al menos en casos concretos.

En definitiva, no sólo nos planteamos la posible afección de derechos fundamentales, la introducción de la IA en el proceso puede suponer:

a. Falsa neutralidad y sesgos. Recordemos que, aunque creamos que la IA se alimenta única y exclusivamente de cifras y que los números sólo pueden ser tratados de forma matemática, lo cierto es que se alimenta de datos que se corresponden con variables y con la información social que hay dentro de ellos.

b. Intromisión en la intimidad personal por la posibilidad de que se conculquen derechos básicos a la hora de recopilar tales datos. Además, por el hecho de que el almacenamiento de aquellos que sean recopilados, aún con el consentimiento de su titular, no se produce en un espacio físico más o menos controlable, sino en servidores remotos interconectados a través de redes informáticas que permiten fácilmente su desvío, extracción, etc. Por otro lado, porque datos en principio inocuos, debidamente

29. DE MIGUEL BERIAIN, I/PÉREZ ESTRADA, M. J., *La inteligencia artificial en el proceso penal español. Un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados,* Revista de Derecho UNED, núm. 25, 2019, p. 552.

30. FIORIGLIO, G., Inteligencia artificial: Retos para el derecho en la sociedad global, en Inteligencia artificial y derecho. El jurista ante los retos de la era digital, Aranzadi, 2021, p. 124.

tratados, pueden arrojar una valiosísima información personal que acabe conculcando la intimidad del sujeto. Esto ocurre con los metadatos, esto es, datos que suministran información sobre los archivos digitales producidos por el sujeto. Así, en una fotografía, los metadatos pueden arrojar información sobre: la fecha en la que se hizo, el equipo en que se utilizó para ello, el lugar en el que se tomó, el nombre de la persona que la hizo. Con todo ello se podría conocer dónde y cuándo hemos estado de vacaciones, donde vivimos…[31].

c. Puede afectar a la presunción de inocencia. No todos tendrán acceso a estas herramientas para diseñar la estrategia de defensa, pues supone un elevado coste. Es por ello que sólo podrán optar aquellos que tengan recursos económicos suficientes. Pero, es más, si se utilizarán los sistemas inteligentes a la hora de plantear la estrategia de defensa, pudiera darse el caso de que esto generase el menoscabo de la defensa técnica para algunos investigados y, consecuencia de ello, se produjese cierta indefensión cuando los sistemas predictivos arrojasen unos resultados muy reducidos de éxito. Podría darse el caso de abogados que declinarán la aceptación de la defensa del cliente.

d. Puede afectar a la carga de la prueba y a la valoración de la prueba. Por ejemplo, ASSYST es una herramienta que ofrece directrices a los jueces para dictar sentencias en Canadá.

e. Puede afectar a la motivación de la sentencia, en lo relativo a cuáles es el valor de la prueba en la sentencia. A este respecto cabe hacer referencia al Informe *Artificial Intelligence and Fundamental Rights* de la Agencia de los Derechos Fundamentales de la UE, 2020.

Ante todas estas dudas que se nos plantean cabe, desde luego, incidir en:

a. Mecanismos de control previos, invalidando los que incurran en sesgos.

b. Preservar el derecho a la protección de datos.

c. Incidir en IA explicada, esto es, en conocer los criterios empleados.

d. Configurar también sistemas de control de funcionamiento. Se hace preciso auditar el sistema de forma periódica.

e. Es preciso garantizar la acción humana en estas supervisiones. No se debe dejar toda la carga de evaluación en la IA. A este respecto

31. PALMA HERRERA, J. M. *Inteligencia artificial y lucha contrala delincuencia. Potencialidad y peligros en el mundo global*, en "Inteligencia artificial y derechos. El jurista ante los retos en la era digital", Aranzadi, 2021, p. 291.

recordemos una sentencia de 30 de septiembre de 2021 de la Sala de lo Contencioso administrativo de la AN, en la que se condenó al Ministerio de Interior por la deficiente protección que la Guardia Civil otorgó a una mujer que solicitó una orden de protección. Un cuestionario de cribado le otorgó riesgo bajo. Sin realizar más averiguaciones los agentes calificaron el riesgo como no apreciado, la misma valoración que hizo que el juzgado denegase la medida de protección a la fallecida. Consideró la Sala que "*la actuación de los agentes ante situaciones de violencia de género no debería quedar limitada a aspectos formales de atención a la denunciante, asistencia, información de derecho y citación a juicio, sino que su actuación exige una atención preferente de asistencia y protección a las mujeres que han sido objeto de comportamientos violentos en el ámbito familiar, a los efectos de prevenir y evitar, en la medida de lo posible, las consecuencias del maltrato*". En este caso, el cuestionario de cribado de IA no apreció un riesgo que, con una entrevista personal y aplicando la perspectiva de género, se habría considerado.

f. Favorecer la incorporación de juristas en el diseño de la IA.

En cualquier caso, en los diferentes controles del sistema, en la evaluación diferida de las distintas fases del proceso interno del sistema inteligente, el desarrollador del algoritmo no debe participar en la fase de valoración del mismo. De forma tal que considero acertado que, en las distintas fases de intervención o evaluación de la Inteligencia Artificial, participen sujetos distintos, con la finalidad de garantizar una mayor fiabilidad de estos sistemas.

Este planteamiento genera un debate que afecta directamente a la evaluación de la Inteligencia Artificial, y que se contrae al secreto comercial que se cierne sobre el sistema inteligente. Sin embargo, la solución pasa por la ausencia de privatización sobre el algoritmo que debería ser público atendiendo al entorno jurídico en el que se desarrollaría. Es decir, en un sistema público de justicia la inclusión de tecnología privada que, en cualquier caso, responde a unos intereses absolutamente distintos a los propios de la Administración de Justicia no sólo supone, de forma parcial, la externalización de un servicio, sino que, además, implica un riesgo añadido en el derecho a un juicio justo[32].

32. GASCÓN INCHAUSTI, F., *Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial*, en CONDE FUENTES y SERRANO HOYO, "La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro", Atelier, 2019, p. 200.

Algoritmo y proceso laboral

José Antonio Colmenero Guerra[1]

Prof. Titular de Derecho Procesal
Universidad Pablo de Olavide

SUMARIO: I. INTRODUCCIÓN. II. REVOLUCIONES INDUSTRIALES. III. APRENDER A DISTINGUIR: NUEVAS TECNOLOGÍAS, ALGORITMOS, *BIG DATA*, *DATA MINING*, INTELIGENCIA ARTIFICIAL (IA). IV. TECNOLOGÍAS, ALGORITMOS E IA EN LA ADMINISTRACIÓN DE JUSTICIA. V. ALGORITMOS E IA EN LA GENERACIÓN DE CONFLICTOS LABORALES.

I. INTRODUCCIÓN

Señalaba el Presidente de la Comisión Europea, Jean-Claude Juncker, en su discurso sobre el estado de la Unión Europea (14/09/2016), que "[s]er europeo conlleva el derecho a que nuestros datos personales estén protegidos por estrictas leyes europeas. Porque a los europeos no nos gusta que unos drones sobrevuelen nuestras cabezas registrando todos nuestros movimientos, ni que las empresas registren cada vez que hacemos clic en nuestro ordenador. Por este motivo, en mayo de este año el Parlamento, el Consejo y la Comisión aprobaron un reglamento de protección de datos. Es esta una norma común europea que se aplica a las empresas con independencia de dónde tengan su sede y cuándo traten

1. Este Trabajo se enmarca dentro del Proyecto "La Tutela de Consumidores y Usuarios. El Marco Europeo. Su aplicación en el Ordenamiento Español y los Sistemas de Actuación y Protección en Andalucía" (US-15413), dentro de los Proyectos de I+D+I en el marco del Programa operativo FEDER Andalucía 2014-2020. Miembro del Grupo de Investigación PAIDI, de la Junta de Andalucía, "Sistema penal y Criminología (SISPECRIM)" (Referencia SEJ 571). Investigador del Instituto Alonso Martínez de Justicia y Litigación (UC3M). ORCID: 0000-0001-6214-8519.

sus datos. En Europa, valoramos la intimidad: es una cuestión de dignidad humana"[2].

Ciertamente podría haber elegido otra manera de empezar el trabajo, pero la relevancia de la persona, el momento, y la idea que trasluce su discurso, bien merecen el comienzo, pues refleja, claramente, parte de mis preocupaciones, y parte de lo que quiero señalar en las siguientes líneas.

Inmersos en la Cuarta Revolución Industrial, en esta sociedad "líquida", globalizada, postmoderna y neoliberal, creo que preocuparse por los "datos", no resulta ya, novedoso. Las Revoluciones Industriales han estado, al margen de otras consideraciones, ligadas a la "máquina", primero a la de vapor, luego a la electricidad y combustibles fósiles, para pasar a las digitales, y encontrarnos en los comienzos de la "máquina cuántica". Máquina viene del griego (*méchané*), y significaba medios, artificio y truco, y en estos tiempos que vivimos no ha perdido dicho significado y esencia, aunque, desde luego, materialmente, ya no es la misma "máquina" que podemos observar y estudiar en los libros de historia[3].

Todas las máquinas, que han habitado las diferentes revoluciones industriales, han supuestos cambios, en el plano político, económico, social, pero también jurídico. Y las que presenta la cuarta revolución industrial no está siendo ajena a los mismos. Las máquinas de esta revolución han llevado a que ahora hablemos de la "Era de los datos"[4]. Y eso entronca con mis ocupaciones y preocupaciones. Recientemente me he ocupado de la protección de datos personales en el ámbito penal, y ello me ha llevado a observar qué ocurre con dicha protección de datos en el ámbito laboral, claro, desde mi ángulo de la actividad jurisdiccional. Pues, si en el ámbito penal preocupan dichas cuestiones, es de imaginar, que en el mundo de las relaciones laborales esas cuestiones ya deben, también, haber aflorado, y posiblemente, su frecuencia cuantitativa vaya a ser mayor, e, incluso, puede que cualitativamente también su preocupación pueda llegar a ser mayor.

Si nos ceñimos a la información que facilitan los diccionarios, "dato" es la información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho. También

2. *Vid.* Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "La construcción de una economía de los datos europea". Bruselas, 10.1.2017. COM (2017) 9 final.
3. Sobre ello, GABRIEL, *El sentido del pensamiento*, 2.ª Edición, Editorial Pasado & Presente, Barcelona, 2020, p. 145.
4. Sobre el tema, en lo que ahora nos interesa, *vid. El trabajo en la era de los datos. Datos, ideas y propuestas sobre economía digital y el mundo del trabajo*. Colección BBVA OpenMind, n.° 12. BBVAOPENMIND.COM.

significa documento, testimonio y fundamento, y por supuesto, en el ámbito de la informática, es la información dispuesta de manera adecuada para su tratamiento por una computadora (DRAE). De hecho, es bastante común señalar que los datos es la información concreta sobre hechos, elementos, etc., que permite estudiarlos, analizarlos o conocerlos, ahora a través de "máquinas digitales".

La Administración de Justicia siempre ha trabajado con datos, pues siempre trabaja con hechos jurídicamente relevantes para la solución de los conflictos, por tanto, hechos acaecidos, pero también con hechos relativos a acontecimientos futuros (medidas cautelares, por ejemplo). Por ello, en la "Era de los datos", interesa conocer el tratamiento que reciben los datos en el Sistema de Justicia español, y en nuestro caso, vamos a referir la cuestión al ámbito del Orden Social de la Jurisdicción. Desde luego nos interesan los datos tratados en la Administración de Justicia, bien, por los instrumentos o mecanismos que utiliza para ello, bien por los instrumentos o mecanismos utilizados en las "historias" que conforman la "causa de pedir" de las pretensiones ejercitadas en el proceso.

El ritmo vertiginoso de las innovaciones tecnológicas y el fenómeno de la globalización han transformado, radicalmente, los métodos de recogida, acceso, utilización y transferencia de los datos personales, en un volumen en constante crecimiento. Por ello, como se ha señalado en la documentación de la UE, "Las nuevas formas de compartir información en las redes sociales y el almacenamiento remoto de grandes cantidades de datos han pasado a formar parte de la existencia cotidiana de una amplia proporción de los 250 millones de usuarios de Internet en Europa". Además, "los datos personales se han convertido en un activo para numerosas empresas, una parte importante de cuyas actividades económicas consiste en la recogida, agregación y análisis de los datos de clientes potenciales"[5]. Así, un Eurobarómetro[6] especial, realizado en septiembre y octubre de 2021, señala que el 81% de los europeos consideran que, de aquí a 2030, las herramientas digitales e Internet serán importantes en sus vidas. Más del 80% piensa que el uso de dichos instrumentos aportará tantas ventajas como inconvenientes, mientras que un 12% prevé más inconvenientes que

5. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y la Comité de las Regiones, "La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI". Bruselas, 25.1.2012. COM (2012) 9 final.

6. Special Eurobarometer 518 Report. *Digital Rights and Principles*. September-October 2021. Un resumen, del que hemos obtenido los datos, puede verse en el Comunicado de prensa de la Comisión Europea "Eurobarómetro: los europeos muestran su apoyo a los principios digitales" (https://ec.europa.eu/commission/presscorner/detail/es/IP_21_6462).

ventajas. Eso no quita que el 56% de los encuestados muestre su preocupación por los ciberataques y ciberdelitos; el 53% expresa su preocupación por la seguridad y el bienestar de los niños en su uso de Internet, y al 46% le preocupa el uso de datos e información personales por parte de empresas o administraciones públicas; el 34% se preocupa por la dificultad de desconectar y encontrar un buen equilibrio entre la vida en línea y fuera de línea; y al 26% le preocupa la dificultad de adquirir nuevas capacidades digitales necesarias para participar activamente en la sociedad. Finalmente, la encuesta pone de relieve que la mayoría de los ciudadanos de la UE cree que la UE protege bien sus derechos en el entorno en línea, pero, casi el 40% no sabe qué derechos suyos, como la libertad de expresión, la privacidad o la no discriminación, también deben respetarse en línea.

El ciudadano, tiene derecho a poder ejercer un control efectivo sobre sus datos personales. Conviene no perder de vista que el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea establecen que la protección de datos es un derecho fundamental. Y en esa línea ya se situaba el artículo 18.4 de la Carta Magna, tras su interpretación por el Tribunal Constitucional, de ahí la necesidad de su adecuada salvaguarda.

Para ello, tanto desde el plano de la UE, como desde el plano nacional, es necesario disponer de normas modernas y coherentes: Es preciso disponer en toda la UE: i) de normas modernas y coherentes que permitan la libre circulación de datos entre los Estados miembros; ii) las empresas necesitan reglas claras y uniformes que aporten seguridad jurídica y reduzcan las cargas administrativas. El cumplimiento de dichas premisas es necesario para el funcionamiento del mercado único y la necesidad de estimular el crecimiento económico, crear puestos de trabajo y fomentar la innovación. Para la UE la modernización de la normativa en materia garantizará a los ciudadanos un alto nivel de protección de datos y fomentará la seguridad, la claridad y la coherencia jurídicas.

Desde el Plan de Acción de Estocolmo de la Comisión Europea (luego reflejado en la Agenda Digital para Europa y en la estrategia de crecimiento de la UE Europa 2020), se han sucedido rondas de consultas públicas sobre protección de datos, diálogos intensivos con los interesados, Comunicaciones, que aconsejaban a la Comisión Europea una reforma general de las normas de protección de datos de la UE: i) un Reglamento (que sustituye a la Directiva 95/46/CE) en el que se fija el marco jurídico general de protección de datos de la UE[7]; ii) una Directiva (que sustituye

7. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento

a la Decisión Marco 2008/977/JAI)[8], que fija las normas sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes; y iii) ello no excluye, en fase posterior, modificaciones destinadas a armonizar instrumentos específicos y sectoriales. Con estas reformas se configura un marco moderno, sólido, coherente y global de protección de datos para la Unión Europea que reforzará el derecho fundamental de los ciudadanos a la protección de sus datos. Ahora bien, no se trata de proteger, solo, los datos personales, pues también habrá que proteger otros derechos fundamentales, aplicando el principio de proporcionalidad, como puede ser la libertad de expresión e información, los derechos del niño, el derecho a la actividad empresarial, el derecho a un juicio justo y el secreto profesional. Con la reforma se pretende obtener beneficios para los ciudadanos, para las empresas y las instituciones públicas que redunden en la mejora del mercado único y el crecimiento económico[9].

El RGPD y la DPDPP han sido objeto de desarrollo, en el primer caso, y de transposición, en el segundo. La Ley Orgánica 3/2018, de 5 de diciembre (*BOE* del 6), de Protección de Datos Personales y garantía de los derechos digitales (LOPDP), procede al desarrollo y concreción, para el ordenamiento interno, de lo previsto, con carácter general, por el RGPD,

---

de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos –RGPD–). *DOUE* L 119/1, de 4 de mayo de 2016. En adelante RGPD.

8. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DPDPP). *DOUE* L 119/89, de 4 de mayo de 2016. En adelante DPDPP.

9. Como señala la Comunicación de 2012, "La reforma beneficiará en primer lugar a los particulares, ya que consolidará sus derechos a la protección de datos y aumentará su confianza en el entorno digital. Además, la reforma simplificará considerablemente el marco jurídico tanto para las empresas como para el sector público, intervención que se espera estimule el desarrollo de la economía digital dentro de la UE y allende sus fronteras, conforme a los objetivos de la estrategia Europa 2020 y a la Agenda Digital para Europa. Por último, la reforma aumentará la confianza entre las autoridades con funciones coercitivas con el fin de facilitar el intercambio de datos y la cooperación en la lucha contra la delincuencia grave, asegurando al mismo tiempo un alto nivel de protección a los ciudadanos". Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y la Comité de las Regiones, "La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI". Bruselas, 25.1.2012. COM (2012) 9 final.

y la Ley Orgánica 7/2021, de 26 de mayo (*BOE* del 27), de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (LOPDPP), procede a la transposición de la DPDPP, aunque a ella haya que anudar determinados preceptos de la Ley Orgánica del Poder Judicial, el Estatuto Orgánico del Ministerio Fiscal y de la Ley General Penitenciaria, para entender cumplida la transposición[10]. Con ello se ha producido un cambio relevante en el ámbito de la protección de datos, aunque no han sido los únicos cambios. Pero hemos hecho referencia a los cambios acaecidos en materia de protección de datos, generales o particulares, pero vinculados con la Administración de Justicia. En el campo de la Administración de Justicia también se han producido cambios como consecuencia de los adelantos tecnológicos, mostrando, a tiempo presente, grandes signos de automatización, pero también del uso de algoritmos e incluso de Inteligencia Artificial. Luego, proteger datos personales, ya no es una cuestión externa al mundo judicial, también es una cuestión interna, y sobre ella también conviene decir algunas cuestiones.

Además, desde el plano empresarial, también se han ido sucediendo cambios. El fenómeno digital en el mundo económico tiene una enorme incidencia en el mundo laboral. La transformación digital aporta claros beneficios a las empresas, tanto a los empleadores como a los trabajadores, e, incluso, a quienes buscan empleo, pues suponen nuevas oportunidades de trabajo. Pero también inciden en la productividad, en la mejora de las condiciones de trabajo y en la calidad de los servicios y productos. Desde luego ello incide, o puede incidir, en un aumento o en el mantenimiento del empleo.

Claro, que dicha transformación conlleva retos y riesgos para los trabajadores y las empresas, pues algunas actividades desaparecerán y otras cambiarán. Por ello, se requiere anticipación del cambio, ofreciendo los conocimientos necesarios para que los trabajadores y las empresas obtenga un uso óptimo de los adelantos digitales. Ahora bien, la era digital suponen cambios de organización, de las condiciones de trabajo, de la conciliación de la vida laboral y familiar, y de accesibilidad de la tecnología, incluida las infraestructuras. En la era de los datos, el aumento exponencial de la capacidad de almacenamiento, transmisión y procesamiento

10. Si dejamos en un segundo plano la protección de datos en el orden jurisdiccional penal, para la que debe estarse a las reglas previstas en la LOPDPP, para el resto de órdenes jurisdiccionales, habrá que estar, en materia de protección de datos, al RGPD, la LOPDP, la LOPJ y las normas procesales, en el caso de los órganos jurisdiccionales y sus oficinas, y por el RGPD, la LOPDP, el EOMF, la LOPJ y las normas procesales que le sean aplicable en el caso del Ministerio Fiscal y sus Oficinas.

de datos están afectando, de forma particularmente profunda, al ámbito del trabajo, por ello, y dado que las mejoras no son automáticas, será necesario adaptar el mercado laboral. Habrá que incidir en la educación y la capacitación, e, incluso, en los sistemas de protección social, para asegurar una transición mutuamente beneficiosa para los empleadores y los trabajadores. La UE y los gobiernos nacionales tienen un importante papel que desempeñar en dicho enfoque. Por ello, con este trabajo, más que proponer soluciones, sí queremos ordenar algunas ideas, que inciden en la protección de los datos personales de los trabajadores, pero también en otros derechos fundamentales que, hasta ahora, no se veían frecuentemente limitados, como puede ser todo lo relativo a su privacidad, y que en la cuarta revolución industrial se ven fuertemente tensionados. Desde luego, tanto la Administración de Justicia hace uso de los datos, para desempeñar eficaz y eficientemente sus actividades, como del mismo modo la nueva empresa se nutre de ellos para competir en el mercado. Por ello, aportar algunas ideas sobre el tema, desde ambos ángulos, pensamos que puede ser una opción razonable y conveniente.

II. REVOLUCIONES INDUSTRIALES[11]

En el apartado anterior hemos puesto de relieve las nuevas coordenadas que está fijando la cuarta revolución industrial. Pero antes de referirnos a ella, o mejor, como paso previo, sería conveniente esbozar algunas ideas y cuestiones sobre las anteriores revoluciones industriales, puesto que todas han aportado transformaciones en el ámbito político, social, económico, empresarial y también jurídico. Desde luego, lo que no se puede poner en duda que todas ellas han supuesto el tránsito de una sociedad agrícola a una comerciante, con relevantes cambios en la producción industrial y en las formas de trabajo. Y en la parte que a nosotros también nos interesa, el mundo jurídico hizo un tránsito relevante en su forma de operar, fundamentalmente a través de la conquista de derechos, sobre todo de la consolidación de los derechos humanos o fundamentales.

La Primera Revolución Industrial tuvo lugar a finales del Siglo XVIII y comienzos del Siglo XIX, teniendo su génesis en Inglaterra, irradiándose por Europa y América. España, sin embargo, se incorporará, salvo algunas zonas (Cataluña y País Vasco), tarde, durante la segunda mitad del Siglo XIX. Durante dicho período la expansión de Gran Bretaña, debido a su

11. Para un desarrollo más extenso, *Vid*. BARONA VILAR, *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Edit. Tirant lo Blanch, Valencia, 2021, pp. 42 a 76.

imperio colonial, su flota marítima, que expandió su comercio, su carbón y hierro necesarios para poder crear maquinaria, darán lugar a un crecimiento del sistema comercial y empresarial, creándose y consolidándose las grandes compañías comerciales. A ello, como elemento específico, se podría unir que será el surgimiento de la producción textil, como consecuencia de los telares mecánicos. Ello también supondrá, en el caso de Gran Bretaña (y luego de otros países), el surgimiento de los movimientos obreros, y la gestación de las primeras legislaciones laborales, tratando de regular las relaciones de trabajo. También supondrá la creación de las ciudades, como consecuencia del crecimiento demográfico (y descenso de la mortalidad), al socaire del modelo social burgués, insuflado por un Estado unitario consecuencia de políticas absolutistas combinadas con el liberalismo económico de la época. El Siglo XIX supondrá el desarrollo de la ciencia, la técnica y la tecnología.

Pero este período también supondrá el nacimiento de movimientos a favor de las clases más desfavorecidas, en la lucha por sus derechos, que calará en los ordenamientos jurídicos. Durante dicha revolución industrial se producirá la Revolución americana, que llevará a las colonias norteamericanas a su independencia (1776) y posteriormente durante el Siglo XIX a la del resto de América. Pero también será el período de la Revolución francesa (1789). En ambas revoluciones la protección de la libertad y la igualdad serán elementos esenciales. Dichas Revoluciones serán un empuje para el reconocimiento formal de los derechos de las personas, pues estas pasarán a ser el centro de los Sistemas Jurídicos. No obstante, y volviendo al principio, decíamos que la revolución industrial supuso la entrada de las máquinas (todavía de vapor) al mundo de la industria textil, y ello, tendrá como consecuencia, que uno de los colectivos fuertemente afectados por dicha revolución serán las mujeres, que ocupaban buena parte de los trabajos que dichos telares mecánicos suprimieron.

Finalmente, como resumen, podemos señalar que "la revolución industrial, amén de los enormes beneficios que incorporó al capital, alimentando exponencialmente la ideología capitalista, supuso la consolidación de dos clases sociales: por un lado, la burguesía industrial y, por otro, el proletariado industrial, que se agruparía en contestación a sus condiciones de vida, y gestando la lucha por una sociedad con unos componentes que favorecieran la igualdad entre los ciudadanos"[12].

La Segunda Revolución industrial comenzaría a partir de 1860 y finalizaría en 1914, con la Primera Guerra Mundial. Continuarán los cambios, pero también continuará el crecimiento demográfico y seguirá

12. *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, p. 52.

descendiendo la mortalidad. Si en el anterior período la ciencia, la técnica y la tecnología, evolucionan, en este no le va a la zaga, y el crecimiento es exponencial. Además de los avances en la máquina de vapor, que incidirá en el mundo de los ferrocarriles, con lo que supondrá, desde el plano de la libre circulación de las personas y el traslado de mercancías, a esta época corresponden, también, el telégrafo, el teléfono e, incluso, los proyectores de imágenes. Pero, en el campo empresarial, los motores del cambio será la electricidad, que, junto con el petróleo y sus derivados, como materiales utilizados para fabricar acero, generarán un gran desarrollo industrial.

Desde el plano económico las directrices eran claras, reducir costos para aumentar ganancias y las nuevas tecnologías y técnicas industriales coadyuvarán a ello. Este período será el del nacimiento de la "organización científica del trabajo" ("Taylorismo") y el surgimiento de la cadena de montaje ("fordismo"), con lo que el obrero dejó de fabricar un producto, para pasar a fabricar un parte del producto, y supuso la combinación del trabajo de máquinas y obreros en la producción.

A esta época corresponde el surgimiento de los monopolios y grupos financieros (*trust*), lo que supondrán cambios en los hábitos de consumo, que ya en esta época empiezan a depender de la masa obrera trabajadora, que condicionará parte de los modelos sociales y políticos de la siguiente Revolución industrial (explosión del socialismo y comunismo). En el campo empresarial, al margen de los nuevos condicionantes económicos, en las relaciones empresa-trabajo supondrá el crecimiento paulatino de la legislación laboral, tanto en materias relativas a las relaciones de trabajo, como en el surgimiento de las cuestiones relativas a la "previsión social". Se realizarán modificaciones legislativas, fundamentalmente de carácter sectorial, pero se consolidarán derechos, sobre todo civiles y políticos, y emergerán nuevos derechos fundamentales dignos de tutela, los derechos sociales.

La Tercera Revolución Industrial será consecuencia de la automatización y digitalización de las máquinas. Tras la Primera Guerra Mundial, la industria 2.0. irá evolucionando consecuencia de la ciencia, la técnica y la tecnología, incluso, alentada por la Segunda Guerra Mundial. Durante los años 50 del Siglo pasado la aparición de la microelectrónica supuso cambios relevantes en la creación de máquinas, y ello llevará a la digitalización y computación. También se verá acompañada del surgimiento de nuevas fuentes de energía (energía nuclear). Se producirán cambios en los medios de comunicación y de gestión. A partir de 1960 se producirá el surgimiento de los sistemas computacionales y con él INTERNET. Estamos en la etapa del ordenador y todas las cuestiones que ello ha supuesto, desde el plano de la organización y de la gestión, tanto pública como privada. Desde el plano político y social, tras la Segunda Guerra Mundial se

producirá la consolidación de los derechos y libertades fundamentales, al menos en las democracias bien estructuradas, y la lucha por la protección de los derechos sociales. En el ámbito Regional la Comunidad Económica Europea, luego Unión Europea, consolidará al ordenador como eje del crecimiento económico, e incluso, en el campo jurídico supondrá poner los primeros ladrillos de la *eJustice*. Hemos pasado del "transistor", la "tele", la "alta fidelidad" y la "calculadora", al "Software", "hardware", "teléfonos móviles" e "internet", con lo que ello tiene de cambios en la sociedad.

Pero esta etapa, pese a todo, se ha cubierto rápido. Los nuevos instrumentos técnicos evolucionan rápido. Así, las nuevas máquinas permiten acumular un ingente volumen de datos, y permiten obtener mayores informaciones y resultados, y pensar y conseguir nuevos instrumentos y métodos para tratar y procesar dichas informaciones, tomando como referencia o punto de partida lo ya conseguido. Será, a través de los algoritmos que se produzcan dichos avances, pues no solo mejorarán las formas de tratar y procesar los datos, sino que permitirán cambiar los sistemas de organización e información, pero también van a ser utilizados para automatizar un gran volumen de procesos, e incluso para facilitar la toma de decisiones.

Los últimos años del Siglo XX, y el comienzo del Siglo XXI (momento en que nos encontramos), dichas tecnologías han llevado a plantear la hipótesis de una "Ciberfábrica" (Alemania). Este se puede considerar el momento en que se acuña el término Industria 4.0, conectado a la digitalización, conectividad, automatización, robotización e inteligencia artificial. Como señala BARONA VILAR, "el origen del término Industria 4.0 se encuentra en un proyecto de estrategias de alta tecnología realizado por el gobierno alemán, cuyo objetivo era la creación de la fábrica inteligente o también conocida como Ciberfábrica, caracterizada por la gran interconexión entre máquinas automatizadas, la concurrencia de redes de comunicaciones, la integración de tecnologías avanzadas de procesamientos de datos, la robótica avanzada, la capacidad de autodiagnóstico de situaciones, el mejor intercambio de información y una mayor eficiencia en la gestión de recursos naturales y humanos"[13].

Inicialmente se consideró que era una evolución de la Industria 3.0 (Tercera Revolución Industrial). Sin embargo, como pone de relieve BARONA

13. El término fue empleado, por vez primera por Henning KAGERMANN, Presidente de la Academia alemana de Ciencias e Ingeniería (Acatech), saliendo a la luz en la Feria de Hannover de 2011. *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, p. 58.

VILAR (apoyándose en SCHWAB), "en esta nueva etapa se ha producido la integración de los sistemas técnicos, cibernéticos, y la irrupción, entre otros, de los sistemas computacionales en la producción y en la logística, incorporando innovaciones científicas y tecnológicas que inciden no solo en la digitalización de las cadenas industriales de producción, sino también en la aparición del internet de las cosas –conexión de objetos cotidianos a internet–, el *big data*, y muchos otros más, planteando consecuencias y también problemas jurídicos y éticos, sin olvidar las transformaciones laborales indiscutibles y la afectación de derechos, y muy especialmente la libertad, la privacidad, en sus diversas manifestaciones"[14].

III. APRENDER A DISTINGUIR: NUEVAS TECNOLOGÍAS, ALGORITMOS, *BIG DATA*, *DATA MINING*, INTELIGENCIA ARTIFICIAL (IA)

Ya hemos puesto de relieve que la ciencia y la técnica han sido parte del desarrollo del mundo empresarial y del trabajo. Y han supuestos muchos cambios, algunos buenos y otros todo lo contrario. Y con la cuarta revolución industrial ocurre lo mismo, sobre la que ahora comienza su desarrollo. No obstante, sí conviene deslindar o distinguir diferentes nombres asociados, pero diferentes, en este campo, sobre todo cuando empieza a atribuirse al "todo" problemas que solo debieran atribuirse a la "parte". Demonizar los adelantos, en muchos casos hablando de los "algoritmos" o de la "inteligencia artificial", como si fueran los males de todo, sin distinguir las actividades que se realizan, y el grado de inmisión o limitación que producen en los derechos de los sujetos, no deja de ser una opción simple. Por ello creemos conveniente, acotar, de forma somera, algunas ideas sobre la cuestión, que permitan aclararnos.

Desde luego, inicialmente, un "algoritmo", desde el plano de las matemáticas, que es donde tradicionalmente se han estudiado, supone un grupo de órdenes consecutivas que presentan una solución a un problema o tarea. Su representación y estudio difiere de las dimensiones que han adquirido en el campo de la informática, donde, además se han asociado a otros términos, entre ellos la "Inteligencia Artificial". No obstante, partamos de una idea, que es la que fascina, pero también preocupa. La máquina no es inteligente, hace lo que las personas quieren que haga. Luego si hablamos de una máquina inteligente, o dotada de inteligencia artificial,

14. *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, p. 58 y 59. La obra de SCHWAB, citada por la Profesora, es *La Cuarta Revolución Industrial*, 4.ª Edic., Barcelona, Edit. Debate, 2018.

hablamos de una máquina que, de alguna manera, trata de emular el pensamiento y razonamiento humano. Dicha opción, que hasta ahora se pensaba lejana, en la cuarta revolución industrial, empieza a ser bastante plausible. El pensamiento o razonamiento humano ante la existencia de problemas, para solucionarlos y resolverlos, tomando decisiones, hace uso de las reglas heurísticas o del descubrimiento, tradicionalmente vinculadas, en el mundo de la Justicia, con la sentencia, es decir la decisión final del proceso. Pues bien, en el campo de la Inteligencia Artificial, la máquina trabaja con reglas heurísticas y matemáticas, tratando de emular el pensamiento humano "con representaciones del conocimiento entendidas como combinaciones de estructuras de datos y de procedimientos de interpretación incorporados a un programa computacional"[15].

Para llevar a cabo dicha actividad los técnicos se valen de los algoritmos, que han adquirido un peso específico en el campo de la informática, pese a que surgen en el Siglo XI, vinculados al mundo de las matemáticas. Ya hemos señalado que son, no obstante, en el campo de la informática "es una secuencia de instrucciones finitas que llevan a cabo una serie de procesos para dar respuesta a determinados problemas. Es decir, un algoritmo informático resuelve cualquier problema a través de unas instrucciones y reglas concisas, mostrando el resultado obtenido"[16]. Ahora bien, esa secuencia de instrucciones que da soluciones a un problema puede tener una incidencia que afecten a derechos de los ciudadanos, o simplemente ser una ayuda o adelanto en las actividades de las personas. Tengamos en cuenta que buena parte de los trabajos que realizamos hoy día, con las máquinas, con las computadoras, se encuentran regidos por los algoritmos. Piénsese, simplemente, en los "paquetes ofimáticos", que se encuentran regidos por algoritmos, o en las plataformas digitales o portales informáticos con los que trabajamos (y ello sin desconocer que ha transformado las formas de trabajo, y que indirectamente pueden suponer perjuicios). Esta forma de ver los algoritmos más que preocupar han supuesto mejoras y adelantos.

No obstante, los algoritmos informáticos han ido evolucionando, y los resultados que se obtienen con ellos, fruto de la "inteligencia artificial", sí que nos empiezan a preocupar. Si el algoritmo es una secuencia de instrucciones y reglas que dan un resultado, la configuración de dichas secuencias y reglas, que generan patrones o modelos, pueden incidir en la vida de las personas, por cuanto que en su génesis se pueden introducir sesgos que perjudiquen a ciertos colectivos de personas, debido, por ejemplo, a

15. *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, p. 103.
16. *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, p. 100.

la generación de perfiles idóneos de sujetos o perfiles inidóneos de sujetos. Luego la configuración de los algoritmos puede que no sea neutra, y ello no depende de la máquina, sino de las personas que los configuran, de ahí la preocupación[17]. Como se ha señalado, "la falsa neutralidad del algoritmo es una cuestión tremendamente inquietante y puede dar lugar a consecuencias jurídicas nefastas"[18].

La inteligencia artificial es una combinación de tecnologías que agrupa datos, algoritmos y capacidad informática[19]. Se basa en el método probabilístico, luego la máquina se ajusta a la realidad que dicho método le permite[20], que no tiene por qué ser la verdadera realidad.

Ahora bien, para anudar algoritmos e inteligencia artificial es conveniente hacer referencia a otros términos y procesos que se sitúan entre unos y otros, y que son los que permiten, de alguna manera, discernir, las verdaderas máquinas inteligentes, en los términos que los estamos exponiendo.

Dentro de esa combinación de tecnologías y procesos, en que consiste la Inteligencia Artificial, encontramos los procesos de *Big data*, *Data mining* y *Machine Learning*. El término *Big data* es novedoso, sin embargo, los orígenes de los grandes conjuntos de datos se remontan a las décadas de los años 60 y 70 del siglo pasado, con la creación de los centros de datos y el desarrollo de las bases de datos relacionales. Como señala Oracle, *Big data* "son datos que contienen una mayor variedad y que se presentan en volúmenes crecientes y a mayor velocidad" (lo que se conoce como "las tres V" –volumen, velocidad y variedad–). Ello significa que "el big data está formado por conjuntos de datos de mayor tamaño y más complejos, especialmente procedentes de nuevas fuentes de datos. Estos conjuntos de datos son tan voluminosos que el software de procesamiento de datos

17. Sobre el tema, *vid.* NAVAS NAVARRO, "Derecho e inteligencia artificial desde el diseño. Aproximaciones", en *Inteligencia Artificial. Tecnología, Derecho*, (Navas Navarro, Coord.), Edit. Tirant lo Blanch, Valencia, 2017, pp. 48 y 49.
18. *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, p. 101.
19. *Vid.* el Libro Blanco sobre la Inteligencia Artificial– un enfoque europeo orientado a la excelencia y la confianza, (COM (2020) 65 final), https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1. Sobre la propuesta de Reglamento sobre Inteligencia Artificial, así como sobre la utilización de la Inteligencia Artificial en el ámbito jurisdiccional, DE HOYOS SANCHO, "El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea", en *Revista General de Derecho Procesal*, n.° 55 (2021).
20. *Vid.* FRANCO, "Inteligencia artificial y Blockchain, el yin y el yan de la tecnología", en https://www.icjce.es/inteligencia-artificial-blockchain-yin-yang-tecnologia, consultado el 11 de febrero de 2022.

convencional sencillamente no puede gestionarlos. Sin embargo, estos volúmenes masivos de datos pueden utilizarse para abordar problemas empresariales que antes no hubiera sido posible solucionar"[21].

Las técnicas de *Data mining* (o "minería de datos") serían aquellas que se centran en "la extracción no trivial de información implícita, previamente desconocida y potencialmente útil a partir de datos. Otra manera de definirlo podría ser: la exploración y el análisis –por medios automáticos o semiautomáticos– de grandes cantidades de datos con el fin de descubrir patrones con significado"[22].

Teniendo en cuenta lo anterior, *Machine Learning* o "aprendizaje automático" "es una disciplina del campo de la Inteligencia Artificial que, a través de algoritmos, dota a los ordenadores de la capacidad de identificar patrones en datos masivos y elaborar predicciones (análisis predictivo). Este aprendizaje[23] permite a los computadores realizar tareas específicas de forma autónoma, es decir, sin necesidad de ser programados"[24]. Lógicamente, en dichos programas, hace uso de algoritmos, *big data* y *data mining*.

21. ORACLE, "¿Qué es el Big data?", en https://www.oracle.com/es/big-data/what-is-big-data/. Consultado el 11 de febrero de 2022. Y como también señalan, sobre el año 2005, la ciudadanía fue consciente de la cantidad de datos que generaban los usuarios a través de Facebook, YouTube y otros servicios online. Ese mismo año, se desarrollaría *Hadoop*, un marco de código abierto creado específicamente para almacenar y analizar grandes conjuntos de datos (y adquiere popularidad *NoSQL*). Con la llegada de Internet de las cosas (IoT), hay un mayor número de objetos y dispositivos conectados a Internet que generan datos sobre patrones de uso de los clientes y el rendimiento de los productos. Sobre la cuestión en el ámbito procesal, BUENO DE MATA, "Macrodatos, inteligencia artificial y proceso: luces y sombras", en *Revista General de Derecho Procesal*, N.° 51 (2020).
22. *Vid*. CLINIC CLOUD, "¿Qué es el data mining? La definición de la minería de datos", en https://clinic-cloud.com/blog/data-mining-que-es-definicion-mineria-de-datos/. Como ponen de relieve, las técnicas de *data mining* pueden ser de dos tipos: i) métodos descriptivos; y ii) métodos predictivos. Los primeros métodos buscan patrones interpretables para describir datos (*clustering*, descubrimiento de reglas de asociación y descubrimiento de patrones secuenciales). Los segundos utilizan variables para predecir valores futuros o desconocidos de otras variables (clasificación, regresión y detección de la desviación).
23. No obstante, como señala BARONA VILAR, "Aunque se hace referencia –y continuaremos haciéndolo– al término "aprendizaje", éste se usa más bien como una metáfora, una suerte de explicación cercana al aprendizaje humano, en cuanto los humanos aprendemos midiendo el progreso de una manera funcional, esto es, tratando de mejorar la función a través de la experiencia; ese aprendizaje maquínico es una suerte de mejora de la función, lo que se realiza a través del examen de mayor número de datos y la búsqueda de patrones adicionales". *Vid. Algoritmización del Derecho y de la Justicia…, op. cit.,* pp. 97 y 98.
24. *Vid*. IBERDROLA, "¿Qué es el Machine Learning?", en https://www.iberdrola.com/innovacion/machine-learning-aprendizaje-automatico. Consultado el 11 de febrero de 2022.

Los algoritmos de *Machine Learning* se pueden dividir en tres categorías[25]. La primera de ellas sería la de aquellos algoritmos de aprendizaje supervisado (*supervised learning*), en los que los técnicos, dotan a la máquina de datos etiquetados y categorizados, y sobre ellos la máquina toma decisiones o realiza predicciones. Un ejemplo, en la vida diaria, sería los programas detectores de *spam*, que utilizan las empresas e instituciones. La segunda categoría serían aquellos algoritmos de aprendizaje no supervisado (*unsupervised machine learning*), donde no se facilitan etiquetas o categorías a la máquina, sino que ésta se enfrenta al conjunto de datos con el objetivo de encontrar patrones que permitan organizarlos de alguna manera., buscando similitudes, diferencias, anomalías. Se utiliza, por ejemplo, en materia de marketing, extrayendo patrones de datos obtenidos de las redes sociales para realizar campañas de publicidad. La tercera categoría serían aquellos algoritmos de aprendizaje por refuerzo (*Reinforcement Learning*), donde el algoritmo aprende a partir de la propia experiencia, siguiendo para ello un sistema de *trial and error* (prueba y error) donde se recompensan las decisiones correctas. Las anteriores categorías se utilizan para realizar clasificaciones o predicciones. El reforzado, por ejemplo, se utiliza, para programas de reconocimiento facial, utilizados en la investigación penal y también se están utilizando para diagnósticos médicos.

Una vez puestos de manifiestos dichos conceptos, y en los que queda visible la presencia de las personas, es obvio que dichas nuevas tecnologías suponen grandes avances, pero también plantean nuevos problemas y peligros, dado que pueden servir a intereses particulares, económicos, de grandes empresas e incluso para el control y poder público de las personas. Ello pone de manifiesto que son necesarias reglas y principios éticos, pero también que son necesarias normas jurídicas, de ahí la preocupación y ocupación de la UE, en su doble vertiente: avance y mejora en su utilización, pero también seguridad y protección en su utilización, pues, como hemos puesto de manifiesto estas técnicas tienen un grado de invasión en la esfera de la privacidad de la persona relevante, pero también inciden en su patrimonio y otros derechos fundamentales[26].

No obstante, esta preocupación difiere dependiendo del tipo de estructuras inteligentes o de Inteligencia Artificial, ya sea "débil o estrecha" o "fuerte". La primera se caracteriza por tener asignada una tarea concreta, y no pueden ir más allá de lo programado. Acumulan datos, pero lo hacen de forma transitoria. Un ejemplo, sería "Siri", que es una inteligencia artificial con funciones de asistente personal. No obstante, que dicho asistente

25. Seguimos la clasificación realizada por IBERDROLA, *op.* y *loc. cit*. en nota anterior.
26. *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.,* p. 105.

personal, tenga unas funciones limitadas, no significa que no pueda ser, por ejemplo, un instrumento que limite derechos fundamentales, por cuanto, es obvio, que acumula información de las personas, y dicha información puede ser utilizada, bien de forma idónea, bien al contrario. La segunda versión, se dice que puede desarrollar una multifuncionalidad. En nuestro caso, por ejemplo, sería plantearse que hiciera funciones de Letrado de la Administración de Justicia, o incluso, de Juez. En esta modalidad se sustituye integralmente al ser humano, y la máquina actúa y responde como un ser humano. Esta segunda versión, que empieza a tener desarrollos, es la que genera mayores preocupaciones en todos los sectores de la vida[27].

IV. TECNOLOGÍAS, ALGORITMOS E IA EN LA ADMINISTRACIÓN DE JUSTICIA[28]

Desde que 1904, el Ministerio de Gracia y Justicia, accediera a que se pudieran presentar escritos hechos con una máquina de escribir, hasta el momento presente, la circunstancias han variado. En el ámbito de la Administración de Justicia se han producido cambios relevantes en el ámbito de las tecnologías, por razones internas y externas. No se puede olvidar en este ámbito que la Unión Europea ha promovido diferentes iniciativas, bien de carácter general, bien de carácter específico. De dichas cuestiones ya me ocupé en otro momento, y no voy a reproducir lo dicho[29]. Del mismo modo, se han producido numerosos avances en el ámbito nacional. Basta con observar las diferentes versiones del art. 230 LOPJ, para llegar a dicha conclusión. Desde luego, la versión del año 2018 (fruto de la LO 4/2018), deja claro la obligación de los juzgados y tribunales (y las fiscalías) de utilizar los medios técnicos electrónicos, informáticos y telemáticos puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones.

27. *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, pp. 105 a 109.
28. Sobre la cuestión, GUZMÁN FLUJA, "Sobre la aplicación de la inteligencia artificial a la solución de conflictos", en *Justicia civil y penal en la era global* (Barona Vilar, Coord.), Edit. Tirant lo Blanch, Valencia, 2017, pp. 67 a 122. También, sobre la metamorfosis de la Justicia en el sistema digital, BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, pp. 344 a 423.
29. *Vid*. COLMENERO GUERRA, "El Ministerio de Justicia ante la modernización tecnológica de la Administración de Justicia", en *Las Tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio* (Gamero Casado y Valero Torrijos, Coordinadores), Edit. Aranzadi, Cizur Menor (Navarra), 2012, pp. 737 a 769. Recientemente, sobre las políticas de la UE en materia de Inteligencia Artificial, BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, pp. 148 a 206.

Desde luego dicha obligación ha venido jalonada de pequeños hitos y reformas desde que en 1994 se decidiera apostar la tecnificación de la Administración de Justicia. Por el camino, junto dicha tecnificación, se ha modificado el funcionamiento de la Oficina Judicial (que desde su reforma todavía no se ha culminado, y eso puede lastrar los adelantos tecnológicos). Pero, también, al hilo de lo realizado en el resto de Administraciones Públicas, se ha aprobado una norma expresa sobre la Administración de Justicia electrónica[30, 31], que vino, previamente, acompañada por un sistema seguro de telecomunicaciones, denominado LexNET (como consecuencia del RD 84/2007, de 26 de enero, *BOE* del 13 de febrero), que se implantó en el territorio gestionado por el Ministerio de Justicia, y que posteriormente ha sido utilizado por la mayoría de las Comunidades Autónomas, salvo algunas que han utilizado un sistema propio (por ejemplo, el sistema AVANTIUS, que actualmente se utiliza en la Comunidades Autónomas de Navarra, Cantabria y Aragón). En el año 2015 se hace una nueva adaptación de LexNET (por RD 1065/2015, de 27 de noviembre –*BOE* del 1 de diciembre–), pero frente al anterior sistema, que no estaba previsto para todos los Profesionales del sector justicia, este se aprueba para ser utilizado por todos ellos, junto con las normas de la Ley 18/2011, de 5 de julio (*BOE* del 6), reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (LUTICAJ), que estableció un verdadero marco tecnológico para el servicio público de Justicia, más allá de la utilización de herramientas tecnológicas concretas como el ordenador o los sistemas de gestión procesal. Si dicha norma supuso el verdadero arranque del sistema judicial electrónico, será, sin embargo, la Ley 42/2015, de 5 de octubre, de reforma de LEC, que introdujo las subastas judiciales electrónicas y la obligatoriedad general de comunicación con la Administración de Justicia por medios electrónicos para los profesionales y otros colectivos (incluidas las personas jurídicas), dejando a salvo el carácter facultativo para las personas físicas (que optar voluntariamente por dicho canal), la que ha acelerado el sistema electrónico judicial.

No obstante, la LUTICAJ ha sido la norma que ha fijado las "reglas del juego" en materia de administración judicial electrónica, pues, las

30. Tanto en las CCAA, con las competencias transferidas, como el territorio gestionado por el Ministerio de Justicia, nos vamos a encontrar con diferentes sistemas informáticos: Minerva (M. de Justicia y Galicia); Fortuny (Fiscalías); Adriano (Andalucía); Atlante II (Canarias); Avantius (Navarra); Cicerone (Valencia); Justizia.eus (P. Vasco); Libra. Nuevo desarrollo (Madrid); Themis II, e.justicia.cat (Cataluña); y Vereda (Cantabria).

31. Sobre estas y otras reformas en materia de Justicia y TICs, DELGADO MARTÍN y OLIVER CUELLO, "Iniciativas recientes de la e-justicia en España", en *E-justicia* [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*, N.° 4 (2007), UOC, pp. 22 a 30.

anteriores regulaciones no habían supuesto más que una amalgama de reglas y aparatos en los juzgados, que no siempre eran de obligado uso y cumplimiento. Con ella, es cierto, que se podría decir que la Administración de Justicia española ha empezado su tránsito real a una "oficina papel cero" (aunque todavía quedan pasos para llegar al final de dicho camino).

La LUTICAJ da forma al "expediente judicial electrónico", generaliza la firma electrónica a efectos de comunicación, así como la práctica de actos de comunicación por medios electrónicos. Crea el Punto de Acceso General de la Administración de Justicia, las Sedes Judiciales Electrónicas. Además, en materia de coordinación, tanto para la gestión y funcionamiento, crea órganos para ello (como es el Comité Técnico Estatal de la Administración Judicial Electrónica –CTEAJE–), así como marca las pautas sobre la interoperabilidad así como en materia de seguridad.

En esta Legislatura están previstas varias reformas en el ámbito de la Administración de Justicia de cierto calado. Dejando al margen el Anteproyecto de Ley de Enjuiciamiento Criminal (y que realiza modificaciones que guardan relación con lo tratado en este trabajo), sí guardan relación, directa e indirecta, con lo que estamos analizando otros tres Anteproyectos: i) Anteproyecto de Ley de Medidas de Eficiencia Procesal del Servicio Público de Justicia; ii) Anteproyecto de Ley Orgánica de Eficiencia Organizativa del Servicio Público de Justicia, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, para la implantación de los Tribunales de Instancia y las Oficinas de Justicia en los municipios; y iii) Anteproyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia, por la que se transpone al ordenamiento jurídico español la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades.

De estos tres Anteproyectos, guarda relación directa con lo que estamos comentando el tercero, relativo a la Eficiencia Digital del Servicio Público de Justicia. Tras la situación de pandemia vivida, y la entrada en vigor de la Ley 3/2020, de 18 de septiembre (*BOE* del 19), de medidas procesales y organizativas para hacer frente a la covid-19 (que trae causa del Real Decreto-Ley 16/2020, de 28 de abril), determinadas medidas tecnológicas, como la celebración de vistas y actos procesales mediante presencia telemática, forman parte del imaginario común en el ámbito de la Administración de Justicia. Estas situaciones han supuesto plantear una modificación relevante (que en algunos aspectos ya se ha llevado a cabo)

o sustitución de la LUTICAJ, por otro texto normativo que suponga una nueva evolución de la Administración de Justicia Electrónica. Ese es el planteamiento del APL relativo a la Eficiencia Digital del Servicio Público de Justicia, derogar la LUTICAJ para sustituirla por un modelo de Administración Judicial Electrónica mejorado[32].

Dejamos para otro momento si lo correcto es el camino adoptado, desde el plano de la política legislativa, por cuanto que en el ámbito del resto de Administraciones Públicas el camino seguido ha sido otro (y para ello basta con observar las Leyes 39 y 40/2015), de fusión de los cambios tecnológicos dentro del sistema normativo del procedimiento a seguir. No obstante, el Anteproyecto, como elementos generales de la Reforma señala que:

> "Desde la responsabilidad y la necesidad de asumir con éxito los retos de la transformación digital en el marco de la Justicia española, el presente texto legislativo busca presentarse como una herramienta normativa completa, útil, transversal y con la capacidad suficiente para dotar a la Administración de Justicia de un marco legal, coherente y lógico en el que la relación digital se descubra como una relación ordinaria y habitual, siendo la tutela judicial efectiva en cualquier caso la prioridad absoluta, pero hallando bajo esta cobertura de normas y reglas un nuevo cauce, más veloz y eficaz, que coadyuvará a una mejor satisfacción de los derechos de la ciudadanía.
>
> La presente ley persigue la adaptación de la realidad judicial española del siglo XXI al marco tecnológico contemporáneo, favoreciéndose una relación digital entre la ciudadanía y los órganos jurisdiccionales y aprovechando las ventajas del "hecho tecnológico" también para fortalecer nuestro Estado social y democrático de Derecho mediante la disposición de medidas orientadas a la

32. En la Exposición de Motivos de dicho Anteproyecto se indica:
"Hoy el 'hecho tecnológico' determina nuestras vidas, la forma de relacionarnos, de adquirir productos o de prestar servicios. La 'tecnologización' de la vida común ha tenido inevitablemente un desarrollo más rápido que el de las Administraciones Públicas. No ha sido sino a la vista de los enormes beneficios del uso de la tecnología para el servicio público y para los ciudadanos y ciudadanas, cuando en la Administración pública se ha apostado firme y decididamente por la misma. Concretamente, la pandemia COVID-19 situó a las Administraciones públicas frente a una dimensión desconocida, haciendo imprescindibles medios tales como la comunicación telemática, el teletrabajo o la gestión deslocalizada, herramientas de exigencia coyuntural por una situación excepcionalísima, pero que el tiempo y la experiencia han evidenciado como necesitadas del oportuno tratamiento normativo, organizativo y funcional".

transparencia, la eficiencia y la rendición de cuentas de los poderes públicos".

Uno de los elementos relevantes de la Reforma, que ya se encuentra presente en la LUTICAJ, es la colaboración y cogobernanza en materia de Administración Electrónica, de ahí que las Administraciones competentes se obligan a garantizar la prestación del servicio por medios digitales, homogéneos, de calidad y que aseguren en todo el territorio del Estado una serie de servicios mínimos: i) la itineración de expedientes electrónicos y la transmisión de documentos electrónicos entre cualesquiera órganos judiciales o fiscales; ii) la interoperabilidad de datos entre cualesquiera órganos judiciales o fiscales; iii) un servicio común, interoperable, personalizado, de acceso a los servicios, procedimientos e informaciones accesibles de la Administración de Justicia que afecten a la ciudadanía; y iv) la identificación y firma de los intervinientes en actuaciones y servicios no presenciales. Desde luego, ello supone que la intervención de los ciudadanos se simplifique.

La reforma plantea diferentes hilos conductores, que suponen un gran avance del sistema. Señalaríamos como el primero de ellos, la ampliación del conjunto de sujetos que deben interaccionar con la Administración de Justicia de forma electrónica, de forma obligatoria, así como la mejora de los sistemas para que aquellos que pueden elegir entre el sistema tradicional o el electrónico se decanten por este último. Entre esas mejoras, se incluyen la puesta al día (por razones comunitarias) en materia de identificación por medios electrónicos. Junto a ellas también destaca la mejora de la tramitación tecnológica del Expediente Judicial Electrónico, que pasa de una orientación al documento, a una orientación al dato, y junto a ello se regula, de forma expresa, las actuaciones automatizadas, proactivas y asistidas.

El Título I del Anteproyecto ("Derechos y deberes digitales en el ámbito de la Administración de Justicia"), actualiza los derechos y deberes reconocidos en la LUTICAJ[33]. Por ello, se reconoce a la ciudadanía, entre otros, el derecho a un servicio personalizado de acceso a procedimientos, informaciones y servicios accesibles de la Administración de Justicia. En el caso de los profesionales que representan y defienden a los ciudadanos, entre sus derechos y obligaciones, se establece que las Administraciones competentes deberán posibilitar la desconexión digital, la conciliación de la vida laboral, personal y familiar y el descanso en los

33. Dicha regulación, señala la Exposición de Motivos, ha tenido como guía el conjunto de principios y derechos recogidos en la recientemente adoptada *Carta de Derechos Digitales*, que tiene como objetivo principal la protección de los derechos de la ciudadanía en la nueva era de Internet y la Inteligencia Artificial.

períodos inhábiles procesalmente y en aquellos en que las personas profesionales estén haciendo uso de las posibilidades dispuestas a tal fin en las normas procesales.

El Título II del Anteproyecto regula el acceso digital a la Administración de Justicia. Manteniendo lo ya regulado en la LUTICAJ, se producen mejoras, que se podrían englobar en tres grandes previsiones. Se mejora la regulación de la Sede judicial electrónica y del Punto de Acceso General de la Administración de Justicia (PAGAJ). Dentro del PAGAJ se crea un servicio nuevo y personalizado para la ciudadanía, la Carpeta en el ámbito de la Administración de Justicia, o "Carpeta Justicia", que además será interoperable con la Carpeta Ciudadana del Sector Público Estatal. Sin entrar ahora en la reflexión sobre la "bondad" de crear una "macro carpeta de Ciudadano", dicha Carpeta, previa identificación, facilitará el acceso a los servicios y procedimientos para las personas que sean partes o interesadas, entre ellos al servicio de cita previa. Entre los servicios que contendrá estará poner a su disposición los actos de comunicación, para que, si tiene obligación de hacerlo, o voluntariamente lo desea, pueda atenderlos[34].

Se actualizan los sistemas de identificación y autenticación conforme a lo previsto en el Reglamento (UE) N.° 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y servicio de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, así como asumiendo los sistema de firma previsto en el art. 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. De ellos destacan que, en determinados supuestos (por ejemplo, en procedimientos judiciales no presenciales), será posible la utilización de un sistema de identificación y firma no criptográfica.

El Título III del Anteproyecto se refiere a la tramitación electrónica de los procedimientos judiciales, orientada al dato. El Expediente Judicial Electrónico y la tramitación orientada al dato, suponen, como se señala en la Exposición de Motivos, "una apuesta clara y decisiva por su empleo racional para lograr evidencia y certidumbre al servicio de la planificación

34. Los sistemas de accesos pueden no estar disponibles para todos, por diferentes razones, por ello, la Exposición Motivos señala que "La transformación digital de la Justicia favorece y posibilita una Justicia más próxima y accesible, pero ello no es neutro desde el punto de vista social y económico, pudiendo identificarse, entre otros, un impacto de género, educativo, geográfico, económico, de edad, o por razón de discapacidad. Será necesario, pues, que, desde el mismo momento del diseño de los sistemas informáticos de Justicia, se aborde específicamente cuáles son, sobre quiénes se produce y por qué surge cada tipo de brecha, y, a través de este análisis, se dispongan los mecanismos necesarios para su eliminación o reducción".

y elaboración de estrategias que coadyuven a una mejor y más eficaz política pública de Justicia". Ello permitirá tomar decisiones estratégicas en la regulación y tramitación de los procedimientos, que redundará en beneficio para la Administración y para los Ciudadanos, pues también se incorpora el concepto de "dato abierto". En esta materia destacan los siguientes aspectos:

i) Tanto la iniciación como la tramitación deberán ser electrónicas para aquellas personas que estén obligadas a comunicarse con la Administración de Justicia por medios electrónicos[35];

ii) Principio general de orientación al dato, por lo que los Sistemas asegurarán la entrada y tratamiento de información en forma de metadatos, conforme a esquemas y datos comunes e interoperables[36];

iii) Se prevé que las Administraciones establezcan sistemas y modelos de presentación masiva, para que puedan ser utilizados por personas jurídicas y otros colectivos, o incluso por profesionales;

iv) Regulación del Expediente judicial electrónico como un "conjunto de datos" estructurados que proporcionan información. Dicho conjunto incluye: documentos, trámites, actuaciones electrónicas o grabaciones audiovisuales correspondientes a un procedimiento judicial. Se identificarán por un número único para cada procedimiento, y tendrán un índice electrónico[37];

v) Un nuevo concepto más amplio de documento judicial electrónico, que deberá contener metadatos que aseguren la interoperabilidad, y llevar asociado un sello o firma electrónica, en el que quede constancia del

35. Los sistemas de información y comunicación empleados conservarán un registro de las actividades de tratamiento (conforme a lo dispuesto en la normativa sobre protección de datos). Además, las personas responsables y encargadas del tratamiento deberán mantener registros de operaciones aplicables a todos los que interactúen con el sistema. La remisión de expedientes administrativos por las distintas Administraciones y organismos públicos se realizará a través de las herramientas de remisión telemática.

36. Como señala Exposición de Motivos, "La gestión sobre los mismos posibilitará o facilitará la interoperabilidad de los sistemas, la tramitación electrónica, la búsqueda y análisis de los datos, la anonimización y seudonimización, la elaboración de cuadros de mando, la gestión de documentos y su transformación, la publicación de información en portales de datos abiertos, la producción de actuaciones automatizadas, asistidas y proactivas, la utilización de sistemas de inteligencia artificial para la elaboración de políticas públicas, y la transmisión de los datos conforme a lo que se determine".

37. Para la transmisión de documentos y la itineración de expedientes se creará un Sistema de Intercambio de Documentos y Expedientes, interoperable con los sistemas de información de las administraciones públicas.

órgano emisor, fecha y hora. También se regula la forma de presentación de documentos en actuaciones orales telemáticas;

vi) Se mejora los actos de comunicación por vía electrónica. Se modifican los actos de comunicación que suponen el primer emplazamiento (junto con la modificación operada por el Anteproyecto de Ley de Eficiencia Procesal del Servicio Público de Justicia). A ello debe sumársele la creación, del Punto Común de Actos de Comunicación, para que los profesionales puedan acceder a todos los actos de comunicación de que sean destinatarios, sea cual fuere el órgano que los hubiese emitido;

vii) Se regulan las actuaciones automatizadas para su uso en tareas repetitivas y automatizables. Se trata de actuaciones procesales producidas por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular[38]. Se va a tratar de actuaciones de trámite simples, que no requieren interpretación jurídica. Entre ellas se incluirán (entre otras): i) el numerado o paginado de los expedientes; ii) la remisión de asuntos al archivo cuando se den las condiciones procesales para ello; iii) la generación de copias y certificados; iv) la generación de libros; v) la comprobación de representaciones; y vi) la declaración de firmeza, de acuerdo con la ley procesal.

Como subtipo de las actuaciones automatizadas, se encuentran las actuaciones proactivas, que son actuaciones automatizadas, autoiniciadas por los sistemas de información sin intervención humana, que aprovechan la información incorporada en un expediente o procedimiento de una Administración pública con un fin determinado, para generar avisos o efectos directos a otros fines distintos, en el mismo o en otros expedientes, de la misma o de otra Administración pública, en todo caso conformes con la ley[39].

La actuación asistida es aquella para la que el sistema de información de la Administración de Justicia genera un borrador total o parcial de documento complejo en base a datos, que puede ser producido por algoritmos, y puede constituir fundamento o apoyo de una resolución judicial

38. Sobre la cuestión, GUZMÁN FLUJA, "Automated justice: la preocupante tendencia hacia la justicia automatizada", en *Derecho Procesal: retos y transformaciones* (González Pulido, Reiforth Muñoz y Bujosa Vadell, Dirs.), Edit. Atelier, 2021, pp. 339 a 380.

39. El CTEAJE favorecerá la colaboración con otras Administraciones públicas en la identificación de procesos que, en su caso, puedan ser proactivos, así como en la definición de los parámetros y requisitos de compatibilidad necesarios para ello. No obstante, los Sistemas deben asegurar: i) que todas las actuaciones automatizadas y proactivas se puedan identificar como tales, trazar y justificar; ii) que sea posible efectuar las mismas actuaciones en forma no automatizada; y iii) que sea posible deshabilitar, revertir o dejar sin efecto las actuaciones automatizadas ya producidas.

o procesal[40]. Luego servirá de apoyo a letrados de la administración de justicia, jueces y fiscales, pues el borrador documental que se genere no constituye, por sí solo, la resolución judicial o procesal, ya que deberá ser validado por el sujeto obligado a la resolución. Por ello, los Sistemas asegurarán que el borrador documental solo se genere a voluntad del usuario y pueda ser libre y enteramente modificado por éste, así como la identificación, autenticación o firma electrónica que en cada caso prevea la ley, además de los requisitos que las leyes procesales establezcan[41].

El Título IV del Anteproyecto regula los actos y servicios no presenciales, materia en la que la situación de pandemia ha servido de fase de ensayo. Lo que sí se hace es ampliar el espectro, pues también se prevé la realización, de manera no presencial, de actos gubernativos y servicios no estrictamente jurisdiccionales. La atención al público se realizará preferentemente por vía telemática, pero la de los profesionales solo será por vía telemática si estos así lo interesan. Por ello, se gestionará un sistema por el personal al servicio de la Administración de Justicia.

Respecto a las actuaciones en los órganos jurisdiccionales, se consolida la vía telemática para la generalidad de los actos procesales, produciendo plenos efectos procesales y jurídicos. Las Administraciones velarán por la interoperabilidad y compatibilidad de los sistemas de videoconferencia. Se procede a la modificación de las normas procesales, estableciendo una regla de preferencia hacia la realización de actos procesales mediante presencia telemática. No obstante, se fijan excepciones para las actuaciones de naturaleza personal (interrogatorios de parte o de testigos, exploración de la persona menor de edad o la entrevista a la persona con discapacidad), además de las propias del proceso penal. No obstante, el órgano jurisdiccional podrá determinar la participación física de cualquier interviniente, en el caso de que estime, en atención a causas precisas y en el caso concreto, debidamente motivadas, que el acto requiere la presencia física de alguno o varios intervinientes. También se procede a la regulación,

40. A favor de la tecnología y los algoritmos en el proceso (penal), aunque trasladable al resto de órdenes jurisdiccionales, recientemente, NIEVA FENOLL, "El tránsito de la fe a la tecnología en el proceso penal", en *Diario La Ley*, n.° 9986 (2022). Con extensión, del mismo Autor, Inteligencia artificial y proceso judicial, Edit. Marcial Pons, Madrid, 2018.

41. En las actuaciones automatizadas, asistidas o proactivas podrá realizarse por el CTEAJE 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. Los criterios de decisión automatizada serán públicos y objetivos, dejando constancia de las decisiones tomadas en cada momento. Los sistemas incluirán los indicadores de gestión que se establezcan por la Comisión Nacional de Estadística Judicial y el CTEAJE, cada uno en el ámbito de sus competencias.

estableciendo sus requisitos técnicos y garantías, de los "puntos de acceso seguros" y de "lugares seguros", desde los que se podrá intervenir por medios telemáticos (entre los que se incluye las oficinas judiciales).

El Anteproyecto ordena el marco jurídico necesario para que las personas que trabajan en la Administración de Justicia puedan desempeñar sus funciones mediante trabajo deslocalizado cuando se precise, con todas las garantías de seguridad, avanzándose en la gestión profesional eficiente.

El Título V del Anteproyecto se dedica a los Registros de la Administración de Justicia y los archivos electrónicos. Se crea el Registro de Datos para el contacto electrónico con la Administración de Justicia, como servicio electrónico homogéneo, en el que la ciudadanía (voluntariamente) y los profesionales (obligatoriamente) proporcionen datos de carácter personal para el contacto electrónico[42].

Los registros electrónicos de entrada o salida de asuntos y documentos judiciales se regulan en términos parecidos a la LUTICAJ, pero se prevé un Registro Electrónico Común de la Administración de Justicia, que posibilitará la presentación de escritos y comunicaciones dirigidas a la Administración de Justicia y a cualesquiera oficinas judiciales y fiscales, de conformidad con la normativa técnica aprobada en el CTEAJE. También se mejora el Registro Electrónico de Apoderamientos Judiciales (REAJ), ya previsto en la LUTICAJ, que se orienta al dato y facilita la interoperabilidad con otros registros externos y con los sistemas de gestión procesal y sedes electrónicas, para que, en los casos que proceda, se pueda dar acceso automático a actuaciones y servicios digitales en base a los apoderamientos que estén en el Registro[43]. Por otro lado, se prevé un Registro de personal al servicio de la Administración de Justicia habilitado para realizar por medios electrónicos determinados trámites, actuaciones o servicios. Finalmente, se prevé la creación de un Sistema de archivo común de la Administración de Justicia, para conservar y acceder a expedientes y documentos electrónicos, plenamente interoperable con los sistemas de gestión.

El Título VI del Anteproyecto ("Transparencia y datos abiertos"), regula el Portal de Datos de la Administración de Justicia, que debe facilitar a la ciudadanía y a los profesionales información procesada y precisa sobre

42. Este registro permitirá la constancia de circunstancias de los profesionales cuyo conocimiento resulte imprescindible, como por ejemplo circunstancias determinantes de la incapacidad, incompatibilidad o prohibición para el ejercicio de la profesión respectiva.

43. Como novedad, se prevé la posibilidad de auto inscripción del apoderamiento para representantes procesales, limitado a ciertos procedimientos que determinará el CTEAJE.

la actividad, carga de trabajo y otros datos relevantes de todos los órganos, servicios y oficinas judiciales y fiscales de España. También regula lo necesario sobre las condiciones y licencias de reutilización de datos, datos automáticamente procesables e interoperabilidad de los datos abiertos.

El Título VII del Anteproyecto, como hace la LUTICAJ, regula la cooperación entre las Administraciones con competencias en materia de Justicia, el Esquema Judicial de Interoperabilidad y Seguridad y las demás normas sobre seguridad[44].

V. ALGORITMOS E IA EN LA GENERACIÓN DE CONFLICTOS LABORALES[45]

Pero la utilización de nuevas máquinas, algoritmos e IA no solo ha acontecido en el ámbito de la Administración de Justicia, como acabamos de reflejar. En el apartado anterior se han puesto de relieve los efectos de la cuarta revolución industrial en el mundo judicial, lo cual, afecta al orden jurisdiccional social. Pero el Juez de lo Social no solo debe ocuparse de dichas cuestiones, pues los efectos de la revolución van a formar parte de los conflictos de los que debe ocuparse. Por ello, los conflictos laborales también van a incluir (de hecho, ya los han incluido, como veremos) cuestiones atinentes a los algoritmos y la IA[46], que tanto preocupa en el mundo de las relaciones laborales, por cuanto que la nueva tecnología ya forma parte de las empresas. Dichas tecnologías han generado oportunidades de nuevas formas de negocio que giran en torno a la obtención y gestión de datos y a la oferta de servicios adaptados a esta nueva etapa. Los algoritmos se han aplicado a las relaciones de trabajo revolucionando la forma en que se prestan los servicios, optimizando recursos y resultados.

44. En dicho Título se potencia el CTEAJE como órgano de cogobernanza de la Administración digital de la Justicia y de impulso y coordinación del desarrollo de la transformación digital de la Administración de Justicia, alineado en el ejercicio de sus funciones con la Conferencia Sectorial de Justicia. También se prevé la constitución, en su seno, de un Consejo Consultivo para la Transformación Digital de la Administración de Justicia, con el fin favorecer que la iniciativa, diseño, desarrollo y producción de sistemas se lleven a cabo en coordinación con el sector privado y los colectivos principalmente afectados. Se regula el Esquema Judicial de Interoperabilidad y Seguridad y se dictan normas para la elaboración y actualización de la política de seguridad de la información en la Administración de Justicia, previéndose un Subcomité de Seguridad (dentro del CTEAJE) y de un Centro de Operaciones de Ciberseguridad de la Administración de Justicia.

45. Sobre aplicaciones de IA en el mundo laboral y empresarial, BARONA VILAR, *Algoritmización del Derecho y de la Justicia…*, *op. cit.*, pp. 223 a 225.

46. Sobre el tema, MERCADER UGUINA, "Algoritmos y Derecho del Trabajo", en *Actualidad Jurídica Uría Menéndez*, n.° 52 (2019), pp. 63 a 70.

Estos métodos contribuyen a mejorar las condiciones de vida de las personas. También han permitido, y hemos tenido de comprobarlo durante el período de pandemia, el mantenimiento de negocios a través de servicios en línea o garantizando la continuidad de las prestaciones de trabajo a distancia. Desde luego, los nuevos elementos en las relaciones laborales han supuestos ventajas, que son compatibles con las finalidades del derecho del trabajo. Fruto de los acuerdos de los interlocutores sociales, y para tratar de garantizar un adecuado uso de los algoritmos y la Inteligencia Artificial en el mundo de la empresa, en aquello que afecta, o pueda afectar a los trabajadores, se ha llevado a cabo una reforma del Estatuto de los Trabajadores por la Ley 12/2021, de 28 de septiembre (*BOE* del 29), para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales[47]. La finalidad de la Ley es la precisión del derecho de información de la representación de personas trabajadoras en el entorno laboral digitalizado, así como la regulación de la relación de trabajo por cuenta ajena en el ámbito de las plataformas digitales de reparto.

Así, se ha modificado el artículo 64 del Estatuto de los Trabajadores, relativo a los derechos de información y consulta de la representación legal de las personas trabajadoras, para añadir un nuevo párrafo d) a su apartado 4. En dicha letra se reconoce el derecho del comité de empresa a ser informado por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles.

También se introduce una nueva disposición adicional, al Estatuto de los Trabajadores, sobre la presunción de laboralidad de las actividades de reparto o distribución de cualquier tipo de producto o mercancía, cuando la empresa ejerce sus facultades de organización, dirección y control, mediante la gestión algorítmica del servicio o de las condiciones de trabajo, a través de una plataforma digital. Dicha presunción no afecta a lo previsto en el artículo 1.3 del Estatuto de los Trabajadores[48].

47. Sobre el tema, *Vid*. GARRIDO PÉREZ, "El nuevo y complejo derecho de información sobre algoritmos y sistemas de inteligencia artificial que inciden en el empleo y las condiciones laborales", en *NET21*, N.° 4, junio de 2021, también, PÉREZ AMORÓS, "¿Quién vigila al algoritmo?: los derechos de información de los representantes de los repartidores en la empresa sobre los algoritmos de las plataformas de reparto", en *e-Revista Internacional de la Protección Social*, Vol. VI, n.° 1 (2021), pp. 173 a 187.

48. "Disposición adicional vigesimotercera. *Presunción de laboralidad en el ámbito de las plataformas digitales de reparto*.–Por aplicación de lo establecido en el artículo 8.1, se presume incluida en el ámbito de esta ley la actividad de las personas que presten

En esta última norma se incorporan los criterios y parámetros establecidos, en unificación de doctrina, por el Tribunal Supremo (STS 805/2020, de 25 de septiembre), haciendo uso del principio de realidad, puesto de manifiesto en otras sentencias anteriores, como la STS 263/1986, de 26 de febrero de 1986, o STS de 20 de enero de 2015 (recurso 587/2014), y en la que se destaca, asimismo, la necesidad de adaptar los requisitos de dependencia y ajenidad al contexto actual. En dicha sentencia se fundamenta lo siguiente:

> "Desde la creación del derecho del trabajo hasta el momento actual hemos asistido a una evolución del requisito de dependencia-subordinación. La sentencia del TS de 11 de mayo de 1979 ya matizó dicha exigencia, explicando que "la dependencia no implica una subordinación absoluta, sino solo la inserción en el círculo rector, organizativo y disciplinario de la empresa". En la sociedad postindustrial la nota de dependencia se ha flexibilizado. Las innovaciones tecnológicas han propiciado la instauración de sistemas de control digitalizados de la prestación de servicios. La existencia de una nueva realidad productiva obliga a adaptar las notas de dependencia y ajenidad a la realidad social del tiempo en que deben aplicarse las normas (artículo 3.1 del Código Civil) (FJ 7.°)".

El órgano jurisdiccional lleva a cabo un análisis de la relación entre la Plataforma de reparto y el trabajador, reiterando criterios anteriores (por todas, SSTS de 22 de abril de 1996, recurso 2613/1995; y de 3 de mayo de 2005, recurso 2606/2004). La Sala Cuarta entiende que las facultades empresariales de dirección, organización o control de la actividad y, en tal sentido, las notas de dependencia y ajenidad, pueden traducirse a la realidad de formas diferentes a las clásicas cuando la empleadora asume los riesgos de la operación y es beneficiaria de sus frutos, realizando una labor de coordinación, organización o control de la prestación u ostentando la potestad sancionadora, y ello aunque sus prerrogativas se manifiesten de forma indirecta o implícita, a través de la gestión algorítmica, de las condiciones de trabajo o del servicio prestado.

La reforma asume que las facultades empresariales, previstas en el artículo 20 del Estatuto de los Trabajadores, pueden ser ejercidas por medio de la gestión algorítmica del servicio o de las condiciones de trabajo a

---

servicios retribuidos consistentes en el reparto o distribución de cualquier producto de consumo o mercancía, por parte de empleadoras que ejercen las facultades empresariales de organización, dirección y control de forma directa, indirecta o implícita, mediante la gestión algorítmica del servicio o de las condiciones de trabajo, a través de una plataforma digital.

Esta presunción no afecta a lo previsto en el artículo 1.3 de la presente norma".

través de una plataforma digital. En consecuencia, la forma indirecta o implícita de ejercicio de las facultades empresariales, no excluye la relación laboral, pues la aparente flexibilidad del trabajo a realizar, en realidad lleva aparejada consecuencias o repercusiones en el mantenimiento de su empleo, en su volumen o en el resto de sus condiciones de trabajo.

Ello no quita que, como se pone de manifiesto en el Preámbulo de la norma:

> "Los algoritmos merecen nuestra atención y análisis, por los cambios que están introduciendo en la gestión de los servicios y actividades empresariales, en todos los aspectos de las condiciones de trabajo y, sobre todo, porque dichas alteraciones se están dando de manera ajena al esquema tradicional de participación de las personas trabajadoras en la empresa. En este sentido, otra de las reflexiones compartidas por la mesa de diálogo social consiste en señalar que no podemos ignorar la incidencia de las nuevas tecnologías en el ámbito laboral y la necesidad de que la legislación laboral tenga en cuenta esta repercusión tanto en los derechos colectivos e individuales de las personas trabajadoras como en la competencia entre las empresas.
>
> La eficacia de la nueva disposición adicional vigesimotercera, basada, como se ha expuesto, en la valoración de la naturaleza real del vínculo, va a depender en gran medida de la información verificable que se tenga acerca del desarrollo de la actividad a través de plataformas, que debe permitir discernir si las condiciones de prestación de servicios manifestadas en una relación concreta encajan en la situación descrita por dicha disposición, siempre desde el mayor respeto a los secretos industrial y comercial de las empresas conforme a la normativa, que no se ven cuestionados por esta información sobre las derivadas laborales de los algoritmos u otras operaciones matemáticas al servicio de la organización empresarial".

Desde luego dicha reforma supone un adelanto en el control de los algoritmos, y de esa manera de la Inteligencia Artificial. No obstante, la utilización de la Inteligencia Artificial en el campo de la empresa supondrá la entrada de dichas cuestiones el ámbito de los procesos laborales, anejados a la "causa de pedir", y por ello sometido a las reglas probatorias, donde habrá que discernir si, la utilización de dichos mecanismos tecnológicos, no han vulnerado derechos y libertades fundamentales del trabajador, pues en dicho caso podrán ser expurgadas del proceso al ser "fuentes" o "medios de pruebas" ilícitos o prohibidos.

A este respecto debe tenerse en cuenta que el *Acuerdo Marco de los interlocutores sociales europeos sobre digitalización* (de junio de 2020) establece, en cuanto al despliegue de la Inteligencia Artificial que debe: i) seguir el principio de control humano; ii) ser seguro, es decir, debe prevenir el daño; iii) realizarse una evaluación de los riesgos, incluidas las oportunidades de mejorar la seguridad y prevenir los daños, por ejemplo, para la integridad física de las personas, la seguridad psicológica, el sesgo de confirmación o la fatiga cognitiva; iv) seguir los principios de equidad, es decir, asegurar que los trabajadores y grupos estén exentos de prejuicios y discriminación injustos; y v) ser transparente y explicable con una supervisión efectiva; el grado necesario de explicabilidad depende del contexto, la gravedad y las consecuencias; habrá que hacer comprobaciones para evitar un resultado erróneo de IA. La utilización de IA en los procedimientos de recursos humanos (contratación, evaluación, ascenso o despido) y en el análisis de la actuación profesional, es necesario salvaguardar la transparencia mediante el suministro de información. A ello hay que sumar que el trabajador afectado debe poder solicitar intervención humana y/o impugnar la decisión junto con la prueba de los resultados de la IA. Finalmente, se señala que los sistemas de IA deben ser diseñados y operados para cumplir con la ley vigente, incluido el RGPD, y garantizar la privacidad y la dignidad del trabajador[49].

No obstante, en esta materia, y dado el entramado de derechos fundamentales que se ven inmerso en el ámbito del art. 20 del Estatuto de los Trabajadores, al hilo de las facultades empresariales, podría ser conveniente trasladar al ámbito laboral, con sus adaptaciones (ya que las posibles limitaciones de derechos fundamentales, y el contexto, en el ámbito penal y laboral difieren), el reconocido como "derecho al entorno virtual", salvo que en este caso, no se trata del seguimiento que puede realizar los poderes públicos, sino una empresa. Dicho concepto engloba "Toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos" (STS 342/2013, de 17 de abril[50]). Ciertamente, dicha jurisprudencia no nace del vacío, pues

49. En esta línea, *vid. Las decisiones algorítmicas en las relaciones laborales*. Servicio de Estudios de la Confederación. Análisis y Contextos, UGT, 8 de febrero de 2021.

50. El razonamiento principal de la Sentencia, contenido en el apartado A del Fund. Jco. 8 es el siguiente:

"El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo son algo más que una pieza de convicción que, una vez aprehendida, queda

expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar –de hecho, normalmente albergará– información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones.

En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal.

La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital.

Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que

tiene apoyo en la jurisprudencia constitucional[51] (que aparece al hilo de dicha sentencia) y del TEDH[52], y sería fácil rastrear, también, su apoyo doctrinal[53]. No se trata de una sentencia aislada, por cuanto que ha tenido

se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías".

51. Así, la STC 173/2011, 7 de noviembre, al hilo de la protección constitucional de la información personal derivada del uso de los instrumentos tecnológicos de nueva generación, señala: "si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) –por lo que sus funciones podrían equipararse a los de una agenda electrónica–, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda de que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información".
52. Sobre el tema RODRÍGUEZ LAINZ, "Sobre la influencia de la jurisprudencia del Tribunal Europeo de Derecho Humanos en la actual regulación legal del llamado "derecho al entorno virtual", en *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios* (Dir. Colomer Hernández), Edit. Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017, pp. 279 a 312.
53. *Vid.* GONZÁLEZ-CUÉLLAR SERRANO, Nicolás, "Garantías Constitucionales en la persecución penal en el entorno digital", en *Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García*, Edit. Colex, Madrid, 2006, pp. 887 a 916; ORTIZ PRADILLO, "Tecnología *versus* Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas", en *La Ley Penal*, n.° 75, 2010; y MARCHENA GÓMEZ, "La vulneración de derechos fundamentales por ministerio

continuidad[54], y, además, dicha idea está presente en la reforma operada en la LECrim en el año 2015, al regular las medidas de investigación que afectan a los derechos fundamentales contenidos en el art. 18 CE, aunque su verdadera aparición fuera en el contexto de la Propuesta de Código Procesal Penal del año 2012 y luego apareciera regulada en los arts. 588 sexies a y 588 sexies b de la LECrim. No obstante, repárese que la regulación constitucional del art. 18.4 pone el acento en la tutela de los derechos constitucionales que están detrás de la garantía del art. 18.4 en las inmisiones procedentes de las potencialidades del uso de la informática; sin embargo, el derecho al entorno virtual supera dicha perspectiva, y se centra en la necesaria protección frente a las injerencias en dichos derechos de los poderes públicos[55], a la que ahora pensamos que también se debe plantear respeto de la empresa privada.

de la Ley (a propósito del art. 33 de la Ley General de Telecomunicaciones)", en *La Ley*, n.° 7572, 2011.

54. Por ejemplo: SSTS 786/2015, de 4 de diciembre; 204/2016, de 10 de marzo; 426/2016, de 19 de mayo; y 489/2018, de 23 de octubre.

55. RODRÍGUEZ LAINZ, "Sobre la influencia…", *op. cit.*, p. 282.

Aplicación del sistema de reconocimiento facial para prevenir la violencia asociada al deporte en los encuentros calificados de alto riesgo

Cristina Domingo Jaramillo

Contratada predoctoral FPU
Departamento de Derecho Penal
Universidad de Granada

SUMARIO: I. INTRODUCCIÓN. II. PROBLEMAS QUE PLANTEA EL RECONOCIMIENTO FACIAL. 1. *Implicaciones éticas y legales derivadas del uso del reconocimiento facial*. 1.1. El reconocimiento facial y los riesgos en cuanto a discriminación. 1.2. Inconvenientes relacionados con la intimidad personal y la protección de datos de carácter personal. 1.3. Debate acerca de la limitación de los derechos fundamentales por motivos de seguridad ciudadana. 2. *Otros problemas asociados*. III. SOBRE LA POSIBLE IMPLEMENTACIÓN DEL RECONOCIMIENTO FACIAL EN ENCUENTROS DEPORTIVOS DE ÁMBITO NACIONAL. 1. *El reconocimiento facial como instrumento para garantizar la prohibición de acceso a los recintos deportivos*. 2. *Implantación de la técnica en los encuentros considerados de alto riesgo*. IV. CONCLUSIONES. V. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

Desde hace tiempo, el deporte se ha convertido en un espectáculo que atrae a miles de personas, especialmente el fútbol. En este último, muy frecuentemente tienen lugar altercados violentos entre los aficionados simpatizantes de equipos rivales (tanto dentro del recinto deportivo

como en sus aledaños[1]), lo cual pone en grave riesgo la seguridad ciudadana. Ante este panorama que acabamos de exponer, ya se han comenzado a implantar sistemas que permiten detectar a aquellos sujetos que tienen impuesta alguna medida de prohibición de acceso a los recintos deportivos por haber protagonizado previamente algún incidente de tipo violento. Dichos sistemas están basados en la biometría, entendida como el método de reconocimiento de personas a través de sus características fisiológicas o comportamentales[2]. La introducción de tales técnicas supone, a juicio de NIETO GARCÍA, CUEVAS VALENCIA y MARTÍNEZ CASTRO, "un salto a la modernización de la experiencia de asistir a los espectáculos deportivos"[3].

Sin embargo, su uso no está exento de controversias, desde el momento en el que permiten identificar de manera unívoca a una persona a través de sus características físicas, fisiológicas o conductuales. Por dicho motivo, puede entrar en conflicto con algunos derechos fundamentales, como ocurre con el de protección de datos de carácter personal[4], la privacidad[5]; y el honor, la intimidad personal y la propia imagen. Este último

1. Sobre el alcance del término aledaños, véase ampliamente RODRÍGUEZ MONSERRAT, M., "La futura intrascendencia jurídica del concepto 'Aledaños' en la prevención de la violencia en el Deporte", *Revista Aranzadi de Derecho de Deporte y Entretenimiento*, n.° 68, 2020, pp. 1 y ss.
2. DÍAZ RODRÍGUEZ, V., "Sistemas biométricos en materia criminal: un estudio comparado", *Revista del Instituto de Ciencias Jurídicas de Puebla*, n.° 31, 2003, pp. 29 y 30. Los datos biométricos pueden obtenerse a través de técnicas manuales o automatizadas y sus objetivos son dos. Por un lado, identificar a un individuo y, por otro, autenticarlo, es decir, verificar su identidad. Observatorio de la Seguridad de la Información, *Estudio sobre las tecnologías biométricas aplicadas a la seguridad*, Ministerio de Industria, Turismo y Comercio, 2011, p. 22; e Instituto Nacional de Ciberseguridad (INCIBE), *Tecnologías biométricas aplicadas a la ciberseguridad*. *Una guía de aproximación para el empresario*, 2016, p. 4.
3. NIETO GARCÍA, M., CUEVAS VALENCIA, R.E., y MARTÍNEZ CASTRO, J.M., "Diseño e implementación de un sistema de detección e identificación de aficionados violentos en estadios de fútbol", *Vínculos,* n.° 2, 2013, p. 40.
4. El derecho a la protección de datos de carácter personal viene regulado a nivel europeo en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD), traspuesto al ordenamiento jurídico interno a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. En este sentido, debemos tener en cuenta que por dato biométrico, según el art. 4 apartado 15 del RGPD, se entienden todos aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".
5. BREY, P., "Ethical Aspects of Facial Recognition Systems in Public Places", *Journal of Information, Communication and Ethics in Society*, vol. 2, 2004, p. 107. Uno de los

se encuentra recogido en el artículo 18.1 CE. En sus orígenes, la biometría fue utilizada con fines legales, por lo común, de investigación criminal pero con el paso del tiempo ha ido adquiriendo otras muchas funciones, entre las que destaca principalmente su aplicación como mecanismo de reforzamiento de la seguridad pública[6] y de restricción del acceso de determinadas personas a ciertos lugares seguros, ya sean estos de tipo físico o virtual[7].

El reconocimiento facial es uno de esos mecanismos que está basado en la detección de las características, en este caso físicas, de un sujeto, a través de su imagen o fotografía, con el objetivo de identificar a ciertas personas cuya imagen del rostro ha sido registrada previamente en una base de datos, para vigilar o autorizar su acceso a un espacio determinado[8]. Así las cosas, en vista de los inconvenientes de la biometría, nos planteamos la cuestión de si el reconocimiento facial podría implementarse en los sistemas de videovigilancia de los recintos deportivos y sus zonas circundantes con el fin de utilizarse como un instrumento facilitador de la detección instantánea de aficionados violentos conocidos, agilizándose con ello la labor de los equipos de seguridad en el control de las manifestaciones violentas durante el transcurso de un encuentro o

---

principales inconvenientes que presenta la biometría se vincula a cuestiones de privacidad. Esta tecnología codifica digitalmente una parte del cuerpo que adquiere un nuevo significado o función, lo que lleva aparejado dos problemas: por un lado, esa parte del cuerpo tiene una función más amplia dentro de un sistema de identificación o autenticación en el que juega un papel específico comparable a otros identificadores tradicionales, como las contraseñas. Por otro lado, supone un proceso de reducción funcional que deriva de la creación de información de partes del cuerpo que salen de su propietario y son usadas y controladas por otras personas.

6. Tal como afirma VALLS PRIETO, J., "El uso de Inteligencia Artificial para prevenir las amenazas cibernéticas", en Valls Prieto, J., (Coord.), *Retos jurídicos por la sociedad digital*, Aranzadi, Navarra, 2018, pp. 77 y 78, el uso de sistemas de Inteligencia Artificial –incluyéndose la biometría dentro de éstos– en materia de seguridad ha supuesto una gran revolución en los últimos años por los avances en la utilización del Big Data y las técnicas de minería de datos. Los nuevos instrumentos en materia de seguridad son de vital importancia en la detección de amenazas criminales futuras y las FCSE las necesitan para prevenir e investigar delitos.
7. *Vid.,* en este sentido, ETCHART, G., LUNA, L., LEAL, C., BENEDETTO, M., y ALVEZ, C., "Sistemas de reconocimiento biométricos, importancia del uso de estándares en entes estatales", *Repositorio Institucional de la* UNLP, 2011, p. 2; y YANG, W., WANG, S., HU, J., ZHENG, G., y VALLI, C., "Security and Accuracy of Fingerprint-Based Biometrics: A Review", *Symmetry*, vol. 11, n.° 141, 2019, pp. 1-3.
8. Este sistema se caracteriza primordialmente por inscribir la imagen del rostro de una persona, ya sea de manera voluntaria o en secreto para después ser comparada cuando ésta desee acceder a un lugar o es detectada encubiertamente. COFFIN, J.S., e INGRAM, D., *Facial recognition system for security Access and identification,* Patente de Estados Unidos, n.° 5.991.429, Washington DC: Oficina de Patentes y Marcas de los Estados Unidos, 1999, p. 1.

competición o si, por el contrario, ello supondría una conculcación de derechos fundamentales muy superior a los beneficios en seguridad que comportaría. En dicho sentido, hemos de tener en cuenta que esta técnica se utilizaría únicamente como prueba para comprobar la identidad de aquellas personas que tienen impuesta la ya mencionada medida de prohibición de acceder a los recintos en los que se lleve a cabo un encuentro o competición deportiva, denegándoles su entrada a los mismos, así como mecanismo facilitador del control de las manifestaciones violentas, a través de la vigilancia constante –tanto dentro como fuera de los estadios– de aquellos aficionados que, aun no siendo objeto de tal medida, son conocidos por sus tendencias violentas y con ello podrían prevenirse estallidos de violencia.

II. PROBLEMAS QUE PLANTEA EL RECONOCIMIENTO FACIAL

Violencia y deporte conforman un binomio inseparable que existe desde épocas históricas, no siendo inusual que durante la práctica deportiva se produzcan manifestaciones violentas, tanto entre los propios jugadores (o, violencia endógena) como entre los aficionados y demás agentes implicados en el entramado deportivo (o, violencia exógena). Esta última es la que más preocupa, especialmente la que tiene lugar entre los aficionados, pues de tales incidentes suelen derivarse problemas de seguridad y orden público que ponen en grave riesgo la integridad física de las personas que participan o asisten a los eventos deportivos[9]. Por constituir el deporte uno de los mayores fenómenos sociales existentes en la actualidad, la problemática de la violencia que en el mismo acontece requiere de una acción inmediata, porque tal como afirma MORILLAS CUEVA, "su activa presencia comunitaria genera una serie de exigencias a las que los poderes públicos han de responder con coherencia y compromiso"[10]. Por

9. BENÍTEZ ORTÚZAR, I.F., "Derecho Penal y deporte en España. Especial referencia a la actividad violenta y a la actitud racista y xenófoba", *Revista Andaluza de Derecho del Deporte*, n.° 4, 2008, p. 64; BARBA SÁNCHEZ, R., "La prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte. La seguridad en los estadios", en Palomar Olmeda, A., (Dir.), *Derecho del Deporte*, Aranzadi, Pamplona, 2013, pp. 878 y 879. En el mismo sentido se pronuncia MORILLAS CUEVA, L., "Tratamiento jurídico-penal de la violencia con ocasión de espectáculos deportivos", en Palomar Olmeda, A., (Dir.), *Derecho del deporte*, Aranzadi, Pamplona, 2013, p. 1046, cuando afirma que "semejante forma de violencia produce resultados tremendamente impactantes". En el siglo pasado, más de 1.500 espectadores murieron y más de 6.000 fueron heridos de gravedad en el transcurso de espectáculos deportivos. A esto hay que añadir la violencia que a diario se produce en el deporte "rey" en España, el fútbol.

10. MORILLAS CUEVA, L., "Tratamiento jurídico-penal de la violencia con ocasión de espectáculos deportivos…", *cit.*, p. 1044.

la internacionalización del deporte, la violencia que alrededor del mismo tiene lugar, no es una cuestión circunscrita solamente a las fronteras de un Estado, sino que se erige como un problema global. En base a dicho motivo, se han promulgado disposiciones legales con el fin de combatir esta lacra y garantizar la seguridad de la ciudadanía en el transcurso de las competiciones.

En relación a nuestro objeto de estudio, destaca el Convenio Europeo sobre la violencia e irrupción de espectadores con motivo de manifestaciones deportivas y especialmente de partidos de fútbol, hecho en Estrasburgo en el año 1985 (en adelante, Convenio de Estrasburgo), puesto que en su artículo 5 el Consejo de Europa pone de manifiesto la necesidad de que los Estados adopten todas las medidas que sean necesarias para "la identificación y tratamiento de los infractores". En tal sentido, para desarrollar el contenido de este precepto, el Comité Permanente aprobó la Recomendación n.° 1/1900, sobre identificación y tratamiento de infractores, en la que sugiere la instalación de sistemas de videovigilancia y circuitos cerrados de televisión (en adelante, CCTV), así como cualquier otra medida que esté dirigida a garantizar el cumplimiento de la prohibición de acceso al recinto deportivo.

Por su parte, en el ámbito nacional y, siguiendo lo establecido por el Convenio de Estrasburgo, en el año 2007 se promulgó la Ley 19/2007, de 11 de julio, contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte (a partir de ahora, LCVD), en la que se contemplan distintas acciones tendentes a prohibir y restringir la conducta de los espectadores. Todas las medidas se caracterizan por la severidad del reproche sancionador, bastante superior al que se prevé por conductas similares en otro tipo de espectáculos, en vista de los riesgos específicos que presentan estos acontecimientos. Entre aquellas, reseñar la implantación de los sistemas propuestos en el Convenio de Estrasburgo. A nuestro juicio, la videovigilancia y los CCTV se muestran como dos instrumentos adecuados para la labor de identificación de los individuos que ejecutan actos violentos[11]

11. Por poner tan solo un ejemplo, la identificación del individuo que arrojó una barra de plástico al terreno de juego durante el derbi sevillano celebrado el pasado 15 de enero de 2022 en el que se enfrentaban el Real Betis Balompié y el Sevilla Fútbol Club. Dicho elemento golpeó en la cabeza al jugador sevillano, Joan Jordán, quien cayó al suelo y tuvo que ser atendido por los servicios médicos. Por tal incidente, el partido fue suspendido en el minuto 41 y celebrado al día siguiente en el Ramón Sánchez-Pizjuán. HAURIE, L., "Suspendido el Betis-Sevilla: Jordán recibió un golpe con una barra lanzada desde la grada", *La Razón*, 15 de enero de 2022, recurso electrónico obtenido a través de la Web: https://www.larazon.es/deportes/futbol/20220115/s5rtxfoj4ncgvpoqqqa3xf2mjq.html, [última consulta: 17-1-22]; y RTVE, *Detenido el aficionado que supuestamente agredió a Joan Jordán en el Betis-Sevilla"*, 17 de enero de 2022, recurso electrónico obtenido a través de la Web: https://www.rtve.es/deportes/20220117/

y prevención de tales incidentes, si bien es cierto que se precisa de una herramienta que permita detectar de forma inmediata a los sujetos que tengan la intención de acceder a un recinto deportivo cuando tienen prohibido el acceso, en tanto agiliza el proceso de entrada, a través de la identificación inmediata y a distancia de dichas personas, facilitando su pase o, por el contrario, impidiéndolo. Por ello, a mi juicio, el reconocimiento facial podría insertarse en los sistemas de vigilancia convencionales para agilizar la detección instantánea de los aficionados violentos conocidos que pretendan acceder a un encuentro deportivo cuando tienen prohibida su entrada. Sin embargo, por los severos problemas en relación a los derechos fundamentales que comporta, surge inmediatamente la incertidumbre sobre si su utilización pudiera reportar unos beneficios en seguridad superiores a la conculcación de aquellos.

1. IMPLICACIONES ÉTICAS Y LEGALES DERIVADAS DEL USO DEL RECONOCIMIENTO FACIAL

Como cualquier otro sistema biométrico, el reconocimiento facial presenta algunos problemas en relación a los derechos y libertades fundamentales y, aunque es cierto que nos encontramos ante una técnica menos invasiva en comparación con otras, como aquellas que están basadas en la recopilación de muestras de ADN, por el hecho de realizarse a distancia e integrarse en los sistemas de vigilancia previamente existentes, es una fuente abierta de imágenes que pueden recogerse sin conocimiento o consentimiento del titular[12]. De modo que, junto a la función preventiva de preservación de la seguridad ciudadana, por cuanto contribuye a identificar a individuos catalogados como violentos en base a sus acciones previas, no son pocos los inconvenientes que su utilización conlleva, siendo especialmente significativos los relacionados con la discriminación y los derechos fundamentales como la intimidad personal y la protección de datos de carácter personal.

1.1. El reconocimiento facial y los riesgos en cuanto a discriminación

En lo que respecta a la discriminación, los inconvenientes vienen como resultado de la existencia de defectos en el diseño del sistema o el uso de

aficionado-lanzo-barra-betis-sevilla-jordan/2258860.shtml, [última consulta: 18-1-22].

12. MANN, M., y SMITH, M., "Automated Facial Recognition technology: recent developments and approaches to oversight", University of New South Wales Law Journal, vol. 40, n.° 1, 2017, pp. 124 y 125.

datos sesgados sin corrección previa[13]. De modo que, cuando el sistema de reconocimiento facial identifica más eficazmente los puntos de referencia con mayor representación en la base de datos, se producen sesgos discriminatorios. Estos últimos aparecen cuando los datos introducidos por las personas en los modelos de aprendizaje automáticos, establecen de modo desigual el género y la raza. Así, se ha comprobado que cuando existe menos diversidad demográfica inserta en dicha base de datos, en comparación con la población a la que se destina, los errores en la detección son superiores, puesto que los individuos pertenecientes a minorías no son reconocidos correctamente[14] produciéndose, en no pocas ocasiones, detecciones erróneas[15]. Este tipo de fallos preocupan de manera especial cuando la técnica pretende la detección de delincuentes y, en cambio, reconoce como sospechosos a personas inocentes. En este sentido, si no se prepara adecuadamente, puede favorecer la discriminación. Por dicho motivo, es necesario entrenar el sistema de reconocimiento facial para que la mayoría de grupos demográficos del lugar en el que se vaya a implementar estén debidamente incluidos en el fichero. Con ello, entendemos que podrían reducirse los problemas de error por esta razón.

1.2. Inconvenientes relacionados con la intimidad personal y la protección de datos de carácter personal

El reconocimiento facial presenta serios problemas en relación al derecho a la intimidad personal y la privacidad, puesto que junto a los inconvenientes que plantea el uso de las cámaras de vigilancia convencionales[16], ha de enfrentarse a los problemas derivados de las técnicas biométricas. Principalmente, este mecanismo es controvertido por el hecho de que el rostro siempre se ha considerado único y el aspecto más distinguido

13. Comisión Europea, *Libro Blanco sobre Inteligencia Artificial– un enfoque europeo orientado a la excelencia y la confianza*, COM(2020) 65 final. Bruselas, 19 de febrero de 2020, p. 13.
14. En este sentido, véase, en mayor profundidad, LEARNED-MILLER, E., y otros, *Facial recognition technologies in the wild: a call for a federal office,* MacArthur Foundation, 2020, p. 9.
15. Se ha demostrado que la técnica detecta con menor facilidad a personas con la piel oscura y mujeres. Así, mientras que el perfil del varón blanco es el mejor localizado, el de mujeres de color es el que más errores reporta. INIOLUWA, D.R., y otros, "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing", *Actas de la Conferencia AAAI/ACM sobre IA, ética y sociedad*, 2020, p. 146; y, más específicamente en relación al género, *vid.,* BUOLAMWINI, J., y GEBRU, T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research*, n.° 81, 2018, pp. 1 y ss.
16. Sobre dichos problemas, véase en mayor amplitud, GIL MEMBRADO, C., *Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado*, Wolters Reuters, Madrid, 2019, pp. 29 y ss.

del cuerpo humano[17]. De forma más general, este derecho puede verse conculcado o, al menos, puesto en peligro, por dos razones. En primer lugar, porque la codificación de una parte del cuerpo, hace que la misma adquiera un nuevo significado o función, derivándose de ello la creación de información de partes del cuerpo de un individuo que exceden de su control y son usadas y controladas por otros[18]. El –art. 8– del Convenio Europeo de Derechos Humanos reconoce el "Derecho al respeto a la vida privada y familiar". En su apartado segundo, señala que la autoridad pública no podrá injerir en este derecho salvo que la intromisión esté prevista legalmente y sea una medida necesaria para garantizar la seguridad pública (entre otras cuestiones) en una sociedad democrática. Por tanto, el derecho a la intimidad deberá estar equilibrado con la seguridad. Igualmente, la intimidad personal encuentra su respaldo constitucional en el apartado primero del artículo 18. Y, en segundo lugar, a lo anterior, se añaden los problemas relativos al consentimiento[19] cuando el registro de los datos tiene lugar sin la anuencia expresa del titular.

Muy vinculado a la intimidad personal, el derecho a la protección de datos de carácter personal se ve en peligro desde el momento en el que el reconocimiento facial se basa en la identificación de una persona a través de la imagen de su rostro, siendo éste, a nuestro juicio, el dato personal por antonomasia, por constituir la parte más visible y pública de las personas, a través de la que resulta más sencillo realizar su identificación. Los datos biométricos, según el artículo 9 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (a partir de este momento, RGPD) son una categoría de datos personales especiales y prohíbe en su primer apartado el tratamiento de los mismos, siempre y cuando estén "dirigidos a identificar de manera unívoca a una persona física". No obstante, en su apartado segundo, incluye una excepción, siempre y cuando concurran determinadas circunstancias, entre las que se encuentra la existencia de un "interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos

17. *Ibd.,* pp. 105-107.
18. BREY, P. "Ethical Aspects of Facial Recognition Systems in Public Places…", *cit.,* p. 107.
19. El consentimiento limita el fin con el que se pueden utilizar los datos. VALLS PRIETO, J., "El uso de Inteligencia Artificial para prevenir las amenazas cibernéticas…", *cit.,* p. 101.

fundamentales del interesado". Por tanto, entendiendo que el mantenimiento de la seguridad pública es un interés público esencial, el uso del reconocimiento facial en eventos deportivos no estaría prohibido por el RGPD, por ser un mecanismo que facilita el mantenimiento de la seguridad en este ámbito al contribuir a evitar la violencia.

1.3. Debate acerca de la limitación de los derechos fundamentales por motivos de seguridad ciudadana

La cuestión de la preservación de la seguridad ciudadana frente a la posible limitación del ejercicio de los derechos y libertades fundamentales plantea serios problemas, sobre todo cuando se utilizan instrumentos muy intrusivos en estos últimos en aras a garantizar aquella, como sucede con el reconocimiento facial. En tal sentido, habría que decidir cuál de los dos prevalece con su uso.

Antes de nada, indicar que el respeto de los derechos fundamentales significa que no pueden ser violados por otras personas y, para que así sea, deben adoptarse medidas positivas tendentes a asegurar que los individuos disfrutan plenamente de dichos derechos[20]. Sin embargo, en España, el Tribunal Constitucional reconoce que no existen derechos fundamentales ilimitados, entendiendo que todos tienen límites. De este modo, ha valorado en cada supuesto concreto si se vulnera el contenido del derecho, siempre respetando el principio de proporcionalidad[21]. La Agencia Española de Protección de Datos entiende que la seguridad pública es un bien constitucionalmente protegido, de forma que los derechos y libertades fundamentales pueden limitarse siempre y cuando tal limitación no sobrepase lo razonable y se tengan en cuenta los principios establecido por el Tribunal Constitucional[22]. En dicha línea, tal como afirma

20. ISHAY, M. R., *The History of Human Rights: from Ancient Times to the Globalization Era,* University of California Press, 2014, pp. 63-116.

21. GIL MEMBRADO, C., *Videovigilancia y protección de datos…*, *cit.,* p. 212; el principio de proporcionalidad ha sido valorado por el Tribunal desde una triple dimensión: "a) las limitaciones que se establezcan en relación con cualquier derecho no pueden obstruirlo más allá de lo razonable, b) las medidas limitadoras han de ser razonables y adecuadas en orden a la consecución del fin perseguido que ha de estar constitucionalmente amparado, y c) la restricción resultante del derecho ha de ser proporcional a la situación en la que se halle aquel a quien se impone". En este sentido, véase también, entre otras la STC (Pleno) 76/2019 de 22 de mayo, [RTC 2019, 76]. Esta última hace referencia expresamente al derecho a la protección de datos de carácter personal pero su contenido puede hacerse extensible a los demás derechos fundamentales expuestos.

22. Agencia Española de Protección de Datos, *Prevalencia en el ejercicio de derechos. Informe Jurídico 0117/2007*, recurso electrónico obtenido de la Web: https://www.aepd.es/informes/historicos/2007-0117.pdf, [última consulta: 12-1-21], pp. 6 y 7.

HOWARD-HASSMAN, la seguridad ciudadana se encuentra amenazada gravemente por la delincuencia. Los Estados son los principales responsables, a través de las fuerzas de seguridad, de proteger a la ciudadanía de los individuos delincuentes. Así, tienen la obligación de garantizarla, haciendo uso para ello de instrumentos que pueden incidir en el ejercicio de los derechos[23].

Las FCSE según el apartado primero del artículo 104 CE tienen como misión la protección del libre ejercicio de los derechos y libertades pero también la de garantizar la seguridad ciudadana. La LO 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana (LOPSC) establece en su Preámbulo que la seguridad es el instrumento dispuesto al servicio de la garantía de los derechos y libertades y no constituye un fin en sí mismo pero, para que los derechos puedan ser ejercidos plenamente, la seguridad debe estar garantizada. Con todo, la limitación de derechos que supone el reconocimiento facial estaría legitimada si con ello se previene la delincuencia. En nuestro caso concreto, los desórdenes públicos que derivan de incidentes violentos protagonizados por individuos que utilizan el espectáculo deportivo como baluarte para dar rienda suelta a sus instintos agresivos. En sentido contrario se pronuncia BARONA VILAR. A juicio de la autora en cita, aunque la técnica venga con la promesa de garantizar una mayor seguridad, se aproxima al escenario "orwelliano" de una sociedad basada en el sometimiento al control de no se sabe muy bien qué o quién. Al hacer uso de algoritmos, técnicas de análisis de datos y creación de bancos de imágenes de caras, entrega a las fuerzas de seguridad un instrumento que, a pesar de identificar delincuentes, limita o restringe los derechos y garantías de la población[24]. Además, la seguridad en los recintos deportivos podría quedar debidamente preservada, como indicamos en líneas superiores, con métodos menos intrusivos como la videovigilancia común. No obstante, dada la gran cantidad de personas que acuden a un evento deportivo, sobre todo en el caso de encuentros futbolísticos de especial trascendencia, la introducción de estos mecanismos puede ser de gran utilidad para agilizar la labor de los agentes

23. HOWARD-HASSMAN, R. E., "Human Security: Understanding Human Rights", *Human Rights Quarterly*, vol. 34, 2012, pp. 99-103. De forma similar, PIÑAR MAÑAS, J. L., "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio", *Documento de Trabajo (Laboratorio de Alternativas)*, n.° 147, 2009, pp. 23 y ss.; y BREY, P., "Ethical Aspects of Facial Recognition Systems…", *cit.*, pp. 104-107. Se entiende que la seguridad implica la protección contra daños a los derechos más básicos, como el derecho a la vida, a la libertad y a la propiedad; y GIL MEMBRADO, C., *Videovigilancia y protección de datos…*, *cit.*, p. 126.

24. BARONA VILAR, S., "Inteligencia Artificial o la algoritmización de la vida y de la justicia: ¿Solución o problema?", *Revista Boliviana de Derecho*, n.° 28, 2019, p. 26.

encargados de la seguridad y de controlar el acceso de los espectadores, no suponiendo, por el contrario, una vulneración de los derechos fundamentales indicados en apartados precedentes, superior a los beneficios de seguridad que reporta, en tanto la violencia asociada al deporte ocurre muy frecuentemente, dejando en ocasiones numerosas muertes y heridos que podrían evitarse si se hace uso de instrumentos como el reconocimiento facial.

2. OTROS PROBLEMAS ASOCIADOS

Junto a las implicaciones éticas y legales expuestas, la instalación del mecanismo de reconocimiento facial presenta dos inconvenientes. A saber, el error y la denominada función de arrastre o *function creep*. En relación al primero, las identificaciones incorrectas que ya fueron mencionadas anteriormente, puede derivar en que personas inocentes sean detectadas de forma errónea. Este problema no es único del reconocimiento facial, ya que puede tener lugar en cualquier sistema que utilice una base de datos destinada a almacenar información de carácter personal[25]. Por no ser una cuestión específica de la técnica objeto de nuestro análisis, podemos considerar que la existencia de errores, no presenta en sí misma un argumento sólido específicamente contra el reconocimiento facial. En dicha línea, hay que traer a colación los falsos y válidos positivos. Los primeros serían aquellas personas identificadas incorrectamente por el sistema, mientras que los segundos hacen referencia a las identificaciones positivas, es decir, los casos en los que el mecanismo reconoce adecuadamente a una persona registrada previamente en la base de datos. En este punto, la cuestión que más controversia genera estriba en si la detección de falsos positivos podría estar legitimada de algún modo. La tendencia pública general parece ir en el sentido de aceptar que se van a sufrir inconvenientes menores para garantizar la seguridad. Por tanto, se acepta el sacrificio de los derechos y la posibilidad de que existan detecciones erróneas si con ello se protege esta última[26].

Relacionado con el error, se han diseñado algunos métodos que permitirían sortear el sistema de reconocimiento facial a través del ocultamiento o la confusión, pudiéndose llevar a la práctica simplemente con el uso de algún complemento que dificulte la visibilidad del rostro, como sombreros, barbas, bufandas o gafas de sol[27]. Por otro lado, se han desarrollado

25. BREY, P., "Ethical Aspects of Facial Recognition Systems…", *cit.*, pp. 104-107.
26. *Ibid.*, p. 104.
27. MERINO, M., "Estos son los métodos con los que intentan sortear el reconocimiento facial los defensores de la privacidad", *Xataka*, 10 de abril de 2019, recurso

varias técnicas que pretenden confundir a las cámaras de videovigilancia. Una de ellas, se basa en la creación de unas imágenes de distintos colores que pueden imprimirse y usarse en el mundo real, ocultando a los individuos de los detectores, lo que sugiere que los sistemas de seguridad podrían ser vulnerables a este tipo de ataques[28].

El segundo problema que mencionamos es el de la función de arrastre, definida como el fenómeno por el que una tecnología diseñada con un propósito concreto, podría utilizarse con otros fines o asignársele funciones adicionales[29]. En este caso, los objetivos para los que se prevé en un principio el sistema podrían extenderse fácilmente a otros que no fueron considerados inicialmente. Para evitarlo, debe especificarse claramente la finalidad que persigue la implementación del instrumento y ser muy cuidadosos en cuanto a su estricto cumplimiento.

A pesar de todos los problemas y cuestiones éticas y legales indicadas, entendemos que la utilización del reconocimiento facial en ciertos lugares públicos, como recintos deportivos en los que se congrega un gran número de personas y las rivalidades pueden llevarse al extremo, podría ser beneficiosa para garantizar la seguridad ciudadana en determinados casos, siempre y cuando se establezcan específicamente las garantías y límites de su puesta en marcha y no se conculquen desproporcionadamente los derechos de la ciudadanía[30]. Sin embargo, ello no puede

---

electrónicoobtenidodelaWeb:https://www.xataka.com/inteligencia-artificial/estos-metodos-que-intentan-sortear-reconocimiento-facial-defensores-privacidad, [última consulta: 2-1-22].

28. THYS, S., VAN RANST-W., y GOEDEMÉ, T., "Fooling automated surveillance cameras: adversarial patches to attack person detection", *arXiv.org,* (Repositorio Institucional de la Universidad de Cornell), Nueva York, 18 de abril de 2019, pp. 5-7. Los autores de la técnica creen que si se combina la misma con un sofisticado simulador de ropa, se puede diseñar una camiseta que podría hacer a la persona invisible a las cámaras de vigilancia automática.

29. BREY, P., "Ethical Aspects of Facial Recognition Systems…", *cit.,* pp. 104 y 105. El autor expone que el problema puede darse de cuatro formas: por ensanchamiento de la base de datos, por la ampliación del propósito inicialmente previsto, por el cambio de usuarios y por el cambio de dominio.

30. Anteriormente, pusimos esta cuestión de manifiesto en DOMINGO JARAMILLO, C., "Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana", *El Criminalista Digital. Papeles de Criminología*, n.° 9, 2021, pp. 20 y ss. Sobre la necesidad de especificar en un documento creado *ad hoc* todos los aspectos del uso y tratamiento de los datos a tratar, teniendo en especial consideración el impacto a la intimidad, se pronuncia VALLS PRIETO, J., "El uso de Inteligencia Artificial para prevenir las amenazas cibernéticas…", *cit.,* pp. 95 y ss., quien afirma (aunque de modo general para los sistemas de Inteligencia Artificial), que la tecnología ha de ser utilizada de manera responsable y ética, entendiendo esto como guías y directrices que orienten un determinado campo. El tratamiento debe ser lo más limitado posible por la importancia de los derechos fundamentales que están en juego.

afirmarse rotundamente sin la realización de un análisis del marco normativo vigente sobre prevención y lucha contra la violencia asociada al deporte en nuestro país.

III. SOBRE LA POSIBLE IMPLEMENTACIÓN DEL RECONOCIMIENTO FACIAL EN ENCUENTROS DEPORTIVOS DE ÁMBITO NACIONAL

Al ser el deporte un fenómeno internacional que traspasa fronteras, los problemas que lleva aparejados tampoco quedan circunscritos a un único país. Tal como señala BENÍTEZ ORTÚZAR, la violencia en los espectáculos deportivos se produce en cualquier lugar del mundo[31]. Esta circunstancia ha motivado la promulgación de disposiciones legales a todos los niveles (internacional, nacional y autonómico) para combatir este fenómeno y garantizar la seguridad durante el transcurso de los eventos deportivos. Destaca, como a continuación será objeto de análisis, la medida de prohibición de entrada en un estadio a los sujetos que han sido sancionados por la comisión de incidentes violentos, con la que se pretende colaborar al mantenimiento de la seguridad.

1. EL RECONOCIMIENTO FACIAL COMO INSTRUMENTO PARA GARANTIZAR LA PROHIBICIÓN DE ACCESO A LOS RECINTOS DEPORTIVOS

Como indicamos previamente, el marco normativo supranacional de referencia en materia de violencia deportiva es el Convenio de Estrasburgo, en cuyo artículo 3.4 letra c) establece la prohibición de acceso a los eventos deportivos a los promotores de disturbios conocidos o potenciales. Siguiendo lo anterior, la LCVD en el apartado tercero de su artículo 24 relativo a las sanciones, recoge la posibilidad de poner en marcha tal medida[32]. En el artículo siguiente, esto es, el número 25, se desarrolla dicha sanción, estableciendo en su apartado primero la obligación que tienen los clubes y los responsables de la organización de los espectáculos deportivos de privar de la condición de socio, asociado o abonado a los sujetos sancionados con la prohibición de acceso a los recintos deportivos,

31. BENÍTEZ ORTÚZAR, I.F., "Derecho Penal y deporte en España…", *cit.*, p. 64.
32. El precepto establece tres graduaciones en función de la gravedad del incidente, quedando redactado como sigue: "Además de las sanciones económicas, a las personas físicas que cometan las infracciones tipificadas en el presente Título se les podrán imponer, atendiendo a las circunstancias que concurran en los hechos y, muy especialmente, a su gravedad o repercusión social, la sanción de desarrollar trabajos

debiendo mantenerse la exclusión del abono o la condición de socio o asociado durante el tiempo de cumplimiento de la sanción. Destaca el apartado segundo del susodicho precepto, en tanto señala la posibilidad de poner en marcha procedimientos de verificación de la identidad para garantizar el cumplimiento de la medida, los cuales habrán de ser realizados por los miembros de las FCS. Igualmente, con el objetivo de garantizar el efectivo acatamiento de la susodicha prohibición, el Reglamento de desarrollo de la LCVD aprobado por RD 203/2010, de 26 de febrero, en su artículo 29.1 establece la obligación que tienen los clubes, sociedades deportivas u organizadores de concretar los mecanismos que consideren necesarios para hacer efectiva la prohibición, ya sea con los medios técnicos de los que dispongan o a través de su personal. Para ello, continúa indicando que la identificación de las personas objeto de esta medida habrá sido previamente facilitada por las autoridades gubernativas o por el Coordinador de Seguridad[33].

En este sentido, destaca que ni la LCVD ni el RD 203/2010 determinan los mecanismos de verificación de la identidad de los sujetos que tienen prohibido el acceso a los espacios en los que se celebre un encuentro o competición, aludiéndose únicamente a criterios de necesidad, por lo que se deja la puerta abierta a la introducción de cualquier técnica que se considere adecuada a tal fin. De este modo, el reconocimiento facial podría ser uno de esos instrumentos que, insertados en los sistemas de vigilancia existentes, contribuya a asegurar el acatamiento de dicha medida.

Uno de los obstáculos con los que se encuentra la implementación del reconocimiento facial en el supuesto que venimos analizando es la ausencia de legislación específica que regule la instalación y los fines del uso del sistema, por lo que hay que remitirse a lo dispuesto en la normativa sobre videovigilancia y tener en cuenta además lo establecido en materia

---

sociales en el ámbito deportivo y la sanción de prohibición de acceso a cualquier recinto deportivo de acuerdo a la siguiente escala:

a) Prohibición de acceso a cualquier recinto deportivo por un período comprendido entre un mes y seis meses, en caso de infracciones leves.
b) Prohibición de acceso a cualquier recinto deportivo por un período entre seis meses y dos años, en caso de infracciones graves.
c) Prohibición de acceso a cualquier recinto deportivo por un período entre dos años y cinco años, en caso de infracciones muy graves".

33. El Coordinador de Seguridad es el miembro de la organización policial que tiene encomendadas las tareas de dirección, coordinación y organización de los servicios de seguridad de los espectáculos deportivos –art. 14.1 LCVD–. Los Coordinadores de Seguridad "serán nombrados entre miembros de los Cuerpos Nacional de Policía o de la Guardia Civil" –art. 51 RD 203/2010–.

de protección de datos de carácter personal[34]. En tal sentido, la instalación de los dispositivos y el tratamiento de las imágenes resultantes de las grabaciones recogidas con la técnica de reconocimiento facial estarían sometidos a lo establecido en la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las FCSE en lugares públicos, tal como queda reflejado en la Disposición Adicional 7.ª1 LCVD. La función de tratamiento de las imágenes la tiene asignada el Coordinador de Seguridad, quien las transmitirá a las autoridades competentes solamente si se aprecia alguna de las conductas violentas, racistas, xenófobas e intolerantes previstas en los apartados primero y segundo del artículo 2 LCVD, lo cual viene establecido en la Disposición Adicional 7.ª2 de ésta. Por su parte, los elementos gráficos que hubieran sido captados por las videocámaras se consideran archivos policiales y su tratamiento se somete a la legislación sobre protección de datos, tal como establece el artículo 14.3 párrafo segundo LCVD, recogiéndose en el inciso final de este último precepto que los datos se conservarán únicamente si son necesarios para la investigación de los incidentes producidos durante la celebración del encuentro en cuestión, inutilizándolos o destruyéndolos en caso contrario. Por este motivo, la protección de los datos personales se vería preservada, al tener que ser eliminados una vez que la medida que legitimaba su uso haya llegado a su fin. Además, ha de indicarse que este derecho se refuerza en el caso de los sujetos que no están registrados en la base de datos por no haber ejecutado actos de violencia y, por tanto, no tener impuesta la medida de prohibición de acceso a los recintos deportivos. Ello se debe a que la imagen de su rostro pasaría desapercibida por el mecanismo, siendo registrada solamente en las grabaciones de las videocámaras convencionales, destruyéndose posteriormente el material resultante en el plazo establecido normativamente.

No solo aquellos, sino también los problemas existentes en relación al consentimiento de los usuarios quedarían salvados desde el momento en el que las entradas habrían de indicar en el reverso que se está en una zona videovigilada, debiéndose en dicho caso hacerse referencia igualmente a que las cámaras están equipadas con el sistema de reconocimiento facial. También los organizadores de los encuentros deportivos tienen la obligación de fijar carteles con dicha información[35] (apartados segundo y

34. Esto es, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

35. En tal sentido, en el caso de la videovigilancia y los CCTV, siguiendo a MILLÁN GARRIDO, A., "Dispositivos de seguridad reforzados (Artículos 8.° a 14)", en

cuarto del artículo 20 RD 203/2010). De este modo, los usuarios estarían prestando su consentimiento –siquiera presunto– a la grabación de sus imágenes y al acceso a un recinto equipado con reconocimiento facial, al conocer previamente estas cuestiones a través de los medios indicados.

2. IMPLANTACIÓN DE LA TÉCNICA EN LOS ENCUENTROS CONSIDERADOS DE ALTO RIESGO

Especial mención merecen los encuentros considerados de alto riesgo[36], por comportar una mayor amenaza a la seguridad pública, en base a la existencia de un peligro superior de que tengan lugar incidentes violentos. Tal como afirma BERNAL GARCÍA, las razones por las que un encuentro puede ser calificado de alto riesgo son diversas y no pueden definirse de manera excluyente, aunque existe una serie de fundamentos comunes a la mayor parte de dichos encuentros. El autor en cita establece los siguientes: "a) alta rivalidad entre los clubes que participan del encuentro; b) alta rivalidad deportiva o ideológica entre los seguidores radicales de los clubes que participan del encuentro; c) desplazamiento masivo de la afición del equipo visitante; d) antecedentes de incidentes violentos de las aficiones de los equipos participantes; e) previsión de aforos completos; f) encuentros correspondientes a últimas rondas o eliminatorias y finales en las que están en juego títulos deportivos; g) amenazas y riesgos tales como terrorismo o grupos que reivindican posicionamientos políticos, ideológicos, religiosos o sociales"[37].

En vista del peligro que supone un encuentro de este tipo, principalmente cuando existe una rivalidad manifiesta entre los seguidores radicales de los equipos que lo disputan, se obliga a los clubes y sociedades anónimas deportivas a reforzar las medidas de seguridad que, como mínimo deben comprender "el control de acceso para el estricto

Palomar Olmeda, A., Gamero Casado, E., (Coords.), *Comentarios a la Ley contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte*, Aranzadi, Navarra, 2008, p. 214, se puede afirmar que su implementación en España no es cuestionable a nivel legal, ya que a los asistentes se les informa tanto en la cartelería como en las entradas de la aplicación de esta medida, por lo que esta circunstancia podría hacerse extensible al reconocimiento facial.

36. La función de declarar un encuentro como de alto riesgo la tiene asignada la Comisión Estatal contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, tal como se establece en la letra b) del artículo 8.4 del Real Decreto 748/2008, de 9 de mayo, que regula dicha Comisión Estatal, previa propuesta de las Federaciones Deportivas y Ligas Profesionales.

37. BERNAL GARCÍA, F., "Dispositivos de seguridad privada en grandes eventos deportivos: encuentros calificados de alto riesgo", en García Tascón, M., y otros, (Eds.), *La seguridad deportiva a debate*, Dykinson, Madrid, 2020, pp. 196 y 197.

cumplimiento de las prohibiciones existentes", tal como se recoge en la letra c) del artículo 10.2 LCVD; a ello se añade en su artículo 13.1 la posibilidad de implantar medidas adicionales, destacando en su letra b) la promoción de sistemas de verificación de la identidad de los individuos que pretendan acceder a los recintos deportivos. En este sentido, el Comité Permanente del Convenio de Estrasburgo en la Recomendación (T-VR) 2002/1, relativa a las directrices para la venta de entradas en los encuentros internacionales de fútbol, clubes y selecciones, recomienda a los países que prevén la medida de prohibición de acceso (entre los que se encuentra España) que difundan todos los datos con los que cuenten, con el objetivo de impedir la entrada a aquellas personas que tienen impuesta esta medida. Incluso propone implementar un sistema técnico que permita localizar y expulsar a tales individuos, a través de la identificación con datos biométricos, entre los que se incluye la fotografía[38]. Así las cosas, entendemos que la Unión Europea deja la puerta abierta a la puesta en marcha de cualquier tipo de mecanismo basado en la biometría, si con ello se facilita la localización y expulsión de las personas que tienen impuesta la medida de prohibición de acceder a los recintos deportivos.

En contra de la introducción de sistemas biométricos con tales fines se han pronunciado algunos autores. Entre ellos, MILLÁN GARRIDO, quien considera que los sistemas de verificación de la identidad de los sujetos que pretendan acceder a los recintos deportivos presentan dificultades materiales y jurídicas en lo relativo al respeto de los derechos fundamentales[39]. No obstante, ya se han comenzado a incluir en algunos estadios nacionales, como ocurre con las huellas dactilares[40] y, específicamente

38. Para ampliar más la información sobre la normativa en materia de violencia deportiva, se recomienda al lector que acuda a la recopilación que de la misma realiza MILLÁN GARRIDO, A., *Legislación sobre violencia en espectáculos deportivos*, Junta de Andalucía, Sevilla, 2005.

39. MILLÁN GARRIDO, A., "Dispositivos de seguridad reforzados…", *cit.*, p. 235.

40. En este sentido, la Liga de Fútbol Profesional en la temporada 2015/2016 anunció la puesta en marcha de sistemas de identificación de los espectadores que acceden a las gradas de animación a través del reconocimiento de la huella dactilar. El pionero en este caso fue el Club Atlético de Madrid y, para su correcta puesta en marcha, durante el periodo de renovación de abonos, se contactó con los integrantes de la grada en cuestión para actualizar los datos personales y tomarles las huellas dactilares y una fotografía: LALIGA, "LaLiga implementa un nuevo sistema de acceso a las gradas de animación", 17 de agosto de 2015, recurso electrónico obtenido a través de la Web: https://www.laliga.es/noticias/laliga-implementa-un-nuevo-sistema-de-acceso-a-las-gradas-de-animacion, [última consulta: 15-9-21]. Este sistema está desarrollado por la empresa EVERIS, socio tecnológico de LaLiga. El sistema permite que únicamente puedan acceder a esas gradas los aficionados que hayan obtenido el abono, pase de temporada o similar a dicha grada, zona o sector, con el

para el caso del reconocimiento facial, el Club Atlético de Madrid prevé su inserción en la próxima temporada[41], si bien el susodicho Club no ha hecho públicas las aplicaciones que va a tener la medida, entendemos que pueden asignársele funciones de preservación de la seguridad, concretamente para impedir el acceso al estadio a las personas que lo tienen prohibido o reconocer a aquellas que cometan alguna infracción durante el transcurso de un encuentro.

Sobre la legalidad de la utilización del reconocimiento facial se ha pronunciado la Audiencia Provincial de Barcelona (Sección 9.ª) en el Auto núm. 72/202 de 15 de febrero, [ARP/2021/706]. En este caso fue la cadena de supermercados MERCADONA la que pretendía usarlo para evitar la entrada en varios de sus establecimientos de unas personas a las que se les había impuesto una medida accesoria de prohibición de acceso a una de las tiendas de la cadena tras haber sido condenados por un delito de robo. Previamente, el Juzgado de lo Penal número 24 de Barcelona, en Auto de 27 de septiembre de 2019 había denegado tal posibilidad. La mercantil, en el recurso interpuesto a dicha resolución, invoca criterios de idoneidad, necesidad y proporcionalidad de la medida solicitada para su utilización. Considera de este modo que es eficaz al objetivo perseguido, como es la identificación de todo sujeto que pretende vulnerar la medida impuesta judicialmente, así como los derechos de la empresa; la entiende necesaria, pues plantea que es el único instrumento

objetivo de evitar que otros espectadores se ubiquen en dichas zonas cuando no les corresponda; y REDACCIÓN DE IUSPORT, "Comenzó a aplicarse la identificación biométrica para el acceso a los estadios", *Iusport*, 22 de agosto de 2015, recurso electrónico obtenido a través de la Web: https://iusport.com/art/9573/comenzo-a-aplicarse-la-identificacion-biometrica-para-el-acceso-a-los-estadios, [última consulta: 24-9-21].

41. DIÉGUEZ RODRÍGUEZ, J.M., "Revés para los planes del Atlético con el reconocimiento facial", *Iusport*, 22 de junio de 2021, recurso electrónico obtenido a través de la Web: https://iusport.com/art/63765/reves-para-los-planes-del-atletico-con-el-reconocimiento-facial, [última consulta: 13-1-22].

    La utilización del reconocimiento facial en el ámbito deportivo no es novedosa y ya en el año 2001 se puso en marcha por primera vez durante la final de la Super Bowl y posteriormente, en varios estadios de fútbol en Uruguay. LA VANGUARDIA, "Comunicado: reconocimiento facial en el fútbol uruguayo", 26 de abril de 2018, recurso electrónico obtenido a través de la Web: https://www.lavanguardia.com/vida/20180426/443015024931/comunicado-reconocimiento-facial-en-el-futbol-uruguayo.html, [última consulta: 10-9-21]; y NARANJO, J. C., "Reconocimiento facial, ¿el fin de la violencia en los estadios de fútbol?", *Crónica de Deportes*, 1 de mayo de 2018, recurso electrónico obtenido a través de la Web: https://cronicaglobal.elespanol.com/deportes/reconocimiento-facial-violencia-estadios-futbol_138041_102.html, [última consulta: 10-9-21]. Esta tecnología comenzó a utilizarse en el año 2017 en los tres estadios más importantes de Uruguay y contribuye a la identificación de las personas que no tienen autorizado el acceso a los partidos de fútbol.

que afronta el problema y lo soluciona, en tanto que las anteriores medidas adoptadas fueron ineficaces por la imposibilidad de controlar por todos los empleados y en todos los establecimientos, el cumplimiento de la medida; y, proporcional, puesto que reporta más beneficios para el interés general que perjuicios a la ciudadanía, al no implicar ningún tratamiento de datos biométricos de forma general, sino únicamente de las personas condenadas en sentencia firme. El Auto de la AP concluye denegando la autorización de la cadena de supermercados de utilizar medios automatizados de captación de datos biométricos de los penados, rebatiendo los argumentos anteriores. Así, considera que no resulta una medida proporcional, como tampoco es necesaria ni idónea. Esto se debe al hecho de que a los condenados se les impuso la prohibición de acceder a un supermercado concreto y no se tuvo constancia de que hubiesen quebrantado la prohibición ni que sean reincidentes, a lo que se añade que la medida interesada no se dirige a la salvaguarda del interés público, sino que más bien se orienta a garantizar los intereses privados o particulares de la empresa en cuestión. Por tanto, finaliza aseverando que la implementación del reconocimiento facial conculcaría las garantías adecuadas para la protección de los derechos y libertades de los interesados, no solo de los condenados, sino del resto de personas que acceden al supermercado.

En este caso concreto, nos posicionamos en favor de la resolución de la AP en el sentido de denegar la pretensión de la empresa de implantar el sistema en sus supermercados, puesto que la medida va a garantizar sus intereses privados, no pudiéndose legitimar así su introducción en los sistemas de vigilancia convencionales, puesto que, lo contrario, vulneraría gravemente los derechos de la ciudadanía y no existe un supuesto interés público para su utilización. Por el contrario, a nuestro juicio, ese interés general sí existiría en el caso del deporte en encuentros de riesgo, en tanto se pretenden evitar las manifestaciones violentas que derivan en desórdenes públicos, mediante la detección inmediata de aficionados violentos en las entradas de los recintos deportivos, denegándoles el acceso, como mecanismo que coadyuve a garantizar la seguridad ciudadana en el ámbito deportivo.

Así las cosas y, en orden a evitar una expansión irracional de la técnica, planteo que únicamente pueda utilizarse con este fin, no debiéndose extender más allá del mismo, no pudiendo insertarse ni en los alrededores del estadio ni dentro del mismo para, entre otras cosas, vigilar a determinados aficiones ultras de cuyos integrantes pueda preverse la comisión de algún tipo de violencia, en cuanto ello supondría una extralimitación de las funciones para las que se previó la

puesta en marcha de este instrumento que conculcaría los derechos y libertades fundamentales de forma muy superior a los beneficios de seguridad, derivando en una vigilancia opresiva; y, si ya en los encuentros de alto riesgo no debe usarse en todo caso, menos aún ha de incluirse en los partidos convencionales, en tanto la seguridad ya se ve adecuadamente garantizada con los sistemas de videovigilancia existentes y los CCTV.

Aun siendo consciente de que algunos derechos fundamentales se verían limitados con esta medida, tal restricción estaría legitimada por la salvaguarda de la seguridad ciudadana en los eventos en los que existe un riesgo racional y fundado de violencia. Sin embargo, la vulneración de dichos derechos ha de ser mínima y deben adoptarse medidas para que se respeten en lo esencial. Por este motivo, para sortear la posible lesión del derecho a la intimidad personal, al honor y la propia imagen del art. 18.1 CE, el instrumento solamente captaría los rostros de aquellas personas registradas previamente por el sistema, es decir, de quienes tienen prohibida la entrada a determinados recintos deportivos para impedir su acceso. De forma que los parámetros del rostro de los demás espectadores no serían detectados y las imágenes grabadas por las cámaras de videovigilancia quedarían sujetas a lo dispuesto por la LO 4/1997. En este sentido, se eliminarían en el plazo de un mes, según lo previsto por el artículo 8.1 de la mencionada Ley, "salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública".

Los datos que se utilicen estarán sometidos a la LOPD, tal como establece el artículo 77 RD 203/2010–. Igualmente, las personas que tengan acceso a esos datos deberán observar la debida reserva, confidencialidad y sigilo, según lo dispuesto en el artículo 8.2 LO 4/1997. En el caso de encuentros internacionales, se debe fomentar el intercambio internacional de información por parte de las Fuerzas y Cuerpos de Seguridad, que se hará conforme al artículo 17 LCVD. El sistema se incorporaría en exclusividad en las cámaras dispuestas en la entrada del recinto y habrá de utilizarse únicamente cuando un encuentro sea calificado de alto riesgo, dejando de funcionar una vez concluida la disputa que motivó su utilización. Y, finalmente, en caso de que se produjese alguna detección errónea, la decisión última de permitir o denegar la entrada le corresponde al personal encargado de la vigilancia del encuentro, en vista de la documentación personal del individuo.

Por tanto, observando los serios problemas que pueden derivarse de la puesta en marcha de los sistemas de reconocimiento facial por la vulneración de ciertos derechos y libertades fundamentales, su uso debe

ser lo más limitado posible, como ocurre con cualquier nueva tecnología de características similares[42]. Por dicho motivo, antes de insertarse el reconocimiento facial en los dispositivos de seguridad de los recintos deportivos, es necesario desarrollar un texto normativo *ad hoc* en el que se recojan específicamente todos los límites y condiciones de su uso porque un empleo inadecuado podría comportar mayores problemas que beneficios, incluso cuando la seguridad pública está seriamente amenazada.

IV. CONCLUSIONES

Debido a las amenazas a la seguridad que se derivan de los encuentros deportivos calificados de alto riesgo, especialmente en el caso del fútbol, el reconocimiento facial podría constituir un instrumento de verificación de la identidad para garantizar el cumplimiento de la medida de prohibición de acceso a los recintos en los que se dispute un encuentro que adquiera tal consideración, con el fin de garantizar que no entren aquellas personas que tienen impuesta esta sanción por haber protagonizado previamente incidentes de violencia. Sin embargo, ello no viene a significar que se justifique la expansión de su uso por todo el perímetro del lugar en el que tienen lugar dichos encuentros, con el objetivo de vigilar y controlar a los aficionados pertenecientes a grupos ultra de los que se presuma la ejecución de actos de violencia, puesto que ello derivaría en una vigilancia excesiva que cercenaría los derechos y libertades fundamentales de los espectadores y no estaría justificada por cuestiones de seguridad, en tanto la misma en este caso, ya se vería adecuadamente salvaguardada con los sistemas de vigilancia convencionales previstos para tales eventos. De forma que la inserción de la técnica, incluso en los encuentros de riesgo debe limitarse, estando presente únicamente en los accesos a los recintos donde aquellos vayan a celebrarse. Así, la detección inmediata y a distancia de los sujetos que tienen denegada la entrada facilita la labor de los encargados de la vigilancia de los eventos deportivos y el uso de este mecanismo estaría justificado para lograr uno de los objetivos principales de la LCVD, concretamente el previsto en la letra b) de su artículo 1.1, como es el de "mantener la seguridad ciudadana y el orden público en los espectáculos deportivos". Empero, su uso tampoco puede extenderse a los demás encuentros, es decir, aquellos en

42. En este sentido, VALLS PRIETO, J., *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*, Dykinson, Madrid, 2017, p. 85.

los que no existe una amenaza severa a la seguridad pública, porque los perjuicios que conllevaría serían muy superiores a los beneficios en seguridad.

En este punto, ha de indicarse que en nuestro país no se podrían utilizar los sistemas biométricos, puesto que está prohibido por el RGPD en su artículo 9, cuando vayan dirigidos a identificar a una persona física. No obstante, dicha prohibición se puede salvar en atención a la letra g) del apartado segundo del mismo precepto, siempre y cuando el tratamiento de este tipo de datos sea necesario por la existencia de un interés público esencial que sea proporcional al objetivo perseguido, respete la protección de datos y establezca medidas para proteger los intereses y derechos fundamentales del individuo. En el caso que venimos analizando, el objetivo principal es el de identificar a los aficionados que tienen impuesta una medida de prohibición de acceso a un estadio en encuentros calificados de alto riesgo. Para ello, se debe poner a disposición de las FCSE y del Coordinador de Seguridad de la competición en cuestión, los datos biométricos de las personas afectadas que previamente deberán haber sido recogidos en una base de datos que cumpla con las garantías de protección de los derechos fundamentales que pueden verse en peligro.

No todo uso de esta tecnología está justificado y habrá de reunir los requisitos de idoneidad, necesidad y proporcionalidad. En el supuesto de los encuentros de alto riesgo, la limitación de los derechos estaría legitimada por la salvaguarda de la seguridad ciudadana pero no así para las demás disputas en las que no se prevén estallidos violentos, al suponer una medida desproporcionada. Esta afirmación trae causa de la consideración de que los sistemas de videovigilancia y los CCTV son un mecanismo adecuado al fin de preservación de la seguridad cuando no existe una amenaza seria y razonable a la seguridad. No obstante, debe indicarse que para que pueda instaurarse con ciertas garantías de éxito, han de tenerse en cuenta determinadas precauciones y límites que, a nuestro juicio, tienen que estar concretamente señalados en un documento específico para el uso de la técnica de reconocimiento facial en tales eventos y, mientras dicho texto no se haya desarrollado, consideramos que este mecanismo probatorio basado en la identificación personal para garantizar el cumplimiento de la medida de prohibición de acceso a recintos deportivos y control de estallidos violentos, no debería implementarse en nuestro país, puesto que del mismo podrían derivarse determinados excesos y conculcaciones de derechos fundamentales del todo inadmisibles en un Estado social y democrático de Derecho como el nuestro.

V. BIBLIOGRAFÍA

AA.VV., *Repuestas jurídicas al fraude en el deporte*, Dykinson, Madrid, 2017.

BARBA SÁNCHEZ, R., "La prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte. La seguridad en los estadios", en Palomar Olmeda, A., (Dir.), *Derecho del Deporte*, Aranzadi, Pamplona, 2013, pp. 877-965.

BARONA VILAR, S., "Inteligencia Artificial o la algoritmización de la vida y de la justicia: ¿Solución o problema?", *Revista Boliviana de Derecho,* n.° 28, 2019, pp. 18-49.

BENÍTEZ ORTÚZAR, I.F., "Derecho Penal y deporte en España. Especial referencia a la actividad violenta y a la actitud racista y xenófoba", *Revista Andaluza de Derecho del Deporte*, n.° 4, 2008, pp. 53-71.

BERNAL GARCÍA, F., "Dispositivos de seguridad privada en grandes eventos deportivos: encuentros calificados de alto riesgo", en García Tascón, M., y otros, (Eds.), *La seguridad deportiva a debate*, Dykinson, Madrid, 2020, pp. 195-200.

BREY, P., "Ethical Aspects of Facial Recognition Systems in Public Places", *Journal of Information, Communication and Ethics in Society*, vol. 2, 2004, pp. 97-109.

BUOLAMWINI, J., y GEBRU, T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research,* n.° 81, 2018, pp. 1-15.

COFFIN, J.S., e INGRAM, D., *Facial recognition system for security Access and identification,* Patente de Estados Unidos, n.° 5.991.429, Washington DC: Oficina de Patentes y Marcas de los Estados Unidos, 1999.

Comisión Europea, *Libro Blanco sobre Inteligencia Artificial– un enfoque europeo orientado a la excelencia y la confianza*, COM(2020) 65 final. Bruselas, 19 de febrero de 2020.

DÍAZ RODRÍGUEZ, V., "Sistemas biométricos en materia criminal: un estudio comparado", *Revista del Instituto de Ciencias Jurídicas de Puebla*, n.° 31, 2003, pp. 28-47.

DIÉGUEZ RODRÍGUEZ, J.M., "Revés para los planes del Atlético con el reconocimiento facial", *Iusport*, 22 de junio de 2021, recurso electrónico obtenido a través de la Web: https://iusport.com/art/63765/reves-para-los-planes-del-atletico-con-el-reconocimiento-facial, [última consulta: 13-1-22].

DOMINGO JARAMILLO, C., "Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana", *El Criminalista Digital. Papeles de Criminología*, n.° 9, 2021, pp. 20-37.

ETCHART, G., LUNA, L., LEAL, C., BENEDETTO, M., y ALVEZ, C., "Sistemas de reconocimiento biométricos, importancia del uso de estándares en entes estatales", *Repositorio Institucional de la* UNLP, 2011, pp. 1-5 (paginación propia).

GIL MEMBRADO, C., *Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado*, Wolters Reuters, Madrid, 2019.

HAURIE, L., "Suspendido el Betis-Sevilla: Jordán recibió un golpe con una barra lanzada desde la grada", *La Razón*, 15 de enero de 2022, recurso electrónico obtenido a través de la Web: https://www.larazon.es/deportes/futbol/20220115/s5rtxfoj4ncgvpoqqqa3xf2mjq.html, [última consulta: 17-1-22].

HOWARD-HASSMAN, R. E., "Human Security: Understanding Human Rights", *Human Rights Quarterly*, vol. 34, 2012, pp. 88-112.

INGRAM, D., *Facial recognition system for security Access and identification*, Patente de Estados Unidos, n.° 5.991.429, Washington DC: Oficina de Patentes y Marcas de los Estados Unidos, 1999.

INIOLUWA, D. R., y otros, "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing", *Actas de la Conferencia AAAI/ACM sobre IA, ética y sociedad*, 2020, pp. 145-151.

Instituto Nacional de Ciberseguridad (INCIBE), *Tecnologías biométricas aplicadas a la ciberseguridad*. *Una guía de aproximación para el empresario*, 2016.

ISHAY, M. R., *The History of Human Rights: from Ancient Times to the Globalization Era,* University of California Press, 2014.

LALIGA, "LaLiga implementa un nuevo sistema de acceso a las gradas de animación", 17 de agosto de 2015, recurso electrónico obtenido a través de la Web: https://www.laliga.es/noticias/laliga-implementa-un-nuevo-sistema-de-acceso-a-las-gradas-de-animacion, [última consulta: 15-9-21].

LA VANGUARDIA, "Comunicado: reconocimiento facial en el fútbol uruguayo", 26 de abril de 2018, recurso electrónico obtenido a través de la Web: https://www.lavanguardia.com/vida/20180426/443015024931/comunicado-reconocimiento-facial-en-el-futbol-uruguayo.html, [última consulta: 10-9-21].

LEARNED-MILLER, E., y otros, Facial recognition technologies in the wild: a call for a federal office, MacArthur Foundation, 2020.

MANN, M., y SMITH, M., "Automated Facial Recognition technology: recent developments and approaches to oversight", University of New South Wales Law Journal, vol. 40, n.° 1, 2017, pp. 121-145.

MERINO, M., "Estos son los métodos con los que intentan sortear el reconocimiento facial los defensores de la privacidad", *Xataka*, 10 de abril de 2019, recurso electrónico obtenido de la Web: https://www.xataka.com/inteligencia-artificial/estos-metodos-que-intentan-sortear-reconocimiento-facial-defensores-privacidad, [última consulta: 21-5-19].

MILLÁN GARRIDO, A.: *Legislación sobre violencia en espectáculos deportivos*, Junta de Andalucía, Sevilla, 2005.

– "Dispositivos de seguridad reforzados (Artículos 8.° a 14)", en Palomar Olmeda, A., Gamero Casado, E., (Coords.), *Comentarios a la Ley contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte*, Aranzadi, Navarra, 2008, pp. 207-254.

MORILLAS CUEVA, L., "Tratamiento jurídico-penal de la violencia con ocasión de espectáculos deportivos", en Palomar Olmeda, A., (Dir.), *Derecho del deporte*, Aranzadi, Pamplona, 2013, pp. 1044-1058.

NARANJO, J. C., "Reconocimiento facial, ¿el fin de la violencia en los estadios de fútbol?", *Crónica de Deportes*, 1 de mayo de 2018, recurso electrónico obtenido a través de la Web: https://cronicaglobal.elespanol.com/deportes/reconocimiento-facial-violencia-estadios-futbol_138041_102.html, [última consulta: 10-9-21].

NIETO GARCÍA, M., CUEVAS VALENCIA, R. E., y MARTÍNEZ CASTRO, J. M., "Diseño e implementación de un sistema de detección e identificación de aficionados violentos en estadios de fútbol", *Vínculos,* n.° 2, 2013, pp. 39-46.

Observatorio de la Seguridad de la Información, *Estudio sobre las tecnologías biométricas aplicadas a la seguridad*, Ministerio de Industria, Turismo y Comercio, 2011.

PIÑAR MAÑAS, J. L., "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio", *Documento de Trabajo (Laboratorio de Alternativas)*, n.° 147, 2009.

RODRÍGUEZ MONSERRAT, M., "La futura intrascendencia jurídica del concepto 'Aledaños' en la prevención de la violencia en el Deporte", *Revista Aranzadi de Derecho de Deporte y Entretenimiento*, n.° 68, 2020, pp. 1-19.

REDACCIÓN DE IUSPORT, "Comenzó a aplicarse la identificación biométrica para el acceso a los estadios", *Iusport*, 22 de agosto de 2015, recurso electrónico obtenido a través de la Web: https://iusport.com/art/9573/comenzo-a-aplicarse-la-identificacion-biometrica-para-el-acceso-a-los-estadios, [última consulta: 24-9-21].

RTVE, *Detenido el aficionado que supuestamente agredió a Joan Jordán en el Betis-Sevilla"*, 17 de enero de 2022, recurso electrónico obtenido a través de la Web: https://www.rtve.es/deportes/20220117/aficionado-lanzo-barra-betis-sevilla-jordan/2258860.shtml, [última consulta: 18-1-22].

THYS, S., VAN RANST-W., y GOEDEMÉ, T., "Fooling automated surveillance cameras: adversarial patches to attack person detection", *arXiv.org*, (Repositorio Institucional de la Universidad de Cornell), Nueva York, 18 de abril de 2019, pp. 1-7 (paginación propia).

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

– "El uso de Inteligencia Artificial para prevenir las amenazas cibernéticas", en Valls Prieto, J., (Coord.), *Retos jurídicos por la sociedad digital*, Aranzadi, Navarra, 2018, pp. 77-106.

YANG, W., WANG, S., HU, J., ZHENG, G., y VALLI, C., "Security and Accuracy of Fingerprint-Based Biometrics: A Review", *Symmetry*, vol. 11, n.° 141, 2019, pp. 1-19.

Sistemas biométricos (el reconocimiento facial en particular) y sus aplicaciones[1]

José Francisco Etxeberria Guridi

Catedrático de Derecho Procesal
Universidad del País Vasco/Euskal Herriko Unibertsitatea

SUMARIO: I. ECLOSIÓN DE LA BIOMETRÍA. II. LOS DATOS BIOMÉTRICOS Y SU PARTICULAR CONSIDERACIÓN (CATEGORÍAS ESPECIALES DE DATOS). 1. *El concepto de datos biométricos*. 2. *Clasificación de las técnicas biométricas (en función de las características sobre las que recaen)*. 2.1. Sistemas biométricos basados en características físicas o fisiológicas. A) Huellas dactilares. B) Reconocimiento facial. C) Reconocimiento vascular o patrón de venas. D) Reconocimiento de iris y análisis de retina. E) Reconocimiento de voz. F) Análisis de muestras de ADN. 2.2. Sistemas biométricos basados en características conductuales o de comportamiento. 3. *Datos biométricos como categorías especiales de datos y datos de carácter sensible*. III. APLICACIONES DE LOS SISTEMAS BIOMÉTRICOS. IV. ALGUNAS GARANTÍAS FRENTE AL USO DE SISTEMAS BIOMÉTRICOS. 1. *Evaluación de impacto relativa a la protección de datos*. 2. *Protección de datos desde el diseño y por defecto*. 3. *Consulta previa a la autoridad de control*. 4. *Un enfoque de la IA basado en los riesgos: la Propuesta de Reglamento IA y los sistemas biométricos*. V. BIBLIOGRAFÍA.

I. ECLOSIÓN DE LA BIOMETRÍA

Define la Real Academia española de la lengua el término "biometría" como el "estudio mensurativo o estadístico de los fenómenos o procesos

1. Realizado en el marco del Proyecto PROMETEO 2018/111 (Claves de la Justicia Civil y Penal en la sociedad del miedo: feminización, Inteligencia Artificial, Supranacionalidad, Eficiencia y Securitization).

biológicos". Se trata ésta de una definición amplísima aplicable en diversas disciplinas y que permite, entre otras muchas utilidades, distinguir en el ámbito de la biología una especie animal de otra. Esta holgura no impide apreciar con claridad los elementos definitorios de la biometría, esto es, medir fenómenos o procesos biológicos para identificarlos. Aplicados a las personas, no cambia un ápice el sentido de la definición. Esto es, se trataría de estudiar y medir determinados rasgos biológicos pertenecientes a las personas, lo que permite clasificarlas. Si lo que se mide son rasgos o características biológicas exclusivas de cada persona, además de su clasificación, será posible su identificación individualizada.

Alguno pudiera pensar que esa definición queda corta en la medida en que los sistemas biométricos a los que nos referiremos se centran también, además de en las características físicas, en comportamientos o en conductas. Nada de eso. La biología, los fenómenos biológicos, incluyen igualmente la conducta o comportamiento en su ámbito de estudio (biología del comportamiento o etología).

Aplicado todo lo anterior a las personas y limitado al estudio de los rasgos o características físicas o conductuales que permiten identificar e individualizar de forma exclusiva y excluyente a aquéllas, es cuando pueden surgir los inconvenientes, cuando no serías restricciones en sus derechos fundamentales. De una parte, los propios rasgos o características físicas pueden evidenciar por sí mismos algún padecimiento, enfermedad o discapacidad que la persona afectada quiera mantener fuera del conocimiento de terceros. De otra parte, puede ocurrir que la identificación biométrica incida negativamente en el ejercicio de los derechos del individuo, bien obstaculizándolos, bien ocasionando alguna clase de intimación que haga desistir a aquél del legítimo ejercicio de tales derechos. Si a ello se añade que en el tratamiento de los datos biométricos con empleo de la Inteligencia Artificial (IA) se produce algún tipo de sesgo o algún error, las consecuencias pueden resultar fatales.

Frente a tales riesgos para los derechos fundamentales de los ciudadanos, no es de extrañar que desde instancias normativas se hayan adoptado y se contemplen medidas jurídicas para evitar que aquéllos se materialicen. Entendemos que en el abordaje normativo de esta cuestión pueden distinguirse un antes y un después fijando como línea divisoria el Tratado de Lisboa. Nos referimos más concretamente al acervo normativo que sobre una serie de cuestiones esenciales entra vigor tras dicho Tratado. Esencialmente el conjunto de normas que se aprueban en materia de protección de datos personales que más adelante analizaremos y que se concretan, sobre todo, en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de

las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD en adelante)[2]. También en la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos[3]. Mediante estas dos normas esenciales

2. El RGPD deroga la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). El salto de una fuente normativa (Directiva) a otra (Reglamento) se justifica en los considerandos del RGPD. Se afirma que siendo válidos los objetivos y principios de la Directiva 95/46/CE, no se ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada. Estas diferencias en el nivel de protección de los derechos y libertades de las personas físicas pueden impedir la libre circulación de los datos de carácter personal en la Unión y suponer un obstáculo al ejercicio de las actividades económicas a nivel de la Unión (9). Se hace preciso garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, asegurando que el tratamiento de dichos datos sea equivalente en todos los Estados miembros (10). Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia (13). *Vid.* al respecto GARCÍA MEXÍA, P., "La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, (Dir. José Luis Piñar), Madrid, Reus, 2016, pp. 23 y ss. Sin embargo, es reconocido por no pocos autores que el RGPD otorga a los Estados miembros amplios márgenes de actuación que pueden traducirse en disensiones y disparidades de unos Estados frente a otros en la regulación interna, con la consiguiente incertidumbre jurídica. *Vid.* DELGADO CARRAVILLA, E. y PUYOL MONTERO, J., *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea*, Valencia, Tirant lo Blanch, 2018, pp. 14-16; GARCÍA MEXÍA, P., *Ibidem*, pp. 26-34.

3. Esta Directiva 2016/680 deroga otra norma europea previa sobre la materia, la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Este cambio de estadio tiene una mayor repercusión si nos atenemos al sistema de fuentes y al ámbito competencial, pues la Decisión Marco se adopta en el margo intergubernamental o conocido como Tercer Pilar (cooperación judicial y policial en materia penal) que se comunitariza. Además, el ámbito de aplicación de la Directiva es más amplio en comparación con la de la Decisión Marco, limitada al ámbito de transmisión de datos transfronterizo. *Vid.* las críticas y déficits de la anterior normativa en OUBIÑA BARBOLLA, S., "Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014", en *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea* (Dir. Ignacio Colomer), Cizur Menor (Navarra), Aranzadi, 2015, pp. 81 y ss.

se consagra en el ámbito de la UE una doble vía en la protección de los datos de carácter personal: una general y garantista en orden a preservar los derechos del titular de los datos personales ante la libre circulación de los mismos, y otra especial o excepcional, al margen de la regulación general y de las garantías en ella contempladas, relacionada con el tratamiento de los datos con fines de prevención, investigación y represión de delitos)[4].

Estos dos pilares normativos cuentan, además, con sustento específico en el Derecho originario de la UE[5]. Son destacables al respecto el expreso reconocimiento del derecho a la protección de los datos de carácter personal en la Carta de Derechos Fundamentales de la UE (CDFUE) cuyo art. 8 tiene por rúbrica, precisamente, "protección de datos de carácter personal" de modo diferenciado al ya clásico derecho al respeto de la vida privada y familiar que también tiene reconocimiento expreso en la CDFUE (art. 7). Junto al anterior, cabe citar igualmente el expreso reflejo en el Tratado de Funcionamiento de la UE (TFUE) del mencionado derecho (art. 16.1) habilitando al Parlamento Europeo y al Consejo para la adopción de las normas correspondientes al respecto con arreglo al procedimiento legislativo ordinario (art. 16.2 TFUE). Este último precepto se remite, a su vez, a las normas específicas que se adopten sobre idéntico derecho en el ámbito de la Política Exterior y de Seguridad Común (art. 39 TUE). Para completar el ciclo y extenderlo al ámbito de la cooperación judicial en materia penal y de la cooperación policial, ha de mencionarse la Declaración número 21 de las Declaraciones Anejas al Acta Final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, conforme a la cual, dicha Conferencia reconoce que "podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del Tratado de

4. *Vid*. GALÁN MUÑOZ, A., "La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea", en *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea,* (Dir. Ignacio Colomer), Cizur Menor (Navarra), Aranzadi, 2015, pp. 43-44; GONZALEZ CANO, I., "Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial penal en la Unión europea", en *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, (Dir. Ignacio Colomer), Cizur Menor (Navarra), Aranzadi, 2017, pp. 62-63.

5. No puede ignorarse, en todo caso, la trascendencia de la actividad del Tribunal de Justicia de las Comunidades Europeas (TJCE) incluso con anterioridad a la aprobación de cualquier normativa comunitaria sobre la materia. *Vid.* ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch/AEPD, 2006, pp. 225-230.

Funcionamiento de la Unión Europea, en razón de la naturaleza específica de dichos ámbitos"[6].

En las anteriores normas calificadas como esenciales en la configuración del nuevo acervo jurídico europeo sobre protección de datos personales –RGPD y Directiva 2016/680– hallamos por primera vez y con una consideración autónoma referencias expresas a los datos biométricos como categoría propia y con sujeción a un estatuto de protección más elevado que el resto de datos personales. Esto no quiere decir que con anterioridad a dichas esenciales normas el estado de la cuestión fuera yermo. Así, la *Commission National de l'Informatique et des Libertés* francesa (autoridad de control independiente de dicho país) ya se refería en su *Délibération* n.° 96.009 (27/02/1996) a la categoría de informaciones "biométricas" y a sus fines de identificación (físicas), pero también de revelación de la personalidad del individuo (comportamiento)[7]. Este interés por los datos biométricos no se reduce a determinadas autoridades independientes de control, también aparece en el seno de las instituciones europeas. Tendremos ocasión de analizar en el presente trabajo los relevantes Dictámenes del Grupo de Trabajo del Artículo 29 (GT29)[8] sobre tecnologías biométricas o reconocimiento facial[9] o algunos informes de la Agencia de los Derechos Fundamentales de la Unión Europea (FRA por sus siglas en inglés –*European Union Agency for Fundamentals Rights*–)[10].

Punto y aparte merece sobre este tema la Propuesta de Reglamento del Parlamento y del Consejo por el que se establecen normas armonizadas

6. *Vid.* sobre este marco legal de la UE sobre protección de datos con mayor amplitud GUTIÉRREZ ZARZA, A., "El Tratado de Funcionamiento de la Unión Europea (TFUE). Una base sólida para el tratamiento y la protección de los datos personales", en *Nuevas tecnología, protección de datos personales y proceso penal,* (Dir. Ángeles Gutiérrez), Madrid, La Ley, 2012, pp. 92-111.
7. CNIL, *Les informations personnelles issues de la voix et de l'image et la protection de la vie privée et des libertés fondamentales*, La Documentation française, París, 1996, pp. 18-19.
8. Así denominado por su regulación en el art. 29 de la Directiva 95/46/CE. Se trataba de un órgano consultivo e independiente compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión. Emitía dictámenes y recomendaciones sobre protección de las personas en lo que respecta al tratamiento de datos personales hasta la entrada en vigor del actual RGPD.
9. Dictamen 2/2012, de 22 de marzo, sobre reconocimiento facial en los servicios en línea y móviles (*Opinion 02/2012 on facial recognition in online and mobile services)*; Dictamen 3/2012, de 27 de abril, sobre la evolución de las tecnologías biométricas (*Opinion 3/2012 on developments in biometric technologies).* Pero mucho antes ya adoptó un "Documento de trabajo sobre biometría", de 1 de agosto de 2003 (WP 80).
10. Informes: *Under watchful eyes: biometrics, EU IT systems and fundamental rights* (2018); *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (2020).

en materia de inteligencia artifical (Ley de Inteligencia Artificial), de 21 de abril de 2021[11] (Propuesta de Reglamento IA). En esta propuesta de Reglamento se pone un particular foco de atención en lo que denomina sistemas biométricos no pudiendo ser más poderosa la razón para ello: la consideración que el tratamiento de estos sistemas tiene de alto riego.

II. LOS DATOS BIOMÉTRICOS Y SU PARTICULAR CONSIDERACIÓN (CATEGORÍAS ESPECIALES DE DATOS)

1. EL CONCEPTO DE DATOS BIOMÉTRICOS

Como se ha dicho, las normas básicas sobre protección de datos que constituyen la doble vía sobre la materia en el ámbito de la UE (RGPD y Directiva 2016/680) contienen como auténtica primicia un importante intento por definir los "datos biométricos" como una categoría autónoma de datos personales[12]. En particular, se refiere el primero de los cuerpos normativos como datos biométricos a los "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" [art. 4.14 RGPD]. No es casualidad que junto a la definición general de esa categoría de datos se mencionen a título de ejemplo las más significativas por ser las de uso más frecuente en el reconocimiento e identificación de personas (reconocimiento facial y por huellas dactilares).

La definición de datos biométricos que recoge el RGPD coincide, punto por punto, con la que se contiene en materia penal en la Directiva 2016/680, inclusión hecha de los ejemplos relativos a las imágenes faciales y huellas dactiloscópicas [art. 3.13]. También en la LO 7/2021 de transposición de dicha Directiva [art. 5.l].

Un documento de la trascendencia de la Propuesta de Reglamento IA, tan estrechamente vinculado al fenómeno biométrico, no puede sino definir de forma coincidente lo que ha de entenderse por datos biométricos, si

11. COM(2021) 206 final.

12. En su "Documento de trabajo sobre biometría" el Grupo de Trabajo del Art. 29 (GT29) consideró que los datos biométricos tenían perfecta cabida en la consideración de datos personales definida en la Directiva 95/46/CE [art. 2.a)] por estimarse "información sobre una persona física", salvo que los datos biométricos se almacenen de manera que no se pueda utilizar ningún medio razonablemente para identificar al interesado.

no quiere romperse la necesaria armonía entre textos jurídicos con numerosos puntos de convergencia. Como ocurre en los textos normativos antes indicados –y a diferencia de la Propuesta de Reglamento IA, están ya en vigor– la definición de datos biométricos es común con aquéllos, incluyendo los ejemplos paradigmáticos de datos biométricos –imagen facial y huellas dactiloscópicas– [art. 3.33]. Coincidencia de noción que se encarga de remarcar la Propuesta de Reglamento IA en su Considerando (7) añadiendo que la interpretación del concepto ha de hacerse en consonancia con tal sentido coincidente[13].

La definición del concepto de dato biométrico ha de ser valorado muy positivamente, pues aporta como primera cuestión seguridad jurídica acerca de su significado. Pero es cierto que, para evitar rigideces, los instrumentos normativos que cuentan afortunadamente con un capítulo destinado a las definiciones lo hacen con una considerable flexibilidad, máxime ante realidades pluri-estatales. Ello puede provocar un efecto distinto al deseado[14]. Algo similar ocurre con la definición de datos biométricos. El legislador europeo ha optado por una fórmula un tanto genérica, seguramente con el objeto de que sirva de acomodo a futuras realidades que encajen en los elementos sustantivos de la definición. Los ejemplos que se mencionan como datos biométricos en dichos instrumentos (imagen facial y dato dactiloscópico) son buena muestra de ello, ante el riesgo de que un hipotético listado de tales datos quedase obsoleto en poco tiempo.

Es por ello relevante y de gran ayuda recurrir a otros documentos institucionales que desarrollen estos conceptos. El GT29 en su importante "Documento de trabajo sobre biometría", de 1 de agosto de 2003 (WP80),

13. Acompaña a la Propuesta de Reglamento IA una Exposición de Motivos que en su apartado (1.2) titulado "Coherencia con las disposiciones existentes en la misma política sectorial" se justifica argumentando que, debido a su carácter horizontal, la Propuesta de Reglamento IA debe ser plenamente coherente con la legislación de la Unión vigente aplicable a los sectores donde ya se utilizan o es probable que se utilicen en un futuro próximo sistemas de IA de alto riesgo. Y en lo que ahora nos interesa, añade que "también está garantizada su coherencia con la Carta de los Derechos Fundamentales de la Unión Europea y el Derecho derivado de la Unión vigente en materia de protección de datos, (…). La propuesta debe entenderse sin perjuicio del Reglamento General de Protección de Datos [Reglamento (UE) 2016/679] y la Directiva sobre protección de datos en el ámbito penal [Directiva (UE) 2016/680], a los que complementa con un conjunto de normas armonizadas aplicables al diseño, el desarrollo y la utilización de determinados sistemas de IA de alto riesgo".

14. Muy consciente de este obstáculo, el Grupo de Trabajo del Art. 29 (GT29) adoptó el "Dictamen 4/2007, sobre el concepto de datos personales" pues apreciaba "una cierta incertidumbre y una cierta diversidad entre los Estados miembros en relación a aspectos importantes de este concepto que *pueden afectar al correcto funcionamiento del actual marco de protección de datos en diversos ámbitos*".

no definió formalmente los datos biométricos, pero sí indicó dos de sus elementos característicos: "tienen que ver con las características comportamentales y fisiológicas de una persona y pueden permitir su identificación inequívoca". Sí incorporó algo parecido a una definición el Dictamen 4/2007 del GT29: los datos biométricos "pueden definirse como propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad".

2. CLASIFICACIÓN DE LAS TÉCNICAS BIOMÉTRICAS (EN FUNCIÓN DE LAS CARACTERÍSTICAS SOBRE LAS QUE RECAEN)

Llama la atención que, en todas esas definiciones anteriores, junto a las más evidentes de carácter físico o fisiológico se haga mención igualmente a las características o rasgos conductuales, comportamentales, de la personalidad o incluso tics. Se pueden distinguir, pues, dos categorías diversas de técnicas biométricas, dependiendo de la naturaleza de las características sobre las que recaen[15]:

a) Por un lado, existen las técnicas basadas en aspectos físicos y fisiológicos que miden las características fisiológicas de una persona. Ya hemos visto que los principales instrumentos de la UE sobre protección de datos [art. 4.14 RGPD; art. 3.13 Directiva 2016/680] mencionan a modo de ejemplo vinculado a los datos biométricos los consistentes en las imágenes faciales y datos dactiloscópicos. Pero esta breve referencia ejemplificativa ha de considerarse precisamente como una llamada de atención relativa a los supuestos de uso más frecuente por el momento, pero no agotan, ni mucho menos, otras modalidades de datos biométricos, como veremos más adelante.

b) En segundo lugar, existen técnicas biométricas de comportamiento, basadas en la medición de aspectos comportamentales de una persona. El RGPD y la Directiva 2016/680 se refieren en esta categoría a la aplicación de técnicas biométricas a las "características conductuales" de la persona física.

15. Esta clasificación ya se formulaba en el "Documento de trabajo sobre biometría" de 2003 (WP80) del GT29 y se recoge posteriormente en el Dictamen 3/2012 del mismo GT29. De acuerdo con el primero de los documentos mencionados, la clasificación descansaría en que los datos utilizados fueran de carácter estable (características o rasgos físicos o fisiológicos) o datos dinámicos sobre el comportamiento.

Antes se ha advertido que uno de los riesgos vinculados a la pretensión de definir con precisión los conceptos que manejamos es que queden obsoletos de inmediato. De ahí que se opte en muchas ocasiones, con el riesgo de indeterminación que ello conlleva también, por fórmulas de mayor o menor flexibilidad. Esto es trasladable a la categorización de las tecnologías biométricas. Junto a las anteriores, se puede mencionar el uso más reciente de las técnicas basadas en elementos psicológicos, que incluyen la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico[16]. En tal sentido, los avances en tecnologías y redes informáticas están propiciando el incremento de lo que se considera "la segunda generación de datos biométricos basada en la utilización de los rasgos de comportamiento y psicológicos solos o combinados con otros sistemas clásicos que conforman sistemas multimodales" (biometría multimodal)[17].

2.1. Sistemas biométricos basados en características físicas o fisiológicas

Antes de entrar a mencionar algunas de las modalidades de tecnología biométrica conviene dejar sentado que existen una serie de propiedades o características comunes a todos los elementos biométricos empleados: a) por un lado, la universalidad, en el sentido de que ha de tratarse de un elemento existente en todas las personas; b) en segundo lugar, el elemento biométrico ha de caracterizarse por su unicidad o singularidad, esto es, ha de tratarse de un elemento distintivo para cada persona. Como se ha dicho, en las definiciones que se recogen del dato biométrico se destaca que ha de tratarse de una característica que permita o confirma la "identidad única" de una persona [art. 4.14 RGPD][18]; c) por último, la propiedad caracterizadora del elemento biométrico ha de ser permanente a lo largo del tiempo para cada persona, pues si es variable, pierde ese carácter distintivo necesario.

16. Aunque no se hiciera mención de dicha posibilidad en los iniciales documentos del GT29 (WP80 de 2003 sobre biometría), sí que aparece en los más recientes. Por ejemplo, en el Dictamen 4/2007 de dicho Grupo sobre el concepto de datos personales, de 20 de junio de 2007 (WP136) al definir los datos biométricos incluía los rasgos de la personalidad.
17. Dictamen 3/2012 de dicho Grupo sobre la evolución de las tecnologías biométricas, de 27 de abril de 2012 (WP193).
18. En efecto, no todos los elementos biométricos son equivalentes y el índice de diferenciación de una persona frente a otra es muy diverso, en función de la biometría utilizada. Indica el GT29 en su "Documento de trabajo sobre biometría" (WP80) que los elementos biométricos más distintivos parecen ser el ADN, la retina y las huellas digitales.

A) Huellas dactilares

Junto con las imágenes faciales constituyen el prototipo de datos biométricos conforme al RGPD y a la Directiva 2016/680 en su definición. Ya se utilicen técnicas de búsqueda de coincidencias diferentes (basadas en minucias o en correlación), es la más antigua y la más utilizada de las técnicas biométricas. Las ventajas atribuidas al dato biométrico en sí son su unicidad y su inalterabilidad y respecto de la técnica biométrica destaca su fácil integrabilidad, usabilidad, elevada precisión y bajo coste[19].

B) Reconocimiento facial

Puede definirse el reconocimiento facial como "el tratamiento automático de imágenes digitales que contienen las caras de personas con fines de identificación, autenticación/verificación o categorización de dichas personas"[20]. Este proceso incluye una serie de subprocesos[21]. La referencia al tratamiento técnico específico y la finalidad de identificación única de la persona resulta esencial en consonancia con el concepto de dato biométrico, para diferenciarlo de la mera captación de imágenes[22]. El uso de esta tecnología se encuentra muy extendido abarcando ámbitos muy diversos, tanto públicos, como privados. En la mayoría de las ocasiones se emplea con fines de control de acceso a determinados espacios físicos, pero también en servicios en línea o móviles[23]. Su empleo en el ámbito de la prevención, investigación, enjuiciamiento y ejecución de infracciones penales ha sido cuestionado por diferentes razones, sobre todo cuando se utiliza como sistema de identificación remota. Entre ellas, cabe mencionar el elevado índice de error, con altas tasas de falsos positivos o falsos negativos. Sin olvidar la incidencia de dicho uso en los derechos fundamentales del individuo, no exclusivamente en el derecho a la protección de datos personales.

19. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf.
20. Dictamen 2/2012 del GT29.
21. También descritos en el Dictamen 2/2012: a) obtención de la imagen; b) detección de la cara; c) normalización; d) extracción de características; e) registro; f) comparación.
22. En relación a las imágenes faciales, hace una importante aclaración el considerando (51) del RGPD: "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física".
23. El Dictamen 2/2012 del GT29 se refiere, en concreto, a esta última aplicación.

Esta tecnología avanza y el análisis de la imagen digital de la cara permite, no solamente identificar de manera unívoca al individuo, sino también características físicas y psicológicas tales como el origen étnico, emociones y bienestar. Estos desarrollos combinados, si fuera el caso, con otros sistemas biométricos pueden servir para detectar si las personas sometidas a tales procesos mienten o dicen la verdad[24]. Sobre esta cuestión, ya contempla la Propuesta de Reglamento IA consideraciones específicas, siendo el punto de partida su definición respecto del "Sistema de reconocimiento de emociones" y entendiendo que se trata de "un sistema de IA destinado a detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos" [art. 3.34]. Habiéndose propuesto como objeto el establecimiento, entre otros, de normas armonizadoras de transparencia aplicables a determinados sistemas de IA, entiende la Propuesta de Reglamento IA que entre estos últimos se encuentran los sistemas de IA de reconocimiento de emociones [art. 1.d)]. Estas obligaciones de transparencia se traducen en el deber que incumbe a los usuarios de tales sistemas de reconocimiento de emociones de informar del funcionamiento de dicho sistema a las personas físicas expuestas a él (art. 52.2).

Desde el punto de vista de su eficacia, se aduce, como se ha indicado, en las posibilidades de error por varias circunstancias. Afectan las condiciones en que son obtenidas las imágenes faciales, pues difieren de si se obtienen en un entorno controlado (iluminación, proximidad, no movimiento…) o si se obtienen a distancia ("sistema de identificación biométrica remota")[25]. No obstante tales dificultades, la tecnología permite

24. Sobre este último punto destaca el Proyecto *iBorderCtrl* relativo al sistema de detección inteligente de mentiras para reforzar las fronteras más concurridas de la UE (*Smart lie-detection system to tighten EU´s busy borders*); Proyecto n.° 700626 financiado por la UE en la que participan Luxemburgo (coord..), Grecia, Chipre, Reino Unido, Polonia, España, Hungría, Alemania y Letonia https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726. En su Informe sobre Inteligencia Artificial aplicada en materia penal, de 13 de julio de 2021, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (A9-0232/2021) informa que este proyecto ha sido ya testado en Letonia, Hungría y Grecia y parte de un análisis basado en IA de 38 micro gestos o expresiones de la cara. Dicha Comisión Parlamentaria insta a la Comisión en su Informe, refrendado por el Parlamento Europeo el 6 de octubre de 2021, a que deje de financiar investigaciones, aplicaciones o programas biométricos que puedan concluir probablemente en una vigilancia masiva e indiscriminada en espacios públicos.

25. Conforme a la Propuesta de Reglamento IA, se trataría de "un sistema de IA destinado a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada" [art. 3.36 en el capítulo de definiciones]. *Vid.* igualmente

realizar en las mencionadas condiciones de control deficiente identificaciones a partir de imágenes utilizando una amplia gama de cámaras, ángulos y condiciones de iluminación[26]. Otro de los inconvenientes que puede plantearse viene derivado de la facilidad con que los sujetos pueden realizar alteraciones en su apariencia (maquillaje, barbas, gafas, sombreros…) o las mismas pueden surgir con el transcurso del tiempo, lo que puede incidir en las capacidades de identificación del sistema y en posibles errores, sobre todo, si sumamos a ello que la captación de la imagen tiene lugar en un entorno no controlado[27].

No menos preocupantes son los riesgos de discriminación que por razón de género o pertenencia a un grupo racial u otro se están planteando en la aplicación práctica de las tecnologías de reconocimiento facial. Las posibles causas de discriminación pueden originarse como consecuencia de la calidad de los datos utilizados en el desarrollo de los algoritmos y del *software*, por un lado, y en el diseño, comprobación e implementación de los algoritmos utilizados para el reconocimiento facial, que pueden incorporar sesgos, consciente o inconscientemente[28], por otro lado. Estas deficiencias se traducen en un porcentaje de falsos positivos o falsos

---

el Informe de la Agencia de los Derechos Fundamentales de la UE (*EU Agency for Fundamental Rights* –FRA– en adelante), de 21 de noviembre de 2019, "*Facial recognition technology: fundamental rights considerations in the context of law enforcement*", pp. 7-8. Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

26. Dictamen 3/2012 del GT29, sobre la evolución de las tecnologías biométricas, p. 23.

27. En todo caso, las principales características faciales de una persona son estables en el tiempo y los sistemas pueden mejorar el reconocimiento recogiendo y asociando diferentes "caras" conocidas de una persona, como indica el Dictamen 3/2012 del GT29, sobre la evolución de las tecnologías biométricas, p. 25. Esas otras caras pueden proceder de bases de datos de imágenes faciales de índole privado que, a su vez, obtienen imágenes en internet y procedentes de redes sociales, imágenes de perfil, etc. La Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo se refiere en su Informe al uso por parte de autoridades competentes en materia penal y de servicios de inteligencia de la base de datos de *Clearview AI* conformada por imágenes (3 mil millones) obtenidas del modo indicado (Informe A9-0232/2021).

28. Como indica MARTÍNEZ MARTÍNEZ, R., "el sesgo no sólo se origina en la programación del algoritmo, en muchas ocasiones depende de los datos con los que se alimenta el sistema cuando aprende", "Inteligencia artificial desde el diseño", en *Revista catalana de dret públic*, n. 58, 2019, 73. FERNÁNDEZ HERNÁNDEZ, C., indica igualmente que los algoritmos reflejan con frecuencia objetivos e ideologías, "La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución", *Derecho Digital e Innovación*, n. 5, 2020, p. 2. Acerca igualmente de la posible existencia de errores o sesgos al elaborar los programas informáticos, *vid*. GUZMÁN FLUJA, V., "Sobre la aplicación de la inteligencia artificial a la solución de conflictos", en *Justicia civil y penal en la era global*, (Ed. Silvia Barona), Valencia, Tirant lo Blanch, 2017, p. 70.

negativos más elevado en el caso de personas afroamericanas o asiáticas que en el caso de las caucásicas, e igualmente más elevado en el caso de las mujeres pertenecientes a los primeros grupos raciales que al segundo[29]. Como ha evidenciado la FRA, una de las causas de discriminación radica en la calidad de los datos utilizados en el desarrollo de los algoritmos, el *software* de reconocimiento facial necesita ser alimentado de grandes cantidades de imágenes faciales; a mayor cantidad de imágenes, mayor precisión en las predicciones. Sin embargo, esa ingente cantidad de datos necesarios ha de satisfacer estándares mínimos de calidad, en el sentido de que las imágenes han de ser representativas de los diferentes grupos étnicos y de género[30].

Este conjunto de circunstancias nutre decisiones como la adoptada por el Parlamento Europeo en orden a solicitar una moratoria en la utilización de los sistemas de reconocimiento facial con fines de prevención, investigación, enjuiciamiento o ejecución en materia penal. Para revertir dicha situación sería necesario, según dicho acuerdo, que: a) los estándares técnicos resulten totalmente respetuosos con los derechos fundamentales; b) se garantice que los resultados que se derivan no son sesgados o discriminatorios; c) el marco legal contempla estrictas garantías frente a posibles abusos y estrictos controles y supervisión democráticos; y d) exista una evidencia empírica acerca de la necesidad y proporcionalidad para el desarrollo de dichas tecnologías[31]. En similares términos se han pronunciado recientemente en una opinión conjunta el Comité Europeo de Protección de Datos (EDPB –*European Data Protection Board*–) y el Supervisor Europeo de Protección de Datos (EDPS –*European Data Protection Supervisor*–). Con fecha de 18 de junio de 2021 adoptaron con motivo de la Propuesta de Reglamento IA elaborada por la Comisión el Dictamen conjunto 5/2021[32] en el que se propone una prohibición general de cualquier

29. *Vid*. al respecto los estudios y conclusiones de BUOLAMWINI, J.; GEBRU, T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", en *Proceedings of Machine Learning Research*, n. 81, 2018, pp. 1-15. Igualmente, acerca de la presencia de diferenciales demográficos (*demographic differentials*) en los algoritmos de reconocimiento facial, GROTHER, P.; NGAN, M.; HANAOKA, K., *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, U.S. Department of Commerce, 2019, [https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf].

30. FRA, "*Facial recognition technology…*", *cit*., p. 27. FRA, "*Data quality and artificial intelligence –mitigating bias and error to protect fundamental rights*" (2019).

31. En realidad, el Parlamento Europeo refrendó en su Resolución de 6 de octubre de 2021 el Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de 13 de julio de 2021, por 377 votos a favor y 248 en contra.

32. *EDPB-EDPS Joint Opinion5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).*

uso de IA que permita la identificación automatizada de características humanas en espacios accesibles al público y en cualquier contexto y, aunque se mencionan igualmente otras características biométricas o conductuales, resulta evidente que se prioriza en dicha prohibición la imagen facial[33].

C) Reconocimiento vascular o patrón de venas

Se fundamenta en el reconocimiento de las venas de la palma de la mano y de las de los dedos. Para ello se obtiene una plantilla de venas mediante una cámara de infrarrojos cuando el dedo o la mano se someten a la misma, dando lugar a una imagen postprocesada de la red vascular. El nivel de precisión del patrón de venas es muy elevado y además es estable en el tiempo, lo que hace un instrumento de identificación/autentificación similar al de las huellas dactilares[34].

D) Reconocimiento de iris y análisis de retina

El primero de los sistemas se fundamenta en las características del iris humano cuyos patrones vienen marcados desde el nacimiento y rara vez cambian y además presentan una gran cantidad de información (más de 200 propiedades únicas). Para ello ha de procederse al escaneado del iris con una cámara de infrarrojos. El hecho de que cada uno de los ojos de cada persona sea diferente, tiene como consecuencia que el reconocimiento de iris sea una de las tecnologías biométricas más resistentes frente a la suplantación[35].

El análisis de la retina presenta igualmente un elevado valor identificativo al basarse en el patrón de los vasos sanguíneos contenidos en la misma y en el hecho de que cada patrón sea único, incluso en el supuesto de los gemelos, ya que no depende de factores genéticos, y de que se mantenga

33. "*For all these reasons, the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces –such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals– in any context*" (apartado 32). De los ejemplos mencionados de características biométricas algunas resultan de difícil aplicación en espacios públicos accesibles y a distancia (remota).

34. Dictamen 3/2012 del GT29, sobre la evolución de las tecnologías biométricas, pp. 19-20.

35. *Vid.* Instituto Nacional de Ciberseguridad (INCIBE), *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario*, en ttps://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf [última consulta: 14-10-2021].

invariable en el tiempo. Esta técnica presenta el inconveniente, en el caso de su uso con fines de identificación –no de verificación o autenticación–, de que requiere la total colaboración de la persona afectada para someterse al proceso de captura de la imagen[36].

E) Reconocimiento de voz

Estas aplicaciones utilizan sistemas de inteligencia artificial como redes neuronales para aprender a identificar la voz. Los algoritmos deben medir y estimar la similitud entre varias muestras. Los patrones de voz son bastante estables y pueden ser eficaces en la identificación inequívoca de una persona. Aunque existen determinados riesgos que pueden dificultar los resultados de estos patrones de voz, por ejemplo, cuando se modifica la misma de forma deliberada o existen ruidos de fondo[37].

F) Análisis de muestras de ADN

En muchos de los documentos que se manejan sobre los datos biométricos aparecen mencionados los datos genéticos o vinculados a los resultados de los análisis de ADN. Es verdad que, tanto el RGPD como la Directiva 2016/680, consideran los datos genéticos como una categoría autónoma y distinta a la de los datos biométricos. En consideración de tales textos, son datos genéticos los "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona" [arts. 4.13 RGPD; 3.12) Directiva 2016/680].

Sin embargo, los datos genéticos aparecen confundidos con frecuencia con los datos biométricos en no pocos documentos utilizados. Así, el "Documento de trabajo sobre biometría" del GT29 (WP80) incluye los resultados de los análisis de muestras de ADN entre los datos biométricos. Sin embargo, excluye de su ámbito de consideración tales datos alegando que "la generación de un perfil de ADN en tiempo real como instrumento de autenticación no parece posible actualmente". Con el tiempo, se han reconsiderado estas objeciones o impedimentos. Hemos mencionado que, tanto la Resolución del Parlamento Europeo, como el Dictamen conjunto 5/2021 del EDPB y del EDPS, incluyen en sus propuestas de prohibición

36. *Vid.* Instituto Nacional de Ciberseguridad (INCIBE), *Tecnologías biométricas…*, *cit.*
37. *Vid.* Dictamen 3/2012 del GT29, sobre la evolución de las tecnologías biométricas, p. 26; Instituto Nacional de Ciberseguridad (INCIBE), *Tecnologías biométricas…*, *cit.*

y moratoria del empleo de tecnologías de IA para la identificación automatizada de las personas en espacios accesibles al público a partir de sus características biométricas los perfiles de ADN. Enmendando, de alguna manera, su anterior documento de trabajo sobre biometría (WP80), considera el GT29 que uno de los principales cambios experimentados en las tecnologías de elaboración de perfiles de ADN es la reducción del tiempo necesario para las operaciones de correspondencia y de secuenciación del ADN. De este modo, añade, es muy probable que en un futuro próximo sea posible elaborar perfiles de ADN y realizar correspondencias de muestras en tiempo real (o casi) lo que será el punto de partida para el desarrollo de sistemas de autenticación o identificación biométrica del ADN con mayores niveles de precisión en comparación con las huellas dactilares, la voz o el reconocimiento facial[38].

2.2. Sistemas biométricos basados en características conductuales o de comportamiento

Las definiciones que de los datos biométricos recogen los distintos instrumentos normativos europeos sobre protección de datos personales coinciden en incluir los correspondientes a las características conductuales. También lo hace la Propuesta de Reglamento IA, como no podía ser de otra manera. Son diversas las modalidades o tecnologías biométricas basadas en el comportamiento, que tienen en común tener como fundamento una determinada acción o actuación de la persona.

Cabe mencionar la "firma biométrica" que consiste en la técnica biométrica que mide la conducta de una persona según lo expresado por la dinámica de su firma manuscrita. Pero, mientras que el reconocimiento de firma manuscrita tradicional se basa en el análisis de las características fijas o geométricas de la imagen visual de la firma (aspecto de la firma), la firma biométrica hace referencia al análisis de las características dinámicas de la firma (cómo se hizo la firma). Las características dinámicas que suele medir de ordinario un sistema de firma biométrica son la presión, el ángulo de escritura, la velocidad y aceleración del bolígrafo, la formación de las letras, la dirección de los rasgos de la firma y otras características dinámicas únicas. Es posible que los sistemas de reconocimiento de firma combinen los dos aspectos mencionados de la misma, el análisis estático y el dinámico[39].

38. Dictamen 3/2012 sobre la evolución de las tecnologías biométricas.
39. Dictamen 3/2012 del GT29, sobre la evolución de las tecnologías biométricas, pp. 29-30; Instituto Nacional de Ciberseguridad (INCIBE), *Tecnologías biométricas…*, *cit.*

Suele también citarse como sistema biométrico basado en el comportamiento el de "reconocimiento de escritura de teclado", técnica basada en la existencia de un patrón de escritura en teclado que es permanente y propio de cada individuo. Así, se mide la fuerza de tecleo, la duración de la pulsación y el período de tiempo que transcurre desde que se presiona una tecla y otra[40].

Existen igualmente "técnicas biométricas basadas en la forma de caminar" de las personas. La misma es objeto de grabación y sometimiento a un proceso analítico que genera una plantilla biométrica única derivada de dicho comportamiento. Aunque se trate de una tecnología todavía en desarrollo[41], es verdad que esta tecnología biométrica puede ser utilizada de forma remota, sin que el sujeto afectado sea consciente de ello. Por este motivo, las técnicas biométricas basadas en la forma de caminar de las personas se incluyen entre las que el Parlamento Europeo y la Opinión conjunta 5/2021 del EDPB y EDPS consideran como de conveniente prohibición cuando se utilizan en espacios accesibles al público con fines identificativos.

3. DATOS BIOMÉTRICOS COMO CATEGORÍAS ESPECIALES DE DATOS Y DATOS DE CARÁCTER SENSIBLE

Siguiendo con el enfoque de los sistemas biométricos desde la perspectiva de la protección de los datos personales[42], hay que añadir que los biométricos pertenecen a la categoría especial de datos y por ese motivo están sujetos a restricciones en su tratamiento y a garantías adicionales en los supuestos excepcionales en que sea posible[43]. No puede ser más

40. Instituto Nacional de Ciberseguridad (INCIBE), *Tecnologías biométricas…*, *cit.*

41. *Vid.* Instituto Nacional de Ciberseguridad (INCIBE), *Tecnologías biométricas…*, *cit.*

42. El enfoque más comprensivo es el mencionado. De este modo, la Resolución del Parlamento Europeo, de 6 de octubre de 2021 (ratificatoria del Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de 13 de julio de 2021) afirma que en la medida en que "el procesamiento de grandes cantidades de datos personales constituye el corazón de la IA, el derecho a la protección de la vida privada y el derecho a la protección de datos personales se aplican a todas los ámbitos de la IA, y el marco jurídico de la Unión sobre protección de datos y privacidad ha de ser satisfecho en su totalidad" (apartado 1). También sobre este extremo y en similares términos se pronuncia la Comisión en su *"Libro Blanco sobre inteligencia artificial –un enfoque europeo orientado a la excelencia y la confianza"*, de 19 de febrero de 2020, COM (2020) 65 final. Igualmente VIDA FERNÁNDEZ, J., "Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea", en *Sociedad digital y Derecho*, (Dirs. Tomás De La Cuadra; José Luis Piñar), Madrid, Ministerio de Industria, Comercio y Turismo, Red.es/BOE, 2018, p. 215.

43. CANO RUIZ, I., "Artículo 9. Categorías especiales de datos", en *Protección de Datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantías Digitales (en relación con el RGPD)*, (Dirs. Mónica Arenas; Alfonso Ortega), Madrid, Sepín, 2019, p. 82.

categórico el RGPD cuando dispone que "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de *datos genéticos*, *datos biométricos* dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física" (art. 9.1 RGPD). Esta restricción en el tratamiento de esta categoría de datos es coincidente en la Directiva 2016/680[44].

La rotunda prohibición de tratamiento se matiza posteriormente en el caso del RGPD con una serie de excepciones a la misma (art. 9.2 RGPD) y que con frecuencia se remite en su especificación al Derecho de la UE o de los Estados miembros. En el uso de la mencionada discrecionalidad el legislador español (LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales) ha resuelto que, con el fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no baste para levantar la prohibición del tratamiento de determinados datos –ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico– (art. 9.1). Para el resto de categorías especiales de datos, en particular respecto de los datos biométricos, no se contiene ninguna garantía adicional similar[45]. Ello hubiera sido posible de conformidad con el propio RGPD, pues dispone que con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud, "los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones" (art. 9.4).

Con anterioridad a estas disposiciones básicas de la Unión, la Directiva 95/46/CE no contemplaba, como se ha dicho, en la relación de categorías

44. En la misma se dispone que el tratamiento de esta clase de datos "solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando: a) lo autorice el Derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos" (art. 10). La relación de datos personales especiales es similar a la de la Directiva 95/46/CE, salvo la incorporación *ex novo* de la referencia, precisamente, a los datos biométricos y genéticos. La categoría de dato biométrico no estaba contenida en la Propuesta inicial de RGPD elaborada por la Comisión; su inclusión en el art. 9.1 RGPD fue resultado de una enmienda del Parlamento Europeo. *Vid.* al respecto MEDIDA GUERRERO, M., "Categorías especiales de datos", en *Tratado de Protección de Datos. Actualizado con la LO 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, (Dir. Artemi Rallo), Valencia, Tirant lo Blanch, 2019, p. 254.

45. Lo que ha dado pie a la doctrina a afirmar la existencia de dos especies diferentes de datos sensibles. *Vid.* MERCADER UGUINA, J. R., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3.ª ed., Madrid, Francis Lefebvre, 2019, p. 27.

especiales de datos del art. 8 los de carácter biométrico o genético. Pese a ello, se advertía en documentos del GT29 que algunos datos biométricos podían considerarse "sensibles" en el sentido del mencionado precepto. En concreto los reveladores del origen racial o étnico o los datos relativos a la salud. Para evaluar el carácter sensible de los datos tratados por un sistema biométrico ha de tenerse en cuenta igualmente el contexto del tratamiento[46]. En esa categoría de datos sensibles se incluyeron los datos de ADN en la medida en que son a menudo portadores de datos relativos a la salud o pueden revelar el origen racial o étnico. A través del reconocimiento vascular o mediante patrón de venas podrían obtenerse datos sensibles relativos a la salud. El reconocimiento de imágenes faciales puede también ser expresivo del origen racial o étnico o, en su caso, de alguna enfermedad. Incluso se apunta algún estudio que evidencia que también las imágenes de las huellas dactilares pueden revelar información étnica de la persona[47].

III. APLICACIONES DE LOS SISTEMAS BIOMÉTRICOS

De la propia definición de los sistemas biométricos y de los datos de idéntica naturaleza a partir de los cuales se construyen los primeros, puede deducirse incuestionablemente que tales sistemas son de aplicación con la finalidad de identificar de forma unívoca a una persona. Esta finalidad general conduce a una relación inagotable de posibles aplicaciones en cualquier ámbito de nuestra existencia, por muy cotidiana que sea o afecte a la actuación del Estado en su función de prevención, investigación o represión penal. A esa finalidad primigenia se le han sumado recientemente otras en las que la identificación o verificación pasa a un segundo plano[48].

a) Medio de autenticación/verificación biométrica (*one-to-one comparison*). En este supuesto se comparan dos plantillas biométricas pertenecientes supuestamente a la misma persona para determinar si, efectivamente, la persona que aparece en ambas es la misma. Este proceso de búsqueda de correspondencias "uno-a-uno" admite varias modalidades. Por ejemplo, lo usual resulta que una de las plantillas biométricas se halle previamente

46. Aunque el RGPD y la Directiva 2016/680 incluyan actualmente los datos biométricos y genéticos en la categoría especial de datos, diferenciaba el "Documento de trabajo sobre biometría" del GT29 (WP80) unos de otros al afirmar que "esto no significa que todo tratamiento de datos biométricos vaya a incluir necesariamente datos sensibles".
47. Dictamen 3/2012 GT29 sobre la evolución de las tecnologías biométricas.
48. *Vid.* "Documento de trabajo sobre biometría" del GT29; Dictamen 3/2012 GT29 sobre la evolución de las tecnologías biométricas.

almacenada y en el momento en que interese se obtenga la segunda plantilla. Pero no siempre resulta necesario el almacenamiento de dicha plantilla en un fichero[49].

b) Medio de identificación biométrica (*one-to-many comparison*). En estos supuestos, la plantilla biométrica que se obtiene se compara con otras plantillas biométricas almacenadas en uno o en varios ficheros o bases de datos, esto es, se trataría de un proceso de búsqueda de correspondencias "uno-a-varios". En esta modalidad de identificación se pueden distinguir aquellos supuestos en los que la comparación se realiza frente a un fichero o base de datos en el que conste que figura la plantilla biométrica de la persona a identificar (*closed-set identification*), de aquéllos en los que la búsqueda de correspondencia se realiza sin tener constancia de dicha circunstancia (*open-set identification*).

c) Medio de categorización/segregación biométrica (*matching general characteristics*). En esta modalidad el sistema biométrico actúa como un proceso que permite extraer características de un individuo con el objeto de determinar su pertenencia a un grupo con características predefinidas a fin de adoptar una medida específica. En este caso, lo importante no es identificar o verificar a un individuo, sino asignarle automáticamente una categoría determinada (la pertenencia a un grupo étnico, la edad, el sexo, etc.).

Esta última finalidad en el uso de sistemas biométricos ha sido incorporada expresamente a la Propuesta de Reglamento IA. En el apartado de definiciones, el "Sistema de categorización biométrica" viene a consistir en "un sistema de IA destinado a asignar a personas físicas a categorías concretas, como un sexo, edad, color de pelo, color de ojos, tatuajes, origen étnico u orientación sexual o política, en función de sus datos biométricos" [art. 3.35]. De forma conjunta con los sistemas de reconocimiento de emociones ya mencionados, los sistemas de categorización biométrica entran dentro del objeto de la Propuesta de Reglamento IA al establecer "normas armonizadas de transparencia aplicables" a tales sistemas de IA [art. 1.d)]. Las obligaciones de transparencia a que se refiere el precepto que inaugura la Propuesta se traducen en que los "usuarios (…) de un

49. La FRA se refiere, por ejemplo, a la posibilidad de que las características biométricas se incorporen a un documento de identidad o a un pasaporte, de modo que en los controles fronterizos se escanee la imagen que aparece en el documento y se compare mediante tecnologías de reconocimiento facial con la imagen que se obtiene en momento real en el punto de control, "*Facial recognition technology…", cit.*, p. 7. Utilizado en los servicios móviles y en línea (reconocimiento facial, de voz, de huella dactilar) puede funcionar conforme a esta modalidad "en lugar de un nombre de usuario y contraseña" para acceder a un servicio o a un dispositivo en línea o móvil y la plantilla (Dictamen 2/2012 del GT29, p. 3).

sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él"[50].

En la medida en que esta nueva modalidad de aplicación de sistemas biométricos no persigue una concreta e inequívoca identificación de las personas, pudiera parecer que resulta más inocua que las anteriores. Sin embargo, el riesgo de que las actuaciones derivadas de la categorización puedan desembocar en consecuencias discriminatorias no puede evitarse. Por tal motivo, el Dictamen conjunto 5/2021 del EDPB y del EDPS propone una prohibición de los sistemas de categorización biométrica en categorías o grupos relativos al origen étnico, el género o la orientación política o sexual, o que causen algún tipo de discriminación proscrita por el art. 21 de la CDFUE, incluyendo tales supuestos en las prácticas de IA prohibidas a que se refiere el art. 5 de la Propuesta de Reglamento IA, tanto por parte de las autoridades públicas, como por las entidades privadas.

IV. ALGUNAS GARANTÍAS FRENTE AL USO DE SISTEMAS BIOMÉTRICOS

Como ha quedado de manifiesto hasta ahora, el empleo de sistemas biométricos en sus distintas finalidades y aplicaciones no puede evitar el riesgo de que se produzcan colisiones con los derechos y libertades de los individuos. El derecho a la privacidad, el derecho a la protección de datos personales o el derecho a la no discriminación por ciertos motivos han estado presentes a lo largo de este trabajo. Es obvio que los riesgos en determinados supuestos se incrementan. De ahí que sean precisas garantías complementarias a las generales sobre la materia, por ejemplo, las derivadas de la pertenencia de los datos biométricos y de los genéticos a las categorías especiales de datos. El marco jurídico de la protección de datos personales puede resultar inspirador al respecto, considerando la nueva perspectiva de responsabilidad proactiva. Podrían, sin ánimo exhaustivo, mencionarse, además de las medidas contempladas con carácter general, las siguientes atendiendo a la naturaleza de los datos biométricos a que nos referimos[51].

50. Así lo dispone el art. 52.2 de la Propuesta de Reglamento IA que excluye dicha obligación cuando se trate, lógicamente, de sistemas de IA utilizados para la categorización biométrica autorizados por la ley para fines de detección, prevención e investigación de infracciones penales. Añade el Considerando (70) de la misma Propuesta que la información y las notificaciones deben facilitarse en formatos accesibles para las personas con discapacidad.

51. *Vid*. sobre este punto DE HOYOS SANCHO, M., "El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea", *Revista General de Derecho Procesal*, n. 55, 2021, pp. 21 y ss.

1. EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

Constituye una de las garantías que resultan aplicables en los procesos en los que se emplean sistemas biométricos[52]. Tanto la RGPD (arts. 35-36), como la Directiva 2016/680 (arts. 27-28), disponen que "cuando sea probable que un tipo de tratamiento, *en particular si utiliza nuevas tecnologías*, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales" (art. 35.1 RGPD). Esta evaluación de impacto se requerirá en determinados supuestos[53], entre los que se menciona el tratamiento a gran escala de las categorías especiales de datos (art. 35.3.b RGPD), por ejemplo, los datos biométricos, o cuando se trata de la observación sistemática a gran escala de una zona de acceso público (art. 35.3.c RGPD)[54]. La AEPD ha incluido los "tratamientos que impliquen el uso de *datos biométricos* con el propósito de identificar de manera única a una persona física" en el listado de tipos de tratamiento que requieren una evaluación de impacto previa[55]. Con anterioridad, el GT29 en

52. MIRALLES LÓPEZ, R., hace una breve referencia a los orígenes anglosajones de la evaluación de impacto (*Privacy Impact Assessment*) y la cuestión de si estos procesos se han de regular normativamente o si su promoción se atribuye a las autoridades de control; también sobre ciertos antecedentes como los controles previos del art. 20 Directiva 95/46 o el Dictamen 5/2010 del GT29; *vid.* "La evaluación de impacto relativa a la protección de datos (comentario al artículo 35 RGPD)", en *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*, (Dir. Antonio Troncoso), Tomo I, Cizur Menor (Navarra), Civitas/Thomson Reuters, 2021, pp. 2140-2141.

53. Como subraya MIRALLES LÓPEZ, R., y el Considerando (76) del RGPD ha de tratarse de criterios o métodos objetivos de valoración; *ibidem.*

54. Así lo entienden la FRA, "*Facial recognition technology*…", *cit.*, p. 26 y el EDPB en sus Directrices 3/2019, p. 37.

55. Conforme al RGPD, las autoridades de control establecerán y publicarán un listado de tipos de operaciones de tratamiento que requieren una evaluación de impacto. Este listado ha de ser comunicado al CEPD (art. 35.4). Originariamente el tratamiento de datos biométricos a que nos referimos no constaba en el listado remitido por la AEPD al CEPD. Éste, en su Dictamen 6/2019, de 12 de marzo, recomendó en sus conclusiones la inclusión de los datos biométricos en la lista definitiva. En dicho Dictamen el CEPD aclara que el listado de supuestos en los que se requerirá una evaluación de impacto según el art. 35.3 RGPD no es exhaustiva ("se requerirá en particular") e insta a la AEPD a incluir expresamente en el listado de tratamientos que requieren dicha evaluación de impacto el tratamiento de datos biométricos con el propósito de identificar a una persona de manera única y el tratamiento de datos genéticos para cualquier fin, siempre que concurra, además, al menos alguno de los restantes supuestos. En el caso que nos ocupa, sobre todo tratándose del empleo de tecnología de reconocimiento facial en espacios abiertos al público, concurren sin duda los supuestos de "tratamientos que impliquen la observación, monitorización,

sus "Directrices sobre la evaluación relativa a la protección de datos (EIPD) y para determinar si el tratamiento 'entraña probablemente un alto riesgo´ a efectos del Reglamento (UE) 2016/279" –última versión de 4 de octubre de 2017– exponía como ejemplo que el tratamiento de "cualquier tipo de datos biométricos" podría considerarse pertinente para la elaboración de una lista de conformidad con el art. 35.4 RGPD.

2. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

Tanto en el marco del RGPD (art. 25) como en el de la Directiva 2016/680 (art. 20) significa que el responsable del tratamiento aplicará, bien en el momento de determinar los medios de tratamiento, como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para hacer efectivos los principios de protección de datos. Como evidencia el art. 28.1 LO 3/2018, la adopción de estas medidas puede suponer la valoración de realizar la evaluación de impacto a la que nos hemos referido o la consulta previa a la autoridad de control a que nos referiremos[56]. En todo caso, nos interesa destacar en estos momentos la incidencia que desde esta perspectiva tiene el principio de exactitud de los datos personales (art. 5.1 RGPD y 4 LO 3/2018) y que afecta a esta materia por los riesgos de sesgo y discriminación mencionados *supra.* Como afirma contundentemente la AEPD en su Documento "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción", de febrero de 2020, que "la exactitud es particularmente crítica cuando el tratamiento está basado en información biométrica, como IA sobre reconocimiento facial, huellas dactilares, voz, etc".[57].

---

supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público" (n.° 3), "tratamientos que impliquen el uso de datos a gran escala" (n.° 7), "tratamientos que impliquen la utilización de nuevas tecnologías" (n.° 10) e incluso, teniendo en cuenta el carácter indiscriminado de la captación y tratamiento de imágenes, "tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social" (n.° 9). Tampoco se puede obviar que el empleo de estas técnicas puede disuadir al ciudadano de ejercitar otros derechos que suelen, por lo general, desarrollarse en espacios públicos o externos (reunión, manifestación, libertad ideológica o sindical, etc.) con lo cual podría concurrir el último de los supuestos comprendidos en el listado de la AEPD ("tratamientos de datos que impidan a los interesados ejercer sus derechos" –n.° 11–).

56. El mismo precepto se refiere en el apartado 2 a la consideración los "mayores riesgos" que pueden producirse en una serie de supuestos entre los que se menciona el tratamiento no meramente incidental de las categorías especiales de datos de los arts. 9 y 10 RGPD y de la LO 3/2018.

57. La AEPD menciona tres factores que pueden influir en la exactitud de los datos: a) la propia implementación de sistema IA; b) el conjunto de datos de entrenamiento o

3. CONSULTA PREVIA A LA AUTORIDAD DE CONTROL

También resultan oportunas las previsiones relativas a la conveniencia de realizar una consulta previa con las autoridades de control antes de proceder al tratamiento cuando "una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo" (arts. 36.1 RGPD y 26 Directiva 2016/680)[58]. Esta obligación de consulta previa estaba contemplada de alguna manera en el art. 20.2 Directiva 95/46. Si la autoridad de control considera que el tratamiento sometido a consulta conforme al art. 36.1 podría infringir el RGPD, procederá a asesorar como corresponda al responsable del tratamiento o, en su caso, al encargado (art. 36.2 RGPD)[59].

4. UN ENFOQUE DE LA IA BASADO EN LOS RIESGOS: LA PROPUESTA DE REGLAMENTO IA Y LOS SISTEMAS BIOMÉTRICOS

La Propuesta de Reglamento IA al que nos hemos referido a lo largo de este trabajo se propone alcanzar un equilibrio entre varios fines de interés general, por un lado, asegurar un nivel elevado de protección de la salud, la seguridad y los derechos humanos, y, por otro lado, garantizar la libre circulación transfronteriza de bienes y servicios basados en la IA, impidiendo que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el futuro Reglamento lo autorice expresamente. Con tal objetivo, entre las varias opciones de intervención reguladora con sus distintos grados, la Propuesta de Reglamento opta por un marco regulatorio que únicamente se aplique a los sistemas de IA de alto riesgo, con la posibilidad de que todos los proveedores de sistemas de IA que no sean de alto riesgo sigan un código de conducta.

---

validación que puede estar viciado con errores, información deliberadamente errónea o sesgos que imposibilitan que las inferencias sean correctas; c) la evolución sesgada del modelo de IA si se implementan técnicas adaptativas.

58. Así se han pronunciado también la FRA, "*Facial recognition technology…*", *cit.*, p. 26 y el CEPD en sus Directrices 3/2019, p. 37.

59. *Vid.* con detalle al respecto DE SALVADOR CARRASCO, L. A., "La consulta previa (comentario al artículo 36 RGPD)", en *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*, (Dir. Antonio Troncoso), Tomo I, Cizur Menor (Navarra), Civitas/Thomson Reuters, 2021, pp. 2213-2234; RECIO GAYO, M., "Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control", en *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, (Dir. José Luis Piñar), Madrid, Reus, 2016, pp. 363-365.

Siguiendo el enfoque basado en los riesgos la Propuesta distingue entre los usos de la IA que generan a) un riesgo inaceptable, b) un riesgo alto, y c) un riesgo bajo o mínimo. Respecto de los primeros usos, la Propuesta dedica un Título II específico relativo a las "prácticas de IA prohibidas" (art. 5.1). En lo que ahora nos concierne, se incluyen entre dichas prácticas prohibidas "el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley" [letra d)]. Se hace absolutamente indispensable en este caso acudir al apartado de definiciones que contempla la Propuesta de Reglamento IA para comprender adecuadamente el significado del supuesto a que se refiere la prohibición. El carácter "remoto" hace referencia a los sistemas de IA destinados a identificar a personas físicas "*a distancia* comparando sus datos biométricos con los que figuran en una base de datos de referencia" (art. 3.36). La identificación en "tiempo real" implica que "la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa". Este término engloba no sólo la identificación instantánea, sino también demoras mínimas limitadas, con el objeto de evitar su elusión (art. 3.37). De otra parte, la identificación biométrica remota en tiempo real, que resulta prohibida en principio, ha de tener lugar en "espacios de acceso público". Al igual que en la definición anterior, y con el mismo propósito garantista, la Propuesta de Reglamento IA opta por una definición amplia de lo que ha de entenderse por tales espacios, pues incluye "cualquier lugar físico accesible para el público, con independencia de que deban cumplirse determinadas condiciones para acceder a él" (art. 36.39)[60]. Por último, la finalidad a la que atiende la identidad biométrica es la de aplicación de la ley, esto es, la finalidad de represión penal[61].

Esta prohibición no es, sin embargo, absoluta, pues acto seguido y en idéntico inciso se añaden una serie de excepciones a la prohibición siempre

60. Algo más que ilustrativa resulta sobre este punto el Considerando (9) de la Propuesta de Reglamento IA. En el mismo se matiza que estos espacios no están condicionados por la naturaleza de la propiedad, que puede ser pública o privada. También se indica que no pierde el carácter de espacio accesible al público la sujeción a condiciones como la exigencia de una entrada o restricciones por motivos de edad. Estarían comprendidos, por lo tanto, espacios como cines, teatros, tiendas o centros comerciales. Sí excluiría, en cambio, del ámbito de aplicación de este supuesto el que no se trate de un espacio físico –espacios en línea–.

61. Poco acertada traducción al castellano del término *law enforcement* que obliga a acudir, en este caso necesariamente, al capítulo de definiciones [art. 3.41] en el que se aclara que se refiere a "las actividades realizadas por las autoridades encargadas de la aplicación de la ley para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública". En otras versiones más expresivas: *à des fines répressives* o *zu Strafverfolgungszwecken*.

que ello resulte "estrictamente necesario" para alcanzar uno o varios de los siguientes objetivos: i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos; ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista; iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo, para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro[62].

Siendo admisible en determinados supuestos el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de represión penal resulta necesario que en esos casos se respeten una serie de presupuestos o condiciones que justifiquen las consecuencias restrictivas que para los derechos de los ciudadanos pudieran derivarse. Ha de reconocerse que las cuestiones y requisitos mínimos que justifican las excepciones a la prohibición se encuentran detallados en la Propuesta más allá de lo que resulta habitual. Así, se hace referencia a la necesidad y proporcionalidad de su uso, en particular a las limitaciones temporales, geográficas y personales (art. 5.2). También se hace referencia a la necesaria autorización previa por parte de la autoridad judicial o una autoridad administrativa independiente que la otorgarán, a su vez, previa solicitud motivada (art. 5.3). La referencia a una autoridad administrativa "independiente" puede resultar perturbadora. Sin embargo, la alternativa a una autorización judicial adquiere pleno sentido desde el punto de vista del ordenamiento español, pues la LO 4/1997, de 4 de agosto, reguladora del uso de videocámaras por las FF. y CC. de Seguridad, contempla que la autorización para instalar de videocámaras ha de ir precedida de un informe preceptivo y vinculante de las Comisiones de Videovigilancia que estarán presididas por el Presidente del TSJ de la Comunidad Autónoma correspondiente y en la que "la presencia de miembros dependientes de la Administración autorizante no podrá ser mayoritaria" (Preámbulo)[63].

62. Así como los dos primeros objetivos parecen ser respetuosos con los principios de especialidad y el de proporcionalidad en sentido estricto –se refieren a búsquedas "selectivas" de víctimas "concretas", amenaza "específica, importante e inminente"– el tercero de los objetivos se nos antoja excesivamente genérico y amplio y contrapuesto a los mencionados principios, pues el listado de eurodelitos es extenso y el supuesto concreto incluye subjetivamente a los que han cometido o se sospecha que han cometido tales delitos.

63. La composición y funcionamiento de tales Comisiones se remite a lo que se disponga reglamentariamente (art. 3.2). En la medida en que las Comunidades Autónomas con competencia en la materia pueden regular reglamentariamente esta cuestión, resulta

Estas Comisiones tienen indudablemente naturaleza administrativa, pero su particular composición permite equipararla a las que se refiere el art. 53 de la Propuesta de Reglamento IA[64]. Sin olvidar que en determinados ordenamientos, como el portugués, corresponde a la autoridad de control independiente sobre protección de datos (*Comissão Nacional de Protecção de Dados*) informar con carácter preceptivo y vinculante el uso de videocámaras por las FF. y CC. de Seguridad[65].

Mención aparte merece la trascendencia reconocida al principio de previsión legal en el texto de la Propuesta de Reglamento IA. El cumplimiento de lo hasta ahora contemplado no implica, sin más, la admisibilidad del uso de sistemas de identificación biométrica remota en tiempo real y con fines de represión legal. Los Estados miembros, en el ámbito de su margen de discrecionalidad, "podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente" dicho uso. Los límites y las condiciones indicadas constituyen el marco mínimo de admisibilidad, pero en caso de que así se decida, los Estados han de establecer "en sus respectivos Derechos internos *las normas detalladas* necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones (…), así como a la supervisión de éstas" (art. 5.4)[66].

Como se ha adelantado en otros apartados, habiéndose recibido satisfactoriamente con carácter general la iniciativa legislativa que supone la

---

que la composición a que nos referimos es diversa, pero siempre con la limitación de mayorías indicada. *Vid.* al respecto la composición contemplada en el Decreto vasco 168/1998, de 21 de julio, el RD 596/1999, de 16 de abril y el Decreto catalán 134/1999, de 18 de mayo.

64. *Vid.* al respecto DE LA IGLESIA CHAMARRO, A., "Las Comisiones de Garantías de la Videovigilancia", *Revista de Derecho Político*, n. 68, 2007, pp. 217 y ss.; ETXEBERRIA GURIDI, J. F., "La Comisión de Videovigilancia y Libertades del País Vasco: funciones y experiencias", en *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales*, (Coords. José Francisco Etxeberria; Ixusko Ordeñana), Valencia, Tirant lo Blanch, 2011, pp. 107 y ss. Plantea mayores objeciones a la independencia de las Comisiones MARTÍNEZ MARTÍNEZ, R., *Tecnologías de la información, policía y Constitución*¸ Valencia, Tirant lo Blanch, 2001, pp. 346 y 349.

65. Conforme a la Ley n. 1/2005, de 10 de enero, que regula la utilización de videocámaras por los fuerzas y servicios de seguridad en lugares públicos, tanto para las instalaciones fijas (art. 3), como para las instalaciones móviles (art. 6).

66. La claridad y la precisión que se derivan del principio de previsión legal y al que se refiere la Propuesta de Reglamento IA, no se satisfacen con la autorización contemplada de forma excesivamente genérica en el art. 10.2 de la LO 7/2021 al referirse al "tratamiento de categorías especiales de datos personales" entre los que se incluyen los biométricos. Dice sin más tal precepto, que las autoridades competentes "podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física" con fines de represión penal. Pero sin especificar las condiciones y presupuestos precisos para tal tratamiento.

Propuesta de Reglamento y el enfoque basado en los riesgos por el que ha optado la misma, las discrepancias son sustanciales acerca de la admisibilidad de la práctica de identificación biométrica remota en tiempo real y en espacios públicos. Sobre este punto la Resolución del Parlamento Europeo de 6 de octubre de 2021 propone la prohibición de tales prácticas hasta que no se satisfagan los requisitos mínimos indicados más arriba. El Dictamen conjunto 5/2021 del EDPB y del EDPS coincide con idéntica propuesta de prohibición, argumentando que las excepciones a la prohibición del art. 5.1.d) están planteadas defectuosamente y añadiendo a la prohibición el uso de tales sistemas biométricos remotos en tiempo real en el "espacio online".

V. BIBLIOGRAFÍA

ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch/AEPD, 2006.

ARIAS POU, M., "Definiciones a efectos del Reglamento General de Protección de Datos", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (Dir. José Luis Piñar), Madrid, Reus, 2016.

BUOLAMWINI, J.; GEBRU, T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", en *Proceedings of Machine Learning Research*, n. 81, 2018.

CANO RUIZ, I., "Artículo 9. Categorías especiales de datos", en *Protección de Datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantías Digitales (en relación con el RGPD)*, (Dirs. Mónica Arenas; Alfonso Ortega), Madrid, Sepín, 2019.

DE HOYOS SANCHO, M., "El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea", *Revista General de Derecho Procesal*, n. 55, 2021.

DE LA IGLESIA CHAMARRO, A., "Las Comisiones de Garantías de la Videovigilancia", *Revista de Derecho Político*, n. 68, 2007.

DE MIGUEL ASENSIO, A., "Libro Blanco sobre inteligencia artificial: evolución del marco normativo y aplicación efectiva", *La Ley Unión Europea*, n. 79, 2020.

DELGADO CARRAVILLA, E. y PUYOL MONTERO, J., *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea*, Valencia, Tirant lo Blanch, 2018.

DE SALVADOR CARRASCO, L. A., "La consulta previa (comentario al artículo 36 RGPD)", en *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*, (Dir. Antonio Troncoso), Tomo I, Cizur Menor (Navarra), Civitas/Thomson Reuters, 2021.

ETXEBERRIA GURIDI, J. F., "La Comisión de Videovigilancia y Libertades del País Vasco: funciones y experiencias", en *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales*, (Coords. José Francisco Etxeberria; Ixusko Ordeñana), Valencia, Tirant lo Blanch, 2011.

FERNÁNDEZ HERNÁNDEZ, C., "La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución", *Derecho Digital e Innovación*, n. 5, 2020.

GALÁN MUÑOZ, A., "La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea", en *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea,* (Dir. Ignacio Colomer), Cizur Menor (Navarra), Aranzadi, 2015.

GARCÍA MEXÍA, P., "La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad,* (Dir. José Luis Piñar), Madrid, Reus, 2016.

GONZÁLEZ CANO, M.ª I., "Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial penal en la Unión Europea", en *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, (Dir. Ignacio Colomer), Cizur Menor (Navarra), Aranzadi, 2017.

GROTHER, P.; NGAN, M.; HANAOKA, K., *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects, U.S. Department of Commerce, 2019*, [https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf].

GUTIÉRREZ ZARZA, A., "El Tratado de Funcionamiento de la Unión Europea (TFUE). Una base sólida para el tratamiento y la protección de los datos personales", en *Nuevas tecnología, protección de datos personales y proceso penal,* (Dir. Ángeles Gutiérrez), Madrid, La Ley, 2012.

GUZMÁN FLUJA, V., "Sobre la aplicación de la inteligencia artificial a la solución de conflictos", en *Justicia civil y penal en la era global*, (Ed. Silvia Barona), Valencia, Tirant lo Blanch, 2017.

MARTÍNEZ MARTÍNEZ, R., *Tecnologías de la información, policía y Constitución*¸ Valencia, Tirant lo Blanch, 2001.

MARTÍNEZ MARTÍNEZ, R., "Inteligencia artificial desde el diseño", en *Revista catalana de dret públic*, n. 58, 2019.

MEDIDA GUERRERO, M., "Categorías especiales de datos", en *Tratado de Protección de Datos. Actualizado con la LO 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, (Dir. Artemi Rallo), Valencia, Tirant lo Blanch, 2019.

MERCADER UGUINA, J. R., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3.ª ed., Madrid, Francis Lefebvre, 2019.

MIRALLES LÓPEZ, R., "La evaluación de impacto relativa a la protección de datos (comentario al artículo 35 RGPD)", en *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*, (Dir. Antonio Troncoso), Tomo I, Cizur Menor (Navarra), Civitas/Thomson Reuters, 2021.

OUBIÑA BARBOLLA, S., "Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014", en *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea* (Dir. Ignacio Colomer), Cizur Menor (Navarra), Aranzadi, 2015.

RECIO GAYO, M., "Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control", en *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, (Dir. José Luis Piñar), Madrid, Reus, 2016.

VIDA FERNÁNDEZ, J., "Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea", en *Sociedad digital y Derecho*, (Dirs. Tomás De La Cuadra; José Luis Piñar), Madrid, Ministerio de Industria, Comercio y Turismo, Red.es/BOE, 2018.

Derecho fundamental a la protección de datos de carácter personal en el ámbito jurisdiccional e Inteligencia Artificial. En especial la LO 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[1]

Iñaki Esparza Leibar[2]

Catedrático de Derecho Procesal

Universidad del País Vasco/Euskal Herriko Unibertsitatea

SUMARIO: I. INTRODUCCIÓN, CONCEPTO Y NECESIDAD DE LA INTELIGENCIA ARTIFICIAL. II. APROXIMACIÓN A LA REALIDAD, EL ESCENARIO DE PARTIDA. PASADO Y PRESENTE. III. IMPULSO DE LA TECNOLOGÍA EN EL CAMPO DE LA JUSTICIA. INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS. EL ROL DE LA COMISIÓN EUROPEA, EN

1. La presente contribución constituye una obligada actualización del trabajo de ESPARZA LEIBAR, I., "La Inteligencia Artificial y el derecho fundamental a la protección de datos de carácter personal", en la obra colectiva dirigida por Silvia Barona Vilar: *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021.

2. Miembro del Consejo Consultivo de la Agencia Vasca de Protección de Datos/DBEB, como experto en derechos fundamentales. Miembro del Grupo de Investigación Consolidado del "Sistema Interuniversitario Vasco", Título del Proyecto: "Derechos Fundamentales y Unión Europea. Especial referencia al espacio de libertad, seguridad y justicia de la Unión Europea". Miembro del grupo de investigación del Proyecto: "Trata de seres humanos y esclavitud: investigación, enjuiciamiento y protección procesal de las víctimas", financiado por el Ministerio de Ciencia, Innovación y Universidades.

PARTICULAR, EL LIBRO BLANCO DE LA UE. PRESENTE Y FUTURO. IV. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y PROCESO PENAL. LA LO 7/2021. V. CONCLUSIONES Y PROPUESTAS. VI. REFERENCIA BIBLIOGRÁFICA.

I. INTRODUCCIÓN, CONCEPTO Y NECESIDAD DE LA INTELIGENCIA ARTIFICIAL

Interesarse por la Inteligencia Artificial (IA en lo sucesivo), trabajar sobre el tema, aprehenderlo y tratar de no quedarse rápidamente desfasado constituye, hoy en día, algo parecido a remar en un canal de aguas bravas, donde solo flotar es ya un éxito. Estamos en pleno *big bang* interdisciplinar, internacional e integral de aplicaciones de la IA, algunas de las cuales tienen que ver muy directamente con nuestro ámbito de interés. Para contrarrestar esa enorme fuerza que nos impulsa de manera casi incontrolable y que está cambiando profundamente la realidad que hemos conocido, es muy conveniente una actitud serena y un método sensato que permitan la sedimentación y consolidación de las cuestiones más básicas, sobre la que podamos construir una propuesta –probablemente efímera pese a todo– realista, viable y segura[3].

Las páginas que siguen constituyen, en consecuencia, el acta sucinta de una reflexión que recientemente venimos haciendo en relación con uno de los temas transversales más relevantes de los últimos tiempos, y que presenta un largo recorrido. En ocasiones (cada vez menos) nos sentimos un poco fuera de lugar al hablar de IA, algoritmos, perfiles, heurística, predicciones, tecnología, etc., pero no podemos dejar de hacerlo ya que, como veremos, ya está incorporada a actividades objeto de estudio del derecho procesal y, sobre todo, porque el potencial al respecto es tan impresionante como indiscutible[4].

3. La IA adquiere pleno sentido cuando constatamos que la realidad es que el 60% de la población del planeta –el porcentaje se incrementa sin pausa cada día y es incluso superior en el caso de las personas jurídicas– es usuaria –muchas veces dependiente– de la tecnología digital que, desde cierta perspectiva, es, en su funcionamiento, un sumidero de datos personales, por lo que todo ello debe ser disciplinado. En este afán por hacer las cosas mejor, la IA debe ser parte importante de la solución.

4. En uno de nuestros, no tan antiguos, trabajos desglosábamos con bastante pormenor los contenidos del proceso debido, jerarquizándolos y advirtiendo de su constante evolución y expansión, al tratarse de un concepto dinámico. *Vid.,* ESPARZA LEIBAR, I., "El proceso debido como único modelo aceptable para la resolución de conflictos en un estado de derecho y como presupuesto para la globalización", capítulo en la obra colectiva, *El Derecho Procesal español del siglo XX. A golpe de tango (Homenaje a Juan Montero Aroca)*. Tirant lo Blanch, Valencia 2012, pp. 319 y ss. Pues bien, el concepto IA no se menciona allí de forma explícita. Hoy debería estar incorporado, al menos,

Ante la objeción, digamos cualitativa, de que el de la IA es un ámbito que no tiene contacto con el mundo del derecho en general, y del derecho procesal en particular, de que se trata de ámbitos no coincidentes, en suma. Afirmamos que dicha objeción debe ser desestimada sin paliativos, y que se trata de hacer aquí una prospección realista sobre hasta dónde puede llegar a imbricarse la IA en el mundo del derecho, y la percepción, ciertamente provisional, es que no se atisban límites apriorísticos[5]. Hay que abordarlo, por tanto, para poder hacer un aprovechamiento correcto, lo que, entre otras cosas, significa acorde con las exigencias de la protección de datos de carácter personal, que son la materia prima, el combustible del que la IA, en buena medida, se nutre. Sin datos personales que la alimenten, la IA pasaría a ser algo completamente inútil, en especial en el ámbito de la jurisdicción[6].

No hemos encontrado todavía una definición de IA plenamente convincente y, sobre todo, clara aunque en cualquier propuesta deben aparecer las ideas de artefactos (máquinas, algoritmos,..) que ayudan al ser humano, *v. gr*., haciendo predicciones, y que, en esa misión de ayuda, van incorporando y avanzando en nuevos planteamientos, actuando en mayor o menor medida por sí mismos, de manera independiente, aunque siempre debería hacerse bajo la supervisión humana, sin cuya intervención carecería, la IA, de estrategia fiscalizable y, consecuentemente, de efectividad jurídica.

Un cajero automático sería un ejemplo, ya consolidado y clásico, aunque innovador en su día, al que confiábamos nada menos que la gestión (cálculos, operaciones, disponibilidad, etc.) de nuestro dinero. ¿Quién, de cierta edad, no comprobaba que el cajero lo había hecho bien? Ahora ya lo damos por supuesto, a nadie inquieta ya que una máquina se ocupe de ello, lo inquietante sería que nos privaran de ese indiscutible avance. También la propuesta automatizada de liquidación del IRPF, realizada por la correspondiente administración tributaria, podría servirnos para ilustrar

como algo "deseable", y mañana su concurso será sin duda "imprescindible" para que la calidad de la justicia pueda alcanzar y mantener los estándares de un estado de derecho.

5. BARONA VILAR, S., "Inteligencia artificial o la algoritmización de la vida y de la Justicia: ¿Solución o problema?", en Revista Boliviana de Derecho, n.° 28, julio de 2019. *Vid.,* también NIEVA FENOLL, J., Inteligencia artificial y proceso judicial, Madrid, Marcial Pons, 2018.

6. Hablamos de la IA aplicada al específico campo de la justicia y el derecho, ya que su implementación en otros campos de actividad, *v. gr*., el de los vehículos para transporte (terrestres, marítimos o aéreos) sin conductor o tripulación, esta no se nutre en lo sustancial de datos de carácter personal, sino de otras variables que no requieren de un tratamiento tan específico.

el desarrollo de la idea. Es decir, el de IA es un concepto relativo, lo que era y ha sido superado, que sigue siendo IA en un estadio incipiente ya metabolizado; lo que cada día se incorpora, y lo que se espera de cara al futuro, el potencial que es imposible de determinar ahora en sus exactos límites, aunque se puede atisbar.

Como punto de partida tomamos prestada la siguiente definición: "La inteligencia artificial es una rama de la computación como puede ser la traumatología en la medicina. Dentro de esta rama lo que encontramos es un conjunto de algoritmos, de recetas matemáticas y lógicas que tratan de simular comportamientos inteligentes. Hay varias áreas dentro de la inteligencia artificial: para tratar de procesar el lenguaje, reconocer y analizar imágenes, predecir basándonos en datos, segmentar ciertas fuentes de información, etc". Preguntada la entrevistada sobre cuáles son sus principales áreas de aplicación, responde: "Las principales áreas podrían ser cualquiera, realmente. Todos aquellos sitios donde necesitemos automatizar una serie de procesos, segmentar ciertas fuentes de información, predecir, analizar el lenguaje, analizar imágenes… Básicamente puedes usar la inteligencia artificial en cualquier área[7]".

Es decir, hablamos de una tecnología transversal, al servicio de cualquier actividad humana a cuya mejora puede contribuir decisivamente, en los términos que veremos, siempre que se utilice correctamente. En lo que a los derechos fundamentales se refiere, y en particular a los datos de carácter personal concierne –datos fiscales, académicos, sanitarios, judiciales, etc.– no será legítima ni posible la utilización de la IA si no es plenamente respetuosa con los mismos. Aquí encontramos el límite infranqueable en su aplicación.

Aplicada a nuestro ámbito, el derecho procesal, la IA tendría potencialmente aplicación en tres niveles o campos diferenciados de actuación, todos ellos con repercusión en derechos fundamentales.

1. IA y procedimientos automatizados. Tramitación y gestión. Actividad de archivo y documentación, notificaciones y actos de comunicación, llevanza de vistas, verificación de la integridad documental, tratamiento de datos, etc. Lo que repercutiría, por ejemplo, en la reducción de las dilaciones indebidas, o en la evitación de suspensiones, incidiendo en la mejora de la Tutela judicial efectiva. Las nuevas formas de tramitación y gestión significan también la necesidad de garantizar un nuevo e integral tratamiento de los datos

7. Entrevista de Aitor Berás a Ana Jiménez Castellanos, socia en el área de Technology Consulting en EY, Artificial Intelligence & Data Science. En Infolibre, el 27.09.2020. "¿Qué es la inteligencia artificial?".

personales involucrados. Hitos verificables de la incorporación de nuevas tecnologías a la justicia serían: el expediente judicial electrónico, de 2011[8], la plataforma de notificaciones electrónicas LexNET, de 2015[9], que permite en todo momento y lugar la relación y el intercambio de información entre operadores jurídicos, o la firma electrónica, de 2003[10], como instrumento para la comprobación de la procedencia e integridad de las telecomunicaciones.

Podemos apreciar que el volcado de la actividad a los nuevos soportes y procedimientos –hacia la justicia virtual, que es el objetivo al que se apunta– avanza a buen ritmo, con el necesario soporte normativo y sin generar problemas insuperables, siendo plenamente conscientes de que son necesariamente los datos de carácter personal, el objeto de protección preferente –mejor de tratamiento– en esta gestión y tramitación automatizadas[11].

2. IA e investigación. En relación específicamente con el proceso penal. Cuya implementación tendrá repercusión en los derechos fundamentales a la intimidad, al secreto de las comunicaciones y a la protección de datos de carácter personal, que habrá que equilibrar con el derecho a investigar los delitos del que es titular el estado y que es fuente de legitimidad. La cuestión se centra, en lo que más nos interesa, en constatar que la obtención de datos de carácter personal es, mediante las tecnologías existentes, potencialmente masiva, casi ilimitada, y en afirmar que su tratamiento, en todo momento, debe ofrecer plenas garantías. El jurisdiccional es un ámbito donde la IA correctamente aplicada podría resultar de gran utilidad.

3. IA y procedimientos autónomos. Diagnóstico y proposición. Análisis del caso concreto, precedentes, jurisprudencia y normas de aplicación, sobre cuya base se realizan propuestas de resolución. Su correcta implementación incidirá en la reducción de las dilaciones indebidas. Además, podría significar, indirectamente, un refuerzo

8. Definido por la Ley 18/2011, de 5 de julio, como: "El conjunto de datos, documentos, trámites y actuaciones electrónicas, así como grabaciones audiovisuales correspondientes a un procedimiento judicial, cualquiera que sea el tipo de información que contengan y el formato en el que se hayan generado".
9. RD 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET.
10. Ley 59/2003, de 19 de diciembre, sobre firma electrónica.
11. Específicamente sobre tramitación automatizada y algunos de los problemas que plantea, *vid.*, PÉREZ ESTRADA, M.J., "La tramitación automatizada del proceso", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021, pp. 489 y ss.

de la independencia e imparcialidad de los jueces. Este es el nivel más novedoso, el objeto de atención estratégica ahora, que requiere de una reflexión tranquila y profunda, dadas sus implicaciones, pero que resulta insoslayable para mejorar la calidad de la justicia, a nuestro juicio.

Lo que es constatable en este momento es que se está produciendo un volcado integral de todos los procedimientos que sustentan la gestión de la cotidianeidad del funcionamiento del Poder Judicial –lo que hemos llamado tramitación automatizada de grandes volúmenes de datos, que incluye la autentificación, la trazabilidad, la mejora de búsquedas e intercambio de información, etc.– a sistemas de los que la IA es un componente esencial (constituye, *v. gr.*, buena parte de la labor del Centro de Documentación Judicial, CENDOJ[12]).

Lo que es previsible es que, en materia de diagnóstico y proposición, en general, y en lo relativo a la gestión del proceso penal en particular, el volcado a aplicaciones basadas en el empleo de IA, se va a producir –de hecho, se está fomentando con determinación desde todas las instituciones involucradas, sobre todo de las europeas– de forma rápida e integral. Esto nos parece imparable y, correctamente gestionado, muy beneficioso para el estado de derecho y sus ciudadanos.

El tercer elemento de la ecuación es que ese volcado o migración que ya se está produciendo, requiere, con carácter previo e imprescindible, de un parque o infraestructura normativa suficiente y clara, que garantice que el cambio se realizará con todas las garantías y de un modo seguro. Aquí es donde apreciamos claroscuros que nos generan preocupación –si bien es cierto que se constatan importantes avances– a los que nos referiremos más adelante[13].

12. *Vid.*, al respecto, European Commission, *Study on the use of innovative technologies in the justice field*, de septiembre de 2020, pp. 214 y 215.

13. En el lado positivo, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de éstos. Que se adapta al ordenamiento jurídico español por medio de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Recientemente, y es una excelente noticia pese a las turbulencias y retrasos, se ha producido la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. Disposición que debe dotar de la necesaria infraestructura normativa al correcto y seguro tratamiento de datos de carácter personal obtenidos de forma masiva en este ámbito. Lo importante es que el 27 de mayo de 2021 el BOE publicaba

Lo que, finalmente, es indiscutible es que la ciencia siempre ha contribuido al avance de las sociedades, y la Justicia no puede quedar al margen de dicha aportación, no nos lo podemos permitir. Es así que debemos encontrar la forma correcta de servirnos de la IA para mejorar la tutela judicial efectiva, la calidad del servicio que el Poder Judicial brinda a la ciudadanía y, con él, reforzar la legitimidad del estado de derecho[14].

La idea, mejor el axioma del que partimos, es que no hay desarrollo posible de la IA sin datos, sin una enorme cantidad de datos, entre ellos los datos de carácter personal, como tampoco es posible una gestión eficiente, segura y correcta de dichos datos, especialmente los de carácter personal, sin IA. Son, por tanto, conceptos simbióticos e interdependientes, siendo su relación la que debe ser disciplinada y su resultado fiscalizable.

II. APROXIMACIÓN A LA REALIDAD, EL ESCENARIO DE PARTIDA. PASADO Y PRESENTE

El escenario de partida nos muestra que efectivamente la IA tiene un enorme potencial para ayudarnos a hacer las cosas mejor, como multitud de variadas iniciativas y experiencias demuestran, por lo que constituye una oportunidad, que no podemos dejar pasar, para la correcta gestión de la actividad jurisdiccional en general, y para lo relativo a la protección de datos, en particular. Nos hemos referido ya a realidades consolidadas como el expediente judicial electrónico, la firma electrónica o LexNET, que constituyen, sin duda, pasos en la buena dirección[15].

---

la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

14. Alertando sobre algunos de los peligros derivados de una IA incorrectamente concebida, diseñada o implementada, *vid.,* GÓMEZ COLOMER, J.L., *La contracción del Derecho Procesal Penal*, Valencia, Tirant lo Blanch, 2020. Centrándose en la indispensable e insustituible independencia judicial, que propicia el estado de derecho, *vid.,* GÓMEZ COLOMER, J.L., "Unas reflexiones sobre el llamado "juez-robot", al hilo del principio de la independencia judicial", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021, pp. 243 y ss. A este respecto, también resulta muy ilustrativa y conveniente la explícita mención de las exigencias ineludibles –en términos de derechos fundamentales– para una correcta e inofensiva aplicación de la IA. *Vid.,* MARTÍN DIZ, F., "Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021, pp. 65 y ss.

15. El Anteproyecto de Ley de Medidas de Eficiencia Procesal del Servicio Público de Justicia, de 15 de diciembre de 2020 es, por ahora, el último hito a tener en cuenta en este propósito de alcanzar la eficiencia, en tanto apuesta por "la necesidad de acelerar

Pero hay mucho más, un salto cualitativo que algunos han empezado a dar y en el que todos estamos concernidos. De hecho, está ocurriendo ya en algunas partes del mundo. En Colombia la Corte Constitucional ha adoptado un sistema de detección de datos que reduce los tiempos de tratamiento (búsqueda de jurisprudencia, datos estadísticos, análisis de períodos de tiempo, resoluciones análogas, palabras clave, etc.) y explotación de los mismos a segundos, con un enorme índice de eficiencia, de en torno al 90%. El sistema es además predictivo, bajo la supervisión del personal jurisdiccional al que ayuda y a cuyas indicaciones se somete. Este ejemplo, que no es único en el continente americano, constituye una aplicación real de la tecnología derivada de la IA, para garantizar la efectividad de la tutela jurisdiccional ante un escenario de deficiente gestión e incluso de amenaza de colapso[16].

También es cierto que la reflexión que realizamos no puede ignorar que el escenario y el momento no están exentos de riesgos que conviene detectar y desactivar o conjurar. No debemos tener prisa para calcular dichos riesgos, asentar las ideas, legislar, capacitar y hacer todo esto bien.

Centrándonos en España, y en aplicaciones derivadas de la IA denominada de mayor riesgo ya que va más allá de la mera gestión, internándose en la proposición de resoluciones, un informe de la Agencia Catalana de Protección de Datos de 2020, sobre este tipo de aplicaciones de la IA que ya se han incorporado al sistema judicial, nos ayuda a visualizar su extensión real en el mencionado ámbito judicial, a la vez que nos advierte de los riesgos reales que surgen[17].

"La aplicación de la inteligencia artificial en el ámbito judicial es un tema muy delicado porque –como en el ámbito de la salud– las decisiones que tome el algoritmo afectan directamente a la vida de las personas. El eco de experiencias similares en Estados Unidos –donde el programa *Correctional Offender Management Profiling for Alternative Sanctions (COMPASS)*

---

la adaptación de la legislación española a las nuevas realidades, en lo concerniente a la implementación de nuevas tecnologías de la información y la comunicación en el servicio público de Justicia", como se señala en el apartado VIII de su Exposición de Motivos.

16. El País, 29 de julio de 2020. "Legaltech. Inteligencia artificial para desatascar la justicia en Colombia", por Catalina Oquendo. Un ejemplo extremo de ejecución penal "algoritmizada", implementado en Hong-Kong, nos lo ofrece BARONA VILAR, S., "La incidencia de la inteligencia artificial en la justicia europea penal: ¿límites o expansión?", capítulo en la obra colectiva dirigida por LLORENTE SÁNCHEZ-ARJONA, M., *Estudios procesales sobre el espacio europeo de justicia penal*, Thomson Reuters Aranzadi, Cizur Menor 2021, p. 339.
17. Autoritat Catalana de Protecció de Dades. "Inteligencia Artificial: decisiones automatizadas en Cataluña", 2020.

decidía la reincidencia criminal– tampoco ayudan a tener confianza en los resultados de la máquina. El medio independiente ProPublica desveló[18] que *COMPASS* –elaborado por la empresa Equivant[19]– tenía sesgos que marcaban una probabilidad más alta de cometer crímenes por los acusados negros que por los blancos".

El mencionado informe muestra que, en Cataluña, hace más de una década que se aplican programas similares al *COMPASS* para detectar la reincidencia criminal en adultos y en jóvenes. Hasta la fecha, ninguna investigación ha demostrado que haya sesgos perjudiciales para los internos. El investigador Carlos Castillo –Director del grupo Web Science and Social Computing de la Universidad Pompeu Fabra (UPF)– ha realizado diversas investigaciones sobre estos sistemas inteligentes y –a criterio suyo– funcionan bastante bien. "Los técnicos que hacen uso de ellos en última instancia, valoran individualmente los resultados que ha dado la máquina y deciden la medida a aplicar", explica Castillo.

Los concretos ámbitos en los que se viene aplicando la IA a la actividad judicial, en Cataluña, cuyo rendimiento es monitorizado y evaluado, son:

1. **Predicción de la reincidencia criminal**

Los permisos de salida se utilizan para facilitar la reinserción y rehabilitación de los internos. El hecho de poder pronosticar, con la eficacia predictiva más grande posible, la probabilidad de infracción futura de un permiso, representa una gran ayuda para los 37 técnicos penitenciarios. El Riscanvi[20] es un protocolo (o herramienta de valoración del riesgo) que se puso en marcha en 2009 en todas las cárceles de Cataluña, para estimar las posibilidades de que una persona vuelva a delinquir una vez haya salido de la cárcel. El Departamento de Justicia de Cataluña hizo un encargo al Grupo de Estudios Avanzados en Violencia (GEAV) de la Universidad

18. "How we analyzed the Compass recidivisim algorithm", Pro Publica (2016). https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.
19. *Human decisions and machine predictions*. https://academic.oup.com/qje/article-abstract/133/1/237/4095198, redirected From fulltext. *Humans decisions and machine predictions* es un interesante estudio estadounidense que demuestra cómo –para determinar el riesgo de reincidencia y las medidas cautelares en un proceso– el aprendizaje automático puede funcionar mejor que las decisiones de un juez. "Los resultados mostraron que, cuando era muy evidente que el preso tenía muy bajo riesgo en reincidir, tanto los jueces como el algoritmo coincidían en liberarlo bajo fianza antes del juicio. Pero que la máquina era más justa que el juez en predecir casos de mayor riesgo de reincidencia criminal. Y esto es porque son sistemáticas, incluso cuando son tan racistas como los jueces".
20. Riscanvi http://cejfe.gencat.cat/es/recerca/cataleg/crono/2017/eficacia-del-riscanvi-2017/.

de Barcelona (UB) y, en el tiempo que lleva en funcionamiento, ya se ha aplicado a unos 20 mil presos.

La predicción de la criminalidad que hacen los algoritmos es individualizada y personalizada. "En las cárceles –en un momento u otro– los técnicos, directores, psicólogos o juristas han de tomar la decisión sobre qué puede pasar ante un permiso de un interno o cuando éste está a punto de salir a la calle para siempre", explica Antonio Andrés Pueyo, Investigador Principal del GEAV y Catedrático de Psicología de la UB. "La preocupación es si volverá a cometer un delito[21]".

El programa también considera el comportamiento violento del interno en prisión: si ha agredido a otro, si ha intentado autolesionarse, suicidarse, etc. Es una tarea individual para cada interno y habitual en el sistema penitenciario. Pero el técnico ya no tiene que retener toda esta información, lo hace el sistema automatizado, aportándole mucho conocimiento cuando tiene que tomar una decisión[22].

2. **Detección de la reincidencia juvenil**

El programa *Structured Assessment of Violence Risk in Youth* (SAVRY) funciona con la misma lógica que el Riscanvi, pero fue elaborado en 2003 en Estados Unidos y no por el GEAV. Es un instrumento utilizado por muchos países del mundo como Canadá o los EE. UU., y también por países europeos como es el caso de Holanda.

---

21. *Vid.*,https://treballiaferssocials.gencat.cat/web/.content/03ambits_tematics/07infanciaiadolescencia/temes_relacionats/jornades_treball_dgaia_2012/docs_3_maig/valoracio_risc_reincidencia.pdf. El profesor Antonio Andrés Pueyo expone que tradicionalmente se hacía un análisis, a partir de unos parámetros y, si el interno cumplía ciertos requisitos, decidían la actuación en función de los resultados. "Hace diez años que se hace de manera automatizada con inteligencia artificial. A partir de 43 variables –que un sistema matemático combina a la perfección– el técnico puede tomar la decisión más acertada", añade Pueyo. "Si un preso pide un permiso para visitar a la familia, y la respuesta del Riscanvi es de alta probabilidad de delinquir, alerta al técnico con una señal roja. El preso sale igualmente, pero se activa un seguimiento diario, una pulsera electrónica o el contacto con un familiar", explica el director del GEAV. *Vid.*, FÉREZ-MANGAS, D.; ANDRÉS-PUEYO, A., "Eficacia predictiva en la valoración del riesgo de quebrantamiento de permisos penitenciarios", en La Ley Penal n.º 134 de 2018.

22. El Riscanvi ya va por su versión 3.0. Cada tres años se actualiza y se incorporan mejoras para que sea más preciso. Ante posibles dilemas éticos, Andrés Pueyo puntualiza que "la respuesta del algoritmo es validada siempre por la Junta de Tratamiento. Y esta puede: a) mantener el mismo nivel de riesgo (bajo, alto) del algoritmo, b) aumentarlo; y/o c) disminuirlo. En los casos b y c, debe justificar este cambio con las evidencias que lo sustentan". Aquí encontramos la esencia de lo que debería ser la correcta implementación de la IA integralmente considerada, que consiste en supervisar siempre la respuesta del algoritmo, para confirmarla o, en caso contrario, rechazarla, con plena posibilidad de modificación del criterio propuesto, en cuyo caso deberá motivarse.

Como explica Andrés Pueyo, tiene menos factores de valoración, tan solo 26, e igualmente se aplica de manera muy individualizada.

El programa es menos automático que el Riscanvi, dejando más margen de actuación al técnico. Ello es debido a que los cambios de comportamiento de los jóvenes pueden ser muy bruscos en comparación con lo que ocurre con los adultos

Tanto en el caso del programa Riscanvi como en el de SAVRY, cuando advierten de un riesgo de reincidencia alto, activan los equipos de tratamiento que decidirán las actuaciones o medidas idóneas para afrontar el riesgo detectado por la aplicación.

3. **Elaboración de estadísticas predictivas para profesionales del derecho**

Existen igualmente herramientas cuya finalidad es ayudar a los profesionales del derecho en la ardua y necesaria tarea de localizar sentencias para leerlas y combinarlas y así extraer nuevas conclusiones[23]. Los modelos matemáticos pueden operar con información cualitativa del análisis de millones de casos, información de los jueces que han dictado sentencia, de la aplicación de artículos y leyes, de fecha, lugar, etc. Los algoritmos combinan toda la información procedente de órdenes e instancias jurisdiccionales, *v. gr.*, de todo el estado español y definen la estrategia procesal más idónea para cada caso.

4. **Orientación para la eventual extradición de migrantes**

La detención y subsiguiente puesta a disposición judicial de un migrante, aboca al juez a adoptar una decisión que puede conllevar la devolución a su país de origen. En dicha resolución se verán eventualmente implicados elementos y situaciones que pueden resultar decisivos para la misma, como la exposición de la persona a un riesgo de muerte, a un riesgo de contraer enfermedad grave, por una epidemia, o a un riesgo de ser sometida a tortura o castigo cruel, inhumano o degradante. El instrumento permitirá al juez –mediante la asignación de una puntuación a cada situación, en función de su gravedad– adoptar una decisión de manera objetiva[24].

23. Nos referimos básicamente a la Jurimetria o analítica jurisprudencial estadística y predictiva, *v. gr.*, (https://jurimetria.wolterskluwer.es/content/Inicio.aspx).

24. Con tal finalidad, el Departamento de Matemáticas e Informática de la Universidad de Barcelona, sobre la base de todos los casos sobre los que se ha pronunciado el Tribunal Supremo, creó un modelo matemático experimental. La decisión final, una vez más, corresponde al juez, al que la herramienta proporciona sólidos elementos que podrá utilizar para la motivación. Evidentemente, el instrumento también es de utilidad para otros profesionales del derecho, singularmente para los abogados defensores.

Queremos también mencionar –de entre todas las existentes– alguna otra iniciativa que, mediante el aprovechamiento de las posibilidades que las nuevas tecnologías ofrecen, busca rediseñar itinerarios de reinserción o la activación de alternativas a las penas privativas de libertad. Es el caso de la actuación liderada por el Gobierno de Navarra, que busca incidir en la mejora de políticas públicas en materia de ejecución penal, y otras, mediante el empleo de la IA[25].

III. IMPULSO DE LA TECNOLOGÍA EN EL CAMPO DE LA JUSTICIA. INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS. EL ROL DE LA COMISIÓN EUROPEA, EN PARTICULAR, EL LIBRO BLANCO DE LA UE. PRESENTE Y FUTURO

La Comisión Europea ha publicado dos importantes documentos que muestran a las claras su interés en promocionar el uso de la tecnología también en el ámbito de la justicia. Se trata del "*Libro blanco sobre Inteligencia Artificial*", publicado el 19 de febrero de 2020, y el informe titulado "*Study on the use of innovative technologies in the justice field*" de septiembre de 2020.

El objetivo de ambos es clarificar el escenario mediante una información exhaustiva, ofrecer ejemplos reales de buenas prácticas, generar confianza ofreciendo las claves que permitan una implementación realista e integral de la IA, cuyo objetivo estratégico final es incrementar la calidad y compatibilidad de los sistemas de producción y servicios públicos nacionales, en general, y del servicio de la justicia, en el que nos fijamos en particular[26].

En esencia, el Libro Blanco muestra una apuesta plena, como objetivo estratégico orientado a la excelencia y la confianza, por la implementación integral de la IA. El informe al que nos hemos referido, muestra también

25. Iustel, Diario del Derecho, edición de 11 de noviembre de 2020. "El Gobierno de Navarra, TRACASA y la UPNA (Universidad Pública de Navarra) colaborarán en la aplicación de inteligencia artificial en el ámbito judicial". TRACASA es una empresa pública implicada en el desarrollo de sistemas avanzados de gestión procesal, innovadora en España. La Comunidad Foral está también apostando decididamente por la justicia virtual, como lo atestigua la creación de la herramienta *Avantius,* para la realización de vistas orales por videoconferencia, perfectamente adecuada para reaccionar y actuar frente situaciones como la derivada de la Pandemia.

26. Una valiosa reflexión a este respecto la hallamos en BARONA VILAR, S., "La incidencia de la inteligencia artificial en la justicia europea penal: ¿límites o expansión?", capítulo en la obra colectiva dirigida por LLORENTE SÁNCHEZ-ARJONA, M., *Estudios procesales sobre el espacio europeo de justicia penal*, Thomson Reuters Aranzadi, *op. cit.*, pp. 317 y ss.

la necesaria mesura y aconsejable prudencia al explicitar y destacar los riesgos que para los derechos fundamentales pueden surgir, urgiendo a su temprana detección y conjuro. "La Comisión se ha comprometido a facilitar el avance científico, preservar el liderazgo tecnológico de la UE y garantizar que las nuevas tecnologías estén al servicio de todos los europeos, de manera que mejoren sus vidas al mismo tiempo que respetan sus derechos[27]".

La finalidad del Libro Blanco es, por tanto, propiciar una profunda y suficiente reflexión, que permita finalmente una implementación ordenada, homogénea, integral (en todos los sectores de actividad) y a gran escala de la IA en Europa, para aproximarnos a la excelencia. Los riesgos que deben ser conjurados para generar confianza se centran en el respeto a los derechos fundamentales, para lo que cuestiones como la protección de datos personales, la transparencia, la responsabilidad, la privacidad o los sesgos en la adopción de decisiones autónomas, deben ser correctamente detectadas y resueltas[28].

Algunas cuestiones más específicas que queremos destacar, y a las que explícitamente se refiere el Libro Blanco, son, por ejemplo, la promoción de la adopción de la IA por parte del sector público[29], para lo que la Comisión preparará un "Programa de adopción de la IA", que respaldará y propiciará, de forma integral, la contratación pública de sistemas de IA[30].

El Libro Blanco sobre IA entronca con la Estrategia Europea de Datos, cuyo objeto es la mejora en el acceso y gestión responsable del "enorme volumen" de datos que se está empezando a generar, y que no podrán ser correctamente tratados sin el desarrollo de la IA, que tampoco tiene sentido –en una relación simbiótica– sin un gran volumen de datos[31].

27. Libro Blanco sobre inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza, Comisión Europea, Bruselas 2020, p. 1.
28. Al respecto, es de gran interés el trabajo de, DE HOYOS SANCHO, M. "Premisas y finalidades del Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: perspectiva procesal del nuevo marco regulador", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021, pp. 129 y ss.
29. "Resulta fundamental que las Administraciones Públicas, los hospitales, los servicios públicos y de transporte, los supervisores financieros y otras áreas de interés público empiecen a adoptar rápidamente productos y servicios que se basen en la inteligencia artificial en sus actividades". Libro Blanco sobre inteligencia artificial, *op. cit.,* p. 10.
30. Libro Blanco sobre inteligencia artificial, *op. cit.,* p. 10.
31. "Promover prácticas de gestión responsable de los datos e incentivar el cumplimiento, en lo que respecta a estos últimos, de los principios FAIR contribuirá a generar confianza y a posibilitar su reutilización. La inversión en infraestructuras y tecnologías informáticas clave es igualmente importante". Libro Blanco sobre inteligencia artificial, *op. cit.,* p. 10.

En el otro platillo de la balanza están los potenciales riesgos. Hemos visto ya las oportunidades que la Comisión Europea detecta, y que fundamentan la nueva estrategia, y ahora debemos fijarnos, la propia Comisión lo hace, en la contrapartida. El riesgo más relevante que se percibe, y que opera como límite, es el de la posible vulneración de los derechos fundamentales, y muy especialmente, la del derecho a la protección de los datos personales y de la privacidad. La cuestión es que "los ciudadanos y las personas jurídicas serán, cada vez más, objeto de acciones y decisiones adoptadas por sistemas de inteligencia artificial o con ayuda de estos; dichas acciones y decisiones, en ocasiones, pueden resultar difíciles de entender o de rebatir eficazmente cuando se requiera. Además, la IA incrementa las posibilidades de hacer un seguimiento y un análisis de las costumbres cotidianas de las personas". El riesgo potencial es evidente y muestra que "la IA también puede utilizarse para rastrear y desanonimizar datos relativos a personas, y generar así nuevos riesgos en torno a la protección de los datos personales[32]".

Las aplicaciones de IA denominadas de "alto riesgo", entre las que se cuentan las que conciernen al campo de la justicia, y casos o herramientas concretas como algunos programas de reconocimiento o análisis facial, o algoritmos para predecir la reincidencia delictiva, que muestran prejuicios raciales o de género, serán objeto de atención preferente y figurarán en una lista que será objeto de revisión y corrección periódicas. La regulación suficiente, clara y actualizada va a ser clave para reducir la incertidumbre y las justificadas dudas que se plantean, dando así seguridad en este enorme salto cualitativo que se está preparando. El marco normativo en vigor en la UE, así como la legislación nacional, referidos a la protección de los derechos fundamentales, y en particular en lo que ahora nos fijamos, normas sobre protección de datos personales y, más específicamente, la Directiva UE 2016/680, sobre protección de datos en el ámbito penal, deberán ser revisadas y eventualmente adaptadas al nuevo escenario, para garantizar su eficacia[33].

También queremos siquiera mencionar –como instrumento complementario de suma utilidad que establece una primera aproximación a los límites de productos y servicios que incluyen la IA– al informe de la

32. Libro Blanco sobre inteligencia artificial, *op. cit.,* pp. 13 y 14.

33. Libro Blanco sobre inteligencia artificial, *op. cit.,* p. 16. En relación con la Propuesta de Reglamento del Parlamento europeo y del Consejo para establecer reglas armonizadas en materia de IA, publicada el 21 de abril de 2021, *vid.,* DE HOYOS SANCHO, M., "El uso jurisdiccional de los Sistemas de Inteligencia Artificial y la necesidad de su armonización en el contexto de la Unión Europea", capítulo en la obra colectiva dirigida por LLORENTE SÁNCHEZ-ARJONA, M., *Estudios procesales sobre el espacio europeo de justicia penal*, Thomson Reuters Aranzadi, Cizur Menor 2021, pp. 347 y ss.

AEPD relativo a la "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción" de febrero de 2020. En el mismo se reconoce que la IA genera muchas dudas en torno a aspectos tan delicados como los derechos de los interesados o la seguridad jurídica de todos los intervinientes en el sistema[34]. Despejar tempranamente esas dudas es por tanto clave para permitir el correcto despliegue de la nueva tecnología.

La propia AEPD –reivindicando acertadamente el innegable protagonismo que a todas las autoridades independientes de control debe corresponder ante este nuevo escenario, y amparada por el art. 24 RGPD– ha hecho pública una guía de requisitos, orientaciones, objetivos, criterios etc., para la realización de auditorías a tratamientos de datos personales que incluyan inteligencia artificial[35]. El objetivo de este necesario control es, evidentemente, el de anular el impacto negativo sobre los derechos fundamentales de los ciudadanos derivado de los tratamientos que incorporan IA[36].

La contundente conclusión que expresa el Libro Blanco es que "la inteligencia artificial es una tecnología estratégica que ofrece numerosas ventajas a los ciudadanos, las empresas y la sociedad en su conjunto, siempre y cuando sea antropocéntrica, ética y sostenible y respete los derechos y valores fundamentales[37]".

34. (https://www.aepd.es/sites/default/files/2020-02/adecuación-rgpd-ia.pdf).

35. https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia.pdf.

36. Un ejemplo claro de vulneración sería la elaboración de perfiles que la LO 7/2021, prohíbe en su art. 14. Mecanismo de decisión individual automatizado. 1. Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada. 2. Las decisiones a las que se refiere el apartado anterior no se basarán en las categorías especiales de datos personales contempladas en el artículo 13, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. 3. Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13.

37. Libro Blanco sobre inteligencia artificial, *op. cit.*, p. 30. Asimismo, de forma coordinada y paralela, centrados en la repercusión de la IA en los derechos fundamentales de los ciudadanos, *vid.*, el informe "Getting the future right. Artificial Intelligence and Fundamental Rights" elaborado por la European Union Agency for Fundamental Rights, Luxembourg 2020. Igualmente, el estudio "Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights", encargado por el Parlamento

Veamos ahora, mediante el ejemplo que constituye la reciente regulación aplicada al orden jurisdiccional penal, de qué manera se puede beneficiar y fortalecer el estado de derecho, mediante la correcta y debida defensa de los derechos fundamentales, en el ámbito jurisdiccional.

IV. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y PROCESO PENAL. LA LO 7/2021[38]

Con ocasión de la actividad jurisdiccional penal, esencialmente investigación, enjuiciamiento y ejecución, la situación de algunos derechos fundamentales, entre ellos el de protección de datos de carácter personal, puede ser de máxima exposición y, por tanto y correlativamente, de clara vulnerabilidad. Por ello debe garantizarse la mínima intromisión necesaria, la proporcionalidad, en su obtención y el mayor esmero en su tratamiento y gestión. De todo ello se ocupa monográficamente la LO 7/2021, cuya Disposición Final cuarta establece la modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, donde mediante la modificación del apartado 3 del artículo 44, se fija la jerarquía, máxima, de las instituciones implicadas[39].

Europeo, Bruselas 2020, que contiene una específica referencia al derecho fundamental a la protección de datos de carácter personal, que nos ocupa.

38. A este respecto, *vid.,* ESPARZA LEIBAR, I., "Protección de datos de carácter personal y proceso penal", capítulo en la obra colectiva, *Justicia con ojos de mujer. Cuestiones procesales controvertidas*, publicada con motivo del Congreso conmemorativo del décimo aniversario de las Jornadas Justicia con Ojos de Mujer (2008–2017), Valencia, Tirant lo Blanch, 2018. Igualmente, desde una perspectiva más amplia, *vid.,* ABERASTURI GORRIÑO, U., "Artículo 8: El derecho a la protección de datos de carácter personal. La autodeterminación informativa como derecho autónomo en la Carta de Derechos Fundamentales de la Unión Europea", capítulo en la obra colectiva, *La Carta de los Derechos Fundamentales de la Unión Europea y su reflejo en el ordenamiento jurídico español*, Dirigida por ORDEÑANA GEZURAGA, I., Cizur Menor, Thomson Reuters, 2014. Resulta hoy particularmente estimulante la lectura de algún "clásico" en la materia, donde ya se aprecian con claridad los conceptos y principios fundamentales a tener en cuenta en materia de protección de datos y proceso penal. La terminología y algunas expresiones muestran a las claras cuánto tiempo ha pasado. *Vid.,* ETXEBERRIA GURIDI, J. F., "La protección de los datos de carácter personal en el ámbito de la investigación penal", Madrid, AEPD 1998. Trabajo galardonado por su temprana y clarividente contribución a la, entonces conceptualmente incipiente, protección de los datos personales.

39. "Artículo 44.3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia".

Si a ello añadimos lo que ocurre con motivo de la incorporación y aplicación de la IA a la cotidianeidad del funcionamiento de los tribunales –aunque no hemos llegado al límite del potencial ni mucho menos, ya atisbamos el futuro inmediato– se puede deducir, entre otras muchas cosas, que estamos asistiendo a un incremento en el tráfico y a una gestión y uso masivos de datos de carácter personal.

Este empleo masivo de los datos de carácter personal sería la contrapartida a una mejor gestión, quizá infinitamente mejor, de la actividad del Poder Judicial. Pero, para que el nuevo escenario no se convierta en un serio problema, lo que habría que garantizar, *in limine*, es que los datos de carácter personal serán correctamente gestionados o tratados, y para saber cómo hacerlo, es una pieza clave la Directiva (UE) 2016/680[40], de reciente transposición –mediante la Ley Orgánica 7/2021, de 26 de mayo– relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, que proporciona el necesario, suficiente y previo soporte normativo para asegurar el respeto integral a los datos de carácter personal[41].

El proceso penal, en general, y dentro de él la fase de investigación, en particular, son sin duda escenarios y circunstancias en las que los derechos fundamentales de los ciudadanos aparecen, siempre ha sido así,

40. La transposición de esta crucial Directiva, que debió hacerse antes del 6 de mayo de 2018 –y a diferencia de lo ocurrido en otros muchos países de referencia, como por ejemplo Alemania que lo hizo el 30 de junio de 2017, o Francia, que culminó la transposición el 12 de diciembre de 2018– ha tardado mucho en realizarse, demasiado, y se ha hecho finalmente mediante la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. El retraso ha comportado, como advertimos reiteradamente, un gran riesgo al haberse mantenido durante demasiado tiempo una situación de notable inseguridad, lo que, a su vez, ha supuesto condenas y sanciones para España. En relación con la mencionada LO, *vid.*, MARTÍNEZ VÁZQUEZ, F., "La nueva Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales", *Diario La Ley*, de 28 de mayo de 2021.

41. Las autoridades competentes a las que se refiere la norma en su art. 4, son: las autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal, las Fuerzas y Cuerpos de Seguridad, las Administraciones Penitenciarias, la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria, el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

tensionados y expuestos. Las exigencias derivadas de un estado de derecho en relación con el proceso que le es debido a cada ciudadano por el hecho de serlo, obliga a que todos los operadores –incluido muy especialmente el legislador, que debe velar por el óptimo mantenimiento del parque normativo– deban actuar de forma eficiente y correcta, ya que los errores podrían ser causa de lesión de derechos fundamentales de los ciudadanos, con todas las consecuencias negativas que de dicha circunstancia se derivan y que inciden en la calidad del sistema de resolución de conflictos[42].

Nunca antes nuestros derechos cívicos han sido tan potencialmente vulnerables. La innovación tecnológica aplicada a la investigación penal aumenta exponencialmente las posibilidades de afectación de los derechos fundamentales, somos transparentes y vamos a serlo más todavía. Por tanto, todo lo relativo a: 1., la obtención, 2., el tratamiento y, 3., la explotación (incluido el intercambio y la cooperación, especialmente en el ámbito del espacio europeo de justicia) de la información recopilada como consecuencia de una investigación penal, debe ser objeto de una exquisita y milimétrica regulación, máxime cuando nos referimos a datos de carácter personal. La calidad del estado de derecho también depende de ello[43].

La idea clave que deseamos asentar es que toda la actividad jurisdiccional, y en particular la investigación procesal penal en un estado de derecho, impone a todos los sujetos implicados (policía judicial, ministerio fiscal, jueces, letrados, etc.) determinados límites y protocolos en su actuación, en cuanto está dirigida a la gestión y obtención de información y otras evidencias que constituyen datos personales[44], que son objeto

42. Los principios relativos al tratamiento de los datos personales a los que se refiere al art. 6, se concretan en que dichos datos sean tratados de manera lícita y leal, que lo sean por las autoridades competentes, que resulten necesarios para los fines de la ley orgánica, que sean adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados, que sean exactos y, si fuera necesario, actualizados y que sean conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados. También se establece que sean tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

43. *Vid.*, PÉREZ ESTRADA, M. J., "Efectos de la vulneración de la protección de los datos personales en el proceso penal", en *La ley penal: revista de derecho penal, procesal y penitenciario*, n.° 135, 2018. También, COLOMER HERNÁNDEZ, I., (Director), *La trasmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Thomson Reuters Aranzadi, Cizur Menor 2015.

44. "Datos personales": Toda información sobre una persona física identificada o identificable ("el interesado"). Art. 3 de la Directiva (UE) 2016/680. Artículo 5 LO 7/2021. Definiciones. A efectos de esta Ley Orgánica se entenderá por: a) "datos personales": toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable a toda persona cuya identidad

de tratamiento intenso y masivo. La razón la constituye la necesidad de preservar y garantizar los derechos fundamentales de los ciudadanos, permitiendo simultáneamente la imprescindible labor investigativa y la eficiencia en la gestión de la actividad procesal[45]. La irregular obtención o tratamiento de información –en particular de datos de carácter personal– en el curso de la actuación procesal puede tener como consecuencia principal su absoluta ineficacia en el proceso (art. 11 LOPJ). Es decir, una catástrofe inasumible.

Pero el cuidado con el que debemos operar no se agota con la obtención de las evidencias en el curso de una investigación penal, tarea ejecutada en esencia por la policía judicial bajo la estricta supervisión judicial. Una vez obtenida cualquier información que constituya un dato personal, su gestión impone ciertas obligaciones que deben permitir garantizar la preservación de su integridad, su verificabilidad y su trazabilidad, en lo que a dicho material concierne, es lo que constituye el "tratamiento"[46].

---

pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

45. Por lo que a los derechos de los interesados y su ejercicio concierne, *vid.* arts. 20 y ss. LO 7/2021.

46. *Vid.* art. 3 de la Directiva (UE) 2016/680. *V. gr*., en el caso del proceso penal, acreditada la ruptura de la cadena de custodia, el material con vocación probatoria afectado se convierte en inseguro, discutible e incluso ineficaz o inválido. Un determinado tratamiento centrado en la actividad procesal penal, acorde con la naturaleza de la información obtenida se impone, por tanto. El símil que pensamos que ilustra bien lo que queremos trasladar es el de una donación de sangre, que consta de tres fases bien diferenciadas, la extracción, la conservación y la transfusión. Todas ellas están sujetas a requisitos y protocolos acordes con las necesidades de cada fase. Cada una de ellas por separado debe ser cuidadosamente respetada en cuanto a sus requerimientos, de lo contrario se frustrarán los fines de la donación. Ocurre lo mismo con la información constitutiva de datos de carácter personal y el proceso penal. La obtención durante la fase de investigación y la explotación, durante el juicio oral, han centrado nuestros esfuerzos, pero no podemos descuidar el período que transcurre entre la obtención y la celebración del juicio oral. Es precisamente entonces cuando los datos de carácter personal deben ser objeto de "tratamiento", es una suerte de cadena de custodia cualificada. La Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, establece los principios generales aplicables a cualquier tratamiento de datos personales, lo que se concreta en que deberán ser tratados de manera lícita y leal, que deberán serlo por las autoridades competentes, que deberán ser los que resulten necesarios para los fines de la ley orgánica, que serán adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados, que serán además exactos y actualizados y, no menos relevante, que deberán ser conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados. De la misma manera, los datos deberán ser tratados de manera que se garantice su

No todos los frutos de la investigación jurisdiccional constituyen datos personales, pero cuando es así, deben activarse las exigencias derivadas del derecho fundamental a la protección de datos de carácter personal, en la medida en que también se podrá ver afectado (pensemos en grabaciones de imágenes o conversaciones mediante sofisticados dispositivos tales como balizas o drones, muestras de ADN, etc.) como consecuencia de una investigación penal[47]. Dichas exigencias se imponen en este contexto, adicional e integralmente a la investigación penal disciplinándola, y su vulneración tendría nefastas consecuencias en el proceso.

El espacio europeo de justicia ha generado al respecto dos instrumentos con incidencia directa es esta materia, la orden europea de investigación, que impone un estándar a los países que lo integran, en cuanto a la obtención, y también la Directiva (UE) 2016/680 en cuanto a la posterior gestión, o mejor tratamiento, de los datos de carácter personal, transpuesta en España mediante la Ley Orgánica 7/2021, de 26 de mayo que estamos analizando. En definitiva y a la postre, ahora contamos ya con el parque normativo básico, que muchos veníamos reclamando con insistencia y que, por ahora, completa, estabiliza y dota de seguridad jurídica a esta parte del sistema de resolución de conflictos.

La privacidad –el objeto de nuestra atención, que comprende el derecho al honor, a la propia imagen y a la intimidad– no lo olvidemos, protege aspectos íntimos a la vez que sumamente vulnerables, que forman parte de la esfera de derechos de cada uno de nosotros. Frente a ella, pensemos por un momento en tecnologías aplicadas a, por ejemplo, investigaciones en materia de criminalidad organizada o ciberdelincuencia (comunicaciones integralmente consideradas, captación de imágenes, registros remotos de equipos informáticos, o registros de dispositivos de almacenamiento masivo de información, etc., arts. 588 quinquies y ss., LECrim) y extraigamos conclusiones[48].

---

adecuada seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. *Vid.,* arts. 5 y 6 LO 7/2021.

47. La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, de temprana declaración, protegido por el artículo 18.4 de la Constitución española. El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que "nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados". Por otra parte, es un derecho que también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, de 2000, y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea de 2007.

48. Capítulo introducido por la Ley Orgánica 13/2015, de 5 de octubre. *Vid.,* al respecto, CALAZA LÓPEZ, S., "La investigación tecnológica en el proceso penal español a

En relación con las imágenes –como ejemplo, dada su banalización, su uso indiscriminado y abusivo en todos los ámbitos– la titularidad del derecho a la propia imagen implica que cada persona tiene derecho a controlar la captación, reproducción y difusión de esa imagen[49]. Todo ello con respecto a la intimidad, ya que debe haber un espacio en torno a cada uno de nosotros, ciudadanos de un estado de derecho, un espacio en el que nuestra personalidad y nuestra actividad se despliegan y desarrollan al amparo de la imprescindible y protectora intimidad; tenemos adicionalmente "derecho al propio entorno virtual" como declara la STS 342/2013, y todo ello puede ser objeto de investigación.

La protección de datos de carácter personal viene a contribuir a que las afectaciones a la privacidad sean las mínimas indispensables, y a que, a lo largo del proceso, tras su obtención, y como consecuencia del mismo sean rigurosamente protegidos por medio de tratamientos perfectamente protocolizados, seguros, trazables y transparentes[50].

Ambos valores –el derecho fundamental de los ciudadanos a la privacidad, frente al derecho de la comunidad, y en su nombre del estado, a investigar los delitos– son perfectamente legítimos y deben ser conjugados y defendidos con igual convicción y diligencia. El escenario previsible es que en la mencionada frontera los incidentes derivados de la tensión entre ambos valores, sean frecuentes. Es por ello que las autoridades independientes de protección –necesaria y debidamente coordinadas– están llamadas a jugar un muy relevante rol en este campo. Ya hemos percibido un salto cualitativo en su actividad, salto que las ha colocado en el centro del tablero de juego de la protección de los datos de carácter personal, también en lo relativo a la jurisdicción[51].

---

la vanguardia europea", capítulo en la obra colectiva dirigida por LLORENTE SÁNCHEZ-ARJONA, M., *Estudios procesales sobre el espacio europeo de justicia penal*, Thomson Reuters Aranzadi, Cizur Menor 2021, pp. 171 y ss. Específicamente en lo que a la videovigilancia concierne –grabación de imágenes y sonidos *vid.*, sección 2.ª del capítulo II de la LO 7/2021, arts. 15-19, relativa al tratamiento de datos personales en el ámbito de la videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

49. Las obligaciones al respecto para las fuerzas y cuerpos de seguridad las detalla el Artículo 18, que se ocupa del tratamiento y conservación de las imágenes. Los derechos de las personas los hallamos en los arts. 20 y ss., todos ellos de la LO 7/2021.

50. En lo que al uso de datos personales por parte de la IA, y en el ámbito del proceso penal, concierne, la vanguardia doctrinal la encontramos en COLOMER HERNÁNDEZ, I., "Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021, pp. 287 y ss.

51. Los arts. 34 y ss., de la LO 7/2021, establecen la obligación de cooperación de responsables y encargados del tratamiento con la autoridad de protección de datos

Como venimos sosteniendo, el correcto volcado de la actividad derivada del proceso penal a instrumentos y protocolos basados en las nuevas tecnologías y eventualmente a la aplicación da la IA, requeriría todavía de una adicional infraestructura normativa que en la actualidad –aunque se han producido importantes avances– no es completa.

V. CONCLUSIONES Y PROPUESTAS

Tenemos la impresión de que cuando acudimos a la magia de la tecnología en una situación difícil o incluso desesperada, no es quizá posible la reflexión sosegada previa –que es lo que pretendemos aquí, y lo que cualquier situación crítica requiere– que sería metodológicamente necesaria para, además de constatar las indudables ventajas, tratar de atisbar los riesgos que las nuevas formas de hacer podrían comportar, y poder así conjurarlos.

Junto a ello, constatamos que la ayuda que ya nos proporciona y que potencialmente nos puede ofrecer la IA, con carácter general, es algo que la ciencia pone a nuestra disposición y que no nos podemos permitir rechazar de ninguna manera.

La IA correctamente aplicada al servicio público justicia, y a la actividad procesal en particular, puede incidir –de hecho, lo hace ya sectorialmente– muy positivamente en la garantía del derecho fundamental a la tutela judicial efectiva y, conviene insistir en que sólo será así si se hace correctamente, si preserva todo el conjunto de derechos y garantías que disciplinan la actividad jurisdiccional en un estado de derecho, mejorándolo y reforzando su legitimidad. Mejora el sistema, mejora el servicio y la correlativa satisfacción ciudadana.

La propuesta general sería por tanto incorporar la IA, su metodología y posibilidades, a la actividad jurisdiccional, más allá de la gestión y la automatización, llegando a la proposición de resoluciones, preservando siempre la supervisión integral y soberana de jueces y magistrados. Se trataría de un volcado integral hacia nuevas y más eficientes formas de

competente, en el marco de la legislación vigente, cuando esta lo solicite en el desempeño de sus funciones, además de consolidar su posición de *auctoritas* en la materia. En relación con su estatus, funciones, potestades, deberes de asistencia y cooperación, tramitación de reclamaciones ante ellas, catálogo de infracciones y sanciones, etc., *vid.* arts. 48 y ss., de la LO 7/2021. Por otra parte, es ciertamente llamativo el hecho –quizá meramente anecdótico– de que, al margen del consenso alcanzado por los partidos políticos en relación con la renovación de la presidencia de la AEPD, se hayan presentado más de una docena –hasta un total de quince– de candidaturas adicionales.

gestión y resolución que, por afectar a derechos fundamentales, y particularmente a la protección de datos de carácter personal, requerirían, previa y necesariamente, de la creación de una infraestructura normativa, también integral y suficiente. La transposición de la Directiva (UE) 2016/680, mediante la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha supuesto un avance sustancial en este ámbito.

La parte que corresponde de forma permanente al legislador, que es tan esencial como insustituible, consiste en regular con celeridad y acierto, las derivadas de la aplicación de la IA a la actividad procesal y la correlativa y adecuada protección de los datos de carácter personal que la nutren.

En todo este planteamiento estratégico –desde la reflexión previa, pasando por el asesoramiento permanente, la coordinación de recursos, y hasta la fiscalización de cada aplicación de IA, etc.– el rol de las autoridades independientes de control –de todas ellas y en todos los niveles, europeo, español y autonómico– en relación con el derecho fundamental a la protección de datos de carácter personal debe ser, en nuestra opinión, integral.

No debemos olvidar la enorme importancia y proyección del tema que nos ocupa ya que nos referimos a un espacio que trasciende el ámbito nacional, por lo que, para su eficacia plena, requiere de una coordinación en el espacio europeo de justicia, que no se podrá producir sin el adecuado soporte normativo.

Las conclusiones y propuestas, más en detalle, se referirán a los diferentes ámbitos de aplicación de la IA, y a la intensidad de su aplicación, desde la perspectiva de su incidencia en los derechos fundamentales de los ciudadanos.

Primera:

Por lo que a la parte de IA que menos recelos despierta, de menor riesgo, centrada en la protocolización, gestión y tratamiento automatizado masivo de datos personales concierne, sin que se llegue a la proposición de resoluciones individualizadas.

Propuesta: es preciso, por tanto, asumir de manera integral e inmediata la digitalización de la Justicia, en una primera fase en lo que es soporte, gestión, tratamiento y protocolización para evitar situaciones de impotencia máxima, como la vivida durante la pandemia. Muy poco presentable para un estado que se pretende moderno y eficiente, y generadora de un

riesgo cierto y real de colapso del sistema, que todavía no está conjurado. Es la antesala de la justicia virtual.

El desarrollo de normativa que soporte integral y adecuadamente esta nueva manera de actuar, e interactuar, los operadores jurídicos, existe ya sectorialmente y su mantenimiento y mejora aparecen como prioritarios.

Segunda:

Por lo que a las aplicaciones de IA denominadas "de alto riesgo" concierne, es decir, entrando en la proposición de resoluciones individualizadas, basadas en el empleo normalizado de la IA.

Propuesta: es preciso, por tanto, culminar, sin demora ni precipitación, la reflexión iniciada examinando las experiencias realizadas, evaluando las conclusiones y conjurando los riesgos, todos ellos, que hayan sido detectados.

Igualmente, corresponderá al legislador generar la infraestructura normativa suficiente. Consideramos que es una cuestión prioritaria de política judicial, que ya está suficientemente amparada, desarrollada y fomentada a nivel de la UE.

Tercera:

Por lo que específicamente al proceso penal concierne, la transposición de la Directiva (UE) 2016/680, mediante la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, (BOE de 27 de mayo de 2021), permite contar con el parque normativo básico que veníamos reclamando insistentemente, que estabiliza y dota de seguridad a esta parte del sistema de resolución de conflictos.

Es muy especialmente digno de mención, dado que avanza un elemento esencial de la estrategia de incorporación de la IA a nuestro ámbito, el art. 14, Mecanismo de decisión individual automatizado, de la LO 7/2021 que, a este respecto, establece en su apartado 1: "Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada".

Cuarta:

Se impone diseñar (esto lo han hecho ya en buena medida las instituciones europeas), e implementar (aquí es donde España debe esforzarse al máximo, y parece que el Plan de choque de la Justicia, responde a tales requerimientos) una política pública, integral y suficientemente dotada de medios económicos, personales, tecnológicos, formativos y normativos (todos ellos son indispensables, aunque por razones obvias queremos subrayar la necesidad de una infraestructura normativa suficiente).

Hay que terminar de configurar –a nivel europeo– la cobertura normativa relativa a las esenciales autoridades independientes de control. Al respecto, en España, la Ley Orgánica 7/2021, de 26 de mayo, establece que lo sean la Agencia Española de Protección de Datos y las –por ahora pocas, aunque meritorias– agencias autonómicas, en su respectivo ámbito de competencias.

La oportunidad debe ser también destacada, ya que nos sitúa ante un momento histórico, óptimo para realizar el esfuerzo requerido por parte de los poderes públicos, y ello en un contexto más amplio, dirigido a "reconstruir España desde y con los datos, situando la digitalización y la inteligencia artificial como pilares esenciales en los que invertir el fondo europeo de reconstrucción[52]". Hemos visto que la apuesta de la UE al respecto es total, lo que nos muestra un contexto favorable, como pocas veces se ha visto.

Quinta:

Indiscutiblemente, lo hemos avanzado ya, corresponde a las autoridades de protección de datos independientes (art. 48 LO 7/2021), un papel central y nuclear en materia de protección de datos[53]. El diseño normativo sitúa a la AEPD en una posición preeminente, a nivel nacional, siendo así que se le atribuye todo lo que concierne a la coordinación con el Comité Europeo de Protección de datos y las autoridades autonómicas homólogas. Igualmente, lo relativo a la tutela del derecho fundamental a la protección de datos de carácter personal y a la actuación ante sus eventuales infracciones (tramitación de reclamaciones, investigación y adopción de medidas provisionales y de garantía, imposición de sanciones,

52. ARENAS RAMIRO, M., en *La Ley privacidad*, n.° 6, de 13 de noviembre de 2020.

53. Parte esencial del grupo por normativo regulador ha sido recientemente modificado (La Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales. El RD 389/2021, de 1 de junio, por el que se aprueba el estatuto de la AEPD. La Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales).

etc.), agotando con ello la vía administrativa. Finalmente, se establece la que deberá ser estrecha colaboración con el CGPJ y la FGE en relación con los tratamientos de datos con fines jurisdiccionales, art. 236 octies LOPJ[54].

Dicha posición, junto con la referencia explícita a los tratamientos automatizados, en lo que se refiere al ámbito de aplicación de la LO 7/2021, arts. 1 y 2 "Será de aplicación al tratamiento total o parcialmente automatizado…", y el art. 14, prohibiendo la elaboración de perfiles; nos hace pensar que, más allá de la genuina vocación, el concurso de las autoridades de protección de datos independientes a la hora de fiscalizar los algoritmos sobre los que descansa el funcionamiento de la IA –algoritmos que se nutren en buena medida de datos de carácter personal, y cuya generación crece exponencialmente– es ya, y va a serlo todavía más, imprescindible.

Las autoridades independientes de control deben, en nuestra opinión, jugar un papel crucial, desarrollando y ejerciendo de manera armonizada su capacidad de fiscalización frente al uso sistemático de la IA, en la medida en que ésta emplee datos de carácter personal. Y ello mediante auditorías preventivas y otros instrumentos, que permitan examinar de forma también sistemática y, en su caso, rebatir los algoritmos, avanzando en transparencia y contribuyendo a la tutela de derechos fundamentales y a la calidad del estado de derecho.

El resultado de todo esto que estamos viendo, y a lo que nos hemos referido en las páginas anteriores, incluso a medio plazo, podría ser impresionante y muy beneficioso para los ciudadanos y para el estado de derecho[55].

VI. REFERENCIA BIBLIOGRÁFICA

ABERASTURI GORRIÑO, U., "Artículo 8: El derecho a la protección de datos de carácter personal. La autodeterminación informativa como

54. Específicamente nos referimos a la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial, y a la Unidad de Supervisión y Control de Protección de Datos de la FGE, a las que se refieren las disposiciones finales de la LO 7/2021.

55. Adicionalmente, la implementación de la nueva Ley Orgánica puede contribuir a mejorar hábitos, a alcanzar otros relevantes objetivos corrigiendo escandalosas malas prácticas a las que pareciera que nos hemos acostumbrado, tales como las habituales filtraciones de sumarios o de expedientes policiales o la vulneración, por banalización, del derecho fundamental a la presunción de inocencia, como acertadamente señala MARTÍNEZ VÁZQUEZ, F., en "La nueva Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales", *op. cit.*

derecho autónomo en la Carta de Derechos Fundamentales de la Unión Europea", capítulo en la obra colectiva, *La Carta de los Derechos Fundamentales de la Unión Europea y su reflejo en el ordenamiento jurídico español*, dirigida por ORDEÑANA GEZURAGA, I., Thomson Reuters Aranzadi, Cizur Menor 2014.

ARENAS RAMIRO, M., en *La Ley privacidad*, n.° 6, de 13 de noviembre de 2020.

BARONA VILAR, S., "Inteligencia artificial o la algoritmización de la vida y de la Justicia: ¿Solución o problema?", en Revista Boliviana de Derecho, n.° 28, julio de 2019.

BARONA VILAR, S., editora, *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021.

BARONA VILAR, S., "La incidencia de la inteligencia artificial en la justicia europea penal: ¿límites o expansión?", capítulo en la obra colectiva dirigida por LLORENTE SÁNCHEZ-ARJONA, M., *Estudios procesales sobre el espacio europeo de justicia penal*, Thomson Reuters Aranzadi, Cizur Menor 2021.

CALAZA LÓPEZ, S., "La investigación tecnológica en el proceso penal español a la vanguardia europea", capítulo en la obra colectiva dirigida por LLORENTE SÁNCHEZ-ARJONA, M., *Estudios procesales sobre el espacio europeo de justicia penal*, Thomson Reuters Aranzadi, Cizur Menor 2021.

COLOMER HERNÁNDEZ, I., (Director), *La trasmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Thomson Reuters Aranzadi, Cizur Menor 2015.

COLOMER HERNÁNDEZ, I., "Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021.

COMISIÓN EUROPEA, Libro Blanco sobre inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza, Bruselas 2020.

DE HOYOS SANCHO, M. "Premisas y finalidades del Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: perspectiva procesal del nuevo marco regulador", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021.

DE HOYOS SANCHO, M., "El uso jurisdiccional de los Sistemas de Inteligencia Artificial y la necesidad de su armonización en el contexto de la Unión Europea", capítulo en la obra colectiva dirigida por LLORENTE SÁNCHEZ-ARJONA, M., *Estudios procesales sobre el espacio europeo de justicia penal*, Thomson Reuters Aranzadi, Cizur Menor 2021.

ESPARZA LEIBAR, I., "El proceso debido como único modelo aceptable para la resolución de conflictos en un estado de derecho y como presupuesto para la globalización", capítulo en la obra colectiva, *El Derecho Procesal español del siglo XX. A golpe de tango (Homenaje a Juan Montero Aroca)*. Tirant lo Blanch, Valencia 2012.

ESPARZA LEIBAR, I., "Protección de datos de carácter personal y proceso penal", capítulo en la obra colectiva, *Justicia con ojos de mujer. Cuestiones procesales controvertidas*, publicada con motivo del Congreso conmemorativo del décimo aniversario de las Jornadas Justicia con Ojos de Mujer (2008–2017), Tirant lo Blanch, Valencia 2018.

ESPARZA LEIBAR, I., "La Inteligencia Artificial y el derecho fundamental a la protección de datos de carácter personal", en la obra colectiva dirigida por Silvia Barona Vilar: *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021.

ETXEBERRIA GURIDI, J. F., "La protección de los datos de carácter personal en el ámbito de la investigación penal", AEPD, Madrid 1998.

FÉREZ-MANGAS, D.; ANDRÉS-PUEYO, A., "Eficacia predictiva en la valoración del riesgo de quebrantamiento de permisos penitenciarios", en La Ley Penal n.° 134 de 2018.

GÓMEZ COLOMER, J. L., *La contracción del Derecho Procesal Penal,* Tirant lo Blanch, Valencia 2020.

GÓMEZ COLOMER, J. L., "Unas reflexiones sobre el llamado "juez-robot", al hilo del principio de la independencia judicial", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021.

LLORENTE SÁNCHEZ-ARJONA, M., directora, *Estudios procesales sobre el espacio europeo de justicia penal*, Thomson Reuters Aranzadi, Cizur Menor 2021.

MARTÍN DIZ, F., "Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021.

MARTÍNEZ VÁZQUEZ, F., "La nueva Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales", Diario La Ley, de 28 de mayo de 2021.

NIEVA FENOLL, J., Inteligencia artificial y proceso judicial, Marcial Pons, Madrid 2018.

PÉREZ ESTRADA, M. J., "Efectos de la vulneración de la protección de los datos personales en el proceso penal", en *La ley penal: revista de derecho penal, procesal y penitenciario*, n.° 135, 2018.

PÉREZ ESTRADA, M. J., "La tramitación automatizada del proceso", capítulo en la obra colectiva editada por BARONA VILAR, S., *Justicia algorítmica y Neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia 2021.

Los registros biométricos y su aplicación al proceso penal desde una perspectiva constitucional[1]

Pablo Gallego Rodríguez

Profesor Ayudante Doctor
Universidad de Córdoba

SUMARIO: I. INTRODUCCIÓN. II. LA ESTRUCTURA JURÍDICO-POLÍTICA DEL ESTADO CONSTITUCIONAL. CUESTIONES PRELIMINARES. III. LA CONSTITUCIÓN ESPAÑOLA DE 1978. IV. LA DOCTRINA DEL TRIBUNAL CONSTITUCIONAL. V. LA LEY ORGÁNICA 7/2021, DE 26 DE MAYO, DE PROTECCIÓN DE DATOS PERSONALES TRATADOS PARA FINES DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN Y ENJUICIAMIENTO DE INFRACCIONES PENALES Y DE EJECUCIÓN DE SANCIONES PENALES. 1. *Cuestiones de partida*. 2. *¿Qué es la biometría?* 3. *La Estrategia Europea de Datos*. 4. *El tratamiento de los datos biométricos*. VI. LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN COM/2021/206 FINAL. 1. *Cuestiones preliminares*. 2. *¿Qué es la inteligencia artificial?* 3. *La Propuesta de Reglamento*. VII. A MODO DE CONCLUSIÓN.

1. El presente trabajo se ha elaborado en el marco del Proyecto de Investigación I+D+i de generación de conocimiento y fortalecimiento científico y tecnológico titulado "Ejes de la Justicia en tiempos de cambio", del Ministerio de Ciencia e Innovación, con REF PID2020-113083GB-100, del que el autor es Investigador y desde el ámbito de las actividades del grupo de Investigación PAIDI SEJ-372, "Democracia, Pluralismo y Ciudadanía" del que el autor es miembro.

VIII. BIBLIOGRAFÍA. 1. *Fuentes clásicas*. 2. *Otras fuentes*. 3. *Sentencias del Tribunal de Justicia de la Unión Europea*. 4. *Sentencias del Tribunal Constitucional*.

I. INTRODUCCIÓN

El interés por identificar[2] de manera unívoca a una persona por lo que es (biometría) y no solo por lo que sabe o tiene es una preocupación histórica vinculada al concepto de seguridad[3].

En España, el germen normativo de la identificación antropométrica lo encontramos en el Real decreto de 14 de septiembre 1896[4], en virtud del cual y, ante la picaresca de los criminales para burlar la ley, se crea, en las cárceles del Reino, y, de un modo normal y regular, un sistema de identificación antropométrico que persigue: abreviar la duración de los procesos, descubrir al criminal de oficio y economizar gastos[5].

2. Historia de los documentos de identidad. España 1820-2016. D.G. Policía; S.G. Logística. En España, a principios del siglo XIX, las cédulas de identidad y los pasaportes interiores incluían una descripción física de su titular con la que se le podía autorizar a transitar por el interior del territorio español. Por otro lado, el diseño del primer DNI es obra de Aquilino Rieusset Planchón ganador del concurso publicado en el BOE en fecha 10 de mayo de 1946 y dotado con un premio de 30.000 pesetas. El primer DNI, contaba con la fotografía de su titular, era de color verde, incluía datos como empleo, profesión o cargo y distinguía entre cuatro categorías dependiendo de la situación económica del titular. Se expidió en Valencia el 20 de marzo de 1951 y estuvo vigente hasta el año 1961, disponible en https://www.dnielectronico.es/PDFs/Historia_de_los_documentos_de_identidad.pdf [última consulta: 15-01-22].

3. Este hecho no guarda relación con las marcas *al rojo vivo* y tatuajes que se han realizado en diversas culturas a esclavos y criminales para dejar constancia de su pertenencia a dichos grupos.

4. Gaceta de Madrid: núm. 258, de 14/09/1896, página 985, disponible en https://www.boe.es/datos/pdfs/BOE//1896/258/A00985-00985.pdf [última consulta: 15-01-22].

5. En la exposición de motivos del Real decreto de 1896 se puede leer: "*Reconocida y ya sancionada por larga experiencia en otras naciones la importancia que para la más corta y pronta administración de justicia en lo criminal tiene el sistema de filiaciones señalamientos antropométricos de los delincuentes, como medio único seguro de identificar á los criminales que al reincidir cambian de nombre para burlar la ley, y único también capaz de abreviar la duración de los procesos, suprimiendo múltiples y siempre lentas actuaciones, el Ministro que suscribe cree llegado el momento de establecer de un modo normal y regular el servicio de identificación antropométrica en las cárceles del Reino. (…) con arreglo á los últimos adelantos i perfeccionamientos del sistema Bertillon; instalado en amplio y bien adecuado local; provisto de todo el material é instrumental necesario para el perfecto funcionamiento del servicio; dotado, en fin, de personal idóneo y ya perito, que viene funcionando desde el primer día del presente año judicial y que ha realizado en tan corto espacio de tiempo la identificación probada de más de 150 detenidos con nombres falsos. (…) En suma, conseguir á un mismo tiempo descubrir al criminal de oficio, que se oculta tras de un nombre falso; ganar el tiempo que por lo general se pierde en largas é infructuosas actuaciones y diligencias de identificación, y economizar á los pueblos los cuantiosos gastos que ocasionan los detenidos en tanto se*

El sistema de identificación antropométrico adoptado es el denominado sistema Bertillon[6]. Su implantación no resultó sencilla y topó con diversas dificultades; principalmente, la falta de medios y de personal cualificado. En este sentido, y con un claro deseo de progreso y de equiparación respecto a otras Naciones, se aprobó el Real Decreto de 18 de febrero de 1901[7] por el que reorganizó el servicio de identificación[8].

Dos siglos más tarde, los criminales siguen intentado burlar la ley y pasar desapercibidos; no obstante, tecnológicamente hablando, nuestra sociedad ha evolucionado notablemente. Esta evolución tecnológica no es homogénea en todos los rincones del mundo y en no pocas ocasiones nuestros nacionales tienen que ingeniárselas para poder identificarse[9] y, llegado el caso, no ser confundidos con delincuentes y/o malhechores.

---

tramitan aquéllas, son razones bastante poderosas para acometer con resolución y urgencia el planteamiento y organización del nuevo y científico procedimiento de identificación (…)".

6. El sistema, conocido bertillonaje debe su nombre a su creador Alphonse Bertillón (París 1853).

7. Gaceta de Madrid: núm. 50, de 19/02/1901, páginas 718 a 719. En su exposición de motivos encontramos: "*(…) Pero sería inútil apreciar la reincidencia y convenir en su importancia si al mismo tiempo no existen medios ó elementos necesarios para reconocer á los reincidentes, muchos de los cuales han escapado á su identificación, bien por las deficiencias de los Registros ó Archivos de antecedentes penales, bien por lo rudimentario del procedimiento de identificación, bien por usar de nombres supuestos, recurso éste al que han apelado siempre gran parte de los reincidentes, con grave perjuicio á veces de personas inocentes y honradas, cuyos nombres han tomado. (…) "la falta de medios y de instrumentos í necesarios, la carencia de suficiente personal apto, el desorden que en todo el servicio se nota, han hecho poco menos que inútil, según lo reconoce la misma Junta local de Prisiones de Madrid, la aplicación de un sistema que tan excelente resultado da en otros países más adelantados que el nuestro en lo que atañe á la legislación penitenciaria. (…)* (…) *Deseoso el Ministro que suscribe de remediar esos males y de hacer que España se coloque en este punto al nivel del progreso penitenciario de otras Naciones, (disfrutando de las ventajas que al Derecho penal y al procedimiento criminal reporta la aplicación idónea del sistema Bertillón para la identificación personal, ha creído cumplir un deber ineludible reorganizando el servicio antropométrico-fotográfico en los establecimientos penales, implantándolo en muchas cárceles en que no existe, creando una escuela de donde salgan verdaderos Antropómetras, personas peritas y capaces y dotando á los establecimientos del material necesario para que los sacrificios del Estado, que en este punto han de ser en el orden económico escasísimos, y el deseo de los Gobiernos no resulte, como en tantas otras cuestiones por desgracia, por entero estériles y baldíos*", disponible en https://www.boe.es/datos/pdfs/BOE//1901/050/A00718-00719.pdf [última consulta: 15-01-22].

8. El servicio, dependiente del Ministerio de Gracia y Justicia, y que constaba de diversos gabinetes antropométrico-fotográficos provinciales, gabinetes antropométricos de identificación en establecimientos penales, un Registro Central de reseñas antropométricas, incorporado al Registro Central de penados y rebeldes, de una Escuela práctica de Antropometría judicial en el Gabinete provincial de Madrid y de una Inspección técnica, disponible en https://www.boe.es/datos/pdfs/BOE//1901/050/A00718-00719.pdf [última consulta: 15-01-22].

9. MIQUEL SILVESTRE, J. A., *Manual de aventura overland. La magia de viajar por tus propios medios*. Silver Rider Prodaktions. 2016. pp. 40-51. Parte 2. Documentos y dinero. Carné de conducir. Para él la regla de oro es que si te piden documentos tienes que

Nuestro sistema judicial-policial cuenta con una poderosa aliada la informática, que junto con el nacimiento de Internet en los años 60, ha supuesto un avance sin precedentes en cuanto al almacenamiento y consulta de datos, a la vez que ha revolucionado las comunicaciones haciendo posible consultar de forma prácticamente instantánea millones y millones de datos. Dada la ingente magnitud de los datos se hace preciso un sistema, una herramienta, que nos auxilie en la búsqueda de la información pertinente y para ello podríamos contar con la inteligencia artificial[10] y que a nuestro parecer debe ser entendida como una herramienta más que proporciona una valiosísima información tanto dentro como fuera en el ámbito penal.

Es innegable que la inteligencia artificial sustentada en datos biométricos puede llegar a suponer un impacto sin precedentes en nuestro sistema de protección de derechos fundamentales, pero al mismo tiempo su utilidad es innegable al proporcionar una valiosísima información incluso para la propia protección de los citados derechos[11].

A lo largo del presente capitulo se analizará el uso de los registros biométricos en combinación con la inteligencia artificial y su aplicación al proceso penal desde una perspectiva constitucional.

Para ello, se partirá del análisis del Artículo 18.4 de nuestro texto constitucional para, seguidamente, analizar tanto la Ley Orgánica 7/2021, de

---

enseñar algo y el, según sus palabras, logró recorrer 17 países sin carné de conducir. Miquel salé de España dirección este con el carné internacional y recorre con normalidad el territorio de la Unión Europea. Las dificultades comienzan en Ucrania dónde su carné internacional de tanto abrirlo y cerrarlo y algún que otro intento de multa/mordida/soborno se rompe y pierde la parte final que es la identificatoria. A pesar de ello logra cruzar Rusia y Kazajstán (con un documento sin foto ni nombre). En Tashkent (capital de Uzbekistán) localiza al cónsul y ante la falta de otros medios y en lo que quedaba de carné escribe su nombre a bolígrafo, le "*plantó[a]*" una foto y el cónsul (honorario) le estampa un sello. Con este documento logra cruzar Kazajstán a Azerbaiján; Georgia; Turquía; Siria; Jordania; Líbano; incluso Israel en dónde según sus palabras, "*te miran hasta los calzoncillos*".

10. En páginas posteriores se profundizará en este término; no obstante, como primera aproximación la inteligencia artificial podría definirse como: "*(…) la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear. La IA permite que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico. La máquina recibe datos (ya preparados o recopilados a través de sus propios sensores, por ejemplo, una cámara), los procesa y responde a ellos. Los sistemas de IA son capaces de adaptar su comportamiento en cierta medida, analizar los efectos de acciones previas y de trabajar de manera autónoma*". En Parlamento Europeo, disponible en https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa [última consulta: 15-01-22].
11. El derecho en cuanto que disciplina científica cuenta con un objeto y con un método que le son propios, métodos y objetos que no son inmutables y que deben adaptarse a la realidad propia del momento histórico y ser capaz de normativizarlo.

26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. "BOE" núm. 126, de 27/05/2021 como la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial –Ley de inteligencia artificial– y se modifican determinados actos legislativos de la unión COM/2021/206 final) para finalizar con una serie de observaciones y cautelas constitucionales a modo de conclusión.

II. LA ESTRUCTURA JURÍDICO-POLÍTICA DEL ESTADO CONSTITUCIONAL. CUESTIONES PRELIMINARES

Antes de analizar los diversos preceptos constitucionales de aplicación al presente trabajo consideramos oportuno realizar un somero análisis de una serie de cuestiones básicas que han servido para diseñar la estructura jurídico-política de nuestro modelo de Estado al que denominamos Estado Constitucional. Con ellas, podremos delimitar, por un lado, el ámbito de aplicación del presente estudio y, por otro, exigir el desarrollo de una legislación adecuada y eficaz en sus diferentes ámbitos de acuerdo con dichos principios.

Para A. HAURIOU el objeto del Derecho constitucional es el: "*encuadramiento jurídico de los fenómenos políticos*"[12]. De la definición se desprenden dos cuestiones; por un lado el objeto que son los fenómenos políticos o fenómenos de poder y por otro el método que es el tratamiento jurídico de este objeto.

A la hora de referirnos a los fenómenos políticos o fenómenos de poder es obligado hacer alusión a la disputa entre el iusnaturalismo (justicia) y el positivismo (coacción; sistemas de normas;…) y llegar así a una definición de síntesis encuadrable dentro de la teoría tridimensional del Derecho: "*Conjunto de preceptos de conducta obligatorios, establecidos por los hombres que viven en sociedad y destinados a hacer reinar el orden y la justicia en las relaciones sociales*"[13]. En la definición se pueden observar tres dimensiones: la normativa (preceptos de conducta obligatorios); la valorativa (destinados a hacer reinar el orden y la justicia) y, la fáctica que se encuentra implícita en el hecho de que esas normas se cumplen. La nota fáctica, coactiva o imperativa implica que el Estado debe garantizar que esas normas se cumplen.

12. HAURIOU, A., *Derecho Constitucional e Instituciones Políticas*, Barcelona 1971, p. 17.
13. *Ibidem*, p. 22.

El poder podría ser observado como "*la capacidad de un individuo, de un grupo o de una institución para determinar a otro sujeto*" o bien "*la capacidad de obligar a otros a hacer algo que no harían si no mediara el influjo de dicho individuo, grupo o institución*"[14].

Ampliando la definición, "*El poder es la capacidad efectiva para que alguien actúe de una manera que él, por su propia cuenta, no elegiría; en otras palabras, la capacidad de forzar a alguien a hacer algo contra su voluntad, por medio de ciertos procedimientos. En el nivel personal, controlamos a los demás persuadiéndoles, amenazándoles, provocándoles, frustrándoles: en el nivel político, la amenaza de aplicación de una sanción, el uso de propaganda, el invocar poderes particulares, todas estas operaciones son típicas de poder*"[15].

De igual forma, para WEBER ha sido el Estado el que ha reclamado de forma exitosa el "*monopolio de la violencia física legítima*"[16].

Por su parte RECASENS hace hincapié en que las normas dictadas o reconocidas por el Estado deben ser cumplidas al tiempo que van dirigidas a la realización de los principios valorativos de la justicia[17].

En nuestro estudio hacemos referencia a un tipo especial de poder que es el poder político y que se caracteriza porque se dirige a la gestión de los intereses que afecta a todos los miembros de una determinada comunidad.

En palabras de BODINO "*además de la soberanía, es preciso que haya alguna cosa en común y de carácter público, como el patrimonio público, el tesoro, el recinto de la ciudad, las calles, las murallas, las plazas, los templos, los mercados, los usos, las leyes, las costumbres, la justicia, las recompensas, las penas y otras cosas semejantes, que son comunes o públicas, o ambas cosas a la vez*"[18].

Las notas que lo diferencian de otros poderes son tres. En primer lugar y como hemos visto en el párrafo anterior se debe ocupar de los asuntos comunes; en segundo lugar es el poder superior a todos y, por lo tanto, no reconoce ningún otro poder superior y, en tercer lugar, se ejerce

14. PINTACUDA, E., *Breve curso de política*, Santander, 1994, p. 126.
15. GOODWIN, B., *El uso de las ideas políticas*, Barcelona, 1997, p. 276.
16. WEBER, M. *La política como vocación* (1919) dentro de El político y el científico "*Hoy, por el contrario, tendremos que decir que Estado es aquella comunidad humana que, dentro de un determinado territorio (el territorio es un elemento distintivo), reclama (con éxito) para sí el monopolio de la violencia física legítima*", disponible en http://www.hacer.org/pdf/WEBER.pdf [última consulta: 15-01-22].
17. RECASENS SICHES, L. *Introducción al estudio del Derecho*, México, 1977, p. 44 "(…) *lo es tan sólo el conjunto de normas dictadas o reconocidas por el Estado, que obtienen real eficacia, y que se encaminan a la realización de los principios valorativos de justicia*".
18. BODINO, J., *Los seis libros de la República*, Madrid 2000, p. 17.

por los denominados gobernantes en nombre de la comunidad a la que representan.

A estos elementos y no exento de cierta polémica hay que añadir un elemento ya que es necesario que ese gobierno sea recto. En palabras de BODINO: "*un recto gobierno de varias familias, y de lo que les es común, con poder soberano*"[19] y según San Agustín "*sin la virtud de la justicia, ¿qué son los reinos sino unos execrables latrocinios?*"[20].

La democracia se basa en el principio de la soberanía popular. Para KRIELE "*en el Estado Constitucional no hay soberano*" ya que el pueblo es el soberano únicamente en el momento en el que está desarrollando su constitución –periodo constituyente– y una vez que se dota de un texto constitucional deja de serlo y pasa a ser súbdito. De este modo, la democracia se articula en un sistema de pesos y contrapesos en el que la idea de límite cobra una especial relevancia ya que el poder se encuentra distribuido entre diferentes órganos que únicamente tienen las competencias constitucionales previamente atribuidas[21].

Todos los sistemas políticos desde los más antiguos a los más recientes y complejos se encuentran organizados sobre tres de elementos esenciales: el territorio, la población, y el poder al que habría que añadir otro que es el reconocimiento por parte de la comunidad internacional. De esta forma, podríamos señalar que todos los sistemas políticos están constituidos de una determinada forma, pero para que se pueda hablar de un sistema constitucional en sentido moderno es necesario, por una lado que existía una división de poderes y, por otro, el reconocimiento de los Derechos de las personas.

Para LOEWENSTEIN: "*El reconocimiento y protección de los derechos y de las libertades fundamentales son el núcleo esencial del sistema político en una democracia constitucional*" y, por otro lado analiza "*el criterio del análisis ontológico radica en la concordancia de las normas constitucionales con la*

19. *Ibidem,* p. 17.
20. SAN AGUSTÍN, *La ciudad de Dios*, Madrid 1941, p. 151.
21. KRIELE, M., *Introducción a la Teoría del Estado*, Buenos Aires 1980, pp. 150-153. "*(…) Pero no hay dentro del Estado constitucional un soberano, es decir, no hay nadie que tenga soberanía, esto es, no hay poder, siquiera latente, que tengas las características de ser indiviso, incondicionado, ilimitado, ser última ratio en caso particulares, que pueda violar y crear derecho. Más aún: la existencia de un soberano en este sentido, por un lado, y del Estado constitucional por otro, son dos situaciones opuestas, mutuamente excluyentes. En otras palabras: la idea de un soberano es dinamita revolucionaria para el estado constitucional. (…) en el Estado constitucional sólo hay competencias, limitadas por el derecho constitucional preexistente. El poder estatal está distribuido entre los órganos, y todo órgano sólo tiene aquel poder jurídico que le ha sido asignado por el orden constitucional*".

realidad del proceso del poder"; es decir, si existe o no concordancia entre el texto constitucional vigente y el efectivo ejercicio del poder[22].

Más recientemente, en palabras de FRIEDRICH "*el constitucionalismo occidental y las Constituciones que se han creado en este sentido se basan en dos principios fundamentales que se complementan recíprocamente: en la división del Poder y en la esfera de libertad que se garantiza y concede al ciudadano (…) se le aprecia como persona, su dignidad es casi siempre inviolable, considerándose fundamentalmente provistos de los mismos derechos a todo hombre o mujer que pertenezcan a una comunidad popular*"[23].

La cuestión es que en el Siglo XXI es sumamente complejo delimitar diversas facetas de los elementos básicos del Estado como sucedía antaño.

En nuestra esfera nacional, como en la de otros países de nuestro alrededor, la arquitectura territorial e institucional, ha sufrido importantísimos avances en los últimos años. Concretamente, en nuestro país en los últimos treinta años por lo que "*ha llegado el momento de reaccionar y constitucionalizar la estructura del Estado*"[24].

Hoy en día vivimos en una sociedad altamente digitalizada, en la que la comunicación es prácticamente instantánea, y en la que los avances tecnológicos parecen hacer realidad las ilusiones más fantasiosas de las películas de ciencia ficción, como podría ser: el famoso motor de curvatura del Enterprise correspondiente a la nave estelar de Star Trek y que permitía viajar a la velocidades superiores a las de la luz[25] y el transportar información directamente implantada en el cerebro como sucedía en

22. LOEWENSTEIN, K., Teoría de la Constitución. Editorial Ariel, Barcelona, 1986, p. 12. Esquemáticamente existen tres clases de Constitución; las normativas en las que se da una efectiva relación entre el texto escrito y la realidad política; las nominales en las que no se da una relación efectiva entre el texto escrito y la realidad política pero se espera que se de en un futuro y las semánticas en las que, al igual que en el caso anterior, no se da una relación efectiva entre el texto escrito y la realidad política a la vez que no se espera que se dé ya que lo que se persigue es engañar o disimular.
23. FRIEDRICH, C.J., *La democracia como forma política y como forma de vida*. Traducción de C. Zabal Schmidt-Völz. Ediciones Olejnik, 2020. p. 12.
24. AGUDO ZAMORA, M., Reforma Constitucional y Estado Autonómico, Tecnos, 2019, p. 37.
25. BOBRICK, A. y MARTIRE, G., "Classical and Quantum Gravity", Volume 38, Number 10, disponible en https://iopscience.iop.org/article/10.1088/1361-6382/abdf6e [última consulta: 15-01-22]// Viajar por el espacio más rápido que la luz no es solo ciencia ficción: hay físicos (serios) trabajando en esta idea, disponible en https://www.xataka.com/investigacion/viajar-espacio-rapido-que-luz-no-solo-ciencia-ficcion-hay-fisicos-serios-trabajando-esta-idea [última consulta: 15-01-22]// Viajar más rápido que la velocidad de la luz es posible. Movernos a través de otros sistemas estelares lleva siendo un sueño desde hace mucho. Ahora, parece que estamos un poco más cerca de lograrlo, disponible en https://www.muyinteresante.es/ciencia/

la película Johnny Mnemonic[26] y que a día de hoy se podría ver reflejada en el proyecto Neuralink[27]. Su presidente Elon Musk, asegura que su empresa empezará a implantar chips cerebrales en humanos en 2022 y que estos permitirán a las personas comunicarse con dispositivos electrónicos a través del pensamiento[28].

Una sociedad al mismo tiempo altamente desnaturalizada e insolidaria en la que las desigualdades se perpetúan como muestran diversos informes; entre ellos, "*20 años de asesoría jurídica en contextos de exclusión*" de la Asociación Pro Derechos Humanos de Andalucía[29].

Estas desigualdades se llegan a incrementar dejando a un lado a diversos colectivos con insuficiencias competencias digitales (mayores, desempleados, migrantes) y que no pueden o no saben manejar las modernas herramientas y a los que no se les garantiza debidamente el Derecho a no ser digital; en palabras de PIÑAR "*Es esencial garantizar el derecho a no ser digital, a que te atienda una persona (…) Somos personas, no personas digitales*" advirtiéndonos de una posible brecha digital por lo que solicita el manteniendo de una línea de contacto humano tanto en las administraciones como en las empresas[30].

Por todo ello, el Estado, detentador del monopolio de la fuerza física legítima[31], debe adoptar de forma urgente las medidas legislativas

---

articulo/viajar-mas-rapido-que-la-velocidad-de-la-luz-es-posible-191615797394 [última consulta: 15-01-22].

26. Película Johnny Mnemonic. Sinopsis: "*Corre el año 2021 y la mitad de la población sufre de una enfermedad llamada 'síndrome de atenuación de los nervios'. Johnny (Keanu Reeves) es un mensajero de información, una persona que lleva los datos más importantes del siglo XXI, directamente implantados en su cerebro. Su información será muy valiosa para una corporación farmacéutica. (FILMAFFINITY)*", disponible en https://www.filmaffinity.com/es/film222381.html [última consulta: 15-01-22].
27. Neuralink. Breakthrough Technology for the Brain disponible en https://neuralink.com [última consulta: 15-01-22].
28. Elon Musk asegura que Neuralink empezará a implantar chips cerebrales en humanos en 2022 disponible en https://www.abc.es/ciencia/abci-elon-musk-asegura-neuralink-empezara-implantar-chips-cerebrales-humanos-2022-202112170110_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F [última consulta: 15-01-22].
29. Asociación Pro Derechos Humanos de Andalucía. 20 años de foto fija de exclusión social en Córdoba, disponible en https://paradigmamedia.org/20-anos-de-foto-fija-de-exclusion-social-en-cordoba/ [última consulta: 15-01-22].
30. PIÑAR MAÑAS, J. l., *Es esencial garantizar el derecho a no ser digital, a que te atienda una persona*, disponible en https://www.eldiario.es/tecnologia/jose-luis-pinar-esencial-garantizar-derecho-no-digital-atienda-persona_128_8543756.html [última consulta: 15-01-22].
31. Tesis desarrollada por WEBER, M., *op. cit.* El Estado es el detentador del monopolio de la fuerza física legítima después de habérsela arrebatado a los poderes medievales, antiguos depositarios de la misma.

oportunas para la correcta protección de los diversos derechos en juego y que principalmente, a los efectos del presente trabajo son la justicia, la seguridad y la libertad.

III. LA CONSTITUCIÓN ESPAÑOLA DE 1978

Nuestro texto constitucional en su artículo 9.1 indica que tanto los ciudadanos como los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico y este hecho enlaza con la idea anteriormente expresada de límites y de pesos y contrapesos.

Ahondando en el grado de exigibilidad de unos y otros, éste no es el mismo ya que, respecto a los ciudadanos, lo que se predica es un deber general de abstención y, respecto a los poderes públicos, esta exigibilidad se encuentra reforzada con la obligación o deber general positivo de realizar sus funciones de acuerdo con la Constitución. En palabras del Tribunal Constitucional STC[32] 101/1983: "*La sujeción a la Constitución que proclama su art. 9.1 es una consecuencia obligada de su carácter de Norma suprema, que se traduce en un deber de distinto signo para los ciudadanos y los poderes públicos; mientras los primeros tienen un deber general negativo de abstenerse de cualquier actuación que vulnere la Constitución, sin perjuicio de los supuestos en que la misma establece deberes positivos (arts. 30 y 31, entre otros), los titulares de los poderes públicos tienen, además, un deber general positivo de realizar sus funciones de acuerdo con la Constitución, es decir, que el acceso al cargo implica un deber positivo de acatamiento entendido como respeto a la misma, lo que no supone necesariamente una adhesión ideológica o una conformidad a su total contenido*".

Por lo que al presente estudio interesa, nuestra constitución ha sido una de las primeras en prestar una especial atención al uso de la informática "*dado que es precisamente en los años de su redacción cuando comienzan a apreciarse los peligros que puede entrañar el archivo y uso ilimitado de los datos informáticos*"[33] tomando como pauta el modelo de diferentes textos constitucionales. Principalmente el texto de la Constitución

32. Sentencia del Tribunal Constitucional 101/1983, de 18 de noviembre (BOE núm. 298, de 14 de diciembre de 1983), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1983-32816.pdf [última consulta: 15-01-22].

33. ELVIRA PERALES, A., y actualizado (2011) por GONZÁLEZ ESCUDERO, A., *Sinopsis artículo 18*. Congreso de los Diputados, disponible en https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2 [última consulta: 15-01-22].

portuguesa de 1976[34] y, en cierta medida, el de la Constitución Griega de 1975[35].

Para ABAD ALCALÁ "*la ligazón entre derechos fundamentales y los textos resultantes en todo proceso constituyente, así como la trascendencia que en éste posee el reconocimiento de estos derechos fundamentales en innegable*"[36]. En nuestro texto constitucional el uso limitado de la informática se ubica en el artículo 18.4 dentro de la Sección 1.ª De los derechos fundamentales y de las libertades públicas; Capítulo II Derechos y libertades; Título I De los derechos y deberes fundamentales lo que nos indica su especial importancia ya que goza del nivel máximo de protección con garantías jurisdiccionales, normativas e institucionales.

Por su parte, el artículo 18.4 CE subraya la especial atención que debe prestar el legislador en cuanto al uso de la informática y como la ley debe limitar su uso para que el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos quede debidamente garantizada. Como podemos observar no se trata de un mero reconocimiento y, nuevamente, se ahonda en el grado de exigibilidad exigible a los a los poderes públicos.

Su aprobación no estuvo exenta de un rico debate parlamentario; como muestra[37]:

a) Enmiendas presentadas al Anteproyecto: Sr. Carro Martínez – N.° 2; Sr. Jarabo Payá – N.° 16; Sr. Gastón Sanz – N.° 79; G. P. Minoría Catalana – N.° 117 (la única en ser tenida en cuenta); G. P. Socialista del Congreso – N.° 339; G. P. Mixto – N.° 470 que hacía notar: "La ley regulará el acopio, uso y difusión de los datos personales contenidos en archivos o registros, susceptibles de acceso automático,

34. Constitución de Portugal de 1976 (con enmiendas hasta 2005). Artículo 35. Utilización de la Informática *"1. Todo ciudadano tendrá derecho de acceso a todos los registros informáticos que le conciernen, a requerir que sean rectificados y actualizados, y a ser informado de la finalidad a que se destinan las informaciones, de conformidad con lo dispuesto en la ley. 2. La ley definirá el concepto de 'dato personal'"*, disponible en https://www.constituteproject.org/constitution/Portugal_2005.pdf?lang=es [última consulta: 15-01-22].
35. Constitución de Grecia de 1975 (con enmiendas hasta 2008). Artículo 9.ª "*Conforme a la ley, todos tienen derecho a la protección de la recogida, tratamiento y uso, especialmente por medios electrónicos, de sus datos personales. Esta protección se encomendará a una autoridad independiente, que se constituirá y operará de acuerdo con una ley específica*", disponible en https://www.constituteproject.org/constitution/Greece_2008.pdf?lang=es [última consulta: 15-01-22].
36. ABAD ALCALÁ, L. *Las libertades informativas en el ámbito internacional.* Editorial Dykinson, 2020. p. 120.
37. Trabajos parlamentarios de la Constitución Española, disponible en https://app.congreso.es/est_consti/ [última consulta: 15-01-22].

con objeto de garantizar las libertades públicas y el ordenamiento constitucional"; Sr. Sancho Rof – N.° 716; G. P. Unión de Centro Democrático – N.° 779.

b) Enmiendas presentadas al texto aprobado por el Pleno del Congreso: D. Camilo José Cela y Trulock – N.° 145; D. Isaías Zarazaga Burillo – N.° 261.

c) Voto particular presentado al Dictamen de la Comisión del Senado: Voto particular n.° 88 (enmienda 261 modificada in voce) – D. Isaías Zarazaga Burillo. (Grupo político independiente y presidente de la comisión especial de política científica (07/12/1977 al 02/01/1979) que hacía notar que: "*vendrán otras muchas técnicas –no sólo la informática–, y resulta imprescindible prevenir y prepararnos para ellas adecuadamente y no quedarnos desplazados en la carrera, aun antes de haber salido de la meta*"[38].

Finalmente del texto del anteproyecto de 5 de enero de 1978: "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos*" se pasa, virtud de la enmienda núm. 117 del G.P. Minoría Catalana, a la "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

Como puede observarse, se añade, *in fine*, la coletilla "*y el pleno ejercicio de sus derechos*" cuestión ésta que no es baladí ya que, junto con una concreta delimitación de dos ámbitos de especial importancia como son el honor y la intimidad personal se deja la puerta abierta a modo de cajón de sastre a garantizar otros derechos que el uso de la informática pudiera afectar. Se reproduce a continuación la justificación contenida en la propia enmienda:

"*La limitación establecida en el presente artículo al uso de la informática, centrada exclusivamente en el honor y la intimidad personal y familiar, parece ignorar que los posibles perjuicios del uso de la informática pueden producirse, además y de manera fundamental, en el ejercicio de los derechos tanto políticos como cívicos por parte de los ciudadanos. Por esta razón, se estima conveniente introducir en el artículo que se enmienda la expresión a que se ha hecho referencia del pleno ejercicio de sus derechos*"[39].

38. ZARAZAGA BURILLO, I., Debate en el Pleno del Senado del Proyecto de Constitución, p. 4487./3. Sesión celebrada el miércoles 27 de septiembre de 1978, p. 4601./ Artículo 18. Extracto: "*(…) Para garantizar el honor y la intimidad personal, familiar y social de los ciudadanos y el pleno ejercicio de sus derechos, la ley limitará la utilización de la informática y otros procedimientos o técnicas que puedan atentar contra los citados derechos*", disponible en https://app.congreso.es/est_consti/ [última consulta: 15-01-22].

39. Congreso de los Diputados. Enmiendas al Anteproyecto de Constitución p. 198, disponible en https://app.congreso.es/est_consti/ [última consulta: 15-01-22].

IV. LA DOCTRINA DEL TRIBUNAL CONSTITUCIONAL

Para nuestro Tribunal Constitucional el orden legislativo debe ser interpretado de la forma más favorable para la *"efectividad"* de los derechos fundamentales. En palabras del Tribunal Constitucional STC 34/1983 de 6 de mayo: "*En materia de derechos fundamentales, como reiteradamente ha señalado este TC, la legalidad ordinaria ha de ser interpretada de la forma más favorable para la efectividad de tales derechos*"[40].

Por su parte, el uso de la informática ha sido una preocupación constante para nuestro tribunal.

En una primera fase se consideró que este derecho se encontraba íntimamente vinculado al derecho a la intimidad pero, en un momento posterior, STC 254/1993 de 20 de julio, se consideró que el texto constitucional había incorporado una nueva garantía en respuesta a una nueva amenaza a la dignidad y a los derechos de la persona[41].

Respecto a la "reserva de configuración legal" (*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*) la STC 254/1993 de 20 de julio, hace hincapié en la directa vinculación y aplicabilidad de los derechos y libertades fundamentales ante los poderes públicos y, por lo tanto, fuente de derechos y obligaciones y no meros principios programáticos[42].

40. STC 34/1983, de 6 de mayo. (BOE núm. 120, de 20 de mayo de 1983), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1983-14443.pdf [última consulta: 15-01-22].

41. STC 254/1993, de 20 de julio (BOE núm. 197 de 18 de agosto de 1993) disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1993-21425.pdf [última consulta: 15-01-22]// corrección de errores disponible en https://hj.tribunalconstitucional.es/docs/BOE/Correcciones/BOE-T-1994-6208.pdf [última consulta: 15-01-22] [FJ 6] "*Dispone el art. 18.4 C.E. que 'La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos'. De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'*".

42. *Ibidem*, [FJ 6] "*(…) cuando se opera con una 'reserva de configuración legal' es posible que el mandato constitucional no tenga, hasta que la regulación se produzca, más que un mínimo contenido, que ha de verse desarrollado y completado por el legislador. Pero de aquí no puede deducirse sin más (…), que los derechos (…) no forman parte del contenido mínimo que consagra el art. 18 C.E. con eficacia directa, y que debe ser protegido por todos los poderes públicos y, en último término, por este Tribunal a través del recurso de amparo (art. 53 CE)*".

Por su parte, la STC 94/1998, de 4 de mayo hace referencia a la STC 254/1993, analizada *ut supra*¸ haciendo propia la declaración de que el artículo 18.4 de nuestro texto constitucional incorporó una nueva garantía a los derechos y libertades fundamentales, con una especial referencia al derecho al honor y a la intimidad. Respecto a este último derecho la sentencia declara que se deber adoptar una actitud positiva que se ver reflejada en un "*derecho de control sobre los datos relativos a la propia persona*".

De igual forma, la sentencia hace referencia a un denominado "*habeas data*" que se concreta en el derecho a controlar el uso de estos una vez que se han incorporado en un programa informático, así como, la posible oposición, por parte de los ciudadanos, a que estos datos de carácter personal sean utilizados con fines diferentes a los que dieron origen a su obtención.

La sentencia incide en que el uso informatizado de datos con fines diferentes a los autorizados podría constituir un "*grave atentado a los derechos fundamentales de la persona*" y, por lo tanto, esta utilización indebida podría ser objeto de la oportuna demanda de amparo. Seguidamente la sentencia hace referencia a la legislación que desarrolla lo previsto en el artículo 18.4 y hace especial mención a modo de "*principio cardinal*" de la protección de datos a los principios de congruencia y racionalidad en su utilización, haciendo una especial mención a modo de tutela reforzada respecto de los datos sensibles, a la vez que prohíbe taxativamente su uso para finalidades diferentes a aquellas que motivaron su obtención legítima a la vez que reconoce una tutela reforzada respecto de los datos sensibles[43].

La doctrina constitucional sobre los límites al uso de la informática es reiterada y así la STC 11/1998, de 13 de enero incide nuevamente en que el ciudadano puede oponerse a que determinados datos de tipo personal sean utilizados con una finalidad diferente a la que originó su obtención[44].

43. STC 94/1998, de 4 de mayo (BOE núm. 137 de 09 de junio de 1998), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1998-13334.pdf [última consulta: 15-01-22]// corrección de errores disponible en https://hj.tribunalconstitucional.es/docs/BOE/Correcciones/BOE-T-1998-24155.pdf [última consulta: 15-01-22]. [FJ 4]. "*La STC 254/1993 declaró que el art. 18.4 C.E. incorpora un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad. La garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático ('habeas data') y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención*".

44. STC 11/1998, de 13 de enero. (BOE núm. 37 de 12 de febrero de 1998), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1998-3143.pdf [última consulta: 15-01-22]. [FJ 4]. "*La STC 254/1993 declaró, con relación al art. 18.4 C.E., que dicho precepto incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona (…) La garantía de la intimidad, 'latu*

Respecto a la inclusión de datos en un soporte informático sin el consentimiento expreso del afectado la STC 202/1999, de 8 de noviembre declaró que este hecho, que carece de soporte legal, supone la restricción desproporcionada del derecho fundamental del afectado[45].

El derecho a disponer datos propios (derecho a la autodeterminación informativa) ya sea por parte de un particular o del propio Estado se encuentra analizado por la STC 292/2000, de 30 de noviembre que entendiendo este derecho de una forma más extensa que el derecho a la intimidad ya que alcanza a todos los datos, íntimos o no, que permitan la identificación de la persona y tengan incidencia en el ejercicio de cualquier derecho[46]. Respecto a sus limitaciones y, para no hacer irreconocible el contenido esencial del citado derecho, es necesario que exista un objetivo legítimo, una previsión legal específica para ello y una conjunto de medidas necesarias y proporcionadas al objetivo perseguido[47].

En igual sentido y más recientemente la STC 17/2013, de 31 de enero (BOE núm. 49 de 26 de febrero de 2013) concreta jurídicamente la posible

---

sensu', adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático ('habeas data') y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

45. STC 202/1999, de 8 de noviembre. (BOE núm. 300 de 16 de diciembre de 1999), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1999-23944.pdf [última consulta: 15-01-22]// corrección de errores disponible en https://hj.tribunalconstitucional.es/docs/BOE/Correcciones/BOE-T-2001-20622.pdf [última consulta: 15-01-22]. [FJ 5] "*El tratamiento y conservación en el preciso soporte informático de los datos atinentes a la salud del trabajador, prescindiendo del consentimiento expreso del afectado, ha de calificarse como una medida inadecuada y desproporcionada que conculca por ello el derecho a la intimidad y a la libertad informática del titular de la información*".

46. STC 292/2000, de 30 de noviembre. (BOE núm. 4, de 04 de enero de 2001), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-2001-332.pdf [última consulta: 15-01-22]. [FJ 6] "*(…) el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo*" y [FJ 7] "*El derecho a la protección de datos atribuye a su titular una haz de facultades, a saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos*". [FFJJ 13 y 14] "*La comunicación de datos personales entre Administraciones públicas, sin previo consentimiento informado del interesado, no puede ser autorizada por una norma reglamentaria, pues defrauda la reserva de ley del art. 53.1 CE*".

47. *Ibidem,* STC 292/2000, de 30 de noviembre. [FJ 9] "(…) *ha exigido que tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad democrática, lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito*".

oposición del ciudadano a que determinados datos personales sean utilizados indiscriminadamente para fines distintos de aquel legítimo que justificó su obtención ya sea por el propio Estado o un particular. En este sentido y salvo previsión legal expresa, basada en bienes de dimensión constitucional y con el debido respeto a las exigencias del principio de proporcionalidad, no se permite la comunicación de datos de carácter personal entre Administraciones públicas para el ejercicio de competencias distintas o que versen sobre materias distintas de aquellas que motivaron su recogida[48].

Respecto al debate sobre si las imágenes grabadas en un soporte físico constituyen o no un dato de carácter personal bajo el amparo del artículo 18.4 de nuestro texto constitucional la STC 29/2013, de 11 de febrero reconoce que estas constituyen un dato de carácter personal que queda integrado en la cobertura del art. 18.4 CE, puesto que el derecho fundamental amplía la garantía constitucional a todos los datos que identifiquen o permitan la identificación de la persona y que, a su vez, puedan servir para la confeccionar un perfil personal o para cualquier otra actividad que pueda llegar a constituir una amenaza para sus derechos[49].

La recientemente la STC 27/2020, de 24 de febrero analiza la vulneración del derecho a la propia imagen ante un reportaje periodístico que se documenta con una fotografía extraída de un perfil personal de Facebook (utilización no autorizada de la imagen ajena en la denominada sociedad digital).

48. STC17/2013, de 31 de enero (BOE núm. 49 de 26 de febrero de 2013), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2013-2167.pdf [última consulta: 15-01-22]. [FJ 4] "*(…) los extranjeros gozan en España del derecho fundamental derivado del art. 18.4 CE en las mismas condiciones que los españoles, (…) la entonces llamada 'libertad informática' se configura como 'un derecho a controlar el uso de los datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5; 94/1998, FJ 4)'".*

49. STC 29/2013, de 11 de febrero. (BOE núm. 61 de 12 de marzo de 2013), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2013-2712.pdf [última consulta: 15-01-22]. Sobre la base de la utilización de grabaciones captadas por las cámaras de video-vigilancia ubicadas en el recinto universitario de la Universidad de Sevilla para sancionar a una trabajadora por el incumplimiento de su horario de trabajo vulnerando, al no haber informado al trabajador de dicho tratamiento y pese a la existencia de distintivos que anunciaban la instalación de cámaras y captación de imágenes, el derecho a la protección de datos. [FJ 5] "*Las imágenes grabadas en un soporte físico constituyen un dato de carácter personal que queda integrado en la cobertura del art. 18.4 CE, ya que el derecho fundamental amplía la garantía constitucional a todos aquellos datos que identifiquen o permitan la identificación de la persona y que puedan servir para la confección de su perfil o para cualquier otra utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo*".

Hoy en día es innegable que los avances tecnológicos afectan al conjunto global de los ciudadanos repercutiendo directamente en sus hábitos y costumbres. Una sociedad en la que los usuarios han pasado de ser meros consumidores de contenidos ser productores de los mismos.

En este contexto, es indudable que los límites del derecho al honor, a la intimidad y a la propia imagen, derechos garantes de la vida privada de los propios ciudadanos, pueden quedar hasta cierto punto desdibujados; no obstante, la sentencia hace hincapié en que en la era digital los usuarios continúan siendo titulares de derechos fundamentales y que su contenido es el mismo que en la era analógica.

Por ello y a pesar de que la fotografía se encontraba en abierto, es decir, accesible para todo el mundo no es posible publicar informaciones obtenidas en las redes sociales para ilustrar noticias si no se obtiene el consentimiento expreso del afectado y, por lo tanto, no se puede considerar como un consentimiento indefinido y vinculante el que se presta para una ocasión o con una finalidad determinada; es decir, el usuario de Facebook que "sube" una imagen para que puedan observarla otros tan solo ha prestado su autorizado a ser observado en su perfil o muro y no se extiende a otros actos posteriores, como pudieran ser su publicación o difusión en otro medios y/o plataformas[50].

De las diferentes sentencias analizadas queda clara la exponencial evolución del contenido del artículo 18.4 de nuestro texto constitucional que: "*ha sido tan drástica como la de la sociedad que se día esta Constitución hace cuarenta años, periodo en el que la interpretación constitucional ha permitido su adaptación a la revolución tecnológica que difícilmente sería vaticinable"* y que "*sin duda, estamos ante derechos llamados a ser protagonistas de los debates sociales e institucionales"*[51].

De igual forma nuestro Tribunal Constitucional ha manifestado en repetidas ocasiones ha manifestado que para lograr la efectiva protección

50. STC 27/2020, de 24 de febrero (BOE núm. 83 de 26 de marzo de 2020), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2020-4112.pdf [última consulta: 15-01-22]. [FJ 3] "(…) *Es innegable que los cambios tecnológicos cada vez más acelerados que se producen en la sociedad actual afectan al conjunto global de los ciudadanos repercutiendo directamente en sus hábitos y costumbres (…) Contemplado de esta manera el panorama tecnológico actual y aceptando que la aparición de las redes sociales ha cambiado el modo en el que las personas se socializan, hemos de advertir sin embargo –por obvio que ello resulte– que los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica. (…). Por ello, el usuario de Facebook que 'sube', 'cuelga' o, en suma, exhibe una imagen para que puedan observarla otros, tan solo consiente en ser observado en el lugar que él ha elegido (perfil, muro, etc.)"*.

51. JIMÉNEZ ALEMÁN, Á. A., *Artículo 18* en Comentarios a la Constitución española de 1978. Tomo I. Dir. CAZORLA PRIETO, L. M., y Coord. PALOMAR OLMEDA, A., Thomson Reuters, 2018. pp. 470

de los citados derechos fundamentales es indispensable contar con el consentimiento inequívoco de su titular para poder captar, reproducir y/o tratar su imagen todo ello a la vez que son excepcionales los supuestos en los que no se requiere dicha autorización y siempre que estos se encuentres aparados por la preceptiva ley orgánica.

Otro área a tener en cuenta es la progresiva y cada vez mayor europeización de este ámbito que partiendo del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa que significó el primer instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos. En virtud del Convenio, las Partes deben adoptar las medidas necesarias en su Derecho nacional para aplicar sus principios, a fin de garantizar, en su territorio, el respeto de los derechos humanos fundamentales en el ámbito de la aplicación de la protección de datos[52].

Por su parte, el citado derecho se encuentra reconocido en la Carta de los Derechos Fundamentales de la Unión Europea en su artículo 8[53] y en artículo 16.1 del Tratado de Funcionamiento de la Unión Europea se consagra como uno de los principios de la Unión.

Su inclusión en la Carta de los Derechos Fundamentales de la Unión Europea ha originado diferentes Sentencias del Tribunal de Justicia de la Unión Europea; entre ellas las de fecha 8 de abril de 2014 "*Digital Rights Ireland, Seitlinger Tschohl y otros*"[54]; la de 13 de mayo de 2014 "*Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. Petición de decisión prejudicial planteada por la Audiencia Nacional*"[55] y la de 6 octubre de 2015 fecha "*Maximillian Schrems y Data Protection Commissioner*"[56].

52. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), disponible en https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108 [última consulta: 15-01-22].
53. Carta de los Derechos Fundamentales de la Unión Europea. (2000/C 364/01). Diario Oficial de las Comunidades Europeas, disponible en https://www.europarl.europa.eu/charter/pdf/text_es.pdf [última consulta: 15-01-22]. "*Artículo 8 Protección de datos de carácter personal*".
54. Sentencia del Tribunal de Justicia de la Unión Europea de fecha 8 de abril de 2014 "*Digital Rights Ireland, Seitlinger Tschohl y otros*". Disponible en https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=ES [última consulta: 15-01-22].
55. Sentencia del Tribunal de Justicia de la Unión Europea de fecha 13 de mayo de 2014 "*Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. Petición de decisión prejudicial planteada por la Audiencia Nacional*", disponible en https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:62012CJ0131 [última consulta: 15-01-22].
56. Sentencia del Tribunal de Justicia de la Unión Europea de fecha 6 de octubre de 2015 "*Maximillian Schrems y Data Protection Commissioner*", disponible en https://eur-lex.

Por su parte, el Tribunal Europeo de Derecho Humanos ha producido una importantísima base jurisprudencial. No es objeto del presente trabajo una análisis detallado de la misma y, dada la importancia del mismo al objeto del presente estudio, se hace una referencia en este momento a la "*Guide to the Case-Law of the of the European Court of Human Rights*. *Data protection. Genetic and biometric data*"[57].

V. LA LEY ORGÁNICA 7/2021, DE 26 DE MAYO, DE PROTECCIÓN DE DATOS PERSONALES TRATADOS PARA FINES DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN Y ENJUICIAMIENTO DE INFRACCIONES PENALES Y DE EJECUCIÓN DE SANCIONES PENALES

1. CUESTIONES DE PARTIDA

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo es el acto legislativo de la Unión Europea por el que se establecen objetivos que todos los países de la UE deben cumplir en materia de protección de datos[58].

Su objeto se recoge en el artículo 1.1 y en él se indica que la Directiva establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Por su parte es el artículo 1.2 el que recoge sus objetivos y según su contenido, el Estado español, la igual que el resto de los Estados miembros

europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62014CJ0362 [última consulta: 15-01-22].

57. Guide to the Case-Law of the of the European Court of Human Rights. Data protection (Updated on 30 April 2021). European Court of Human Rights (Tribunal Europeo de Derechos Humanos; TEDH), disponible en https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf [última consulta: 15-01-22].

58. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016L0680 [última consulta: 15-01-22].

debe, como mínimo: proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. Respecto al intercambio de datos personales por parte de las autoridades competentes en el interior de la Unión, en caso de que el Derecho de la Unión o del Estado miembro exijan dicho intercambio, éstos no deben quedar restringidos ni prohibidos por motivos relacionados con la protección de las personas físicas.

Por su parte, es el artículo 2 el que delimita su ámbito de aplicación que se circunscribe al tratamiento de datos personales por parte de las autoridades competentes a los fines establecidos en el apartado anterior a la vez que se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Es el propio artículo 2 el que, a estos efectos, indica que la presente normativa no se aplica al tratamiento de datos personales en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión por parte de las instituciones, órganos u organismos de la Unión.

En cuanto al plazo de transposición, recogido en el artículo 63, se establece que los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en Directiva.

Nuestro país incumple dicho plazo debido al inestable contexto político existente en el Gobierno español, que se encontraba en funciones durante un largo periodo, y no disponía de la mayoría política necesaria para aprobar la correspondiente ley orgánica. No obstante, para el Tribunal de Justicia de la Unión Europea, las circunstancias del ordenamiento jurídico interno de un Estado miembro no justifican el incumplimiento de las obligaciones y los plazos resultantes de las directivas de la Unión ni, por lo tanto, la transposición tardía o incompleta de estas según se desprende de la Sentencia del Tribunal de Justicia de la Unión Europea de 25 de febrero de 2021 (Asunto C-658/19 Comisión/España)[59].

La STJUE condena con una "*multa ejemplar*" a nuestro país ya que es la primera vez que se impone al mismo tiempo dos tipos de sanciones económicas –previstas en artículo 260.3 del Tratado de Funcionamiento de la Unión Europea–, todo ello a la vez que se condena a nuestro país en costas. La primera de las sanciones económicas es el pago a tanto alzado de

59. STJUE de 25 de febrero de 2021 (Asunto C-658/19 Comisión/España), disponible en https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62019CJ0658 [última consulta: 15-01-22].

unos 15.000.000 de euros[60] y, la segunda, el pago de una multa coercitiva diaria 89548,20 euros desde la fecha de la sentencia, al considerar la Comisión que este es el medio económico apropiado para garantizar que nuestro Estado realizase la oportuna transposición la mayor brevedad posible.

La oportuna transposición se realiza a través de un Proyecto de Ley Orgánica tramitado por vía de urgencia no exento de un rico debate parlamentario (67 enmiendas en el Congreso de los Diputados; 76 enmiendas en el senado) cuya votación de conjunto es ampliamente respaldada siendo los resultados los que siguen: sí: 277; no: 5 y abstenciones: 67[61].

El resultado final es la aprobación de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[62].

A los efectos de la presente investigación son de especial importancia el contenido del artículo 1 que fija el objeto de la ley y que no es otro que la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter persona; el artículo 4 que hace referencia a las autoridades competentes para su tratamiento y los artículos 13 y 14 que respectivamente hacen referencia al tratamiento de categorías especiales de datos personales entre los que se incluyen los datos biométricos y a los mecanismos de toma de decisión individual y automatizado.

Para comenzar con el análisis de la Ley realizaremos en primer lugar un breve repaso por las cuestiones más relevantes a nuestros efectos del preámbulo que, aunque carece de valor normativo, es especialmente relevante ya que, aparte de su función meramente ornamental, contiene los criterios hermenéuticos aplicables.

El preámbulo comienza haciendo referencia a las crecientes amenazas para la seguridad en el contexto nacional e internacional y al componente transfronterizo de las mismas y como este hecho justifica, a modo de objetivo ineludible, la cooperación internacional y la transmisión de

60. *Ibidem*, STJUE de 25 de febrero de 2021. "*Que imponga a dicho Estado miembro, con arreglo al artículo 260 TFUE, apartado 3, una multa coercitiva diaria de 89548,20 euros, con efecto a partir de la fecha del pronunciamiento de la presente sentencia, por incumplimiento de la obligación de comunicar las medidas de transposición de esta Directiva*".

61. Disponible en, https://www.congreso.es/busqueda-de-iniciativas?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_iniciativas_mode=mostrarDetalle&_iniciativas_legislatura=XIV&_iniciativas_id=121%2F000046 [última consulta: 15-01-22].

62. Disponible en https://www.boe.es/eli/es/lo/2021/05/26/7/con [última consulta: 15-01-22].

información de carácter personal entre los servicios policiales y judiciales de los diferentes países.

Seguidamente se aborta el tratamiento de una serie de categorías especiales de datos –los que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical o los genéticos o biométricos– que sólo puede llevarse a cabo cuando sea estrictamente necesario y se cumplan ciertas condiciones.

Respecto a los datos biométricos, –huellas dactilares; imagen facial– objeto de la presente investigación, éstos no siempre forman parte de la denominada categoría especial y sólo forman parte de ella, cuando su tratamiento está dirigido a la identificación de manera unívoca de una persona física, que resulta necesaria para poder singularizar a los autores o partícipes de una infracción penal y de esta forma atribuir o exonerar, sin género de dudas, su participación en determinados hechos, gracias a posibles indicios o vestigios biométricos.

Esta identificación se lleva a cabo por distintas autoridades competentes (Fuerzas y Cuerpos de Seguridad; Administraciones Penitenciarias; Ministerio Fiscal; etc.). No obstante, como hemos visto, el tratamiento de los datos no es igual en todos los supuestos y, de igual forma, no es el mismo para todos los agentes ya que, por ejemplo, se excluye al sistema de Defensa Nacional del ámbito de aplicación de ciertos tratamientos.

El preámbulo continúa describiendo la vertiginosa evolución tecnológica de nuestra sociedad; los riesgos para garantizar y proteger los derechos de los interesados y de la ciudadanía en general y los medios electrónicos de los que se dispone para hacer frente a ella.

Posteriormente se abordan diversos aspectos como: la prohibición de la adopción de decisiones individuales automatizadas; la valoración previa del riesgo y el registro de operaciones y todo ello para concluir en la necesidad de disponer de una habilitación legal que facilite una respuesta rápida y adecuada en el uso de estos datos.

El objeto de la presente Ley se recoge en el artículo 1 y no es otro que el de establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal con unos fines determinados que son:

a) la prevención,

b) la detección,

c) la investigación y

d) el enjuiciamiento

de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Este tratamiento se realiza por parte de las denominadas "autoridades competentes" descritas en el artículo 4 y que es toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos por la Ley. Es decir, en el ámbito de sus respectivas competencias, autoridades competentes serían: Las Fuerzas y Cuerpos de Seguridad; Las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria; el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo a las que habría que añadir a las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Con todo ello queda bien claro el objeto –tratamiento de datos personales– así como los fines –prevención; detección; investigación y el enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública–.

En el artículo 5 encontramos la definición de "datos biométricos" y esta hace referencia a datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Esta definición coincide casi de forma literal [de conducta// conductuales] con el recogido en artículo 3.33) Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados Actos Legislativos de la Unión[63] que analizaremos someramente en el siguiente apartado y, de igual forma en artículo 4, punto 14, del Reglamento(UE) 2016/679 del Parlamento Europeo y del Consejo[64]; en el artículo 3, punto 18, del

63. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican Determinados Actos Legislativos de la Unión, disponible en https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF [última consulta: 15-01-22].

64. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[65]; y en el artículo 3, punto 13, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[66].

2. ¿QUÉ ES LA BIOMETRÍA?

Para el Instituto Nacional de Ciberseguridad español la biometría es "*un método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento"* y, por ello, "*se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar*"[67].

En cuanto a sus características y las tecnologías para medirlas estas son[68]:

a) Características: universalidad: todos los individuos las tienen; singularidad o univocidad: distinguen a cada individuo; permanencia en el tiempo y en distintas condiciones ambientales; medibles de forma cuantitativa.

b) Tecnología: rendimiento: nivel de exactitud; aceptación: por parte del usuario; resistencia al fraude y usurpación.

---

la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1), disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf [última consulta: 15-01-22].

65. Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE (DO L 295 de 21.11.2018, p. 39), disponible en https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-81849 [última consulta: 15-01-22].

66. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva sobre protección de datos en el ámbito penal) (DO L 119 de 4.5.2016, p. 89), disponible en https://www.boe.es/doue/2016/119/L00089-00131.pdf [última consulta: 15-01-22].

67. *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario.* INCIBE (Instituto Nacional de Ciberseguridad) 2016 p. 4, disponible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf [última consulta: 15-01-22].

68. *Ibidem*, p. 5.

Su proceso de registro se basa en los siguientes parámetros[69]:

a) Captura de los parámetros biométricos.

b) Procesamiento creando una plantilla con las características personales de los parámetros capturados.

c) Inscripción de la plantilla procesada guardándola en un medio de almacenamiento adecuado. Una vez que la inscripción está completa, el sistema puede autenticar a las personas mediante el uso de la plantilla.

En el proceso de autenticación se captura una muestra biométrica y esta se compara con la base o plantilla de la previamente registrada con el objeto de lograr su identificación[70]. Este proceso puede realizarse de dos formas diferentes[71]:

a) Identificación: la comparación de la muestra recogida se realiza frente a una base de datos de rasgos biométricos registrados previamente. No hay una identificación previa por lo que el método requiere de un proceso de cálculo complejo ya que es necesario comparar la muestra con todas y cada una de las almacenadas hasta localizar la que coincida.

b) Verificación: el proceso es más sencillo ya que en un primer momento se aporta un registro que puede ser un nombre de usuario, tarjeta o algún otro método. Este registro selecciona de la base de datos un patrón anteriormente registrado y se procede a la comparación cuyo resultado es positivo o negativo.

Dentro de las tecnologías biométricas nos encontramos con diferentes tipos[72]:

a) aquellas que analizan su comportamiento: reconocimiento de firma; reconocimiento de escritura de teclado; reconocimiento de voz; reconocimiento de la forma de andar.

69. *Ibidem*, p. 5.

70. MORENO DÍAZ, A. B., Reconocimiento facial automático mediante técnicas de visión tridimensional, disponible en https://oa.upm.es/625/ [última consulta: 15-01-22]. Tesis doctoral, Universidad Politécnica de Madrid, 2004, p. 3. "*Una de las razones para desarrollar sistemas biométricos ha sido la de complementar el uso de información conocida por el usuario (por ejemplo, un número secreto o una palabra clave) o poseída por éste (por ejemplo, una tarjeta magnética). Estos métodos tradicionales se basan en propiedades o elementos que pueden ser perdidos, hurtados u olvidados. Tales problemas desaparecen con la utilización de características biométricas para identificación personal, por ser propias y permanentes para cada individuo*".

71. *Ibidem*, p. 6.

72. *Ibidem*, pp. 7-12.

b) aquellas que analizan características fisiológicas de las personas: huella dactilar; reconocimiento facial; reconocimiento de iris; reconocimiento de la geometría de la mano; reconocimiento de retina; reconocimiento vascular.

c) Otras: líneas de la palma de la mano; forma de las orejas; piel, textura de la superficie dérmica; ADN, patrones personales en el genoma humano; composición química del olor corporal.

Como podemos observar y lejos de lo que inicialmente podríamos pensar, las diversas tecnologías biométricas que nos encontramos son sumamente numerosas.

Por otro lado, son numerosos los equívocos y bulos que se dan con relación a la identificación y a la autenticación biométrica. Por ejemplo, la idea general es que la autenticación biométrica es fuerte cuando es un sistema débil –un sistema de autenticación fuerte es aquel que requiere que se proporcione, al menos, dos de los siguientes elementos: algo que se sabe, algo que se tiene o algo que se es (biometría)– o que todo tratamiento biométrico implica identificación/autenticación y no es así de forma estrictamente necesaria ya que por ejemplo, el tratamiento biométrico del movimiento del ratón utilizado para determinar si es un humano o un robot el que está accediendo a una página web, implica tratar la información biométrica para diferenciar humano de máquina[73].

De igual forma, debemos prestar una especial atención a nuestros datos biométricos, ya que estos permanecen, salvo causas excepcionales como accidentes, lesiones, etc., inmutables y no podemos modificarlos o cambiarlos a nuestro antojo tal y como podríamos hacer con la clave de acceso a nuestra cuenta de correo.

Hoy en día generamos una cantidad ingente de datos de todos los tipos, que a primera vista parecería imposible o computacionalmente imposible tratar, pero este es otro equívoco ya que los ordenadores cuánticos combinados con el uso de la inteligencia artificial podrían analizarlos con una rapidez y precisión difícilmente imaginable en nuestros días.

Por ello podemos afirmar que los datos, utilizados por las tecnologías digitales están transformado, como antaño sucediera en el tránsito de la Edad Media al Estado Moderno, nuestra forma de relacionarnos con los demás a la vez que nuestro sistema económico.

73. 14 equívocos con relación a la identificación y autenticación biométrica. 2020. AEDP (Agencia española de protección de datos) pp. 3-4, disponible en https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf [última consulta: 15-01-22].

3. LA ESTRATEGIA EUROPEA DE DATOS

Teniendo en cuenta la Estrategia Europea de Datos Las cifras previstas para 2025 serían las siguientes[74]:

a) 530% – incremento del volumen global de datos. de 33 zetabytes[75] en 2018 a 175 zetabytes.

b) 829.000 millones de euros. valor de la economía de los datos en la EU27 frente a 301.000 millones de euros (2,4% del PIB de la UE) en 2018.

c) 10,9 millones de profesionales de los datos en la EU27. frente a 5,7 millones en 2018.

d) 65% porcentaje de población de la UE con competencias digitales básicas. frente al 57% en 2018.

La innovación basada en los datos implicará mejoras en diversas áreas entre las que se podrían destacar la medicina y la movilidad. Cada día generamos mayores cantidades de datos por lo que es sumamente importante la forma en la que estos se recogen y utilizan ya que solo

74. Disponible en https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es [última consulta: 15-01-22].

75. 1.024 Byte (B) representan un Kilobyte (KB); [el resto de magnitudes se representan de igual forma; es decir, la cantidad anterior se debe multiplican por 1.024 para representar una unidad de la siguiente]; Megabyte (MB); Gigabyte (GB); Terabyte (TB); Petabyte (PB); Exabyte (EB); Zettabyte (ZB); Yottabyte (YB). Para hacernos una idea de las magnitudes "*un zettabyte ofrece espacio suficiente para 12 288 millones de vídeos 4K*" y el término "era del zettabyte" describe dos hitos: "*Por un lado, se refiere al crecimiento general de los datos digitales utilizados en todo el mundo. Por otro lado, el término se refiere al momento en que el uso de datos a nivel mundial alcanzó el orden de magnitud de los zettabytes. Esto da lugar a dos posibles inicios de la era zettabyte: ya en 2012, la cantidad total de datos digitalizados utilizados en todo el mundo superó el zettabyte. Otra definición marca el inicio de esta era en 2016, año en el que el tráfico de datos mundial a través de Internet superó esta cantidad de datos*". En "Zettabyte: la unidad de almacenamiento explicada de forma sencilla", disponible en https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/que-es-un-zettabyte/ [última consulta: 15-01-22]. Por otro lado, "*Si grabáramos una película HD a 1080p y nos ocupara 1 ZB, su duración sería de nada más y nada menos que 36 millones de años. Con solo 125 ZB podríamos grabar en HD la historia entera del planeta Tierra, desde su formación hasta el día de hoy*", disponible en https://computerhoy.com/noticias/internet/era-del-zettabyte-asi-sera-internet-2015-8521. Para más información: Cisco Annual Internet Report (Internet adoption and network performance. The Cisco Annual Internet Report forecasts global Internet adoption, device/connection proliferation and network performance. By the year 2023), disponible en https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html [última consulta: 15-01-22].

confiaremos en estas innovaciones en la medida en que estas estén sujetas "*al pleno respeto de sus estrictas normas en materia de protección de datos*"[76].

La Estrategia Europea de Datos dibuja, en línea con la comunicación de la Comisión titulada "*Modelar el futuro digital de Europa*" y el Libro Blanco sobre la inteligencia artificial, las medidas políticas e inversiones que harán posible una economía de los datos en los próximos cinco años. Estas acciones se llevarán a cabo a través de cuatro pilares[77]:

a) Un marco de gobernanza intersectorial para el acceso a los datos y su utilización.

b) Catalizadores: inversiones en datos y refuerzo de las capacidades e infraestructuras de Europa para albergar, tratar y utilizar los datos, interoperabilidad.

c) Competencias: empoderar a las personas, invertir en cualificaciones y en pymes.

d) Espacios comunes europeos de datos en sectores estratégicos y en ámbitos de interés público.

Al igual que la primera expresión del Estado Moderno es la Monarquía Absoluta[78], hoy en día, un reducido número de grandes empresas posee la mayor parte de los datos del mundo. Esta concentración debe ser corregida y por ello, es importante que la Unión Europea actúe cuanto antes ya que "*cuenta con la tecnología, los conocimientos técnicos y una mano de obra altamente cualificada*" a la vez que se garantice un elevado nivel de "*privacidad, protección, seguridad y ética*"[79].

---

76. Una Estrategia Europea de Datos. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Bruselas, 19.2.2020. COM(2020) 66 final, disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 [última consulta: 15-01-22].

77. *Ibidem*.

78. Kriele, M., *op. cit*. p. 61. En este sentido: "*En sus comienzos, la idea de soberanía es idéntica al absolutismo*".

79. *Op. cit*. Una Estrategia Europea de Datos. "*(…) competidores como China y los Estados Unidos ya están innovando rápidamente y proyectando sus conceptos de acceso a los datos y uso de datos en todo el mundo. En los Estados Unidos, la organización del espacio de datos se deja al sector privado, con considerables efectos de concentración. En China se da una combinación de supervisión gubernamental con un fuerte control por parte de las grandes empresas tecnológicas de cantidades masivas de datos sin suficientes garantías para los individuos*".

4. EL TRATAMIENTO DE LOS DATOS BIOMÉTRICOS

Prosiguiendo con el análisis de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales a los efectos del presente trabajo es de especial importancia el contenido del artículo 13 que se encuentra en consonancia con el artículo 10 de la Directiva 2016/680 y que hace referencia al tratamiento de categorías especiales de datos personales.

Según se desprende de su contenido el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física sólo se permitirán cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:

a) Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.

b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.

c) Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

Respecto al apartado c) datos que el interesado haya hecho manifiestamente públicos *motu proprio* no es posible tratar los datos que figuran en un boletín oficial como manifiestamente públicos ya que la Agencia Española de Protección de datos ha entendido que estos datos han sido publicados por imperativo legal y no por la propia voluntad del interesado. Por otro lado, como nos indican "*si alguien publica en las redes sociales en abierto que es simpatizante de una opción política x, podría llegar a ampararse el uso de los datos si se cumplen el resto de los presupuestos*"[80].

Para los citados autores "*es impensable que los cuerpos policiales o el resto de autorizades competentes tengan un fichero con datos de opiniones políticas o convicciones religiosas de las personas por el mero hecho de tenerlas*" salvo que éstas tengan "*una serie de opiniones políticas extremistas que hagan apología del odio o se tratan de una investigación por terrorismo en el que se dan las circunstancias que hagan necesario tratar datos*" en cuyo caso y "*en una infinidad de ejemplos*" similares nos indican que su opinión se podrían tratar esos datos ya que existe el amparo legal "*claro*" para realizarlo[81].

80. AYLLÓN SANTIAGO, H. S. y FERNÁNDEZ GONZÁLEZ, C. M. Tratamiento de datos de carácter personal en el ámbito policial, Reus, 2021, p. 104.

81. *Ibidem*, p. 105.

Por otro lado, es el segundo apartado el que nos indica quienes podrán tratar estos datos, las autoridades competentes a las que nos hemos referido en el anteriormente y a los meros fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

El artículo 14 de la Ley Orgánica hace referencia a los mecanismos de decisión individual automatizado, prohibiendo las decisiones basadas únicamente en un tratamiento automatizado en el que se incluye la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente.

A su vez, en el citado artículo se contiene una posible habilitación que pasaría por la autorización expresa por una norma nacional con rango de ley o por el Derecho de la Unión Europea. Dicha norma –norma habilitante para el tratamiento– deberá establecer las medidas adecuadas para la salvaguarda de los derechos y libertades e incluir el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

El contenido del artículo 14.2 es sumamente interesante y a nuestro criterio podría contener el presupuesto habilitante para utilización de los mecanismos automatizados, ya que indica que éstas no se basarán en las categorías especiales entre las que encontramos los datos biométricos salvo y aquí viene lo realmente importante a nuestros efectos que se hayan tomados las medidas adecuadas para la salvaguarda de los derechos y libertades y los intereses legítimos de los interesados. Para nosotros este punto es especialmente importante y debe conectarse con el contenido de los artículos 35 y 36 que hacen referencia respectivamente a la evaluación del impacto y a consulta previa.

Por último el tercer apartado del artículo 14 prohíbe la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13. Lo cual al mismo tiempo constituye una garantía ya que en este apartado, en el que se incluye la biometría, no se recoge ninguna posible habilitación.

El tratamiento de los datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de seguridad se recoge de forma exhaustiva en la sección 2.ª del Capítulo II (artículos 15 a 19). Su tramitación ha generado un amplio debate parlamentario hasta el punto de que el Dictamen del Consejo de Estado[82] propició modificaciones al texto inicialmente presentado.

82. Dictamen del Consejo de Estado de 28 de enero de 2021 (675/2020 (INTERIOR), disponible en https://www.boe.es/buscar/doc.php?id=CE-D-2020-675 [última consulta: 15-01-22].

Por nuestra parte, dadas las importantísimas implicaciones para la protección de los derechos y libertades en cuanto a la utilización de sistemas de grabación de imágenes y sonido por los Cuerpos y Fuerzas de Seguridad en lugares públicos y para clarificar el régimen jurídico aplicable coincidimos con MARCOS AYJON en que "*debería publicarse una norma que aglutine todo el régimen jurídico del tratamiento de los datos personales procedentes de la utilización de estos instrumentos de grabación de imágenes y sonidos*"[83].

La Ley Orgánica en el artículo 35 establece una salvaguarda en la protección de los derechos y libertades de las personas físicas, ya que exige una previa evaluación de impacto cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, que suponga por su naturaleza, alcance, contexto o fines, un alto riesgo para los derechos y libertades de las personas físicas. De igual forma, se habilita a las autoridades de protección de datos a establecer con carácter orientativo una lista de tratamientos que estén sujetos a la realización de una evaluación de impacto.

Por su parte, la evaluación de impacto incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos peligros, así como las medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar su conformidad con la Ley Orgánica e igualmente tendrá en cuenta los derechos e intereses legítimos de los interesados y de las demás personas afectadas.

Otra de las salvaguardas contenidas en la ley es la que se recoge en el artículo 36, por la que se obliga al responsable o el encargado del tratamiento de datos personales que, vayan a formar parte de un nuevo fichero, a realizar una consulta previa a la autoridad de protección de datos antes de tratar datos que hayan sido calificados como alto nivel de riesgo o cuando debido a la utilización de tecnologías, mecanismos o procedimientos novedosos se pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados.

Con todo ello, consideramos que en nuestro ordenamiento existen las herramientas oportunas para la protección de los derechos y libertades al tiempo que lo organismos internaciones están haciendo un notable esfuerzo para su consecución.

83. MARCOS AYJON, M., "La nueva Ley Orgánica para la protección de datos personales en la prevención, investigación, enjuiciamiento de delitos y ejecución de penas", La Ley privacidad, N.° 8, 2021 p. 12.

Prueba de ello es la reciente orden de 3 de enero de 2022 por la que el Supervisor Europeo de Protección de Datos ordena a EUROPOL –Agencia de la Unión Europea para la Cooperación Policial– borrar unos 4 petabytes[84] de datos provenientes informes delictivos; escuchas telefónicas; solicitudes de asilo de con más de 6 meses de antigüedad y sin categorizar correspondientes a personas que no tienen un vínculo establecido con una actividad delictiva[85]. En igual sentido nos encontramos con la Propuesta de Reglamento en materia de inteligencia artificial que seguidamente pasamos a analizar.

VI. LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN COM/2021/206 FINAL

1. CUESTIONES PRELIMINARES

Para IZQUIERDO-CARRASCO los avances en la informática, en el procesamiento de las imágenes y en la inteligencia artificial han promovido importantes avances en los sistemas de reconocimiento facial automático. Su uso conjunto con otros sistemas –como los de videovigilancia– han permitido su utilización "*no sólo en la fase de investigación y persecución del delito, sino también con otros fines más 'amplios como la búsqueda de personas desaparecidas, el control en fronteras o incluso como un instrumento de carácter preventivo en materia de seguridad ciudadana*"[86] pudiendo llegar incidir/

84. The Guardian A data 'black hole': Europol ordered to delete vast store of personal data, disponible en https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data [última consulta: 15-01-22].

85. European Data Protection Supervisor (EDPS) orders Europol to erase data concerning individuals with no established link to a criminal activity, disponible en https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en [última consulta: 15-01-22]. Wojciech Wiewiórowski, EDPS, declaro que: "*Europol has dealt with several of the data protection risks identified in the EDPS' initial inquirí (…) understanding the operational needs of Europol and the amount of data collected so far, I have decided to grant Europol a period of 12 months to ensure compliance with the Decision for the datasets already in Europol's possession*"./ / Decision on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699), disponible en https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf [última consulta: 15-01-22].

86. FRA-European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, disponible en

afectar a los derechos fundamentales (dignidad; protección datos personales; discriminación; el derecho a un recurso efectivo ante la ley y a un juicio justo; etc.)[87].

2. ¿QUÉ ES LA INTELIGENCIA ARTIFICIAL?

La inteligencia artificial dista mucho de ser un tipo avanzado de software o un tipo de programa informático, ya que estos únicamente se conforman por líneas o árboles de comandos sin posibilidad ni capacidad de salirse de ellos mientras que, a grandes rasgos, la inteligencia artificial busca soluciones sin la intervención humana en base a los datos que tiene a su alcance.

Para el Libro Blanco sobre inteligencia artificial esta se está desarrollando de una forma vertiginosa y "*Cambiará nuestras vidas, pues mejorará la atención sanitaria (por ejemplo, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades), aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, aumentará la seguridad de los europeos y nos aportará otros muchos cambios que de momento solo podemos intuir*"; de igual forma "*conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos*"[88].

Su origen aunque pueda parecernos reciente lo podemos encontrar, según un novedoso estudio realizado en la Universidad de Stanford, en los poetas griegos[89]. Por su parte, el modelo de neurona de MCCULLOCH-PITTS intenta modelar el comportamiento de una neurona "*natural*" similar a las que podemos localizar en el cerebro humano[90].

---

https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law [última consulta: 15-01-22]. 2020, p. 4.

87. IZQUIERDO-CARRASCO, M., La utilización policial del reconocimiento facial automático en despliegues ocasionales en la vía pública y los derechos fundamentales. Capítulo III, en Inteligencia artificial y defensa. Nuevos horizontes. Thomson Reuters Aranzadi, 2021, p. 66.
88. Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza. Bruselas, 19.2.2020, COM(2020) 65 final, disponible en https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf [última consulta: 15-01-22].
89. MAYOR A., *Gods and Robots: Myths, Machines, and Ancient Dreams of Technology*, Princenton. University Press, 2018.
90. MCCULLOCH-PITTS A Logical Calculus of Ideas Immanent in Nervous Activity, disponible en https://interactivechaos.com/sites/default/files/docs/mcculloch_pitts_logical_calculus_1943.pdf [última consulta: 15-01-22].

Es comúnmente aceptado que en la Conferencia de Dartmouth sobre inteligencia artificial[91] celebrada en el verano de 1956 en la Universidad Dartmouth College, ubicada en Hanover, Nuevo Hampshire (Estados Unidos) John McCarthy, Marvin Minsky, Nat Rochester y Claude Shanno –que hoy en día son considerados los padres de la Inteligencia Artificial– acuñan el concepto al tratar de resolver problemas de búsqueda heurística.

La Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión COM/2021/206 final[92] propone un marco reglamentario con una serie de objetivos específicos:

a) Garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión;

b) Garantizar la seguridad jurídica para facilitar la inversión e innovación en IA;

c) Mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA;

d) Facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado.

3. LA PROPUESTA DE REGLAMENTO

La Propuesta de Reglamento se encuentra, como su nombre indica, en fase de debate por lo que únicamente nos detendremos en dos de sus aspectos de especial relevancia para la presente investigación dejando su estudio para una posterior investigación.

En el artículo 5 se detallan las prácticas de inteligencia artificial que se encuentran prohibidas entre las que encontramos aquellas que se sirvan de técnicas subliminales; aquellas que aprovechen la vulnerabilidad de un grupo de personas para alterar de manera sustancial su comportamiento; aquellas que tengan por finalidad evaluar y clasificar la fiabilidad

91. Dartmouth Summer Research Project on Artificial Intelligence.
92. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206 [última consulta: 15-01-22].

de las personas y, lo más relevante para el presente estudio el uso de los sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público. Salvo que su uso sea estrictamente necesario para alcanzar alguno de objetivos siguientes:

a) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;

b) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;

c) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo 62, para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro.

Por su parte, el artículo 5 hace referencia al uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público que deberán tener en cuenta:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

b) las consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Resulta especialmente relevante el contenido del apartado 3 ya que el uso del sistema de identificación biométrico remoto y en tiempo real estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema.

Por su parte, el apartado 4 parece fijar una cláusula de salvaguarda, ya que nos indica que ante una en una situación de urgencia debidamente justificada, se podrá empezar a utilizar el sistema antes de obtener la autorización correspondiente, que podrá solicitarse durante el uso o después.

A nuestro criterio, este apartado no está exento de riesgos para la protección de los derechos y libertades fundamentales de las personas por mucho que se indique que la autoridad judicial o administrativa

competente únicamente concederá la autorización cuando esté convencida, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso del sistema de identificación biométrica remota "en tiempo real" es necesario y proporcionado.

Al mismo tiempo creemos que la propuesta de Reglamento debería ser más prolija, aun a riesgo de "*sufrir*" dificultades en cuanto a su aprobación en el desarrollo del apartado 4 en el que se establece que los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público y que a tal fin, tendrán que establecer en sus respectivos Derechos internos las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones.

Por último, en el artículo 6 se establecen las reglas de clasificación para los sistemas que se consideran de alto riesgo.

Como hemos indicado anteriormente, no es objeto de la presente investigación hacer un estudio detallado de la Propuesta de Reglamento, que en líneas generales parece limitar la habilitación legal para la utilización de los denominados sistema de identificación biométrica remota "en tiempo real". Por otro lado, es evidente que estos sistemas pueden comportar importantísimas ventajas en la prevención, detección, investigación y enjuiciamiento de infracciones penales a la vez que pueden comportar serías repercusiones negativas para los derechos fundamentales de las personas.

4. Voces discrepantes

Europa ha mantenido una posición dubitativa respecto al uso de la inteligencia artificial, según se desprende del informe National Strategies on Artificial Intelligence: A European Perspective[93] y algunos países como Suecia han multado el uso del reconocimiento facial para controlar la asistencia –escuela de Skelleftea– mientras que otros como Francia proponen a través de CNIL –Commission Nationale de l'Informatique et des Libertés[94]– distinguir cuándo un reconocimiento facial es necesario y cuando no.

Hoy en día existen voces discrepantes que abogan por la prohibición absoluta de su uso y férreos defensores.

93. Van Roy, V., Rossetti, F., Perset, K. and Galindo-Romero, L., AI Watch – National strategies on Artificial Intelligence: A European perspective, 2021 edition, EUR 30745 EN, Publications Office of the European Union, Luxembourg, 2021, disponible en https://publications.jrc.ec.europa.eu/repository/handle/JRC122684 [última consulta: 15-01-22].
94. Disponible en https://www.cnil.fr/.

Para ABAD ALCALÁ "*no podemos obviar cómo los individuos son titulares de derechos para iniciar y llevar a cabo litigios en diversos organismos y foros internacionales, así las personas contribuyen activamente a la formación del Derecho internacional*"[95].

Esta disputa –defensores detractores– nos recuerda en cierto sentido a la que os describe DIPPEL sobre el derecho a portar armas en los Estados Unidos de América: "*La intensa lucha en la que en la actualidad están inmersos los feudos políticos de los partidarios del derecho a llevar armas y los que defienden el control de las misas, o en otras palabras, entre los partidarios de los derechos colectivos, de los derechos individuales y la teoría insurgente (insurrectionist) acerca del verdadero significado de llevar armas, eclipsa el hecho de que esta disposición normativa llegó al naciente constitucionalismo norteamericano a través de las primeras constituciones estatales y que es ahí, a las casi constantemente violadas constituciones estatales, a donde hay que mirar para aproximarse al significado de la Segunda Enmienda*"[96].

De igual forma, cada vez son más los colectivos que abogan por la supervisión humana de los sistemas de inteligencia artificial. Por ejemplo, la Eurocámara votó en octubre de 2021 una resolución no vinculante sobre los modelos de inteligencia artificial empleados por los cuerpos policiales para facilitar el reconocimiento a través de datos biométricos, así como para garantizar sistemas de vigilancia masivos. La resolución prosperó por 377 votos a favor, 248 en contra y 62 abstenciones analiza los riesgos que conllevan los sesgos en algoritmos a la vez que enfatiza en la necesidad de que estos modelos estén bajo supervisión humana y sometidos a un intenso escrutinio legal, sobre todo en contextos transfronterizos[97].

En este mismo sentido son varios los colectivos que en defensa de los derechos civiles han emprendido una Iniciativa Ciudadana Europea para que la Unión Europea vete los sistemas de vigilancia biométrica dentro de sus fronteras; entre ellos Reclaim Your Face[98].

El ámbito recreativo no queda al margen de estas tecnologías y del uso indiscriminado de la inteligencia artificial. Hoy en día existen diversas aplicaciones de uso doméstico como: Morphin; Reface/

95. ABAD ALCALÁ, l. *op. cit.*, p. 44.
96. DIPPLER, H., *Derechos humanos: de derechos de la sociedad a derechos del individuo* en Constitucionalismo moderno. Marcial Pons, 2009, p. 223.
97. European Parliament. News Use of artificial intelligence by the police: MEPs oppose mass surveillance, disponible en https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance [última consulta: 15-01-22].
98. Reclaim Your Face, disponible en https://reclaimyourface.eu/ [última consulta: 15-01-22].

Doublicat; Familiar; DeepFaceLab; FaceSwap que permiten crear un Deepfake de forma fácil a la vez que numerosos tutoriales en red[99]. Es una actividad que a primera vista parece no comportar grandes riesgos y que puede llegar a producir importantísimas vulneraciones para los derechos de las personas como sucedió con la aplicación DeepNude que con una simple foto de una persona y en pocos segundos la inteligencia artificial nos facilitaba una imagen de la persona en cuestión desnuda. Por ello, consideramos que su utilización debe ser adecuadamente regulada.

Por último, compartimos el planteamiento y reflexiones de MILIONE sobre posibles escenarios futuros en los que en aras a una mayor seguridad ésta se lograse a consta de nuestras libertades dando lugar a lo que sería una "*seguridad inhumana*" para nada deseable. En sus palabras: "*Reflexionando sobre posibles escenarios futuros, además de admitir, aunque solo sea por un periodo de tiempo muy acotado, la suspensión del derecho a la asistencia letrada ¿no nos valdría también permitir la suspensión del principio de prohibición de la tortura, ante la existencia de suficientes 'compelling reasons', por un periodo de tiempo igualmente muy reducido, o por una parte determinada del cuerpo humano, o limitando el suplicio a la dimensión exclusivamente psicológica en lugar de también a la física?, ¿podría, entonces, ser oportuno sacrificar nuestro patrimonio de valores, y de paso nuestra propia civilización jurídica, en el altar de 'lo más útil en lo inmediato'?"*. Su exposición continúa haciendo referencia al TEDH en los siguientes términos: "*deberíamos desear que el supremo intérprete del CEDH (…) no acceda a negociar nuestro sistema de valores para otorgarnos un poco más de seguridad, de una 'seguridad inhumana' que se lograría al precio de nuestras libertades*" para concluir su exposición con "*Es nuestro deseo más sincero que esto no llegue a ocurrir*"[100].

En igual sentido pero aplicado al uso de los sistemas de inteligencia artificial en el ámbito judicial compartimos igualmente el planteamiento de CASTELLANOS CLARAMUNT y MONTERO CARO para quienes la utilización de la inteligencia artificial es probable que mejore la transparencia; la previsibilidad de la aplicación de la ley; la coherencia de la jurisprudencia; agilicen los procesos; etc. pero para los cuales los "*procesos no pueden limitarse a algoritmos y deben tenerse en cuenta [las]*

99. Aura Prods Cómo hacer un DEEPFAKE de forma fácil? Tutorial Español (DeepFaceLab), disponible en https://www.youtube.com/watch?v=-Mef-Bx1bbs [última consulta: 15-01-22].

100. MILIONE, C., La noción de seguridad en la Doctrina del Tribunal Europeo de Derechos Humanos: referencias al Derecho a la Tutela Judicial Efectiva, Revista de Derecho Político, N.° 107, 2020, pp. 262-263.

circunstancias particulares, garantizando, en consecuencia, el respeto de los derechos fundamentales"[101].

VII. A MODO DE CONCLUSIÓN

A finales de los años 70 la sociedad española aún no estaba familiarizada con el uso de la informática; no obstante, los padres de la Constitución de 1978, conscientes de los posibles riesgos que podría llegar a entrañar el archivo y uso de los datos informáticos prestaron especial atención a su regulación. Fruto de ella esta preocupación, el artículo 18.4 de nuestro texto constitucional y, en palabras del Tribunal Constitucional, ha incorporado una nueva garantía constitucional que debe ser entendida como un derecho de control sobre los datos y que comprende, entre otros aspectos, el de oposición a que determinados datos sean utilizados con fines distintos de aquel legítimo que justificó su obtención a la vez que reitera que los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica.

Hoy en día vivimos en un nuevo tipo de Estado, el Estado digital, en el que la ciudadanía manifiesta un alto grado de dependencia digital y en el todo parece valer para obtener un cierto reconocimiento digital.

Una sociedad altamente polarizada ya que una parte, en aras de la seguridad, parece querer revivir el antiguo principio del derecho romano "*intra armas silent leges*", mientras que para otra cualquier actuación con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección frente a las amenazas contra la seguridad pública ocasiona una intromisión ilegítima en el ámbito de los derechos y libertades fundamentales.

Lo constable a día de hoy es el auge de las redes de delincuencia organizada que constituyen negocios multimillonarios y que operan a escala internacional utilizando los últimos avances tecnológicos para tartar de burlar la ley.

Ante esta situación nuestro marco legal tanto nacional como internacional se muestra impreciso e ineficaz limitándose, en muchas ocasiones, a parchear el sistema. Por ello, es preceptiva la constitución de equipos multidisciplinares que aborden e integren las diferentes tecnologías existentes

101. CASTELLANOS CLARAMUNT, J. y MONTERO CARO, L., "Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales", disponible en: https://institucional.us.es/revistas/Ius_Et_Scientia/VOL6-2/Ius_et_Scientia_vol_6_n2_06_castellanos_claramunt-montero_caro.pdf [última consulta: 15-01-22]. IUS ET SCIENTIA, 2020, Vol. 6, N.° 2, Editorial Universidad de Sevilla 2020 p. 81.

–bases de datos biométricas; computación cuántica; inteligencia artificial– y que ofrezcan una respuesta legal global que dote a nuestros cuerpos y fuerzas de seguridad de las herramientas oportunas –formación; confianza, trazabilidad– para una rápida, eficaz y adecuada persecución de los delitos a la vez que doten a nuestro sistema judicial de una más que necesaria modernización y que respeten y protejan los derechos fundamentales de las personas a la vez que pongan fin a desigualdades de los colectivos más desfavorecidos a los que una sociedad plural no debe desatender.

VIII. BIBLIOGRAFÍA

1. FUENTES CLÁSICAS

ABAD ALCALÁ, L. Las libertades informativas en el ámbito internacional. Editorial Dykinson, 2020.

AGUDO ZAMORA, M., Reforma Constitucional y Estado Autonómico, Tecnos, 2019.

AYLLÓN SANTIAGO, H. S. y FERNÁNDEZ GONZÁLEZ, C. M. Tratamiento de datos de carácter personal en el ámbito policial, Reus, 2021.

BOBRICK, A. y MARTIRE, G., "Classical and Quantum Gravity", Volume 38, Number 10.

BODINO, J., Los seis libros de la República, Madrid, 2000.

CASTELLANOS CLARAMUNT, J. y MONTERO CARO, L., "Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales".

DIPPLER, H., Derechos humanos: de derechos de la sociedad a derechos del individuo en Constitucionalismo moderno. Marcial Pons, 2009.

FRIEDRICH, C.J., La democracia como forma política y como forma de vida. Traducción de C. Zabal Schmidt-Völz. Ediciones Olejnik, 2020.

GOODWIN, B., El uso de las ideas políticas, Barcelona, 1997.

HAURIOU, A., Derecho Constitucional e Instituciones Políticas, Barcelona, 1971.

IUS ET SCIENTIA, 2020, Vol. 6, N.° 2, Editorial Universidad de Sevilla 2020.

IZQUIERDO-CARRASCO, M., La utilización policial del reconocimiento facial automático en despliegues ocasionales en la vía pública

y los derechos fundamentales. Capítulo III, en Inteligencia artificial y defensa. Nuevos horizontes. Thomson Reuters Aranzadi, 2021.

JIMÉNEZ ALEMÁN, Á. A., Artículo 18 en Comentarios a la Constitución española de 1978. Tomo I. Dir. CAZORLA PRIETO, L. M., y Coord. PALOMAR OLMEDA, A., Thomson Reuters, 2018.

KRIELE, M., Introducción a la Teoría del Estado, Buenos Aires, 1980.

LOEWENSTEIN, K., Teoría de la Constitución. Editorial Ariel, Barcelona, 1986.

MARCOS AYJÓN, M., "La nueva Ley Orgánica para la protección de datos personales en la prevención, investigación, enjuiciamiento de delitos y ejecución de penas" La Ley privacidad, N.° 8, 2021.

MAYOR A., Gods and Robots: Myths, Machines, and Ancient Dreams of Technology, Princenton. University Press, 2018.

MCCULLOCH-PITTS A Logical Calculus of Ideas Immanent in Nervous Activity.

MILIONE, C., La noción de seguridad en la Doctrina del Tribunal Europeo de Derechos Humanos: referencias al Derecho a la Tutela Judicial Efectiva, Revista de Derecho Político, N.° 107, 2020.

MIQUEL SILVESTRE, J. A., *Manual de aventura overland. La magia de viajar por tus propios medios* Silver Rider Prodaktions. 2016.

MORENO DÍAZ, A. B., Reconocimiento facial automático mediante técnicas de visión tridimensional, Tesis doctoral, Universidad Politécnica de Madrid, 2004.

PINTACUDA, E., Breve curso de política, Santander, 1994.

RECASENS SICHES, L. Introducción al estudio del Derecho, México, 1977.

SAN AGUSTÍN, La ciudad de Dios, Madrid, 1941.

WEBER, M. La política como vocación (1919) dentro de El político y el científico.

ZARAZAGA BURILLO, I., Debate en el Pleno del Senado del Proyecto de Constitución.

2. OTRAS FUENTES

14 equívocos con relación a la identificación y autenticación biométrica. 2020. AEDP (Agencia española de protección de datos).

ABC Elon Musk asegura que Neuralink empezará a implantar chips cerebrales en humanos en 2022.

Asociación Pro Derechos Humanos de Andalucía. 20 años de foto fija de exclusión social en Córdoba.

Aura Prods Cómo hacer un DEEPFAKE de forma fácil? Tutorial Español (DeepFaceLab).

Carta de los Derechos Fundamentales de la Unión Europea. (2000/C 364/01). Diario Oficial de las Comunidades Europeas.

Cisco Annual Internet Report (Internet adoption and network performance. The Cisco Annual Internet Report forecasts global Internet adoption, device/connection proliferation and network performance. By the year 2023).

Congreso de los Diputados. Enmiendas al Anteproyecto de Constitución.

Constitución de Grecia de 1975 (con enmiendas hasta 2008).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

Dictamen del Consejo de Estado de 28 de enero de 2021 (675/2020 (Interior).

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

ELVIRA PERALES, A., y actualizado (2011) por GONZÁLEZ ESCUDERO, A., Sinopsis artículo 18. Congreso de los Diputados.

European Data Protection Supervisor (EDPS) orders Europol to erase data concerning individuals with no established link to a criminal activity.

European Parliament. News Use of artificial intelligence by the police: MEPs oppose mass surveillance.

FRA-European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement.

Gaceta de Madrid: núm. 258, de 14/09/1896.

Gaceta de Madrid: núm. 50, de 19/02/1901.

Guide to the Case-Law of the of the European Court of Human Rights. Data protection (Updated on 30 April 2021). European Court of Human Rights (Tribunal Europeo de Derechos Humanos; TEDH).

Historia de los documentos de identidad. España 1820-2016. D.G. Policía; S.G. Logística.

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. "BOE" núm. 126, de 27/05/2021.

Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza. Bruselas, 19.2.2020, COM(2020) 65 final.

Neuralink. Breakthrough Technology for the Brain.

Parlamento Europeo ¿Qué es la inteligencia artificial y cómo se usa?

Película Johnny Mnemonic. Sinopsis.

PIÑAR MAÑAS, J. l., Es esencial garantizar el derecho a no ser digital, a que te atienda una persona. Declaraciones El diario.

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican Determinados Actos Legislativos de la Unión.

Reclaim Your Face.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario. INCIBE (Instituto Nacional de Ciberseguridad) 2016.

The Guardian A data 'black hole': Europol ordered to delete vast store of personal data.

Trabajos parlamentarios de la Constitución Española.

Una Estrategia Europea de Datos. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Bruselas, 19.2.2020. COM(2020) 66 final.

Van Roy, V., Rossetti, F., Perset, K. and Galindo-Romero, L., AI Watch – National strategies on Artificial Intelligence: A European perspective, 2021 edition, EUR 30745 EN, Publications Office of the European Union, Luxembourg, 2021.

Viajar más rápido que la velocidad de la luz es posible. Movernos a través de otros sistemas estelares lleva siendo un sueño desde hace mucho. Ahora, parece que estamos un poco más cerca de lograrlo.

Viajar por el espacio más rápido que la luz no es solo ciencia ficción: hay físicos (serios) trabajando en esta ideo, Xataka.

Wojciech Wiewiórowski, EDPS, declaraciones.

3. SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

- STJUE de 25 de febrero de 2021 (Asunto C-658/19 Comisión/España).
- STJUE de fecha 13 de mayo de 2014 "Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. Petición de decisión prejudicial planteada por la Audiencia Nacional".
- STJUE de fecha 6 de octubre de 2015 "Maximillian Schrems y Data Protection Commissioner".
- STJUE de fecha 8 de abril de 2014 "Digital Rights Ireland, Seitlinger Tschohl y otros".

4. SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL

- STC 101/1983, de 18 de noviembre (BOE núm. 298, de 14 de diciembre de 1983).
- STC 11/1998, de 13 de enero (BOE núm. 37 de 12 de febrero de 1998).
- STC 202/1999, de 8 de noviembre (BOE núm. 300 de 16 de diciembre de 1999).

- STC 254/1993, de 20 de julio (BOE núm. 197 de 18 de agosto de 1993).
- STC 27/2020, de 24 de febrero (BOE núm. 83 de 26 de marzo de 2020).
- STC 29/2013, de 11 de febrero (BOE núm. 61 de 12 de marzo de 2013).
- STC 292/2000, de 30 de noviembre (BOE núm. 4, de 04 de enero de 2001).
- STC 34/1983, de 6 de mayo (BOE núm. 120, de 20 de mayo de 1983).
- STC 94/1998, de 4 de mayo (BOE núm. 137 de 09 de junio de 1998).
- STC17/2013, de 31 de enero (BOE núm. 49 de 26 de febrero de 2013).

Derechos fundamentales, proceso e Inteligencia Artificial: una reflexión[1]

Juan-Luis Gómez Colomer

Catedrático de Derecho Procesal
Universidad Jaume I de Castellón

SUMARIO: I. UNA PERSPECTIVA GENERAL. II. PROPUESTAS DE REGULACIÓN. III. EL CONTENIDO BÁSICO. IV. SU CONCRECIÓN EN EL ÁMBITO DE LA JUSTICIA. V. CONCLUSIONES.

I. UNA PERSPECTIVA GENERAL

Una visión científica por no expertos del mundo de la Inteligencia Artificial[2], que empieza a despuntar en los años 50 del siglo pasado, pero que en realidad solamente a partir de finales del siglo XX se la ve pujar con fuerza en el mundo que nos rodea, se está abriendo paso para iluminar

1. Este artículo forma parte de un libro sobre el Juez-Robot que estoy elaborando en estos momentos, cuyas líneas generales sobre el tema concreto de la relación entre la Inteligencia Artificial y los derechos fundamentales de los ciudadanos avanzo parcialmente ahora. Las fuentes bibliográficas extranjeras (alemanas y anglosajonas) pude consultarlas presencialmente en el *Institut für Strafrecht und Strafprozessrecht Abteilung 3: Deutsches und Ausländisches Strafrecht und Strafprozessrecht* de la *Rechtswissenschaftliche Fakultät* (*Albert-Ludwigs-Universität* de *Freiburg im Breisgau*, Alemania), dirigido por el Prof. Dr. Dr.h.c. Walter Perron, a quien agradezco profundamente su extraordinaria acogida y constante apoyo. También pude consultar mucha bibliografía en el *Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht* (antiguo *Max-Plank-Institut für ausländisches und internationales Stafrecht*), igualmente sito en *Freiburg im Breisgau*. Mi agradecimiento a sus directores Prof. Dr. Ralf Poscher y Profra. Dra. Tatjana Hörnle, por aceptarme y permitir mi acceso, igualmente presencial, en estos tiempos de pandemia tan preocupantes. Ello fue posible gracias a la concesión de una beca de la Generalitat Valenciana – Programa BEST/2021 (julio a septiembre de 2021), y otra beca de la *Alexander von Humboldt-Stiftung* (*Wiedereinladung*, de octubre a diciembre de 2021), instituciones a las que igualmente quiero manifestar expresamente mi más profundo agradecimiento.
2. A partir de ahora, abreviada IA.

sobre aspectos concretos muy problemáticos de nuestra vida actual. Esa visión científica es jurídica, y afecta a la cuestión general de comprensión del fenómeno de la IA e intento de regulación legal de la misma, debido a que con su enorme desarrollo, empiezan a verse también, si no se han visto ya, los enormes peligros que encierra este nuevo mundo.

Es cierto que interesan otras visiones también, como la filosófica, en especial, la ética, la económica o incluso la perspectiva desde las ciencias de la salud. Pero son ajenas a nuestros intereses ahora. A nosotros lo que nos preocupa es la visión jurídica que tiene lugar desde el punto de vista procesal, y de todas las posibles cuestiones dentro de esa visión, de momento sólo una, en verdad, me llama poderosamente la atención. El problema que quiero abordar aquí, detectándolo, analizándolo, observando lo existente y proponiendo soluciones a los problemas planteados, dentro de la limitada extensión que un escrito de estas características me permite, es el de la protección jurídica frente a los riesgos que el uso y aplicación de la IA conlleva, y más en particular, la tutela al más alto nivel, la tutela constitucional. Creo que es, sin duda, uno de los puntos estrella en estos momentos.

Pero es necesario antes comprender con carácter general el tema, siquiera sea en sus trazos más significativos[3]. Para lograrlo, es útil repasar las informaciones accesibles a la ciudadanía, de manera que sepamos exactamente cuál es el estado de la cuestión en estos momentos.

En este sentido, lo primero que hay que decir es que se habla mucho en los medios de información sobre IA, pero se constata que quienes han escrito en los *mass media* sobre inteligencia artificial y sus aplicaciones en la Justicia (organización, tribunales, procesos civiles y penales), específicamente los pocos que se han atrevido a hablar en concreto del juez-robot, no son cualquier ciudadano, son abogados, informáticos o periodistas especializados que se han adentrado en este mundo informando al público brevemente sobre diversos contenidos relacionados con la IA. Podemos decir que esta información transmite a toda la sociedad lo que una pequeña parte de ella piensa.

Ordenando las ideas expresadas acerca de estos temas, podemos resumir lo siguiente[4]:

3. No pretendo una cita exhaustiva de bibliografía, porque como se verá me voy a centrar en las normas europeas sobre IA y derechos fundamentales. Me limitaré a la que en el tema tratado aporta al menos algo de interés.
4. Tampoco voy a citar ni a autores ni a medios concretos de información (prensa, TV o radio). Lo que aquí expreso se puede constatar fácilmente utilizando cualquier potente buscador en internet y haciendo la pregunta adecuada.

1.°) En general, todas las informaciones parten de considerar la introducción de la IA en el mundo de la Justicia como algo imparable, inevitable y positivo. Primero, porque el mundo del Derecho no puede ser ajeno a la enorme evolución tecnológica y considerable progreso científico que se manifiestan en otros mundos, como el de la Medicina, la Economía, la Ingeniería o la propia Administración, en los que la IA ocupa un papel cada vez más relevante[5]; y segundo, porque se constata, también paulatinamente, que la IA mejora aspectos de la Justicia sobre los que existe una gran preocupación social, como por ejemplo la rapidez de tramitación y resolución de los conflictos, un aspecto que lleva décadas enquistado provocando un caótico atasco judicial con dilaciones indebidas inasumibles. Esto es muy significativo, porque por culpa de la extrema lentitud de la Justicia una buena parte de la ciudadanía ha dejado de tener fe en ella, por ello, la aplicación de la IA para resolver este gran problema la hace muy atractiva.

2.°) Toda la información habla de las ventajas e inconvenientes de la aplicación de la IA en la Justicia, en cualquiera de sus ramas, pero en donde más incidencia tiene es en la práctica ante los tribunales penales, por ser la más problemática.

3.°) Las ventajas que se destacan son, principalmente, la enorme ayuda que implica para la descongestión judicial acabada de mencionar, porque los asuntos se resuelven rápidamente, la gran utilidad que significa para el juez manejar correctamente los datos y evitar que se pierda en montañas de papeles, y la nada menospreciable satisfacción de facilitar resoluciones justas e iguales en casos que son o idénticos o muy parecidos, lo que proporciona una gran seguridad jurídica.

4.°) Los inconvenientes son también claros, pues se reconoce principalmente que no es posible aplicar los avances en todos los campos del proceso, ni en todas las materias. Por ejemplo, en la línea problemática indicada, no lo ven apropiado para el proceso penal, aunque las aplicaciones se orientan principalmente a las predicciones (a tratar más adelante) para la adopción de medidas cautelares penales de naturaleza personal; tampoco lo consideran procedente para asuntos civiles de familia, en los que la decisión humana se entiende hoy como imprescindible ante la cantidad de problemas entrelazados que existen, la mayoría de los cuales requieren una sensibilidad y una emoción de la que carecen las "máquinas".

5. Por ejemplo, sobre la automatización de la administración alemana, procedimientos y decisiones, con base en la IA, v. MARTINI, M./NINK, D. (2017), *Wenn Maschinen entscheiden… – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz*, Neue Zeitschrift für Verwaltungsrecht – Extra In Zusammenarbeit mit der Neuen Juristischen Wochenschrift, núm. 10, pp. 1 y ss.

5.°) En el ámbito de la Justicia civil y penal, también en los órdenes contencioso-administrativo y laboral, incluso en el militar, hay dos aspectos sobre los que se quiere trasmitir a la sociedad alguna reflexión ulterior:

a) El primero hace referencia a la enorme utilidad de la aplicación de la IA en materia de predicciones judiciales, destacando dos aspectos:

1. Un primer ámbito, aunque los campos pueden ser muchos, se centra sobre todo en los programas que hasta ahora se han construido y que mayor importancia tienen, Así por ejemplo, se suele citar mucho el programa COMPAS, diseñado en California en el año 1998, para predecir si un imputado o acusado por determinados delitos tiene un riesgo elevado de fugarse si se decreta su libertad provisional, con el riesgo de reiteración delictiva que ello supone, hasta la espera del juicio, o si no lo tiene, de manera que con la ayuda de la predicción el juez pueda tomar una decisión más adecuada a la realidad del caso y de la persona que podría haber cometido el delito o los delitos que lo han provocado. Con relación a él se cita el *caso Loomis*, en 2013, que creó un precedente judicial en el estado de Wisconsin, Estados Unidos[6]. Pero hay muchos programas más, como PredPol, Precobs, Xlaw, Hart, Vaak, Cortica, o el español Eurocop, diseñado por mi universidad[7].

2. Un segundo ámbito de predicción que se está utilizando consiste en estudiar las sentencias dictadas por un juez, o por cada juez de un tribunal, o por el conjunto del tribunal, agrupando asuntos relativamente iguales durante un período de tiempo. Este análisis predictivo ayuda a los abogados en sus estrategias para intentar vencer la probable

6. Véanse GRECO, L. (2020), *Poder de julgar sem responsabilidade de julgador: A impossibilidade jurídica do juiz-robô*, Ed. Marcial Pons, Sâo Paulo, pp. 28 y 29; ARMENTA DEU, T (2021), *Derivas de la Justicia. Tutela de los derechos y solución de controversias en tiempos de cambios*, Ed. Marcial Pons, Madrid, pp. 262 y ss.; MIRANDA BONILLA, H. (2021), *Algoritmos y derechos humanos*, Revista de la Facultad de Derecho de México, tomo LXXI, núm. 280, pp. 720 y 721; MARTÍNEZ ZORRILLA, D. (2019), *El juez artificial: ¿próxima parada?*, Oikonomics, núm. 12, pp. 5 y ss.; y MIGUEL BERIAIN, I. de (2018), *Does the use of risk assessments in sentences respect the right to due process? A critical analysis of de Wisconsin v. Loomis ruling*, Law, Probability and Risk, núm. 1 (17), pp. 45 y ss.

7. Este programa pretende aumentar la capacidad predictiva, preventiva y operativa de la Policía, especialmente la Policía Local, de momento. Para lograrlo se creó mediante acuerdo entre la Universidad Jaume I de Castellón, el Ayuntamiento de Castellón y su Policía Local la "Cátedra Eurocop", con el fin de ayudar a resolver las necesidades que tienen los Cuerpos y Fuerzas de Seguridad, posibilitando que cuenten con las más avanzadas herramientas tecnológicas para predecir y prevenir delitos, infracciones, faltas, actos incívicos, etc. No es un programa ajeno a ciertas sensibilidades sociales que ven este tipo de usos atentatorio contra los derechos de los ciudadanos, v. https://www.lavanguardia.com/tecnologia/20190318/461013536935/inteligencia-artifical-vigilancia-predictiva-policia.html; y https://www.elsaltodiario.com/tecnologia/estado-policial-espanol-2.0-empresas-privadas-eurocop-vigilar-ciudadanos.

oposición psicológica de los jueces a sus intereses con relación a sus clientes, o para orientar mejor la argumentación hacia una victoria en el caso. Un programa desarrollado en 2016 por la Universidad de Londres, la Universidad de Sheffield y la Universidad de Pennsylvania para el estudio de casi 600 casos del Tribunal Europeo de Derechos Humanos, para ver si un algoritmo podía predecir el fallo con base en esos precedentes, llegó al sorprendente resultado de coincidir la predicción con la realidad posterior en casi el 80% de los casos[8]. No es el único estudio predictivo hecho[9].

b) El segundo se refiere a la posibilidad de que una máquina pueda juzgar. La enorme evolución tecnológica en esta materia está llevando más allá de las predicciones y se adentra en el delicado tema de las resoluciones judiciales, en definitiva, en estudiar si es posible que una computadora inteligente pueda decidir cualquier asunto litigioso civil o cualquier delito penal.

La idea central que preside este avance es, obsérvese que, en forma recurrente, pues hablamos casi siempre de lo mismo, aligerar el enorme colapso de los tribunales en todos los países democráticos, de manera que el ciudadano sienta de verdad que su derecho a la tutela judicial efectiva y a un proceso sin dilaciones indebidas sea respetado y amparado por el estado, el único ente que debe organizar el sistema judicial en una democracia.

Pero no es tan fácil, primero porque el avance tecnológico no ha llegado tan lejos, y segundo, porque, y en esto coinciden todos, nadie cree en serio, al menos hoy en día, que desaparezca para siempre el juez humano de la vida judicial.

6.°) Llegamos con estas reflexiones al juez-robot, sobre el que se ha escrito también, pero poco, quizás porque nadie cree, insistimos, al menos de momento, en que pueda ser realidad un día.

Pero dos países ya lo han empezado a implementar[10], y de ello se da cumplida cuenta en la escasa prensa que ha tratado el tema:

---

8. *Vide* ALETRAS, N./TSARAPATSANIS, D./PREOŢIUC-PIETRO, D./LAMPOS, V. (2016), Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective, PeerJ Computer Science 2:e93, pp. 1 y ss.
9. Para la Corte Suprema de los Estados Unidos, v. RUGER, TH./KIM, P.T./MARTIN, A.D./QUINN, K.M. (2004), *The Supreme Court Forecasting Project: Legal and Political Science. Approaches to Supreme Court Decision-Making*, Columbia Law Review, vol. 104, pp. 1150 y ss.
10. CÁRDENAS KRENZ, R. (2021), *¿Jueces robots? Inteligencia artificial y Derecho*, Revista Justicia & Derecho, Universidad Autónoma de Chile, vol. 4, núm.2, pp. 3 y 4.

a) En Estonia, uno de los países más avanzados del mundo en esta materia, existe desde el año 2000 el juez-robot, que resuelve pequeñas reclamaciones civiles de cuantía hasta 7.000 €.

b) En China existen desde 2019 los llamados "Tribunales de Internet", o juzgados *online*, con competencias en litigios sobre comercio electrónico, pagos virtuales, transacciones en la nube y conflictos en materia de propiedad intelectual.

Los procesos se desarrollan de una manera ultrarrápida. Las partes únicamente proporcionan los hechos y las pruebas que tengan y la máquina mediante un sistema de algoritmos (basados en un complejísimo cálculo estadístico), dicta sentencia.

En ninguno de los dos países, sin embargo, la IA se ha apoderado totalmente del proceso. En primer lugar, sólo actúan en procesos civiles, y, en segundo lugar, proponen la decisión a un juez, quien debe revisar al procedimiento y ratificarla o no. Los recursos, de caber, se tramitan ante jueces "humanos".

En China han dado un paso más y han creado una máquina que actúa de Fiscal, encargado de acusar en algunos pocos delitos, generalmente de escasa dificultad probatoria, según los pocos datos que hasta este momento conocemos. El Fiscal-Robot está en pruebas en la gran urbe china de Shanghái. Es capaz de formular escritos de acusación contra sospechosos con base exclusivamente en una descripción verbal, con una precisión de hasta el 97% de acierto. De momento ha sido capaz de "comprender" ocho delitos: Fraude con tarjetas de crédito, juegos de azar, conducción imprudente, asalto intencional, obstrucción a un oficial, robo, fraude e incluso disidencia política.

7.°) Finalmente, la ciudadanía es puesta al corriente de dos cuestiones negativas que el uso de la IA en el campo del Derecho Procesal implica: Se denuncian ciertos problemas éticos con la utilización de los programas de predicción, y se advierte sobre la posible colisión del uso de estas altísimas tecnologías con las constituciones democráticas y algunos de los derechos humanos (constitucionales) que reconocen.

a) El problema ético surge principalmente con relación a los programas de predicción porque los algoritmos, generalmente creados por empresas privadas, no se someten a información pública, es decir, nadie sabe cuál es su contenido, y no hay manera legal de obligar a la empresa a que lo haga público porque los resultados de su trabajo, el producto final, están protegidos por sus derechos de propiedad intelectual. Esto ha provocado en varios asuntos de

gran trascendencia impugnaciones por parte de la defensa, cuando su cliente ha resultado perjudicado por la predicción, porque no se podía defender frente a un algoritmo "secreto".

Otra cuestión, no menor, ha sido que al no conocerse con qué criterios actúa el algoritmo, ni quién lo ha elaborado, no se puede saber si realmente la información que contiene es objetiva, imparcial, igualitaria y ajustada a la ley. De hecho, se ha demostrado que en algunos casos estos programas tenían sesgos claramente orientados a favor de la mayoría (*v. gr*., de los ricos), e incluso prejuicios en favor de los blancos cuando los acusados eran negros (*caso Loomis*, cit.).

b) El segundo tema es jurídico y atañe a la posible violación de determinados derechos constitucionales por el uso de estos programas de predicción, y también de resolución en el caso del juez-robot.

En líneas generales, se informa de los posibles derechos fundamentales afectados: Por ejemplo:

1. Posible violación del principio de igualdad por los sesgos y prejuicios de determinados algoritmos causantes de discriminación.

2. También puede quedar en entredicho el derecho de defensa, ya que no sabemos cómo "razona" la máquina.

3. Y el derecho al recurso, puesto que la máquina no motiva y por tanto la parte perjudicada no sabe por qué ha sido condenado.

4. El derecho a un proceso equitativo o derecho al juicio justo (*Due Process of Law*, nuestro derecho al proceso con todas las garantías) puede quedar igualmente perjudicado, porque carece de sentido tanto hablar de competencia territorial, como hablar de audiencias y, por tanto, de los principios de oralidad e inmediación, entre otras muchas instituciones procesales que devienen superfluas o irrelevantes.

5. El uso de la IA en temas de Justicia puede conllevar negativamente también, ante la enorme cantidad de datos que necesitan los programas hasta ahora creados para predecir o resolver, el aprovechamiento por parte de estados, entes o empresas poco escrupulosas de los mismos, para realizar paralelamente sobre la población una vigilancia masiva y total de su vida personal, profesional y social, sus costumbres, sus preferencias, sus pasiones, sus virtudes, sus gustos, sus logros, sus defectos, sus miserias, etc., lo que implicaría un control total que ni siquiera Orwell pudo llegar a imaginar. Derechos como la intimidad, la inviolabilidad del domicilio, el secreto de las comunicaciones, o a la protección de datos, estarían totalmente a disposición de esas personas jurídicas para un uso torticero

público (o privado) de los resultados obtenidos como consecuencia de la búsqueda de información.

Para terminar con este repaso a la información que recibe la sociedad sobre la IA, destaco uno de los aspectos cruciales del sistema, a saber, el de la responsabilidad. ¿Quién se hará cargo de los posibles daños y perjuicios de una predicción errónea o de un fallo equivocado, ambos adoptados por una máquina de juzgar? Debe decirse que se ha pensado ya en el tema de la responsabilidad y que se han tomado en cuenta las Recomendaciones del Parlamento Europeo que afectan a una posible futura regulación de los robots[11], pero estamos empezando, por tanto, hay mucho que analizar.

En resumen, siendo ello así, dado que la IA sigue imparablemente su curso, no va a haber más remedio que cambiar muchas cosas para que las grandes estructuras, formadas por principios por los que mucha gente ha llegado a dar su vida a lo largo de la Historia, no se tambaleen y se destruyan definitivamente. Ello incluye, especialmente, toda la materia de los derechos fundamentales propios de un estado de derecho, los que conforman una democracia verdadera.

A este interesante tema dedicamos las palabras siguientes, que conforman el núcleo central de esta contribución.

II. PROPUESTAS DE REGULACIÓN

Expuesto el estado de la cuestión, destaca como una de las cuestiones trascendentales hoy conocer con precisión la protección legal que al máximo nivel puede tener el ciudadano como usuario o destinatario de la IA frente a los riesgos antes esbozados. Con otras palabras, la pregunta que hay que hacerse es si está protegida constitucionalmente la persona frente a la IA. La respuesta es, en principio, afirmativa, pero no es plenamente satisfactoria.

Nadie duda en estos momentos que la IA, como resultado del progreso en materia de nuevas tecnologías que significa, afecta al concepto

11. Informe de la Comisión de Asuntos Jurídicos del Parlamento Europeo con Recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, de 27 de enero de 2017 (A8-0005/2017), que se puede consultar en https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html; y Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica [2015/2103(INL)], que se puede consultar en https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html.

normativo y a la realidad práctica que implican los derechos fundamentales[12], los derechos de máximo nivel reconocidos en todas las democracias. Esta afectación es muy relevante.

El impacto se suele canalizar a través de cuatro ámbitos, no todos ellos positivos, como veremos inmediatamente[13]:

1.°) La IA hace que el ejercicio de los derechos fundamentales sea distinto a como se actuaría en caso de no existir. Si pensamos en el derecho a acceder a información libre y veraz, o en el derecho a la libertad de expresión, el mundo ha cambiado radicalmente en 30 años.

2.°) La IA ha hecho nacer nuevos derechos fundamentales, que hasta que se reconozcan expresamente por las constituciones democráticas de todos los países, deben basarse en los ya existentes. Por ejemplo, si en el estado concreto no estuviera reconocido expresamente el derecho de acceso a Internet se fundaría en el principio de igualdad; el derecho a la protección de datos en el derecho a la intimidad, y así con todos los demás.

3.°) La IA, en cuanto avance tecnológico, es positiva y negativa, porque, así como es indudable el enorme beneficio que su uso proporciona a los ciudadanos, y también a las personas jurídicas públicas y privadas, tampoco es dudoso que se hayan puesto de manifiesto amenazas intolerables para las personas. El mismo derecho a la intimidad puede ser el más significativo[14], pero también han aflorado problemas de discriminación, contraria al principio de igualdad, que no pueden ser permitidos.

---

12. Derechos humanos en la terminología internacional en inglés, usándose también la expresión "derechos civiles", términos que usaremos como sinónimos, aunque desde un punto de vista técnico riguroso no lo sean exactamente, de hecho hay una gran discusión conceptual sobre las semejanzas y diferencias entre derechos humanos, derechos civiles y derechos fundamentales, v. ASÍS ROIG, R. de (2012), *Concepto y fundamento de los derechos humanos*, en Juan José Tamayo (Dir.), "10 palabras clave sobre derechos humanos", Ed. Verbo Divino, Estella (Navarra), pp. 15 y ss.

13. Véanse MIRANDA BONILLA, H. (2021), *Algoritmos y derechos humanos*, *cit.*, pp. 709 a 711; MERINO RUS, R. (2020), *Los derechos humanos, la democracia y la igualdad en la era de los algoritmos y la inteligencia artificial*, Colección Red Gernika Doc. 20, Ed. Asociación de Investigación por la Paz Gernika Gogoratuz, Gernika-Lumo (Bizkaia), pp. 23 y ss.; TORRES MANRIQUE, J. I. (2017), *Breves consideraciones acerca del aterrizaje de la inteligencia artificial en el derecho y su influencia en la realización de los derechos fundamentales*, Pensamiento Americano, vol. 10 núm. 19, pp. 11 y ss.; y SAN MIGUEL CASO, C. (2021), *La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?*, Ius et Scientia, vol. 7, núm 1, pp. 293 y ss. Sobre el tema siguen siendo imprescindibles PECES-BARBA MARTÍNEZ, G. (1999), *Curso de derechos fundamentales. Teoría general*, Ed. Universidad Carlos III de Madrid y BOE, Madrid *passim*; y PÉREZ LUÑO, A. E. (2013), *Los derechos fundamentales* (11.ª ed.), Ed. Tecnos, Madrid, *passim*.

14. El uso de la inteligencia artificial puede suponer un peligro real y auténtico para el derecho constitucional a la intimidad del ser humano, v. BOURCIER, D. (2003),

4.°) La IA puede significar igualmente límites o restricciones inasumibles a la libertad que disfrutamos, especialmente restringiendo nuestros derechos fundamentales de forma contraria al Estado de Derecho. En el ámbito penal y en el procesal penal este aspecto es muy destacable (*v. gr.*, con relación al derecho de defensa).

A la vista de esa realidad, se han producido varias iniciativas para tratar de concienciar a las administraciones públicas sobre la importancia de respetar los derechos fundamentales (los derechos humanos) en las aplicaciones de IA. Unas tienen carácter privado y otras son públicas[15].

1) Iniciativas privadas: Deben destacarse las dos siguientes:

a) El 27 de mayo de 2018 se aprobó en Toronto (Canadá) una declaración, propiciada por Amnistía Internacional, *Acces Now*[16], y otras asociaciones privadas, sobre "Nuevos principios de derechos humanos relativos a la inteligencia artificial"[17], centrada básicamente en la protección del derecho a la igualdad y la no discriminación en los sistemas de aprendizaje automático. Su fin no es otro que entender aplicables las normas internacionales en materia de derechos humanos en el uso y desarrollo de la IA, porque se es muy consciente del enorme peligro que entraña el uso de la IA con relación a ciertos grupos de personas vulnerables o a comunidades marginadas, ya que la discriminación y los sesgos parciales aumentan considerablemente en estos casos.

Así, la Declaración de Toronto expone el deber de los Estados de prevenir la discriminación en el diseño o la implementación de los sistemas de aprendizaje automático en contextos públicos o mediante asociaciones público-privadas, garantizando la transparencia y la rendición de cuentas, fijando mecanismos de supervisión independiente, y promoviendo la igualdad (apartados 14 y ss.). También propone fijar las responsabilidades de los actores privados en el contexto del desarrollo y la implementación de sistemas de aprendizaje automático, tales como detectar posibles resultados discriminatorios a través de la identificación y evaluación de

---

Inteligencia artificial y Derecho, Ed. UOC, Barcelona, p. 149; NIEVA FENOLL, J. (2018), *Inteligencia artificial y proceso judicial*, Ed. Marcial Pons, Madrid, p. 150; y BULL, H.-P. (2015), *Sinn und Unsinn des Datenschutzes*, Ed. Mohr Siebeck, Tübingen. pp. 111 y ss.

15. Véase COTINO HUESO, L. (2017), *Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales*, Dilemata. Ética de datos, sociedad y ciudadanía, núm. 24, pp. 131 y ss.

16. Una ONG fundada en 2009, con sede en Nueva York, que defiende los derechos humanos en un Internet de libre acceso para todos los ciudadanos.

17. *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems*, accesible en: https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf.

riesgos, tomar medidas efectivas para prevenir y mitigar la discriminación y ser transparentes (apartados 38 y ss.). Finalmente, pretende establecer el derecho a un recurso efectivo y exigir cuentas a los responsables de las violaciones, exhortando a los gobiernos a que garanticen estándares de debido proceso para el uso del aprendizaje automático en el sector público, y que actúen con cautela al utilizar sistemas de aprendizaje automático en el sistema penal (apartados 52 y ss.)[18].

b) Las Directrices Universales para la IA, aprobadas el 23 de octubre de 2018 en Bruselas por la organización *The Public Voice* y respaldadas por más de 70 organizaciones científicas y más de 300 expertos en la materia[19].

Las Directrices Universales se proponen "para informar y mejorar el diseño y el uso de la IA. Las Directrices pretenden maximizar los beneficios de la IA, minimizar el riesgo y garantizar la protección de los derechos humanos. Estas Directrices deben incorporarse a las normas éticas, adoptarse en la legislación nacional y en los acuerdos internacionales, e incorporarse al diseño de los sistemas. Afirmamos claramente que la responsabilidad principal de los sistemas de IA debe recaer en las instituciones que financian, desarrollan y despliegan estos sistemas"[20].

c) Finalmente, hay otros documentos privados[21], y sin duda periódicamente irán apareciendo muchos más, que no hace falta citar en este estudio, pues todos van en la misma línea en el tema de derechos humanos que ahora estamos tratando.

2) Propuestas públicas:

Me limitaré a Europa. Nuestro continente es también muy consciente de ello. Los documentos europeos consultados que han tratado el tema hasta ahora, se preocupan de contemplar, en el ámbito de la normativización de la IA, las posibilidades de colisión con el sistema de derechos

18. ASÍS ROIG, R. de (2020), *Inteligencia artificial y derechos humanos*, Materiales de Filosofía del Derecho, núm. 4, pp. 4 y 5.

19. Accesibles en https://thepublicvoice.org/ai-universal-guidelines/.

20. Traducción privada del inglés realizada por el autor de este texto. Para GRECO, L. (2020), *Poder de julgar sem responsabilidade de julgador…*, *cit.*, pp. 43 a 64, ésta es la cuestión principal. Véase también HILGENDORF, E. (2012*), Können Roboter schuldhaft handeln? Zur Übertragbarkeit unseres normativen Grundvokabulars auf Maschinen*, en BECK, S. (Hrsg.), "Jenseits von Mensch und Maschine. Ethische und rechtliche Fragen zum Umgang mit Robotern, Künstlicher Intelligenz und Cyborgs", Ed. Nomos, Baden Baden, pp. 119 y ss.

21. Por ejemplo, los llamados "23 Principios de Asilomar sobre la IA", de 2017, apoyados por más de 2000 científicos, v. https://www.robotechnics.es/asilomar/; o la hecha por un grupo organizado de la sociedad civil de América Latina sobre "Declaración sobre ética y protección de datos en la IA", en https://www.tedic.org/etica-y-proteccion-de-datos-en-la-inteligencia-artificial/.

fundamentales diseñado por el Consejo de Europa en el CEDH, y por la Unión Europea en diferentes textos legales.

Debo destacar dos propuestas:

a) A nivel del Consejo de Europa: La Carta Ética Europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno, elaborada por la Comisión Europea para la Eficiencia de la Justicia (CEPEJ) del Consejo de Europa, durante su 31.ª reunión plenaria celebrada en Estrasburgo los días 3 y 4 de diciembre de 2018[22]. Para la Carta Ética, el tema se aborda de forma distinta, concretando esos derechos fundamentales con relación al ámbito de Justicia[23].

b) A nivel de la Unión Europea: Las Directrices Éticas para una Inteligencia Artificial fiable. Dictamen del Grupo independiente de expertos de alto nivel sobre Inteligencia Artificial, creado por la Comisión Europea en junio de 2018, de 8 de abril de 2019[24]. Para las Directrices Éticas, los derechos fundamentales son la base de la IA fiable.

En ambos documentos se concretan los derechos fundamentales con relación al ámbito de la Justicia. Pero si pensamos desde el punto de vista español, que es lo que interesa, no todos esos derechos fundamentales encuentran acomodo, ni directo ni fácil, en nuestra Constitución, al menos tal y como están expresados porque el lenguaje no siempre es claro. A continuación, se podrán ver las razones.

III. EL CONTENIDO BÁSICO

La Unión Europea, en efecto, a través de sus Directrices Éticas para una IA fiable, entra directamente en la materia de los derechos fundamentales afectados por la inteligencia artificial. Como hemos dicho, ello es debido a que considera que los derechos fundamentales son la base

22. Se puede consultar en https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. Se puede consultar en español (traducción no oficial) en: https://campusialab.com.ar/wp-content/uploads/2020/07/Carta-e%CC%81tica-europea-sobre-el-uso-de-la-IA-en-los-sistemas-judiciales–.pdf.

23. Véase GASCÓN MARCÉN, A. (2020), *Derechos humanos e inteligencia artificial*, en PÉREZ MIRAS, A./TERUEL LOZANO, G.M./RAFFIOTTA, E. C./IADICICCO, M.P. (Dir.) y ROMBOLI, S. (coord.), "Setenta años de Constitución Italiana y cuarenta años de Constitución Española", Volumen V – Retos en el siglo XXI, Ed. BOE y CEPC, Madrid, pp. 341 y ss.

24. En la misma fecha se resumió su labor mediante un comunicado de prensa específico, titulado „Inteligencia artificial: La Comisión continúa su trabajo sobre directrices éticas", que se puede consultar en https://ec.europa.eu/commission/presscorner/detail/es/IP_19_1893.

de una IA fiable para garantizar una IA ética y robusta[25]. A ello hay que sumar, en un avance más preciso, los principios éticos establecidos por la Carta Ética específicamente sobre el uso de la IA en los sistemas judiciales y su entorno. De esta manera, las Directrices Éticas y la Carta Ética se complementan, razón por la que deben estudiarse conjuntamente.

Los principios son los siguientes[26]:

1.°) Principio de respeto de los derechos fundamentales: En primer lugar, debe garantizarse por quienes elaboran los sistemas de IA que el diseño y la implementación de herramientas y servicios de IA sean compatibles con los derechos fundamentales reconocidos por el Convenio Europeo de Derechos Humanos. En concreto, la Carta Ética destaca que la IA no debe socavar los principios de derecho de acceso al juez y el derecho al juicio justo (igualdad de armas y respeto por la confrontación).

Pero también destaca que la IA debe respetar el principio del Estado de Derecho (*Rule of Law*) y la independencia de los jueces en su toma de decisiones.

2.°) Principio de no discriminación: Prevenir específicamente el desarrollo o intensificación de cualquier discriminación entre individuos o grupos de individuos. Esto significa que la IA no debe contribuir a reproducir o agravar la discriminación, o a conducir a análisis o usos deterministas.

Un tema preocupante se da cuanto se usan datos sensibles, por ejemplo, el origen racial o étnico, los antecedentes socioeconómicos, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical, los datos genéticos, los datos biométricos, datos relacionados con la salud o datos relacionados con la vida sexual u orientación sexual.

3.°) Principio de claridad y seguridad: En realidad son dos distintos. Se trata de que la IA, con respecto al procesamiento de decisiones y datos judiciales, utilice fuentes certificadas y datos intangibles con

25. Directrices Éticas, p. 11.

26. Carta Ética, pp. 6 a 10. *Vide* BIURRUN ABAD, F.J. (2018), *El Consejo de Europa adopta la primera Carta Ética Europea sobre el uso de inteligencia artificial en los sistemas judiciales*, Actualidad jurídica Aranzadi, núm. 947, pp. 22 y ss.; COTINO HUESO, L. (2017), *Big data e inteligencia* artificial…, *cit.*, pp. 136 y ss.; GOÑI SEIN, J.L. (2019), *Defendiendo los derechos fundamentales frente a la inteligencia artificial*, Lección inaugural del curso académico 2019-2020 Universidad de Navarra, https://www.unavarra.es/digitalAssets/244/244921_1Leccion-inaugural-Castellano-19-20_web.pdf., pp. 20 y ss.; y OLIVA LEÓN, R. (2021), *Inteligencia artificial y marco ético europeo*, accesible en https://www.algoritmolegal.com/tecnologias-disruptivas/inteligencia-artificial-y-marco-etico-europeo/, pp. 4 y 5. Una excelente y amplia exposición en NINK, D. (2021), *Justiz und Algorythmen: über die Schwächen menschlicher Entscheidungsfindung und die Möglichkeiten neuer Technologien in der Rechtsprechung*, Ed. Duncker & Humblot, Berlin, pp. 260 y ss.

modelos elaborados de manera multidisciplinaria, en un entorno tecnológico seguro. Para ello debe contarse con la experiencia de los operadores jurídicos, con los investigadores juristas y con los informáticos, actuando en equipos mixtos de programación.

Los datos a ingresar deben provenir de fuentes certificadas y no deben modificarse hasta que realmente hayan sido utilizados por el mecanismo de aprendizaje. Todo el procedimiento de cumplimentación del software debe ser rastreable para garantizar que no se haya producido ninguna modificación para alterar el contenido o el significado de la decisión que se está procesando. Los modelos y algoritmos creados también deben poder almacenarse y ejecutarse en entornos seguros, para garantizar la integridad e intangibilidad del sistema.

4.°) Principios de transparencia, imparcialidad y justicia: También se trata de tres principios distintos, mediante los cuales se pretende que los métodos de procesamiento de datos sean accesibles y comprensibles. Así, se debe alcanzar un equilibrio entre la propiedad intelectual de ciertos métodos de procesamiento y la necesidad de transparencia (acceso al proceso de diseño), imparcialidad (ausencia de sesgo), justicia e integridad intelectual (priorizar los intereses de la justicia), cuando se utilizan herramientas que pueden tener consecuencias legales o afectar significativamente a la vida de las personas.

Debe quedar claro que estas medidas que se aplican a todo el diseño y a la cadena operativa, como el proceso de selección y la calidad y organización de los datos, influyen directamente en la fase de aprendizaje.

5.°) Principio bajo control del usuario: Significa la exclusión de un enfoque prescriptivo y la garantía de que los usuarios sean actores informados y que controlen las elecciones realizadas. Así, la autonomía del usuario debe aumentarse y no restringirse mediante el uso de herramientas y servicios de IA. Los profesionales del sistema de justicia deben poder revisar, en cualquier momento, las decisiones judiciales y los datos utilizados para producir un resultado y continuar sin estar obligados a ello a la luz de las características específicas de ese caso en particular.

Además, el usuario debe ser informado en un lenguaje claro y comprensible acerca de si las soluciones ofrecidas por las herramientas de IA son vinculantes, sobre las diferentes opciones disponibles y si tiene derecho a asesoramiento legal y derecho a acceder a un tribunal. También debe estar claramente informado de cualquier procesamiento previo de un caso por IA antes o durante un proceso judicial y tener derecho a objetar, de modo que su caso pueda ser escuchado directamente por un tribunal en el sentido del artículo 6 del CEDH.

Explicar esta base jurídica no es difícil: La Unión Europea se funda en un marco normativo que permita el cumplimiento de sus funciones con plena garantía para los estados miembros y sus ciudadanos, sabiendo todos qué se puede hacer y cómo, y qué no se puede hacer y por qué. Ese mismo marco normativo establece las sanciones frente a los incumplimientos. Todo ello permite mover el imponente engranaje de la Unión Europea hacia las metas que se propusieron con su creación y posterior evolución.

El marco normativo está integrado por muchas normas de desigual valor, pero por encima de todas ellas están las normas fundamentales, entre las que se encuentran aquéllas que establecen los derechos fundamentales de los ciudadanos, en realidad normas de protección jurídica máxima frente a la poderosa maquinaria pública que es la Unión Europea y todos y cada uno de los estados que forman parte de ella.

Cuando se introduce la IA en el uso cotidiano de las instituciones europeas y de los ciudadanos para desarrollar sus actividades, ese marco normativo debe ser tenido en cuenta, especialmente el respeto que el uso de la IA debe tener en todo momento por los derechos fundamentales declarados por la Unión Europea. Estamos por tanto ante una cuestión de primer nivel, que debe resolverse normativamente, sabiendo todos los estados y todos los ciudadanos europeos exactamente qué se puede hacer y qué no, y cuál es el grado de tutela conseguido, fijándose las sanciones pertinentes en caso de incumplimiento.

El marco jurídico de los derechos fundamentales viene constituido por los Tratados de la Unión Europea[27], por la Carta de los Derechos Fundamentales de la Unión Europea de 2010[28], y también por la legislación internacional de derechos humanos.

Su respeto es esencial para lograr que el uso de la IA sea aceptado por todos. Según la Unión Europea, "proporciona la base más prometedora para identificar los principios y valores éticos abstractos que se pueden poner en práctica en el contexto de la IA"[29]. No olvidemos que el art. 51 de la Carta de Derechos Fundamentales de la Unión Europea, establece que los derechos recogidos en la misma son jurídicamente vinculantes para las instituciones y los Estados miembros de la UE cuando aplican el Derecho de la Unión; y tampoco descuidemos, de acuerdo con el art. 52

27. Véase la información al respecto que proporciona el Parlamento Europeo, en https://www.europarl.europa.eu/about-parliament/es/in-the-past/the-parliament-and-the-treaties.
28. DOUE núm. 83, de 30 de marzo de 2010, pp. 389 a 403 (DOUE-Z-2010-70003).
29. Directrices Éticas, p. 12.

del mismo texto legal, que la legislación internacional de derechos humanos y, en particular, el Convenio Europeo de Derechos Humanos, son de obligado cumplimiento para los Estados miembros de la UE, incluso en campos que quedan fuera del ámbito de aplicación del Derecho de la UE.

La Carta de los Derechos Fundamentales de la Unión Europea agrupa los derechos fundamentales en torno a los conceptos de dignidad, libertad, igualdad y solidaridad, derechos de los ciudadanos y justicia. Según las Directrices Éticas, "la base común a todos estos derechos puede considerarse arraigada en el respeto de la dignidad humana, reflejando así lo que describimos como un "enfoque centrado en la persona» en el que el ser humano disfruta de una condición moral única e inalienable de primacía en las esferas civil, política, económica y social"[30].

No olvidemos que los sistemas de IA pueden favorecer y obstaculizar el ejercicio de los derechos fundamentales por los ciudadanos, por tanto, pueden ser tanto beneficiosos como perjudiciales. Estos riesgos deben ser asumidos, controlados y en la medida de lo posible eliminados o minimizados[31]. El principal problema hace referencia una vez más a los sesgos injustos que atentan contra el principio de no discriminación y la equidad[32].

Como primera consecuencia de ello, los derechos fundamentales forman parte de la IA fiable (IA lícita), porque son derechos exigibles de primer nivel a efectos de garantizar un uso legítimo y legal de esa IA en el seno de la Unión Europea, cumpliendo la legislación aprobada.

Como segunda consecuencia, y de ahí la intrínseca unión que existe entre ambos, los derechos fundamentales son también derechos individuales que están arraigados en la condición moral inherente a los seres humanos, por lo que también forman parte del segundo componente de la IA fiable (la IA ética), siendo cruciales para garantizar la fiabilidad. No olvidemos que "la reflexión ética puede ayudarnos a comprender el modo en que el desarrollo, despliegue y utilización de la IA pueden afectar a los derechos fundamentales y sus valores subyacentes, y de qué manera pueden contribuir a ofrecer orientaciones más detalladas a la hora de tratar de identificar aquello que debemos hacer en lugar de lo que podemos hacer (actualmente) con la tecnología"[33].

Desde esa perspectiva, las Directrices Éticas hacen mención a los siguientes derechos fundamentales como base para una IA fiable:

30. Directrices Éticas, *loc. cit*.
31. Directrices Éticas, p. 19.
32. Directrices Éticas, p. 23.
33. Directrices Éticas, *loc. cit*.

1) Respeto de la dignidad humana. El reconocimiento de la dignidad humana y su protección se establece en el art. 1 de la Carta en los siguientes términos: "Dignidad humana. La dignidad humana es inviolable. Será respetada y protegida". Se trata de un valor propio del ser humano que en ningún caso puede menoscabarse.

La dignidad del ser humano como valor a proteger está presente en todo el Título I del CEDH. En España, la dignidad de la persona, juntamente con los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás, es uno de los fundamentos del orden político y de la paz social (art. 10.1 CE).

La utilización de la IA debe respetar la dignidad humana. Por tanto, "implica que todas las personas han de ser tratadas con el debido respeto que merecen como sujetos morales, y no como simples objetos que se pueden filtrar, ordenar, puntuar, dirigir, condicionar o manipular. En consecuencia, los sistemas de IA deben desarrollarse de un modo que respete, proteja y esté al servicio de la integridad física y mental de los seres humanos, el sentimiento de identidad personal y cultural y la satisfacción de sus necesidades esenciales"[34].

2) Libertad individual. El art. 6 de la Carta, que no es el único que se refiere a la libertad, proclama en general: "Derecho a la libertad y a la seguridad. Toda persona tiene derecho a la libertad y a la seguridad".

Dados los términos tan generales que implica la palabra libertad, existen precisiones en el CEDH (arts. 5, 9, 10, 11, etc.), y en la CE (arts. 16, 17, 19, 20, 24, etc.).

El uso de la IA se proyecta sobre varios aspectos con relación al derecho fundamental a la libertad. En primer lugar, la persona deber ser libre para tomar decisiones vitales por sí misma, ejerciendo un mayor control sobre su vida, lo que implica libertad frente a intromisiones soberanas, y que se garantice públicamente que las personas en riesgo de exclusión disfruten de igualdad de acceso a los beneficios y las oportunidades que ofrece la IA. En segundo lugar, la libertad individual exige mitigar la coerción ilegítima, las amenazas a la autonomía mental y a la salud mental, la vigilancia injustificada, el engaño y la manipulación injusta. En tercer lugar, la IA debe favorecer la protección de la libertad de empresa, la libertad de las artes y de las ciencias, la libertad de expresión, el derecho a la privacidad y la vida privada, y la libertad de reunión y asociación[35].

34. Directrices Éticas, p. 13.
35. Directrices Éticas, *loc. cit*.

3) Respeto de la democracia, la justicia y el Estado de Derecho. La Carta reconoce explícitamente en el articulado determinados derechos fundamentales relacionados con la Justicia en sus arts. 47 a 50. Que sólo mencione a la democracia y al estado de derecho en su preámbulo no es óbice sin embargo para considerar que la carta no puede aplicarse más que en un estado democrático.

Los términos "democracia", "justicia" y "Estado de Derecho" también aparecen, como no podía ser menos, en el CEDH (menos expresivo en este punto, v. arts. 19 a 51), y en la CE (más expresiva y concreta, v. arts. 1, y 117 a 127).

En este sentido, la IA debe ser utilizada para mantener e impulsar procesos democráticos, así como para respetar la pluralidad de valores y las elecciones vitales de las personas. Asimismo, "los sistemas de IA deben incluir un compromiso de garantizar que su funcionamiento no menoscabe los compromisos esenciales en los que se fundamenta el Estado de Derecho –así como las leyes y reglamentos de obligado cumplimiento– y de asegurar el respeto de las garantías procesales y la igualdad ante la ley"[36].

Desarrollaré inmediatamente este subapartado, descendiendo a la cuestión de los derechos fundamentales procesales afectados por el uso de la IA, por ser el que más me interesa.

4) Igualdad, no discriminación y solidaridad, incluidos los derechos de las personas en riesgo de exclusión. La Carta es muy explícita en este punto. Veamos:

a) El art. 20 establece el principio de igualdad ante la ley: "Todas las personas son iguales ante la ley".

b) El art. 21 establece el principio de la no discriminación:

"1. Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual.

2. Se prohíbe toda discriminación por razón de nacionalidad en el ámbito de aplicación de los Tratados y sin perjuicio de sus disposiciones particulares".

c) El art. 23 proclama la igualdad entre mujeres y hombres:

36. Directrices Éticas, *loc. cit*.

"La igualdad entre mujeres y hombres deberá garantizarse en todos los ámbitos, inclusive en materia de empleo, trabajo y retribución.

El principio de igualdad no impide el mantenimiento o la adopción de medidas que supongan ventajas concretas en favor del sexo menos representado".

d) El principio de solidaridad se desarrolla en los arts. 27 a 38.

e) La protección de personas con riesgo de exclusión se fija en los arts. 24 (niños), 25 (personas mayores) y 26 (discapacitados).

El principio de igualdad se reconoce expresamente en el art. 14 de la CE. Sin duda alguna, comprende la prohibición de toda discriminación. El principio de solidaridad se menciona en varios preceptos constitucionales, siendo la económica la más relevante a nuestro juicio, dada la época en que se redactó nuestra norma suprema (art. 138 CE).

No se trata de que la IA vete cualquier tipo de discriminación, eso en ocasiones no es posible o puede no ser conveniente. Se trata más bien de que la IA evite generar resultados injustamente sesgados (por ejemplo, los datos utilizados para la formación de los sistemas de IA deben ser lo más inclusivos posibles, de forma que estén representados los diferentes grupos de población). Esto también requiere un adecuado respeto de las personas y grupos potencialmente vulnerables, como los trabajadores, las mujeres, las personas con discapacidad, las minorías étnicas, los niños, los consumidores u otras personas en riesgo de exclusión[37].

5) Derechos ulteriores de los ciudadanos. Finalmente, la Carta establece otros muchos derechos fundamentales para la protección y disfrute de sus ciudadanos, que no afectan a derechos de ciudadanos no europeos, obviamente. Por ejemplo, el derecho de voto, el derecho a una buena administración, el derecho de acceso a documentos públicos o el derecho de petición a la administración.

En este sentido, positivamente debe señalarse que los sistemas de IA ofrecen un potencial muy importante para mejorar el alcance y la eficiencia de las autoridades públicas en materia de prestación de bienes y servicios públicos a la sociedad; pero, al mismo tiempo, determinadas aplicaciones de la IA también pueden afectar negativamente a los derechos de los ciudadanos, que deben protegerse, para lo que hay que estar prevenidos[38].

37. Directrices Éticas, *loc. cit*.
38. Directrices Éticas, pp. 13 y 14.

IV. SU CONCRECIÓN EN EL ÁMBITO DE LA JUSTICIA

Las formulaciones anteriores son, sin embargo, demasiado generales y poco efectivas para una verdadera protección. Es necesario ser más concretos.

Si nos fijamos en España, en materia procesal se plantean problemas constitucionales específicos. Además de la posible incidencia en el proceso civil o penal de los derechos fundamentales a la protección de datos, a la intimidad y a la igualdad[39], establecidos por nuestra Constitución, específicamente en el proceso penal se pueden plantear tres muy relevantes. El primero afecta al derecho de defensa, el segundo a la presunción de inocencia, y el tercero al derecho al juez imparcial.

Si combinamos esta cuestión con la propuesta de la Carta Ética, observamos que ésta se centra en los derechos fundamentales procesales, omitiendo los descritos por las Directrices Éticas, con las que aparentemente sólo hay una coincidencia parcial en el principio de igualdad. Para la Carta, los derechos fundamentales implicados son los cinco siguientes[40]:

1) Derecho de acceso a un tribunal. El derecho de acción o derecho de acceso a un tribunal de justicia se declara, bajo la denominación "derecho a la tutela judicial efectiva", en el art. 47, I de la Carta de los Derechos Fundamentales de la Unión Europea. "Derecho a la tutela judicial efectiva y a un juez imparcial: Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo". También se reconoce en el art. 6 CEDH, y en el art. 24.1 CE.

La idea es que la utilización de la IA para resolver controversias *online* no afecte al derecho de acción, es decir, al derecho de acceso a un tribunal de justicia, consagrado en esos preceptos citados, incluso si este derecho no es absoluto y se presta a limitaciones implícitas.

En 2015, la Asamblea Parlamentaria del Consejo de Europa adoptó una resolución sobre "Acceso a la justicia e Internet: potencial y desafíos"[41], en la que advertía que se debe garantizar que "las partes que se involucren en los procedimientos de ODR conserven el derecho de acceder a un procedimiento de apelación judicial que satisfaga los requisitos de un tribunal justo de conformidad con el artículo 6 del Convenio" (punto 7.3).

39. NIEVA FENOLL, J. (2018), *Inteligencia artificial y proceso judicial*, *cit.*, p. 127.
40. Carta Ética, pp. 34 y 35.
41. Resolución 2081: *Access to Justice and the Internet: Potential and Challenges*; de 27 de noviembre de 2015, Asamblea Parlamenaria del Consejo de Europa, Committee on Legal Affairs and Human Rights, accesible en https://pace.coe.int/en/files/22245.

2) Principio adversarial. Llamado por la Carta Ética principio "adversario", se reconoce, parcialmente, en el art. 48.2: "Presunción de inocencia y derechos de la defensa. 2. Se garantiza a todo acusado el respeto de los derechos de la defensa". Es el derecho a ser oído del art. 6.1 CEDH, y nuestro principio de contradicción (y derecho de defensa) del art. 24.2 CE.

El respeto al derecho de defensa plantea cuestiones de suma relevancia. Se trata de que la IA sea accesible a las partes en las cuestiones básicas que afectan al conflicto. Por ejemplo, la información relativa al número de decisiones procesadas para obtener la escala (la posible predicción o una de las varias posibles predicciones), el origen de esas decisiones, la representatividad de las muestras seleccionadas, la distribución de decisiones entre diferentes criterios (como el contexto económico y social). Ello les permitirá comprender cómo se han construido las escalas, de cara a conocer los límites de sus alegaciones y poderlas debatir con mayor y mejor conocimiento ante un juez[42].

3) Igualdad de armas. Recogido en el art. 6 de la Carta y en el art. 14 CEDH, así como en el art. 14 CE, la denominación (de origen alemán) responde a su formulación internacional para los procesos civil y penal.

El reconocimiento en los sistemas de IA responde a la idea de que su uso no cause desequilibrios entre las partes. Si pensamos en las grandes empresas tecnológicas y en los destinatarios que más pueden beneficiarse de sus caros productos, la desigualdad está servida, de ahí la advertencia que se hace. Pero no sólo se está pensando en las grandes empresas, en los más ricos, también en las poderosas administraciones públicas e incluso en quienes tengan sólidos conocimientos informáticos. Frente a ellos, la mayoría de la población, con escasos o nulos conocimientos informáticos, no tendría nada que hacer si no se estableciera esta protección. Por ello, "es importante que ninguna persona se quede sola frente a sus pantallas y que se les informe que pueden buscar asesoría legal y recibir asistencia cuando sea necesario"[43].

4) Imparcialidad e independencia de los jueces. Los principios de independencia e imparcialidad de los jueces, tema nuclear en esta materia, se regulan en el art. 47, II de la Carta: "Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley…" También se recoge en el art. 6.1 CEDH. La CE reconoce expresamente la independencia judicial, en la que va implícita la imparcialidad, en el art. 117.1.

42. Carta Ética, pp. 34 y 35.
43. Carta Ética, p. 35.

Para la Carta Ética la cuestión relevante es que la norma que deriva de la tendencia mayoritaria, a la que nos hemos referido ya en varios lugares, puede tener efectos indirectos sobre la independencia e imparcialidad del poder judicial, particularmente en países en donde la independencia del poder judicial no se logra por completo. En ellos, añade la Carta, "no podemos descartar el riesgo de que tales normas ejerzan una presión indirecta sobre los jueces cuando se toman decisiones y soliciten su aprobación, o que el ejecutivo supervisará a aquellos que se aparten de la norma"[44].

5) Derecho a un abogado. Este derecho fundamental se recoge en el art. 47, II y III de la Carta, tanto en su modalidad general como en particular para quienes carezcan de recurso económicos: "Derecho a la tutela judicial efectiva y a un juez imparcial:

… Toda persona podrá hacerse aconsejar, defender y representar.

Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia".

Se reconoce igualmente en el art. 6.2, c) CEDH y en el art. 24.2 CE.

Se complementa con lo indicado para el derecho de defensa. La cuestión que preocupa a la Carta Ética es que, en los casos en los que las posibilidades de éxito sean muy escasas, atendida la consulta de las herramientas proporcionadas por la IA, pueda afectar la decisión del abogado de ayudar a su cliente. "La práctica profesional debe apuntar a minimizar el riesgo de que las personas que requieren asesoramiento legal puedan ser privadas de él", concluye la Carta[45].

Desde una perspectiva española, el derecho de defensa (arts. 17.3 y 24.2 CE) puede resultar afectado, en algún caso incluso anulado totalmente, por la utilización de la IA[46]. Piénsese en el funcionamiento interno de la IA y se comprenderá inmediatamente que si los algoritmos que ha utilizado la máquina inteligente (juez-robot) para decidir no son conocidos por la defensa, ¿cómo podrá controlar ésta la validez del razonamiento jurídico que ha llevado al juez-robot a la decisión? Nunca sabrá qué datos

44. Carta Ética, *loc. cit*.

45. Carta Ética, *loc. cit*.

46. *Vide* GUZMÁN FLUJA, V. (2017), *Sobre la aplicación de la inteligencia artificial en la solución de* conflictos…, *cit.*, p. 92; NIEVA FENOLL, J. (2018), *Inteligencia artificial y proceso judicial*, *cit.*, p. 127; BARONA VILAR, S. (2019), *Inteligencia artificial o la algoritmización de la vida y de la justicia…*, *cit.*, p. 43; BARONA VILAR, S. (2019), *Cuarta revolución industrial (4.0) o ciberindustria en el proceso penal…*, *cit.*, p. 9; y PÉREZ ESTRADA, J. (2019), *El uso de algoritmos en el proceso* penal, *cit.*, p. 237.

ha tenido en cuenta y qué datos no, ni el porqué, ni habrá podido influir en la adición o eliminación de algoritmos previamente a la decisión de la máquina. Y eso que considero que la actividad probatoria todavía es humana, porque si no lo fuera, ¿de qué estaríamos hablando? Piénsese, por ejemplo, en la actividad para decidir qué documentos se admiten o no, o si la firma es auténtica y fiable o no, etc. Por otra parte, si la decisión la adopta el juez-robot y no hay ni valoración de la prueba ni motivación, ¿con base en qué fundamentación fáctica y jurídica va a poder recurrir la defensa la condena?

6) Derecho a la presunción de inocencia. El derecho constitucional a la presunción de inocencia (art. 24.2 CE) también está en juego[47], un aspecto igualmente de enorme trascendencia.

La máquina decide implacablemente si condena o no. Si condena indiscutiblemente es porque existe para ella al menos una prueba de cargo. Pero es indudable que no se ha producido una actividad probatoria que permita llegar al "cargo", es decir, una actividad humana que ponga en discusión mediante determinados medios legalmente establecidos la existencia y veracidad de los hechos o su inexistencia o falsedad, lo que enfrenta la decisión directamente con la presunción de inocencia. Adicionalmente queda afectada la máxima "in dubio pro reo", porque tampoco puede haber control sobre la duda al carecer la máquina de sensibilidad para dudar[48].

7) El delicado tema de la protección de datos. Un aspecto final, de singular importancia, queda por tratar en este apartado, a saber, la protección de datos de los ciudadanos frente a la IA.

La regulación puede contemplarse desde distintos niveles:

47. Carta Ética, p. 40: "A la luz de lo anterior, cuando se utilizan algoritmos en el contexto de un juicio penal, parece esencial garantizar plenamente el respeto del principio de igualdad de armas y la presunción de inocencia establecido por el artículo 6 del CEDH. La parte interesada debe tener acceso y poder desafiar la validez científica de un algoritmo, la ponderación dada a sus diversos elementos y cualquier conclusión errónea a la que llegue cada vez que un juez sugiera que él/ella podría usarlo antes de tomar su decisión.. Además, este derecho de acceso también está cubierto por el principio fundamental de protección de datos personales. Todas las personas tienen derecho a no estar sujetas a decisiones que les afecten de manera significativa únicamente sobre la base del procesamiento automatizado de datos, sin que su punto de vista se haya tenido en cuenta de antemano".

48. Véanse GUZMÁN FLUJA, V. (2017), *Sobre la aplicación de la inteligencia artificial en la solución de* conflictos…, *cit., ult. loc. cit*.; NIEVA FENOLL, J. (2018), *Inteligencia artificial y proceso judicial*, *cit., ult. loc. cit*; BARONA VILAR, S. (2019), *Inteligencia artificial o la algoritmización de la vida y de la justicia*, *cit., ult. loc. cit*; y BARONA VILAR, S. (2019), *Cuarta revolución industrial (4.0) o ciberindustria en el proceso penal*…, *cit., ult. loc. cit*.

a) La protección de datos es en España un derecho constitucional. En 1978 no cabía hablar en estos términos, de ahí que nuestra Constitución se refiera a la protección de la intimidad y demás derechos frente a la informática.

Dispone en efecto el art. 18.4 CE: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Fue el Tribunal Constitucional quien empleó la terminología actual reconociendo implícitamente en ese precepto el derecho fundamental a la protección de datos, incluso, yendo más allá, habló del *habeas data* (STC 94/1998, de 4 de mayo, FJ 4). Para nuestro TC, la llamada libertad informática es así el derecho a controlar el uso de los datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

El TC español se ha visto obligado a profundizar en la diferencia entre el derecho a la intimidad y el derecho a la protección de datos para conceptualizarlo con mayor precisión (STC 292/2000, de 30 de noviembre, FJ 6).

En resumen, para nuestro TC, el derecho fundamental a la protección de datos persigue garantizar a la persona afectada un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado[49].

49. Véanse PUENTE ESCOBAR, A., *Principios y licitud de tratamiento*, en RALLO LOMBARTE, A (Dir.) (2019), "Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales", Ed. Tirant lo Blanch, Valencia, pp. 115 y ss.; CASAS BAHAMONDE, M.E., *El derecho a la protección de datos de carácter personal en la Jurisprudencia del Tribunal Constitucional*, en VARIOS AUTORES (2015), "20 años de protección de datos en España", Ed. Agencia Española de Protección de Datos, Madrid, pp. 91 y ss.; MITJANS I PERELLÓ, E., *La protección de datos en el entorno digital*, en VARIOS AUTORES (2015), "20 años de protección de datos en España", Ed. Agencia Española de Protección de Datos, Madrid, pp. 399 y ss.; SORIANO ARNANZ, A (2021), *Decisiones automatizadas: Problemas y soluciones jurídicas más allá de la protección de datos*, Revista de Derecho Público: Teoría y Método, vol. 3, pp. 20 y ss.; COLOMER HERNÁNDEZ, I., *Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales*, en BARONA VILAR, S. (2021), "Justicia algorítmica y neuroderecho. Una mirada multidisciplinar", Ed. Tirant lo Blanch, Valencia, pp. 287 y ss.; ESPARZA LEIBAR, I., *La Inteligencia Artificial y el derecho fundamental a la protección de datos de carácter personal*, en BARONA VILAR, S. (2021), "Justicia algorítmica y neuroderecho. Una mirada multidisciplinar", *cit.*, pp. 265 y ss.; y RUGGERI, St., *Circulación de datos personales y tutela de derechos fundamentales en*

Este derecho ha sido desarrollado en nuestro país por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[50].

b) La Constitución española se basó en el art. 8.2 del Convenio Europeo de Derechos Humanos, de 1950, que por su fecha tampoco podía haber hecho otra cosa terminológicamente:

"Artículo 8. Derecho al respeto a la vida privada y familiar.

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

c) También es un derecho fundamental en la Unión Europea:

1) La Constitución Europea se refiere al derecho fundamental a la protección de datos:

a) En el art. I-51 (Protección de datos de carácter personal):

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

2. La ley o ley marco europea establecerá las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes"; y

b) En el art. II-68 (Protección de datos de carácter personal).

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

---

materia de Justicia penal, en BARONA VILAR, S. (2021), "Justicia algorítmica y neuroderecho. Una mirada multidisciplinar", *cit.*, pp. 309 y ss.

50. Véase la *Guía del derecho fundamental a la protección de datos de carácter personal*, publicada en 2005 por la Agencia Española de Protección de Datos, accesible en Internet en: https://datos.redomic.com/Archivos/GuiasUtiles/G33.pdf.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

2) El art. 8 de la Carta de Derechos Fundamentales de la Unión Europea de 2000, dispone: "Protección de datos de carácter personal.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Esta materia ha sido desarrollada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

d) En España, los datos personales de un ciudadano sólo pueden tratarse, es decir, recogerse y emplearse, si (ex art. 6 LOPD):

1) El interesado ha dado su consentimiento.

2) El tratamiento es necesario para el mantenimiento o cumplimiento de un contrato o precontrato de una relación negocial, laboral o administrativa.

3) El tratamiento es necesario para proteger un interés vital del interesado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

4) El tratamiento es necesario para cumplir las funciones de las Administraciones Públicas en el ámbito de sus competencias.

5) Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo del responsable del fichero o de un tercero a quienes se comuniquen los datos.

6) Cuando una ley habilite el tratamiento sin requerir el consentimiento inequívoco de su titular.

El tratamiento de datos de carácter personal ha de realizarse de acuerdo con los principios de información, calidad, finalidad, consentimiento y seguridad. Dichos principios se plasman en diversos preceptos de la LOPD (arts. 4 a 10).

Un tema específico es el de los datos sensibles, porque están especialmente protegidos. Están afectados (arts. 7 y 8 LOPD):

1. Los datos de ideología, creencias, religión o afiliación sindical no pueden ser tratados ni almacenados en ficheros. Sólo pueden ser objeto de tratamiento con el consentimiento expreso y por escrito del afectado; y

2. Los datos relativos al origen racial, a la salud y a la vida sexual sólo podrán ser recogidos, tratados y cedidos, si alguna Ley así lo dispone por razones de interés general, o en caso de que el afectado haya consentido expresamente.

En particular por lo que afecta a los datos sensibles relativos a la salud, pueden ser objeto de tratamiento, si resulta necesario para la prevención o para el diagnóstico médicos, para la prestación de asistencia sanitaria o de un tratamiento médicos o para la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario. También pueden ser tratados estos datos cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para prestar su consentimiento.

V. CONCLUSIONES

Como vemos, todo tiene sus riesgos. El peligro no viene de la información en sí misma, sino de su utilización por el ser humano en contra de otro ser humano, en contra de un conjunto de seres humanos, en contra de grupos de población a los que une una característica que entra dentro de la diversidad, por ejemplo, el color de su piel, o en contra de seres vulnerables, como personas con discapacidad, mujeres, niños o personas mayores, lo que es especialmente repudiable.

El uso de la IA puede ser muy satisfactorio, muy bueno, muy conveniente, pero también todo lo contrario, de ahí que desde las iniciativas privadas y públicas que hemos visto, se incida en definir claramente los límites que la IA no puede traspasar por existir un derecho humano o un derecho fundamental que se opone a ello.

Tenemos ejemplos de ello, algunos también citados aquí, que deben hacernos pensar. El *caso Loomis*, citado, sería el apropiado, por los sesgos

discriminatorios que se revelaron en el algoritmo. Pero lo que más nos puede preocupar es que no seamos capaces con la trepidante evolución de la IA en el mundo jurídico y en concreto en el mundo judicial, de distinguir esos peligros y evitarlos.

Hay aspectos muy positivos que de pronto dejaron de parecerlo y que sin embargo hoy se ven ya normales. Estoy pensando en la utilización de la IA para la gestión de datos e información en los procesos ante los tribunales. Cuando empezó a extenderse su uso se pensaba que nuestra intimidad quedaría totalmente al descubierto porque lo que se estaba introduciendo en las recopilaciones de sentencias eran nuestras condenas y absoluciones. Sin embargo, ha quedado demostrada la utilidad de las bases de datos jurídicos (jurisprudencia y legislación) y no existe hoy ningún jurista (juez, fiscal, abogado, profesor), que no las utilice, habiendo sido relativizado con la protección de datos el tema de la intimidad (y otros derechos que podrían estar afectados, como el derecho a la propia imagen o el mismo derecho al honor).

El peligro viene en la actualidad cuando el enorme desarrollo de la IA se utiliza no para averiguar qué se dijo en el pasado, sino para querer influir en lo que se va a decir en el futuro, es decir, para la predicción. Me preocupa sobre todo que la predicción judicial se quiera conseguir mediante la IA para influir en las decisiones de los jueces, en cualquier materia, pero sobre todo en materia penal.

La predicción no es por sí tampoco negativa. Como estrategia procesal para estar mejor preparado de cara al desarrollo de nuestro asunto civil o causa penal, no es malo querer saber qué se ha sentenciado en casos similares, ni qué ha sentenciado ese juez concreto que es el competente, en casos similares, ni es tampoco malo finalmente querer saber cuáles son las preferencias argumentales de los tribunales para dar la razón en casos muy semejantes. Forma parte de la vida jurídica querer ganar el caso, en realidad, querer hacer Justicia para la parte que lo solicita, y por ello cualquier instrumento cognoscitivo de apoyo debe ser admisible, siempre y cuando los límites estén claramente establecidos.

Pero una cosa muy distinta, porque es dar un paso más, es querer utilizar la IA para decir al juez qué debe decidir en el caso, sustituyendo el razonamiento humano por el artificial, porque entonces la decisión no la toma un ser humano, sino una máquina. Si fuera así, ya no estamos en la predicción, pues hemos aumentado la intensidad y estamos en la decisión. Este es el verdadero peligro que nos acecha hoy en día, y no parece que vayamos a poder conjurarlo en forma satisfactoria y completa inmediatamente, más bien al revés.

Este tema nos lleva a la cuestión central del juez-robot, que no abordaremos en este escrito. No obstante, sí debo avanzar respeto a ello que deberíamos ser capaces de distinguir dos cosas:

1.ª) En principio, y sin matices, debe rechazarse el uso de la IA como sustituto total de la decisión humana. Aquí vulneraríamos tantos principios constitucionales, o lo que es lo mismo, tantos derechos humanos/fundamentales, que asombra ya que a alguien se le ocurra proponerlo. Piénsese, por ejemplo, de acuerdo con lo tratado en este texto, en las violaciones que implicaría que una máquina decidiera el litigio o la causa respecto al derecho a la igualdad procesal o de armas, al derecho de acceso a la Justicia (derecho de acción) y prohibición de la indefensión, al derecho al juez ordinario predeterminado por la ley, el derecho al principio contradictorio (adversarial), al derecho de defensa (a un abogado de confianza o de oficio), al derecho a la prueba, al derecho a un proceso oral y público, al derecho a la motivación de la sentencia, el derecho a la presunción de inocencia, o, finalmente en estos ejemplos, respecto al derecho al recurso[51].

El aspecto concreto que más me preocupa es el ataque a la independencia y a la imparcialidad judiciales que se produciría si se implementara el juez-robot, principios constitucionales muy importantes en España. Constituiría una agresión sin precedentes y absolutamente directa a las esencias del Poder Judicial democrático, investido de independencia e imparcialidad por ser un tercero ajeno al conflicto quien debe decidirlo.

2.ª) Lo que sí sería admisible es fijar los límites de un uso adecuado de la IA para ayudar al juez a tomar la decisión correcta. No parece que el uso de la abundante información que ello comporta, articulando un cálculo de probabilidades razonable con relación al caso concreto analizado, sea por sí mismo negativo.

Este segundo caso, que sería en mi opinión aceptable, debería regularse supranacional, internacional e internamente. Los límites se configurarían con base en los criterios de transparencia y de respeto a los derechos humanos (fundamentales) que en este artículo hemos considerado, fijándose normas absolutamente claras, con fundamento ético sobre lo que se puede y no se puede hacer. Por tanto, el peligro que nos acecha, real y existente, quedaría bajo control si las normas en materia de IA que se anuncian, especialmente el proyectado Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de

51. Hace una enumeración más amplia de derechos fundamentales procesales afectados, bajo lo que considera es el "derecho al debido proceso", discutible en algunos aspectos, ASÍS ROIG, R. de (2020), *Inteligencia artificial y derechos humanos*, *cit.*, p. 11.

Inteligencia Artificial (Ley de Inteligencia Artificial)[52], se aprueban y son asumidas por los estados internamente de una manera eficaz.

Queda por tratar una delicada cuestión, que afecta en concreto a los datos protegidos. El problema surge, a pesar de esa rica y clara legislación y jurisprudencia que hemos recogido *supra*, cuando una administración pública recopila datos autorizados, es decir, en forma legal, de sus ciudadanos, y, o bien ella misma o bien empresas subcontratadas los utilizan para un fin distinto al previsto, por ejemplo, para espiarlos o controlarlos, con la excusa de querer detectar grupos criminales organizados, perseguir a evasores de impuestos, etc., etc., pero en realidad con márgenes tan amplios que incluyen a toda la población, que se convierte así en sospechosa[53].

El peligro puede estar en la propia configuración del algoritmo, además de en su uso torticero, evidentemente. Por un lado, los algoritmos suelen ser opacos, es decir, no cumplen con el principio de transparencia, por lo que llegado el caso de tener que ir a juicio por un tema relacionado con ellos, la administración pública o la empresa privada que los ha utilizado suele negarse a proporcionar información sobre los mismos, aduciendo precisamente esa opacidad (o sea, estar protegida la información por sus derechos de propiedad intelectual).

Por otro lado, y esto es más grave, los datos personales se utilizan masivamente en todos los ámbitos posibles de aplicación del algoritmo,

52. Accesible en https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF.

53. Esto ha sucedido en Holanda, *caso Sistema de Indicación de Riesgos (SyRI)*, en el que un tribunal estatal de La Haya ha sentenciado, con fecha 5 de febrero de 2020 (disponible en https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865), que el sistema holandés de recopilación de datos aplicado a la persecución del fraude fiscal no supera el juicio de necesidad ni el de proporcionalidad que es exigible a toda injerencia en la privacidad de las personas y que, en consecuencia, vulnera el art. 8.2 CEDH. Véase LAZCOZ MORATINOS; G./CASTILLO PARRILLA, J.A. (2020), *Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: El caso SyRI*, Revista Chilena de Derecho y Tecnología, vol. 9, núm. 1, pp. 207 y ss. El autor explica en este texto cómo funciona el algoritmo SyRI y cuáles son los contenidos más importantes de la sentencia; Pueden consultarse igualmente MIRANDA BONILLA, H. (2021), *Algoritmos y derechos humanos*, *cit.*, pp. 729 y 730; FERNÁNDEZ, C.B. (2020), *Primera sentencia europea que declara ilegal un algoritmo de evaluación de características personales de los ciudadanos*, Diario La Ley, accesible en Internet: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbH1czUwMDAyNDa3NDJUK0stKs-7Mz7M1MjACC6rl5aekhrg425bmpaSmZealpoCUZKZVuuQnh1QWpNqmJeYUp-6qlJuXnZ6OYFA8zAQCfSdkrYwAAAA==WKE; y OUBIÑA BARBOLLA, S., *Límites a la utilizaicón de algoritmes en el sector público: Reflexiones a propósito del caso Syri*, en BARONA VILAR, S. (2021), "Justicia algorítmica y neuroderecho. Una mirada multidisciplinar", *cit.*, pp. 655 y ss.

cuando lo previsto normativamente es que esos datos personales únicamente se utilicen para los fines para los que se han creado. Se vulnera así el principio de minimización, en virtud del cual los datos personales sólo deben tratarse si la finalidad del tratamiento no puede alcanzarse en forma razonable utilizando otros medios.

Finalmente, el manejo masivo de datos con fines legítimos sólo tiene sentido si se aplica a la población completa o a grandes sectores de población, porque si sólo se aplica a determinadas zonas, comunidades o grupos, el riesgo de discriminación, es decir, los sesgos de falta de objetividad e imparcialidad, es elevadísimo, causando un efecto estigmatizador en el resultado tan relevante que lo anula por sí mismo.

Si ello es así, ¿dónde queda el derecho fundamental del ciudadano a la protección de sus datos personales? Evidentemente, finalidades como las del ejemplo puesto son admisibles, pues todo estado tiene derecho a perseguir el fraude fiscal. La cuestión clave consiste en que ese mismo estado, en la configuración del algoritmo por él mismo o por una empresa privada, debe introducir u ordenar que se introduzcan las cláusulas de seguridad necesarias para que no se produzcan los indeseados resultados indicados. Debe fijar unos límites, traspasados los cuales el uso de la IA es ilegítimo, cuando no delictivo.

¿Se imaginan qué ocurriría si ese algoritmo lo utilizara el juez-robot?

Ideas para un debate sobre la predicción del crimen

Vicente C. Guzmán Fluja

Catedrático de Derecho Procesal
Universidad Pablo de Olavide, Sevilla

SUMARIO: I. REFLEXIONES SOBRE LA INTELIGENCIA ARTIFICIAL Y EL DERECHO PROCESAL. II. ALGUNOS APUNTES SOBRE LA PREDICTIBILIDAD DE LAS DECISIONES JUDICIALES. III. PREDICCIÓN DEL CRIMEN: EN LAS FRONTERAS DEL PROCESO PENAL. IV. SISTEMAS DE PREDICCIÓN DE LA COMISIÓN DE HECHOS DELICTIVOS. 1. *Ideas previas*. 2. *Sistemas "place-based"*. 3. *Sistemas "person-based"*. 4. *En común: ética de los datos y de los algoritmos*. V. DERECHOS Y GARANTÍAS PROCESALES PENALES. EN ESPECIAL, LA PRESUNCIÓN DE INOCENCIA.

I. REFLEXIONES SOBRE LA INTELIGENCIA ARTIFICIAL Y EL DERECHO PROCESAL

La inteligencia artificial (en adelante IA) ha llegado al derecho procesal para quedarse. Todos estamos de acuerdo en esta premisa, y buena cuenta de ello da el hecho de que en los últimos años se haya producido un notable incremento de las investigaciones que se ocupan de examinar, evaluar y comentar críticamente los cambios que la IA ha ido generando en el Derecho Procesal, así como los posibles cambios que puedan producirse en un futuro.

El acuerdo, sin embargo y como se puede comprobar en la doctrina nacional y de derecho comparado, no alcanza a la consideración de si estos cambios son positivos, negativos, o si tienen una parte de cada, sin que tampoco haya coincidencia en qué aspectos del Derecho Procesal y

del funcionamiento de la Justicia se mejoran, cuáles pueden ir a peor y, sobre todo, qué aspectos resultan admisibles o no, y en qué medida, desde la perspectiva de la preservación de los derechos y garantías inherentes al Derecho Procesal.

En este sentido, expongo tres aspectos de lo que, en mi opinión, depara y puede deparar en un futuro, la relación entre Derecho Procesal e IA:

En primer lugar, la IA a es una herramienta a la que, sobre todo, podemos considerar en su impacto presente en el Derecho Procesal, es decir, en los resultados que se presentan en el momento actual, los cuales son palpables, mensurables. Ello es lo que permite que se pueda emitir un juicio crítico sobre qué de bueno o de malo tiene ese impacto. Pero no significa que no debamos preocuparnos por qué podrá pasar en el futuro de la relación Derecho Procesal – IA, porque resulta importante estar preparados para los posibles cambios y, en función de su alcance previsible y probabilidad de implantación, trabajar en la depuración de los que resulten no admisibles por alterar la propia esencia de los principios, derechos y garantías que integran el Derecho Procesal. Ahora bien, determinar a dónde se podrá llegar en un futuro próximo, medio, o lejano, es difícil de saber, no cabe predecir (y este trabajo va sobre predictibilidad) más que de una manera genérica, hasta dónde llegará el desarrollo de la IA y, en consecuencia, su aplicación del Derecho Procesal, ni cómo aquélla terminará cambiando a éste. Como ya he tenido oportunidad de exponer, todo ello depende de cómo y cuándo se generen la IA generales, frente a las actuales específicas, y fuertes, frente a las actuales débiles, y de hasta dónde pueda evolucionar la computación cognitiva (basada en "machine learning", "deep learning", redes neuronales cada vez más complejas, entre otros factores), y, en especial, de si será posible el uso generalizado de la computación cuántica, circunstancia que supondría un cambio tan profundo que podría llamarse la nueva singularidad. Lo que sí me atrevo a aventurar es que a los posibles grandes beneficios que todo esto pudiera tener para el Derecho Procesal vendrán anudadas también grandes amenazas y dilemas éticos y jurídicos, para los que es mejor ir preparando las mejores soluciones.

En segundo lugar, la IA es, como se acaba de decir, una herramienta, todo lo potente que se quiera, pero una herramienta (muy lejos de tener consciencia de su existencia, y de tener reconocida personalidad jurídica). La pregunta es si esta herramienta permite hoy hacer cosas nuevas en el marco del derecho procesal, cosas diferentes de las que antes de la IA se hacían. En mi opinión todavía no, pues lo que la IA posibilita es hacer mejor, perfeccionar, optimizar, lograr una mayor eficiencia en las tareas hacen los operadores humanos en el proceso, o hacer las tareas

más rápido, o descargar de trabajo a jueces, abogados, fiscales, policía, y demás personas con funciones procesales). Precisamente, un ejemplo claro está en la predictibilidad de las decisiones a lo largo del proceso, ese santo grial tan perseguido a lo largo del tiempo, porque es innegable que ha sido, y es, una aspiración constante, tratar de predecir el resultado de un proceso, o tratar de predecir la reincidencia criminal, o tratar de predecir la comisión de hechos delictivos. Y para conseguirlo, se ha trabajado con las herramientas disponibles en cada momento histórico, manuales, automatizadas o bajo IA en los últimos tiempos. También hay que decir que, a mayor potencia y capacidad operativa de las herramientas usadas, mayor riesgo para los derechos y garantías procesales. Y debemos convenir que la IA es una herramienta mucho más potente que las anteriores, por su manejo de datos en grandes cantidades y con enorme celeridad, y por valerse de algoritmos cada vez más complejos y sofisticados; por esta razón, la IA es, también, una herramienta con una capacidad más invasiva de los mencionados derechos y garantías.

En tercer lugar, la IA es, o debería ser, una herramienta de doble impacto. El primer impacto, es muy visible, ya que la IA proporciona una ayuda cierta que permite avanzar en el logro de viejos anhelos procesales que tienen que ver, entre otros, con la eliminación de las barreras al acceso a la justicia, la optimización de la organización y planta judicial, el alcance de niveles satisfactorios de eficacia y eficiencia, la mejora de los procedimientos, tanto desde su diseño legislativo como a través de una mejor gestión procesal y de recursos humanos y materiales. Hay dos cuestiones en las que la influencia de la IA sobre el Derecho Procesal es muy llamativa: una de ellas, se aborda en este trabajo, y se refiere a la ya mencionada predictibilidad de las decisiones, que muestra ya diversas aplicaciones prácticas, bien en el nivel de sistema de ayuda a la toma de esas decisiones, bien, incluso, en el nivel de ser herramienta decisora en temas calificados de escasa complejidad; la otra, está anudada a la anterior y quizá pasa algo más desapercibida, porque todavía no ha encontrado ese reflejo práctico, me refiero a la uniformidad jurisprudencial, dado que puede extenderse a los primeros niveles de la pirámide de la decisión judicial, de modo que la IA pueda ayudar a una mayor uniformidad de decisiones desde la primera instancia hasta la casación (donde sabemos que la uniformidad en la aplicación e interpretación de la ley es seña definitoria del recurso). He aquí una cuestión compleja, en la que cabe estudiar como afecta la IA, y la predictibilidad que puede alcanzar, al logro de la uniformidad jurisprudencial teniendo en cuenta que esta cuestión enfrenta a la realidad de cómo funciona la creación judicial del derecho, o la vinculación al precedente judicial, ya sea propio, horizontal o vertical, y que supone enfrentar predictibilidad y uniformidad a evolución y creatividad jurisprudencial.

es herramienta de ayuda a la toma de decisiones y herramienta decisora en temas de poca complejidad.

El segundo impacto es menos visible, pero muy importante a mi juicio. La IA nos coloca ante la necesidad de recuperar algo que, quizá, hemos ido desvalorizando al darlo por descontado. Me refiero al estudio e investigación de las instituciones básicas de nuestra disciplina, su profundización constante, porque es ahí donde vamos a encontrar la medida de la bonanza o aceptabilidad de los cambios que la IA genera y puede generar en el Derecho Procesal. Quiero decir que, si todavía no hemos despejado totalmente la respuesta a cuestiones como la teoría de la decisión judicial, o la teoría de la argumentación, o la construcción del juicio de hecho mediante estándares objetivos de prueba, cuanto más avancemos en estos aspectos, más fructífera podrá ser la aportación de la IA. Lo mismo, si pensamos en derechos fundamentales como el debido proceso, o la presunción de inocencia, porque en la medida en que la IA les afecta, debemos preguntarnos si debemos mantener los contenidos esenciales de ambos derechos y desde ahí medir la aceptabilidad de la afectación que sufren, o si deben cambiar esos contenidos, si debe construirse un concepto amplio de ambos derechos, con el riesgo de desdibujarlos, como forma de reacción para encajar mejor la afectación.

En las líneas que siguen, me ocuparé de hacer una reflexión general sobre la predictibilidad de las decisiones judiciales, enlazando con lo que acabo de expresar más arriba. Desde este marco, me centraré en una de las manifestaciones más peliagudas de la IA en relación con el derecho procesal, más concretamente, con el proceso penal: la predicción de la criminalidad, cuestión que tiene implicaciones para la toma de decisiones dentro del proceso penal ya iniciado, pero que también atañe a etapas temporales previas a la incoación de un proceso penal concreto, de forma que se puede decir que la predicción del crimen nos sitúa muchas veces en las fronteras del proceso penal, debiendo analizarse cómo puede producirse el tránsito de esa frontera, de lo que se ha determinado extraprocesalmente a su utilización dentro de un proceso penal determinado, sin infringir las garantías esenciales del sujeto pasivo. Pasaré al análisis de los distintos sistemas de predicción del crimen, señalando sus bases comunes y desarrollando los dos modelos principales: "placed-based" y "person-based", que muestran muy diferentes efectos en lo que se refiere a su relación con los derechos y garantías esenciales del proceso penal. En cualquier caso, comprender el alcance de estos sistemas debe llevarnos a plantear un tema trascendente como es el de la necesaria ética de los datos y de los algoritmos: la IA predictiva de crímenes maneja una enorme cantidad de datos y usa algoritmos complejos con capacidad de autoaprendizaje que, si no se revisten desde

la ética, pueden deparar resultados sesgados, discriminatorios, incorrectos o inadecuados a lo que se pretende. Por último, haré algunas reflexiones sobre la afectación de derechos fundamentales, especialmente sobre cómo la IA usada para predecir la comisión de hechos delictivos puede socavar la presunción de inocencia.

II. ALGUNOS APUNTES SOBRE LA PREDICTIBILIDAD DE LAS DECISIONES JUDICIALES

Abundando en lo dicho más arriba, la IA está siendo utilizada en muchos sectores institucionales, de prestación de servicios públicos, productivos, económicos (por ejemplo, la salud, la economía digital, el empleo, el entretenimiento, el comercio electrónico), y también en el Derecho en general y en la Justicia en particular, y más concretamente en los métodos de solución de conflictos, entre los que se cuenta, cómo no, el proceso judicial. Son muchos los campos del proceso judicial dónde la IA puede ser útil, pero donde ha habido una fuerte aplicación es en lo que se ha dado en llamar "predictibilidad" de las decisiones judiciales.

En el momento actual es posible hablar de una generalización del uso de sistemas expertos legales, basados en inteligencia artificial, que ofrecen la posibilidad de predecir, dentro de unos márgenes "aceptables" de seguridad, la decisión que va a tomar el juez para resolver un caso, aunque también cabe hablar de predicción en relación con otras decisiones previas a la resolución final del caso. En este sentido, y centrándonos en el proceso penal, la predictibilidad abarca desde cuándo, dónde y quién va a cometer (o ser víctima de) un delito, lo que se llama policía predictiva (que tiene un componente acusado de prevención y proactividad frente al crimen), hasta la predictibilidad de la decisión judicial final sobre el caso penal, pasando por la aplicación de los instrumentos de evaluación de riesgos de posible conducta reincidente del acusado para poder tomar decisiones sobre su situación personal durante la tramitación del proceso o, incluso, para influir en la imposición de la pena y en el seguimiento del cumplimiento de la condena[1]. Cabe señalar que, hasta ahora, los casos más llamativos de acierto en la predictibilidad están referidos a órganos judiciales que no son estrictamente jurisdiccionales, sino que tienen un

1. Ya se puede intuir que no estamos ante cuestiones pacíficas que deban ser aceptadas sin más. Un poco más adelante haré valoraciones más específicas sobre ello, pero adelanto que en algunos casos puede decirse que la predictibilidad puede compatibilizarse adecuadamente con el respeto a los derechos y las garantías inherentes al proceso penal mientras que en otros casos esa compatibilidad es imposible y avecinan la deriva hacia el autoritarismo en el control del crimen.

mayor o menor componente político como son la Corte Suprema de Estados Unidos y el Tribunal Europeo de Derechos Humanos[2].

La certeza, o certidumbre, en la aplicación e interpretación de la ley es una de las bases que garantiza el cumplimiento del principio de igualdad de forma que siempre se ha aspirado a que el trabajo de los jueces al decidir pueda ser predecible[3]. Esto es algo tan viejo como la consolidación del Estado de Derecho. Realmente, y hay que poner las cosas en su sitio, la idea de que las resoluciones judiciales, sobre todo las sentencias, sean predecibles no es, ni mucho menos, nueva. De hecho, debe considerarse inherente al correcto funcionamiento de las garantías del Estado de Derecho, entre las que sin duda está alcanzar, en la mayor medida posible, la igualdad en la aplicación e interpretación de la ley, lo que se trata de plasmar a través del recurso de casación como instrumento uniformador de la jurisprudencia del que disponen las Cortes Supremas. Pero, es más, el sistema judicial en todas sus instancias debe operar bajo condiciones de certidumbre, si se quiere certeza, y seguridad jurídica para erradicar, o al menos prevenir eficazmente, la incertidumbre, el azar o la arbitrariedad en la aplicación e interpretación judicial de las normas jurídicas, lo que finalmente podrá contribuir a evitar litigiosidad innecesaria[4]. Esta idea, la de que los jueces deben decidir bajo parámetros de predictibilidad, deja margen, como no puede ser de otro modo, para que la jurisprudencia pueda evolucionar y cambiar, apartándose de líneas jurisprudenciales previas mediante el adecuado y razonado ejercicio de la motivación[5]. Por lo tanto, como una de las

2. Véase ALETRAS N., TSARAPATSANIS D., PREOŢIUC-PIETRO D., LAMPOS V., (2016) "Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective", *PeerJ Computer Science* 2:e93, 19 pp. https://doi.org/10.7717/peerj-cs. 93; Medvedeva, M., Vols, M. & Wieling, M. "Using machine learning to predict decisions of the European Court of Human Rights", *Artificial Intelligence and Law,* volumen 28, 22020, pp. 37–266; en lo que se refiere a la Corte Suprema Federal de USA, hay un gran número de estudios previos sobre la predictibilidad de sus decisiones cito a título indicativo, RUGER, T., W., KIM, P., T., MARTÍN, A., D., QUINN, K., M., "The Supreme Court forecasting Project: legal and political science approaches to predicting Supreme Court decisionmaking", *Columbia Law Rewiew*, Vol. 104, 2004, pp. 1150-1209, y MARTÍN KATZ, D., BOMMARITO II, M.J., BLACKMAN, J., "A general approach for predicting the behavior of the Supreme Court of the United States", PLoS ONE 12(4), 2016: e0174698. https://doi.org/10.1371/journal.pone.0174698.

3. En general, puede verse En este sentido ver CONSTANTINO, en "La prevedilità della decisione tra uguaglianza e appartenza", en *Rivista di Diritto Processuale*, 2015, pp. 645 y ss.

4. Con más detenimiento, PÉREZ DAUDÍ, V., "El precedente judicial. La previsibilidad de la sentencia y la decisión automatizada del conflicto", *Iustel, Revista General de Derecho Procesal* 54 (2021), 30 pp.

5. Al respecto, y siendo una cuestión de complejo alcance, a los efectos de ilustrar la idea del texto baste con citar ahora, sin entrar críticamente en las conclusiones de la autora, a GARRIDO GOMEZ, María Isabel, "La predecibilidad de las decisiones judiciales", *Ius*

bases que hacen realidad la vigencia del principio de igualdad en la aplicación e interpretación de la ley está la predictibilidad (o la previsibilidad) de la decisión judicial en un caso concreto consistente en que, salvo que haya razones y argumentos para un cambio jurisprudencial, el juez decidirá con el mismo criterio y en la misma línea en la que fueron resueltos casos iguales o semejantes al último que tiene en sus manos.

En este sentido, las partes procesales y los encargados de defender su respectiva posición dentro del concreto proceso siempre han hecho una proyección de resultado esperado en relación con su caso atendiendo diversos factores, entre ellos, señaladamente, las decisiones previas referidas a casos iguales o semejantes, y conforme a esas previsiones han hecho los asesoramientos pertinentes o han llevado a cabo las estrategias procesales más oportunas. Bien sea por la vía del sistema de precedentes obligatorios (el complejo y cambiante sistema de "stare decisis") o por la vía de la jurisprudencia asociada al imperio de la ley, a la correcta y uniforme aplicación e interpretación de la ley, hay un elemento de esperabilidad del sentido de la decisión, sin perjuicio de la adecuada flexibilidad que rompe esa predictibilidad en algunos casos[6].

Lo que resulta nuevo, pero tampoco tanto ya que los estudios sobre la posibilidad del uso de la inteligencia artificial para predecir el resultado de los casos judiciales pueden comenzar a datarse desde la década de los años 50 del siglo pasado[7] (e incluso

---

et Praxis, Talca, volumen 15, n. 1, p. 55-72, 2009, disponible en <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122009000100003&lng=es&nrm=iso>. accedido en 17 jun. 2019. http://dx.doi.org/10.4067/S0718-00122009000100003.

6. De nuevo ante la complejidad de la cuestión baste ahora con citar dos obras recientes, la primera que expone las ideas de certeza del Derecho, seguridad jurídica y predictibilidad de las decisiones judiciales en una comparativa entre sistemas de *common law* y de *civil law*, MARQUÈS I BANQUÈ, M., "La certeza del derecho y la individualización de la pena en el *common law*", en Estudios Penales y Criminológicos, volumen XXXVII, 2017, pp. 123-178; la segunda, que expone la idea de predictibilidad como estabilidad también en relación a la comparativa entre sistemas de *common law* y de *civil law*, ALVIM BAMBIER, T., A., "La uniformidad y la estabilidad de la jurisprudencia y el estado de derecho –civil law y common law", *THEMIS: Revista de Derecho*, ISSN 1810-9934, número 58, 2010, pp. 71-80. Recientemente, señalando que en España no rige el sistema de precedente, salvo respecto de sentencias del TC o del TJUE, sino el de previsibilidad de las decisiones expresada en las funciones nomofiláctica y uniformadora del tribunal Supremo, PÉREZ DAUDÍ, V., "El precedente judicial. La previsibilidad de la sentencia y la decisión automatizada del conflicto", *Iustel, Revista General de Derecho Procesal* 54 (2021), 30 pp.

7. PEÑA OROZCO, C. A., "Impacto de la inteligencia artificial en el quehacer jurídico", *Revista Pensamiento Americano,* número 5, Julio-Diciembre 2010, pp. 63-64, hace un breve repaso por los inicios de la aplicación de la IA al Derecho y alude al nacimiento de la jurimetría, que implica la posibilidad de predecir, mediante programas

antes[8]), es que, con el avance de la inteligencia artificial en las dos décadas del siglo XXI, se haya desarrollado la tecnología adecuada para lograr que las inteligencias artificiales puedan estar en condiciones de predecir las decisiones de los casos judiciales de forma más eficiente de la que podrían hacerlo las personas; los índices de acierto de la solución predicha por la máquina van constantemente en aumento y la jurimetría se extiende a otras predicciones que generan la ilusión de que asistimos a algo nuevo (predicción sobre las probabilidades de reincidencia de un acusado o de un condenado).

En realidad, la novedad está en la aplicación de IA a estas tareas, pero si lo pensamos bien no se está haciendo nada, a través de las máquinas, que no hayan intentado hacer antes, de variadas formas, los humanos: predecir el resultado de un caso judicial, predecir la solución a un conflicto, predecir la posible estrategia que va a desarrollar la parte contraria en un caso concreto, predecir cuál será la mejor estrategia posible para ganar un caso, tratar de saber, de antemano, qué abogado, qué fiscal, qué juez será el más adecuado para afrontar el caso concreto, etc[9]. Son objetivos que siempre se han querido alcanzar y así se ha hecho con mayor o menor tasa

---

informáticos, las decisiones judiciales, citando como precursores a Lee Loevinger, primero en "Jurimetrics: The Next Step Forward", *Minnesota Law Review*, April 1949, y posteriomente el mismo autor en "Jurimetrics: Science and Prediction in the Field of Law", *Minnesota Law Review*, 1961; a ellos, y entre otras obras, cabe añadir Reed C. Lawlor, "What computers can do: Analysis and Prediction of Judicial Decisions", American Bar Association Journal, April 1963.

8. Dentro de los diversos programas que desarrolla la EJTN (European Judicial Training Network, http://www.ejtn.eu, una de las principales plataformas y promotoras para la formación e intercambio de conocimientos del poder judicial europeo, que representa los intereses de más de 120,000 jueces, fiscales y entrenadores judiciales europeos en toda Europa) está THEMIS competición abierta a futuros magistrados de la UE que reciben formación de nivel inicial, es un evento para debatir temas, compartir valores comunes, intercambiar nuevas experiencias, debatir nuevas perspectivas y practicar habilidades judiciales. En la semifinal D de la edición de 2017, Budapest 3-6 de julio, el equipo francés, compuesto por Adrien Fauchier Delavigne, Ariane Gajzler, Anna Marin, presentó el trabajo "The challenges facing justice in the future: judges confronted with the advent of Big Data Analytics", http://www.ejtn.eu/Documents/Team%20FR%20semi%20final%20D.pdf, en cuya página 8 se afirma que "The idea of applying scientific processes to judicial matters goes back a long way in History. In the 18th century mathematicians such as Poisson and Condorcet were already working in France on rationalizing judicial activity through statistics and probabilities". Como explican en nota a pie de página, Siméon-Denis Poisson, escribió, en 1837 (siglo XIX) *Recherches sur la probabilité des jugements en matières criminelles et matière civile]*, mientras que Nicolas de Condorcet, escribió en 1785 (siglo XVIII) *Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix*.

9. Sobre la definición de jurimetría y su extensión a los diversos sectores de la actividad jurídica relacionada con la solución de conflictos, véase BARONA VILAR, S.,

de éxito, pero dentro de la limitación del propio conocimiento humano, de las capacidades de cada uno, y de la limitación de las herramientas que estaban disponibles para alcanzar esos objetivos (por ejemplo, desde los grandes volúmenes que recopilaban la jurisprudencia y que exigían una ardua tarea manual de consulta, hasta la aparición de las bases de datos informatizadas que facilitaron la consulta al posibilitar que se consultaran más sentencias en menos tiempo).

La pregunta que debemos hacernos es ¿qué aportan las inteligencias artificiales a lo que son capaces de hacer los operadores jurídicos humanos? Es decir, se trata de determinar si la tarea jurídica decisoria humana es mejorada, tanto cuantitativa como, sobre todo, cualitativamente, cuando se ponen a hacerla las inteligencias artificiales. Lo que encierra está pregunta es si las inteligencias artificiales nos sirven, cuando menos, para avanzar en la aplicación e interpretación del derecho de manera que ésta sea más previsible, proporcione más certidumbre y seguridad jurídica, y responda a parámetros de igualdad. A su vez, se trata de determinar si ese posible avance nos ayuda a comprender mejor algunos aspectos básicos que sustentan la solución judicial de conflictos como, por ejemplo, la teoría de la decisión y la teoría de la argumentación, de modo que las IA puedan ayudar a entender con más precisión el comportamiento del juez humano. En última instancia, se trata de saber si estamos ante un instrumento que permite alcanzar unas cotas mayores de justicia en la solución de los conflictos, justica aprehensible y comprensible para las personas, a la vez que permite reducir los errores y los puntos opacos que dificultan el control de la decisión judicial. En el otro lado de la balanza está la cuestión de si, inherente a todo esto, puede conducir a una justicia más eficiente pero deshumanizada.

Si todo lo que se ha dicho sobre la predictibilidad de las decisiones judiciales, sobre todo penales, es ya suficiente para hacernos reflexionar en profundidad, especialmente preocupante puede ser el efecto que las herramientas de IA han producido sobre otro aspecto de la predictibilidad, la que se refiere a las conductas criminales futuras.

III. PREDICCIÓN DEL CRIMEN: EN LAS FRONTERAS DEL PROCESO PENAL

La predicción del crimen y la policía predictiva, no son recientes ni novedosos, se puede considerar que también ha sido una antigua

Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice (1a ed.), Tirant lo Blanch, 2021.

aspiración y un objetivo de política criminal, primero realizado casi como una labor artesanal y manual por la policía, y en una larga evolución, incorporando las tecnologías adecuadas que iban apareciendo, cada vez más avanzadas y sofisticadas hasta generalizarse el uso de la IA y de los análisis masivos automatizados[10].

Cuando hablamos de la posibilidad de predecir el crimen, la comisión de hechos delictivos futuros, probables, pero no ciertos, estamos en los límites del derecho procesal penal y, como toda frontera poco explorada, es peligrosa. Es razón de más, junto con muchas otras que luego se apuntarán, para ocuparnos de la cuestión, porque el cruce de la frontera nos sitúa dentro del proceso penal, pero éste va a estar ya condicionado de alguna manera por lo acontecido fuera. Lo que es importante es tener en cuenta que no es suficiente con los esfuerzos y preocupaciones que se desplieguen desde el derecho procesal, porque realmente el análisis de cómo, dónde, porqué se cometen delitos, quienes, y porqué son proclives a reincidir, qué factores permiten prevenir o anticipar conductas delictivas, está en el ámbito de la criminología, a la que recientemente se unen otras ciencias como la neurociencia (y la neurocriminología), la genética (con todas las luces y sombras que se quiera), la psicología forense, o la psiquiatría forense. Lógicamente, en ese trabajo, reconociendo la enorme importancia de todas estas ramas del saber, usamos una perspectiva eminentemente procesal en el análisis.

En realidad, las cuestiones referentes a la predicción del crimen a través de los sistemas de policía predictiva están puestas de manifiesto por la doctrina[11], haciéndose hincapié en tres cuestiones: hay un evidente

10. A título de ejemplo, ya en 1990 puede verse un estudio al respecto: ANDERSON, D., "Seattle and Tacoma PDs Automated Crime Analysis", *National F.O.P. Journal Volume 19,* Issue 2, Spring 1990, Pages 50-52," by mapping past incidents of burglaries, vandalisms, and rapes, the police hope to predict and prevent similar crimes from occurring by adding police presence to neighborhoods and during the shifts that are most likely to see action. They can also use the maps to forewarn each shift of criminal activities that are likely to occur". En efecto, no es novedoso el análisis cuantitativo de la criminalidad para establecer patrones y poder "predecir" la criminalidad, sino que es algo que ya existía en el siglo XIX, véase sobre esto y la posterior evolución, BACHNER, J., "Predictive Policing: Preventing Crime with Data and Analytics", Washington, DC: IBM Center for The Business of Government, 2013, publicado en www.businessofgovernment.org, spring, 2014, pp. 86-90. Puede verse también mi aportación sobre el tema, GUZMÁN FLUJA, V., "Proceso penal y justicia automatizada", *Revista General de Derecho Procesal*, N.° 53, 2021.

11. En este trabajo no se analiza la implementación de herramientas de policía predictiva en España, pero puede verse al respecto, entre otros, GONZÁLEZ-ÁLVAREZ, J. L., SANTOS HERMOSO, J., CAMACHO-COLLADOS, M., "Policía predictiva en España. Aplicación y retos futuros", *Behavior & Law Journal,* volumen 6, número 1, 2020, pp. 26-41, donde se analizan herramientas como *veripol, previogen,* y otras.

auge de la utilización de las herramientas de policía predictiva, habiendo numerosas experiencias prácticas al respecto; no se puede establecer una valoración positiva general de tales herramientas, puesto que muestran diferentes niveles de eficacia y exactitud en las predicciones, no siempre son exitosas en la prevención o reducción del crimen, o no tanto como se esperaría, dependen mucho de la tipología delictiva a la que están referidas; presentan problemas éticos y jurídicos en relación a la afectación de derechos y garantías de las personas, pero también en la propia configuración de las herramientas. Pero también hay un acuerdo generalizado en que no existen todavía suficientes evidencias ni sobre los beneficios, ni sobre los inconvenientes, y se necesita profundizar en la obtención de dichas evidencias[12]. Por otro lado, sería interesante establecer la comparativa entre las prácticas de la policía tradicional y las prácticas de policía predictiva, porque quizá se pueda establecer que en ambas se encuentran presentes beneficios y amenazas similares en términos de prácticas discriminatorias, de relativa inefectividad y de focalizarse de forma desproporcionada en las minorías[13]. De justicia es también reconocer que la policía predictiva tiene una mayor capacidad amplificadora de beneficios y amenazas, porque se basa en al análisis de más datos, más rápido y más generalizados o referidos a una cantidad mayor de personas.

Merece la pena hacer un breve excurso sobre la terminología que se utiliza, ya que el verbo predecir se define por la RAE como "anunciar por conocimiento fundado (no por revelación, intuición o conjetura) algo que ha de suceder" (no entro aquí en si el término más correcto debería ser pronosticar: predecir algo futuro a partir de indicios[14]). Es decir, la base

12. Es costumbre en la doctrina anglosajona, hacer investigaciones consistentes en revisar el estado de la cuestión de un determinado tema, haciendo un repaso por las contribuciones más importantes y extrapolando de ellas los elementos más señeros o que más se deben tener en cuenta. En relación con la policía predictiva hay varios, citaré aquí tres recientes: ALBERT MEIJE, A., WESSELS, M., "Predictive Policing: Review of Benefits and Drawbacks", *International Journal of Public Administration*, volumen 42, 2019, pp. 1031-1039; MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences* 10 (6), junio 2021, 234, 14 pp., https://doi.org/10.3390/socsci10060234; ALIKHADEMI, K., DROBINA, E., PRIOLEAU, D., RICHARDSON, B., PURVES, D., GILBERT, J. E., "A review of predictive policing from the perspective of fairness", *Artificial Intelligence and Law*, 2021, pp. 1-17. De ellos se desprenden las tres afirmaciones efectuadas en el texto, que se desarrollan en este trabajo y que serán sustentadas por otras citas doctrinales que se reputen necesarias o útiles.

13. Al menos está es la tesis sostenida por BROWNING, M., ARRIGO, B. "Stop and Risk: Policing, Data, and the Digital Age of Discrimination", *American Journal of Criminal Justice*, volumen 46, 2021, pp. 298-316.

14. Pronosticar y predecir el delito, sobre las diferencias entre estos términos, que pueden parecer fútiles pero que puede no serlo, véase PAULSEN, D., BAIR, S., HELMS,

es un conocimiento fundado (no una revelación, intuición o conjetura, ni adivinación), que en este caso proviene del análisis de datos mediante el cual se determina algo que ha de suceder, pero en términos de probabilidad, no de seguridad (no siempre la probabilidad es del 100%). Entrando en juego la IA, sabemos que ese análisis lo es de una gran cantidad de datos, mediante un algoritmo, cada vez más complejo y sofisticado con capacidad de autoaprendizaje, todo lo que permite refinar en alto grado la predicción criminal (algo que siempre se ha hecho, artesanalmente o con herramientas menos sofisticadas). Se debe ser consciente de que todo lo que conlleve una tarea predictiva de la criminalidad, con altos grados de exactitud, con transparencia, con datos y algoritmos "limpios", implica emplear recursos de alto coste, y con la espada de Damocles que supone el juicio sobre su ajuste, o no, a los derechos y garantías fundamentales, por lo que es razonable preguntarse, para qué hacer todo esto.

En este sentido, a mi entender, predecir la comisión de hechos delictivos puede llevar a dos finalidades que no son excluyentes, pero que deben tener una relación de prioridad: la primera es prevenir la comisión de hechos delictivos, en general o de hechos concretos, y por tanto dirigir los esfuerzos básicamente a la evitación de la criminalidad[15]; la segunda es la de estar en condiciones mejores u óptimas para, si no se logra evitar, poder perseguirlo e investigarlo, bien por la cercanía y prontitud de la respuesta policial al crimen fruto de las estrategias de patrullaje y vigilancia, bien por los datos e informaciones que se han logrado reunir en la tarea predictiva. Creo que lo ideal es prevenir mediante estrategias policiales, o políticas públicas en general, de anticipación y disuasión, para reducir la criminalidad, pero como no siempre será posible, o no siempre se conseguirá, la información acumulada sobre el hecho delictivo predicho y realizado (intentado o consumado), podrá servir para su mejor, más adecuada y más rápida investigación en el proceso penal correspondiente, aunque realmente no es tan simple como parece. Entiéndase bien

D., "Pronosticar y predecir", Análisis delictual: técnicas y metodologías para la reducción del delito, fundación paz ciudadana, Chile, 2012, pp. 124-144, traducción autorizada por los autores del original en inglés "forecasting and prediction" de 2010.

15. Esta finalidad preventiva de la criminalidad es generalmente reconocida como un efecto principal de la policía predictiva, además de la doctrina citada hasta ahora, puede verse también EGBERT, S., KRASMANN, S., "Predictive policing: not yet, but soon preemptive?", *Policing and Society: An International Journal of Research and Policy*, Volumen 30, Issue 8, 2020, pp. 905-919; HARDYNS, W., RUMMENS, A., "Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges", European Journal on Criminal Policy and Research, volumen 24, 2018, pp. 201-218. En España puede verse, entre otros, GONZÁLEZ-ÁLVAREZ, J. L., SANTOS HERMOSO, J., CAMACHO COLLADOS, M., "Policía predictiva en España. Aplicación y retos futuros", *Behavior & Law Journal*, *cit.*, pp. 26-41.

que la prevención es preferible a la reacción, pero que la prevención no debe depender sólo de la acción policial, sino que debe reposar en otras políticas, sociales, económicas, de integración que pongan el acento en la persona no en su consideración como delincuente ni como posible-futuro delincuente.

Dicho lo anterior, lo que ofrece la policía predictiva basada en IA desde la perspectiva preventiva es alcanzar unos niveles de predicción delictiva que permite un mayor nivel de éxito en las políticas públicas de contención de la criminalidad y en la optimización de las estrategias policiales sobre el terreno, con una mayor eficiencia en la asignación de sus recursos humanos y materiales, a la vez que permite la adopción efectiva de modelos de "intelligence led policing", "inteligencia policial" policía basada en datos y de carácter anticipativo más que reactivo (modelo que convive con los de policía comunitaria, policía orientada a los problemas, entre otros[16]). Cabe recordar que esto no es tampoco estrictamente novedoso, porque desde hace algunas décadas una línea de trabajo policial es la llamada policía proactiva, como contrapunto a la policía reactiva al crimen, configurada en sus orígenes como como una medida extraordinaria de investigación, pensada para adelantarse a la comisión de hechos delictivos especialmente graves y cometidos por organizaciones criminales[17],

16. Una breve evolución histórica de los modelos policiales puede verse en PINTOR LATORRE, M., "Inteligencia policial en España ¿un buen camino hacia la prevención del delito?, en *La Criminología que viene. Resultados del I encuentro de jóvenes investigadores en Criminología*, 2019, pp. 141-148, en concreto pp. 142-144, en las que define el modelo de inteligencia policial como "es la policía guiada por la inteligencia que definida a rasgos generales enfatiza una estrategia preventiva basada en el análisis y su influencia sobre la toma de decisiones, de un modo similar al empresarial, mediante la identificación de objetivos clave (delincuentes/grupos habituales, víctimas reiteradas, hot-spots, etc.) para un impacto efectivo en la reducción del delito y del daño que provoca en la sociedad". En la abundante literatura anglosajona sobre el tema, llama la atención el estudio comparativo CARTER, J. G., FOX, B., "Community Policing and Intelligence-Led Policing: An Examination of Convergent or Discriminant Validity", *Policing: An International Journal,* diciembre 2018, https://doi.org/10.1108/PIJPSM-07-2018-0105, 31 pp.; más reciente, PIRES PEREIRA, A. R., PASCOAL ROSADO, D., COMBA LOPES, H. S., "From the Traditional Police Model to Intelligence-Led Policing Model: Comparative Study", en *Information and Knowledge in Internet of Things*, Guarda T., Anwar S., León M., Mota Pinto F.J. (eds.) EAI/Springer Innovations in Communication and Computing, Springer, 2022, pp. 457-473.

17. Así, por ejemplo, en *Policía. Investigación de delitos. Manual de instrucciones para la evaluación de la justicia penal 3*, Oficina de las Naciones Unidas contra la Droga y el Delito, UNODC, Naciones Unidas, Nueva York, 2010, pp. 11-12; y en *Policía. Sistemas policiales de información e inteligencia. Manual de instrucciones para la evaluación de la justicia penal 4,* Oficina de las Naciones Unidas contra la Droga y el Delito, UNODC, Naciones Unidas, Nueva York, 2010, pp. 20; puede verse también VERVAELE, J. A. E., "Medidas de investigación de carácter proactivo y uso de información de inteligencia en

reconociéndose que tiene una alta capacidad limitativa de derechos y garantías, lo que se justificaba en atención a la concreta tipología delictiva de gran capacidad de amenaza a los bienes jurídicos esenciales y básicos (terrorismo, tráfico de personas, tráfico de drogas a gran escala, entre otros). Por ello, la proactividad policial conecta con la prevención y con la obtención de información que mejore las condiciones de investigación de los delitos, sólo que ahora hay un uso más generalizado y no constreñido a los graves delitos mencionados, una mejora vía utilización de las herramientas de IA y una multiplicación cuantitativa y cualitativa de riesgos para los derechos y garantías fundamentales.

Por lo tanto, en lo que interesa remarcar, la policía predictiva favorece que se haga difusa la frontera entre la prevención criminal y la investigación y esclarecimiento de los delitos, porque se produce esa zona indefinida en la que se hace una predicción sobre la producción de una conducta criminal, sobre la base de datos e informaciones, que posibilita, como objetivo lógico, su evitación, y, si no se logra, la investigación del delito ya cometido que bebe de esos datos e informaciones. Por lo tanto, datos e informaciones cuyo destino final no se sabe de antemano, como tampoco se sabe qué régimen de tratamiento tendrán en función de que tengan uno u otro destino. Y datos e informaciones que pueden quedar en un preocupante limbo si se ha producido un falso positivo, sobre todo cuando lo es por errónea vinculación de una persona con actos sospechosos de ser potencialmente criminales. Después veremos algo más sobre este tema.

Así, si de lo que se trata es de prevenir y evitar la comisión de hechos delictivos, y para ello se hace un ejercicio de predictibilidad que permita la intervención temprana y la evitación, parece claro que ahí estamos fuera del proceso penal, lo que no significa que no haya cuestiones problemáticas que resolver. Pero, si la evitación no es posible, y el delito predicho se comete, se pasará a la tarea de su investigación, debiendo reconocerse que el punto de partida en este caso es diferente al que habría si no hubiese mediado esa labor predictiva/preventiva. Frente a la investigación reactiva del delito, que implica reconstruir los hechos delictivos una vez han ocurrido, la investigación basada en la predicción y en la proactividad se produce a la vez que se va desarrollando la dinámica criminal. Como se ha dicho de una forma gráfica, "la sospecha individualizada de actividad criminal una vez provocó una revisión de la cartera de datos de una persona, pero ahora la cartera de datos genera una sospecha individualizada"[18].

---

el Proceso Penal", *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar probar el delito*/coord. por Julio Pérez Gil, 2012, pp. 27-86.

18. MILLER, K., "Total surveillance, big data, and predictive crime technology: privacy's perfect storm", *Journal Technology of Law and Policy*, volumen 19, 2014, pp. 105-146, donde

Hay otros aspectos de la policía predictiva que no suelen ser tan visibles, seguramente porque no están en la parte preventiva. Uno que destaca es el referido a lo que se llama el efecto "incitativo" de la policía predictiva: se trataría de un efecto que no casaría con la idea preventiva o de evitación del delito, sino que partiría de que la predicción delictiva "se cumple", y puede contribuir a un aumento de la criminalidad como reacción ante el éxito del mecanismo predictivo que provoca un ciclo de retroalimentación: éxito en la predicción, intensificación de la policía predictiva, aumento de la vigilancia policial y respuesta en forma de aumento de la criminalidad o de niveles crecientes de violencia[19]. Algo parecido es lo que se denomina "efecto de profecía autocumplida" que puede tener la predictibilidad, dado que anuncia un probable futuro criminal, ya sea en relación a zonas donde se van a cometer nuevos delitos, ya sea en relación a personas que van a volver a cometer delitos, sobre la base principalmente de hechos delictivos ya ocurridos, de forma que parecería que determinadas zonas o determinadas personas, no pueden escapar a su futuro y quedan señaladas permanentemente en un bucle del que no pueden salir, como si estuvieran destinados a seguir en él para siempre, pero que puede ser erróneo[20]. Por lo demás, hay un posible efecto de "perpetuación del crimen", dado que el análisis de datos puede ser, y de hecho en determinados delitos lo es, usado por los delincuentes para contrarrestar a la policía predictiva, haciendo, por ejemplo, ingeniería inversa, o para mejorar sus actividades delictivas[21].

---

añade que "si bien las técnicas predictivas se han utilizado en áreas específicas de la criminología durante décadas, el movimiento hacia la vigilancia predictiva mediante la vigilancia automatizada, el procesamiento semántico y las herramientas analíticas magnifica los daños a la privacidad y al debido proceso de cada tecnología, al tiempo que confunde aún más los sistemas tecnológicos. y limitaciones metodológicas. Además, lo hacen con poca disminución compensatoria del riesgo de actividad criminal o terrorismo".

19. ANDREJEVIC, M., "Automated Justice and Post-Disciplinary Power", COLLEGIUM HELVETICUM, Automated Justice: Algorithms, Big Data and Criminal Justice Systems, EURIAS-Conference, Friday, April 20, 2018, disponible en vídeo en https://video.ethz.ch/speakers/collegium-helveticum/digital-societies/automated_justice/84c3f617-8784-4203-b7a8-50a176811933.html.

20. LINDENMUTH, K., "Prevention or Self-Fulfilling Prophecy? Predictive Policing's Erosion of the Presumption of Innocence", *Law School Student Scholarship*, 2019, 28 pp.; SHEEHEY, B., "Algorithmic paranoia: the temporal governmentality of predictive policing", *Ethics and Information Technologies,* 21, 2019, pp. 49-58, en concreto pp. 50-51; la policía predictiva crea un circuito de retroalimentación fuera de control, que no permite conocer la verdadera tasa de criminalidad, problema que puede tener solución, véase ENSIGN, D., FRIEDLER, S. A., NEVILLE, S., SCHEIDEGGER, C., VENKATASUBRAMANIAN, S., "Runaway Feedback Loops in Predictive Policing", *Proceedings of Machine Learning Research,* volumen 81, 2018, pp. 1-12.

21. MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.,* pp. 8-9.

La policía predictiva, de esto se hablará después, trabaja con grandes cantidades de datos sobre criminalidad, de forma que al analizarlos es capaz de extraer determinados patrones de comportamientos pasados que pueden extrapolarse hacia el futuro, determinando el mayor o menor grado de probabilidad de que se vuelvan a producir las conductas criminales. Es necesario hacer dos aclaraciones, una sobre los datos y otra sobre los patrones– Ambas muestran algunas debilidades y problemas asociados a la policía predictiva.

En cuanto a los datos, la predicción policial de conductas criminales futuras se basa tanto e datos pasados como en datos actuales, tomados y analizados en tiempo real, fruto de la vigilancia policial actual, vigilancia en tiempo real o vigilancia instantánea, que permite tanto la alimentación continua de los datos pasados, cuanto, en determinados casos, la detección y supresión, anticipación, o represión de la conducta delictiva, del criminal o de la víctima, es decir, no la previsión futura sino la detección del crimen en tiempo real[22]. Lo cierto es que esta vigilancia policial continuada puede estar basada en el acceso policial a múltiples datos que se producen en tiempo real y que se pueden obtener de múltiples fuentes, circuitos cerrados de televisión en vías públicas, geolocalización por dispositivos móviles, datos de acceso y navegación por internet, redes sociales, entre otras muchas, lo que posibilita una vigilancia masiva que puede dirigirse a la predictibilidad criminal, y que puede resultar muy invasiva de la privacidad y lesiva de los derechos fundamentales de las personas[23]. Por ello, hay que preguntarse de qué manera hay que responder a esta

22. Es decir, la policía predictiva puede dirigirse a establecer probabilidades de conductas criminales futuras, pero su combinación con la vigilancia en tiempo real determina la posibilidad de suprimir la conducta delictiva "al instante", véase WILSON, D., "The Real-Time Cop: Imaginaries of Technology, Speed and Policing", COLLEGIUM HELVETICUM, Automated Justice: Algorithms, Big Data and Criminal Justice Systems, EURIAS-Conference, Friday, April 20, 2018, disponible en video en https://video.ethz.ch/speakers/collegium-helveticum/digital-societies/automated_justice/84c3f617-8784-4203-b7a8-50a176811933.html; BANG, S. H., KIM, T., JI, B., LIMB, Y., CHO, H., "Real-time Crime Prediction Method using Criminal Records", Conference: The 11th Asia Pacific International Conference on Information Science and Technology (APIC-IST), at Sapporo, Japan, 2016, pp. 1-5, https://www.researchgate.net/publication/317588198_Real-Time_Crime_Prediction_Method_using_Criminal_Records.

23. Sobre estos problemas, que son sin duda graves, puede verse, entre otros muchos, BRAYNE, S., "Big data surveillance: The case of policing", *American Sociological Review,* volumen 82 (5), 2017, pp. 977-1008; también, haciendo hincapié en que la policía predictiva ha evolucionado hacia una "platform policing" definida como "larger cloud-based modular informational policing architectures, thereby generating and incorporating diverse technologies and data streams", WILSON, D., "Platform Policing and the Real-Time Cop", *Surveillance & Society*, volumen 17(1/2), 2019, pp. 69-75; MINOCHER, X., RANDALL, C., "Predictable policing: New technology, old bias,

vigilancia policial masiva, si debe prohibirse o si se debe confiar en la policía y regularla con todas las garantías posibles, proponiéndose que se someta al "tyrant test" (test del tirano), ya que es realidad de lo que se habla es de ejercicio de poder y control de las autoridades sobre los ciudadanos[24]. Al final, se trata de hacer un adecuado balance entre qué y cuánto se consigue, en términos de reducción de los niveles de delincuencia y de incremento de la seguridad, frente a qué y cuánto precio se paga o se está dispuesto a pagar en términos de pérdida o disminución de derechos.

Una última cuestión que conviene apuntar se refiere precisamente a los patrones que se extraen de las herramientas de policía predictiva, y sobre los que descansa la predicción y su grado de acierto. Precisamente, la existencia de una gran variedad de herramientas de policía predictiva provoca otro problema referido a la exactitud de su funcionamiento, porque cada uno de ellos define los patrones de forma diferente, se basan en datos o indicadores que pueden ser no coincidentes, y ello puede conducir a resultados diferentes para un mismo objetivo predictivo[25], es decir, puede generar que un mismo indicador funcione de manera distinta y pueda originar malos resultados en la predictibilidad[26]. Esto también influye en los niveles de falsos positivos y de falsos negativos que son diferentes en atención a la herramienta predictiva utilizada. por tanto, hay que trabajar en la definición de patrones atendidos los objetivos predictivos, trabajar en la determinación de los datos a utilizar, y procurar que las diversas herramientas ofrezcan resultados homogéneos en términos de predictibilidad[27].

---

and future resistance in big data surveillance", *Convergence –The International Journal of Research into New Media Technologies*, volumen 26, Issue 5-6, 2020, pp. 1108-1124.

24. Sobre un análisis de las tecnologías de vigilancia policial, se plantean estas cuestiones y se establecen las bases de en qué podría consistir ese "tyrant test", véase el interesante análisis de FERGUSON, A. G., "Surveillance and the Tyrant Test", *The Georgetown Law Journal*, volumen 110, 2021, pp. 205-289.

25. Se parte de que cualquier predicción presupone la aparición de patrones dentro de los datos analizados, es decir: los fenómenos no basados en patrones no pueden identificarse algorítmicamente y, por lo tanto, no estar sujetos a una lógica de pronóstico. A partir de ahí, es necesario saber quién, cómo y cuándo define un patrón, qué variables se utilizan, y ello dentro de esa variedad de herramientas, véase KAUFMANN, M., LEESE, M., EGBERT, S., "Predictive Policing and the Politics of Patterns", COLLEGIUM HELVETICUM, Automated Justice: Algorithms, Big Data and Criminal Justice Systems, EURIAS-Conference, Friday, April 20, 2018, disponible en video en https://video.ethz.ch/speakers/collegium-helveticum/digital-societies/automated_justice/84c3f617-8784-4203-b7a8-50a176811933.html.

26. MARTÍNEZ GARAY, L., MONTES SUAY, F., "El uso de valoraciones del riesgo de violencia en Derecho Penal: algunas cautelas necesarias", *InDret 2/2018,* pp. 8-9.

27. Falso positivo es un error que consiste en determinar un alto riesgo de reincidencia criminal respecto de individuos que no vuelven a cometer crímenes; falso negativo

En definitiva, la revisión de la literatura existente en materia de policía predictiva y vigilancia policial, de la que aquí se ha dado una pequeña muestra, hace ver que se trata de herramientas cuyo uso está en auge, que progresan y mejoran con el paso del tiempo, pero que están lejos, todavía, de ofrecer unos resultados homogéneos, constantes y crecientes en términos de reducción de la criminalidad. Por otro lado, las cuestiones éticas y jurídicas que subyacen en estas herramientas, al amenazar y restringir derechos y garantías fundamentales, no están tampoco resueltos, como se verá en su momento, entre ellos los referidos a uso dentro del proceso penal de información obtenida antes de que se inicie y antes de la propia comisión del hecho delictivo.

En este panorama, la incipiente actividad legislativa sobre inteligencia artificial en la Unión Europea viene a apuntar en la línea de priorizar la salvaguarda de los derechos fundamentales y garantías de las personas ante la creciente utilización en todos los ámbitos de la IA, la robótica y tecnologías conexas. En relación con el proceso penal y la policía predictiva, resultan de gran interés, en este sentido, la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas [2020/2012(INL)]; la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, de 21 de abril de 2021, con especial incidencia en la prohibición del uso de determinadas tecnologías, como la que posibilita el reconocimiento facial (identificación biométrica remota en tiempo real, artículo 5), salvo contadas excepciones; y la Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales [2020/2016(INI)], que se basa en el Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de 13 de julio de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades

es cuando se asigna a un individuo un riesgo bajo de reincidir, pero sin embargo reincide. La tasa de error en los falsos positivos suele ser importante porque la mitad de los sujetos calificados de alto riesgo están mal clasificados (porque no vuelven a delinquir); las tasas de error en los falsos negativos son mucho menores, sobre un 10% de los sujetos clasificados de bajo riesgo están mal clasificados (porque vuelven a delinquir, véase DOUGLAS, T., PUGH, J., SINGH, I., SAVULESCU, J., FAZEL, S., "Risk assessment tools in criminal justice and forensic psychiatry: The need for better data", *European psychiatry: the journal of the Association of European Psychiatrists, volumen 42*, 2017, pp. 134-137; también MARTÍNEZ GARAY, L., MONTES SUAY, F., "El uso de valoraciones del riesgo de violencia en Derecho Penal: algunas cautelas necesarias", *cit.*, pp. 39-40, y pp. 11-13 refiriéndose a riesgos absolutos, riesgos relativos.

policiales y judiciales en asuntos penales [2020/2016(INI)][28]. Los dos últimos se pronuncian expresamente sobre el uso de la policía predictiva, y en el siguiente epígrafe tendré la oportunidad de examinarlos en los aspectos de interés para este trabajo[29].

IV. SISTEMAS DE PREDICCIÓN DE LA COMISIÓN DE HECHOS DELICTIVOS

1. IDEAS PREVIAS

El objetivo en esta parte del trabajo es distinguir entre los diferentes sistemas de predicción de la comisión de hechos delictivos para tratar de establecer qué grado de peligro o amenaza pueden representar para los derechos y garantías de las personas. No se trata, por lo tanto, de analizar la gran cantidad de herramientas concretas basadas en IA que son utilizadas por la policía predictiva, aunque pueda hacerse mención a alguna de ellas.

La idea esencial es clara: la predicción de delitos en cuanto a lugar, tiempo o tipo de delito no supone un grado de intromisión en la esfera de derechos de las personas como la predicción de autores grupales o individuales, o, en otra perspectiva, la predicción de víctimas, también grupales o individuales[30]. La razón es sencilla, y es que los datos sobre los que se realiza el análisis predictivo, en el primer caso, pueden (y deben) desagregarse de cualquier referencia personal que pueda haber en ellos,

28. Los cuatro documentos citados pueden consultarse en los siguientes enlaces, en el mismo orden de cita en el texto: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.pdf; https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF; https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.pdf; https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_ES.pdf.

29. Para análisis más en profundidad de estos textos y la política legislativa de la UE en materia de inteligencia artificial, puede verse, entre otros, DE HOYOS SANCHO, M., El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea", Revista General de Derecho Procesal 55, 2021, 29 pp.; SCHUMANN BARRAGÁN, G., "La inteligencia artificial aplicada al proceso penal desde la perspectiva de la UE" en Pereira Puigvert, S., Ordóñez Ponz, F. (dirs.), Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos, Aranzadi, Cizur Menor, 2021, pp. 517-539.

30. HUNG, T-W., YEN, C-P., "On the person-based predictive policing of AI", *Ethics and Information Technology*, volumen 23, 2021, p. 165, señalan que, de todos los métodos mencionados, "person-based PP is the most controversial, as it singles out individual names and faces". En la misma línea, FITZPATRICK, D. J., GORR, W. L., NEILL, D. B., "Keeping Score: Predictive Analytics in Policing", *Annual Review of Criminology*, volumen 2:1, 2019 pp. 473-491, en especial pp. 488-489.

ya que son irrelevantes para el objetivo marcado, dando lugar a la anonimización, debiendo tomarse las cautelas para que no pueda haber posterior desanonimización; en estas condiciones, y siempre que se cumplan en el marco de la legislación de protección de datos personales, la predicción de hechos criminales en coordenadas espacio-temporales podría ser asumible desde la perspectiva de los derechos y garantías fundamentales, aunque no está exenta de problemas. En el segundo caso, la predicción delictiva es inescindible del manejo de datos personales, pasados y/o presentes, que generan una determinada "sospecha" criminal sobre grupos o individuos, o generan un señalamiento de potencial víctima sobre grupos o individuos. Esto es mucho más delicado, porque lo que se está haciendo básicamente es extraer patrones conductuales, establecer perfiles o hacer perfilados, y es evidente que estamos ante una amenaza invasiva mucho más dañina de la esfera de derechos y garantías.

Por otra parte, también hay diferencias en los niveles de seguridad, acierto y eficacia de la policía predictiva en función del objetivo que se marque: serán mayores si de lo que se trata es de establecer coordenadas espacio-temporales donde es más probable que sucedan crímenes, disminuirán si lo que se quiere es referir la predicción, además, a tipos delictivos concretos (aunque también depende del tipo de delito), bajarán si lo que se quiere, es determinar grupos de riesgo como criminales o como víctima, seguirán bajando si la predicción quiere referirse a personas concretas, como criminales o como víctimas, y será casi mágico concretar la futura comisión (más o menos inminente) de un delito concreto por un criminal concreto y contra una víctima concreta en un lugar concreto.

Los sistemas de predicción de criminalidad pueden dirigirse a seis objetivos específicos: la determinación de lugares y tiempos en los que es más probable que ocurra un hecho delictivo; la determinación de qué tipos delictivos concretos son más probables que ocurran; la determinación de grupos de personas que tienen más probabilidades de cometer un delito; la determinación de personas concretas e individualizadas que tienen más probabilidad de delinquir; la determinación de grupos de personas entre las que es más probable que se localicen víctimas; la determinación de personas concretas e individualizadas que pueden ser víctimas de un delito. También se usa para predecir qué características tendrá, con más probabilidad, el autor de un hecho delictivo ya cometido. Los dos primeros reciben la denominación, respectivamente, de sistemas "place-based" (o "area-based") y sistemas "event-based", los otros cuatro se agrupan bajo sistemas "person-based"[31]. En la exposición que sigue, y

31. Esta clasificación sirve para cubrir básicamente los diversos aspectos a los que abarca la policía predictiva, pero puede ser objeto de matizaciones. Sobre ello,

siguiendo la práctica más habitual de la doctrina, los agruparé en dos, los sistemas basados en las personas y los sistemas basados en el lugar o área y en el que se suele incluir también el tipo de delito esperado. También puede decirse que no funcionan como compartimentos estancos y que pueden combinarse[32].

Una cuestión que debe ser mencionada cuando se trata del examen de instrumentos que analizan la probabilidad de hechos delictivos es que, por debajo de los análisis de datos, está la realidad de que la delincuencia está originada por seres humanos y su comportamiento como tales sirve para explicar muchos patrones de conducta. Esto se utiliza para establecer que las dinámicas delictivas tienden a ser reiterativas, de forma que los delincuentes suelen seguir rutinas, tienden a hacer el mismo trabajo de la misma manera, suele estar concentrada en determinadas áreas geográficas, suelen tener como objetivo determinados grupos de víctimas, o contra objetivos iguales o similares[33].

---

entre otros, puede verse, HUNG, T-W., YEN, C-P., "On the person-based predictive policing of AI", *Ethics and Information Technology*, volumen 23, 2021, pp. 165-176; BRAYNE, S., ROSENBLAT, A., BOYD, D., "Predictive Policing", *Data & Civil Rights: A New Era of Policing and Justice*, 10.27.2015, 11 pp., http://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf, accedido el 12 de noviembre de 2021; FERGUSON, A. G., "Predictive Policing Theory", *The Cambridge Handbook of Policing in the United States* (ed. Tamara Rice Lave & Eric J. Miller), Chapter 24, Cambridge Univ. Press, 2019, pp. 491-510; GONZÁLEZ-ÁLVAREZ, J. L., SANTOS-HERMOSO, J., CAMACHO-COLLADOS, (2020) "Policía predictiva en España. Aplicación y retos de futuro", *Behavior & Law Journal,* volumen 6, número 1, 2020, p. 27.

32. O'DONNELL, R., "Challenging Racist Predictive Policing Algorithms under the Equal Protection Clause", New York University Law Review, volumen 94, junio 2019, p. 552, pone el ejemplo del programa Palantir.

33. Véase, entre otros, WADUGE, N. D., "Machine Learning Approaches For Detect Crime Patterns", septiembre de 2017, https://www.researchgate.net/profile/Nisal-Waduge/publication/319465093_Machine_Learning_Approaches_For_Detect_Crime_Patterns/links/59ad2cf2458515d09ce167f3/Machine-Learning-Approaches-For-Detect-Crime-Patterns.pdf, 6 pp., quien añade que las encuestas indican que el 50% de los delitos son cometidos por el 10% de los delincuentes; ROSENBERG, A., "Predicting Crime: Is Stealing a Car Like Choosing a Restaurant?", *Chicago Policy Review (Online)*, Feb 3, 2014, 4 pp., quien argumenta que la mayoría de los delincuentes cometen delitos muy cerca de donde trabajan, donde viven, donde vive su novia o novio, o el punto de anclaje para su actividad; y, aludiendo a la teoría de concentración delictiva, GRAHAM FARRELL, G., PEASE, K., "Preventing repeat and near repeat crime concentrations", in N. Tilley and A. Sidebottom (Eds.), *Handbook of Crime Prevention and Community Safety*, 2nd Edition, 2017, 14 pp., señalan que algunos objetivos tienen características que los señalan como atractivos, los delincuentes aprenden que algunos objetivos o lugares son atractivos lo que aumenta las posibilidades de cometer más crímenes, mientras que la interacción de posibles delincuentes y objetivos adecuados crea lugares de alto crimen.

2. SISTEMAS "PLACE-BASED"

Se puede considerar que la predicción de comisión de hechos delictivos bajo sistemas "place-based", representa el primer nivel, o nivel menos invasivo con los derechos de las personas, de la policía predictiva. En esencia es el análisis de los datos disponibles para tratar de establecer en qué lugares y momentos es más probable que se cometa un hecho delictivo, a lo que se puede añadir, generalmente, la referencia a un tipo o tipos concretos de delitos. Por lo tanto, determinan unas concretas coordenadas espacio-temporales que permiten a la policía tomar decisiones estratégicas sobre las técnicas de prevención delictiva mediante presencia policial y sobre la posibilidad de actuación inmediata en caso de que la probabilidad se actualice y el crimen se cometa. Puede decirse que hay tres caracteres comunes a todos los sistemas "place-based", el primero, ya visto, es que se focalizan en predecir lugares, tiempos y tipos de crímenes, y los otros dos son, respectivamente, que reconocen que el riesgo criminal tiene conexión con las vulnerabilidades sociales, y que creen que la interacción criminal puede reducir las tasas de delincuencia[34].

El método más conocido es el que proporciona lo que en inglés se denominan "hotspot", zona o puntos calientes, que son una referencia geográfica que será más útil en cuanto se complete con la referencia temporal (horas o momentos en que es más probable que se cometa un crimen), más refinados si se superponen, es decir, si sumamos para una misma zona geográfica diversos momentos sucesivos (generando ya no zonas entendidas como cuadrículas, sino, círculos, anillos, líneas, cilindros, cubos, etc.)[35]. Como se ha dicho, además de los datos sobre crímenes, en

34. En extenso, sobre las diversas herramientas place-based, como PredPol, Risk Terrain Model (RTM), HunchLab, FERGUSON, A. G., "Predictive Policing Theory", *The Cambridge Handbook of Policing in the United States* (ed. Tamara Rice Lave & Eric J. Miller), Chapter 24, Cambridge Univ. Press, 2019, pp. 491-510, donde en la página 497 señala estos tres caracteres comunes.

35. La literatura es muy abundante, pudiendo citarse EFTELIOGLU, E., SHEKHAR, S., TANG, X. "Crime hotspot detection: A computational perspective", en Data Mining Trends and Applications in Criminal Science and Investigations, Omowunmi E. Isafiade, Antoine B. Bagula eds., 2016, pp. 82-111; FERGUSON, A. G., "Predictive Policing Theory", The Cambridge Handbook of Policing in the United States, *cit.*, pp. 498-499. Un "hot-spot", como se ha dicho, se representa como cuadrado, pero también bajo otras formas geométricas, AGARWAL, S., YADAV, L., & THAKUR, M.K., "Circular and Cylindrical Hotspots Detection for Spatial and Spatio-temporal Data". Twelfth International Conference on Contemporary Computing (IC3), 2019, pp. 1-5, explican la evolución y clases de "hot-spot", y distinguen entre los basados en datos espaciales, y ahí los puede haber circulares, en forma de anillo, lineales, elípticos, etc., y los basados en datos espacio-temporales, y que pueden ser esféricos, cúbicos, cilíndricos, etc., los cilíndricos, por ejemplo, son una colección superposición de hotspots circulares durante un período de tiempo.

el análisis predictivo se tienen en cuenta factores como la densidad poblacional, iluminación, condiciones económicas, entre otros.

Pero hay otros dos modelos: por un lado, el de policía orientada a los problemas (problem-oriented policing), con dos claves: tratar de comprender por qué los crímenes se dan en determinados lugares concretos y reconociendo que en ello influyen factores subyacentes sociales, económicos y ambientales a los que no se puede responder o solucionar sólo con acción policial, sino con la intervención de otros agentes públicos; por otro lado, el de Policía orientada a la comunidad (community-oriented policing), que se basa en reforzar la confianza mutua entre sociedad y policía estableciendo vínculos y relaciones comunitarias, lo que implica que en cada lugar o área la policía debe buscar ser percibida como miembro de la comunidad que ayuda a la búsqueda de soluciones antes que buscar provocar un efecto disuasorio de la delincuencia[36].

En cuanto a herramientas concretas, las más conocidas son PredPol, Risk Terrain Model (RTM que tiene en cuenta factores ambientales que generan y atraen el delito, como la existencia de centros comerciales), HunchLab[37], pero existen muchos otros entre los que se puede citar el uso de Sistemas de Información Geográfica (SIG, información cartográfica donde emplazar los datos, con referencia a las características del terreno),el sistema Multilayer Perceptron (basado en redes neuronales),o el sistema Kernel Density Estimation[38].

En la línea apuntada por la mayoría de los analistas del tema, pueden señalarse al menos cuatro elementos que merecen una discusión específica y que inciden en la mayor o menor eficacia que puedan tener estos

36. Véase FERGUSON, A. G., "Predictive Policing Theory", *The Cambridge Handbook of Policing in the United States, cit.,* pp. 499-503.

37. Un análisis de los tres, con vinculación de cada uno de ellos, por su orden de enumeración, con las técnicas de "hotspots", de policía orientada a los problemas, y de policía orientada a la comunidad, en FERGUSON, A. G., "Predictive Policing Theory", *The Cambridge Handbook of Policing in the United States, cit.,* pp. 498-503.

38. Por dar alguna referencia, sobre los SIG y su uso para prevención criminal, en una mirada histórica y evolutiva que termina con el más actual "Perfil Geográfico", fruto de la geografía, la psicología y la criminología, REYES YUNGA, D. F., "El perfil geográfico criminal una nueva propuesta para la investigación geoespacial de delitos", *Revista GEOESPACIAL,* volumen 16/2, 2019, pp. 16-32; sobre multilayer perceptron y su aplicación a la policía predictiva puede verse Araujo, A., Cacho, N., Thome, A. C., Medeiros, A., Borges, J., "A predictive policing application to support patrol planning in smart cities", *International Smart Cities Conference (ISC2),* IEEE, 2017, pp. 1-6; sobre Kernel, puede verse HART, T. C., ZANDBERGEN, P.A. "Kernel density estimation and hotspot mapping: examining the influence of interpolation method, grid cell size, and bandwidth on crime forecasting", *Policing-an International Journal of Police Strategies & Management*, volumen 37, 2014, pp. 305-323.

sistemas "place-based", que es variada y con impactos desiguales en los niveles de reducción del crimen.

El primer elemento es que la identificación de áreas y tiempos en los que resulta más probable la comisión de hechos delictivos conlleva que la policía pueda tomar decisiones estratégicas y tácticas sobre su prevención o evitación, y una forma de llevarlas a la práctica es aplicando patrones específicos de patrullajes en esas zonas y momentos concretos. Esta decisión puede contribuir, aparte de la efectividad en la reducción de la criminalidad que, como se ha dicho, es dispar, a que la delincuencia puede responder buscando otras zonas o lugares en los que cometer delitos por haber en ellos menos vigilancia policial, con lo que los delitos, no disminuyen realmente, sino que se desplazan[39].

El segundo elemento es que se produce una estigmatización de determinadas zonas geográficas identificadas como de riesgo o alto riesgo delictivo, con las negativas consecuencias que ello puede traer para esa zona y para gran parte de las personas que viven en ellas, que pueden tener más dificultades para progresar o para recibir servicios públicos o privados, porque será difícil que puedan escapar a la etiqueta de marginalidad. Esto puede redundar en que sigan viendo la delincuencia como la única alternativa que les queda y así se retroalimenta un proceso que entorpece la reducción de la criminalidad[40].

El tercer elemento es que todavía hay un número limitado de delitos que pueden ser predichos mediante estas herramientas, normalmente robos con fuerza, robos de automóviles, y con más dificultad a otros tipos de delitos y suponen IA más sofisticadas y programas predictivos más caros[41].

El cuarto elemento suele ser menos atendido, y consiste en que estos sistemas son costosos en adquisición, mantenimiento y actualización,

39. Véase, por ejemplo, MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.*, p. 8; HATTEN, D., PIZA, E. L., "When Crime Moves Where Does It Go? Analyzing the Spatial Correlates of Robbery Incidents Displaced by a Place-based Policing Intervention", *Journal of Research in Crime and Delinquency*, 2021, 45 pp.

40. BUTLER-WARKE, A. 2020. Foundational stigma: place-based stigma in the age before advanced marginality. British journal of sociology [online], 71(1), pages 140-152. KOOS, K. K., "Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlow World", *90 Chicago-Kent Law Review*, volumen 90, 2015, pp. 301-334.

41. MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.*, pp. 8-9.

no todos los departamentos policiales pueden disponer de ellos o disponer de los más avanzados, y esto influye en la calidad de los resultados obtenidos que serán dispares para áreas geográficas que pueden tener características similares, y, además, influye en la manera en que los diversos niveles policiales pueden colaborar, interconectar y operar conjuntamente[42]. Esto influye sobre todo en la calidad de los datos que se utilizan.

3. SISTEMAS "PERSON-BASED"

En estas líneas me centraré en aquellos sistemas "person-based" que se dirigen a predecir de forma individualizada y concreta qué personas van a cometer delitos con más alto grado de probabilidad[43]. Aquí existen muchos más motivos de preocupación, porque las herramientas predictivas pueden representar amenazas de alto grado para los derechos y garantías de las personas, amenaza que puede extenderse luego, en algunos casos, a las propias de un proceso penal. Por ello, lo que se diga en este epígrafe debe ser conectado con lo que se dice en la última parte de este trabajo.

Entre las cuestiones que pueden abordarse en este momento, encontramos las referidas a la generación de discriminaciones grupales o individuales, si nos referimos a la posibilidad de predecir posibles colectivos con tendencias mayores a cometer delitos o personas pertenecientes a esos colectivos en términos de raza, etnia, o cualquier otra característica específica identificadora de unos colectivos frente a otros. También están las que se refieren a tratar de predecir qué personas es más probable que cometan crímenes y de qué clase, lo que se aplica a la detección de posibles "nuevos criminales" en potencia, pero también a la extracción de patrones sobre criminales ya conocidos. Y está la posibilidad de relacionarlos con una banda, grupo u organización, o incluso determinar si éstas están planificando la comisión de delitos específicos. Y surgen, por otro lado,

42. FERGUSON, A. G., "Predictive Policing Theory", *The Cambridge Handbook of Policing in the United States*, *cit.*, p. 505.

43. Aunque es también interesante la predictibilidad referida a las víctimas, que también cuenta con varios estudios doctrinales, pudiendo citarse, entre otros AKPINAR, N-J., DE-ARTEAGA, M., CHOULDECHOVA, A., "The effect of differential victim crime reporting on predictive policing systems", *FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and TransparencyMarch,* 2021 pp. 838-849; RICHARDSON, R., SCHULTZ, J. M., CRAWFORD, K., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice", New York University Law Review Online, volumen 94, mayo, 2019, pp. 15-55.

los problemas relacionados con el perfilado criminal, debiendo cuidarse sobe todo los que se producen por tratamiento automatizado de los datos personales, y con el requisito de la sospecha criminal, que siempre había sido la base de la vinculación de una persona con un delito[44].

Se comprende que, al menos, hay dos líneas de problemas: la injerencia en derechos de las personas, en su privacidad (con todas las vías de obtención de datos que proporciona la vigilancia masiva) que permite que se vayan relacionando datos de forma que al final pueden localizarse esos "posibles nuevos delincuentes"; el análisis de datos pasados de criminalidad, complementados con los que se puedan obtener en tiempo real, y que genera un pronóstico de reincidencia delictiva. En ambos casos, siempre está presente, en atención a la herramienta predictiva usada, a los datos con que se ha alimentado y al algoritmo usado, la posibilidad de que haya falsos positivos, que suelen producirse en un porcentaje alto, y falsos negativos, que se dan con menos frecuencia[45].

Por otro lado, surgen los problemas asociados a la generación de perfilados criminales, que involucra muy directamente el análisis de datos personales, y que serán más evidentes cuando se originan por el tratamiento automatizado de estos datos. En este sentido, se ha establecido que tanto el Reglamento General de Protección de Datos de la UE, como la específica norma para el proceso penal, la Directiva UE 680/2016, no son un marco completamente seguro y cierto para la protección ante los usos de policía predictiva, y se requieren acciones más contundentes, sobre todo en relación con el tratamiento automatizado de datos personales y el perfilado criminal, dado que las garantías del artículo 11 de la Directiva, prohibición de estos tratamientos y perfilados como regla general, y

44. Entre otros, LINDENMUTH, K., "Prevention or Self-Fulfilling Prophecy? Predictive Policing's Erosion of the Presumption of Innocence", *Law School Student Scholarship*, *cit.*, pp. 14-16; STRIKWERDA, L., "Predictive policing: The risks associated with risk assessment", *The Police Journal: Theory, Practice and Principles*, volumen 94, 2021, pp. 426-431; BROWNING, M., ARRIGO, B. "Stop and Risk: Policing, Data, and the Digital Age of Discrimination", *American Journal of Criminal Justice, cit.*, pp. 302 y ss; MORGADO S.M.A., FELGUEIRAS S. (2021) Big Data in Policing: Profiling, Patterns, and Out of the Box Thinking. In: Rocha Á., Adeli H., Dzemyda G., Moreira F., Ramalho Correia A.M. (eds.) Trends and Applications in Information Systems and Technologies, WorldCIST 2021, Advances in Intelligent Systems and Computing, Springer, pp. 217-226.

45. Hablamos de herramientas de evaluación de riesgos en materia criminal, y sobre los aspectos comentados puede verse MARTÍNEZ GARAY, L., MONTES SUAY, F., "El uso de valoraciones del riesgo de violencia en Derecho Penal: algunas cautelas necesarias", InDret 2/2018, pp. 8-9; DOUGLAS, T., PUGH, J., SINGH, I., SAVULESCU, J., FAZEL, S., "Risk assessment tools in criminal justice and forensic psychiatry: The need for better data", European psychiatry: the journal of the Association of European Psychiatrists, volumen 42, 2017, pp. 134-137.

excepciones justificadas y protegidas con el derecho al control o intervención humana, pueden convertirse en meramente formales[46].

Y, desde luego, surge la inquietante cuestión de la existencia de una sospecha como elemento base para vincular a una persona con un crimen. De los muchos elementos en juego, reparemos ahora en que la policía predictiva genera sospechas de futura comisión de hechos delictivos, pero es una sospecha que se construye a medida que se analizan los datos, es decir, no hay una sospecha policial previa, ni tampoco el análisis de datos está basado en órdenes de búsqueda de ningún tipo. Simplemente el propio análisis de datos es susceptible de generar la sospecha sin ningún otro elemento. Esto puede suceder y sucede, se entiende que se debe a que la idea de sospecha siempre ha funcionado en relación con los "pequeños datos", pero la policía predictiva genera sospechas mediante el análisis de grandes cantidades de datos[47]. Cabe, desde luego, tener un debate en la línea del que se mantiene en USA sobre la extensión de la garantía de la cuarta enmienda a la policía predictiva, debate amplio y que no tiene un signo claro[48], aunque lo lógico es posicionarse con la visión que represente mayores y mejores garantías de derechos frente a lo ilegal y frente a lo legal pero opresivo[49].

La Unión Europea parece apuntar en esta última línea, al establecer dos líneas de trabajo que permiten albergar esperanzas sobre la correcta

46. Véase, en el ámbito de la UE, LYNSKEY, O., "Criminal justice profiling and EU data protection law: Precarious protection from predictive policing", *International Journal of Law in Context*, volumen 15(2), pp. 162-176. Un análisis más completo en BRILHA RIBEIRO, R. A., BENTO DE MATOS SOEIRO, C. B., "Analysing criminal profiling validity: Underlying problems and future directions", *International Journal of Law and Psychiatry*, Volume 74, 2021, artículo 101670.

47. Puede verse sobre la cuestión, que involucra cuestiones de índole constitucional en USA con la cuarta enmienda, BROWNING, M., ARRIGO, B. "Stop and Risk: Policing, Data, and the Digital Age of Discrimination", *American Journal of Criminal Justice, cit.,* pp. 307 y ss; los autores hacen una comparación entre la policía predictiva y la llamada "doctrina Terry" de "stop and frisk" que debe practicar la policía cuando sospecha que una persona está involucrada o puede estarlo de presente o de futuro, con la comisión de un hecho delictivo, y que genera problemas parecidos a los de la policía predictiva, pp. 301-302 y 305.

48. Por citar algunos artículos, KOOS, K. K., "Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlow World", *90 Chicago-Kent Law Review*, *cit.,* pp. 301-334; MILLER, K., "Total surveillance, big data, and predictive crime technology: privacy's perfect storm", *Journal Technology of Law and Policy*, *cit.,* pp. 105-146; FERGUSON, A. G., "Surveillance and the Tyrant Test", *The Georgetown Law Journal, cit.,* pp. 262 y ss.

49. FERGUSON, A. G., "Surveillance and the Tyrant Test", *The Georgetown Law Journal, cit.,* p. 264, señala que la cuarta enmienda fue una respuesta a los poderes del gobierno tiránico y también a la vigilancia gubernamental que, aunque autorizada, puede ser opresiva.

regulación de la policía predictiva y sobre el uso de herramientas que son particularmente invasivas de los derechos fundamentales de las personas.

En este sentido, en el artículo 5.1.d) de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, de 21 de abril de 2021, incide en la vigilancia policial predictiva al establecer la prohibición del uso de determinadas tecnologías, como la que posibilita el reconocimiento facial (identificación biométrica remota en tiempo real), salvo contadas excepciones. Nótese que es una prohibición, es decir, se considera que es una herramienta tan invasiva de derechos, que no debe ser utilizada en las condiciones que describe el artículo y que son, habitualmente, la de la vigilancia policial predictiva: hacer identificación biométrica de forma remota (por ejemplo, a través de CCTV), en espacios de acceso público y con finalidad de aplicación de la ley. Pero es una prohibición que tiene excepciones, para alcanzar concretos objetivos, que se establecen en tres: a) a búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos; b) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista; c) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo (con penas privativas de libertad de duración máxima de, al menos, tres años). Merece la pena hacer notar que, en el tercer caso, la identificación biométrica remota puede usarse en relación con personas "que han cometido, o se sospecha que han cometido" un hecho delictivo, estamos en la fase reactiva, no preventiva; pero en el segundo caso, se puede usar para prevenir amenazas específicas o atentados terroristas, es decir, uso preventivo (que puede tener extensión predictiva) en caso de delitos especialmente graves.

En todo caso, las tres excepciones están sujetas, apartados 2 y 3 del artículo 5, a otras condiciones: atendidas las circunstancias concretas, un juicio de ponderación entre el perjuicio que produciría no usar el sistema y el daño que produciría su uso en los derechos de las personas; la necesidad de autorización judicial previa (o autoridad pública competente) salvo casos de urgencia en los que la autorización podrá ser vía control posterior.

Por su parte, la Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales [2020/2016(INI)],

aparte de insistir en la restricción del uso de la identificación biométrica remota en las condiciones explicadas, se refiere a la policía predictiva. Comienza reconociendo que se trata de herramientas que pueden amplificar y reproducir sesgos y discriminaciones, por lo que recomienda que se estudien más en profundidad (parágrafo 22); en el momento actual, la policía predictiva puede determinar patrones y correlaciones, pero no pueden hacer predicciones fiables del comportamiento individual, por lo que se opone al uso de la IA por parte de las autoridades policiales para hacer predicciones conductuales relativas a individuos o grupos sobre la base de datos históricos y comportamientos pasados, pertenencia a un grupo, ubicación o cualquier otra característica de este tipo, para tratar así de identificar a personas que probablemente vayan a cometer un delito (parágrafo 23). Parece claro que se está refiriendo a las herramientas policiales predictivas "person-based", y que no entiende compatible con los derechos y garantías de las personas que se pueda hacer concreciones individuales para asignar probabilidades de comisión futura de hechos delictivos. Puede entenderse que no hay oposición al uso de herramientas predictivas "place-based", aunque ello no significa que estén exentas de problemas, como se ha visto. Por último, habrá que esperar a las futuras concreciones de esta oposición en relación con lo que la propuesta de Reglamento antes examinada denomina "la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista", porque cabe preguntarse si estas circunstancias también justificarían excepciones a la oposición al uso de la policía predictiva "person-based".

Veremos a continuación que muchos de los problemas de la policía predictiva, como de cualquier otra herramienta basada en IA, radica en lo que se puede llamar la ética de los datos y de los algoritmos. Hay una preocupación amplia por estos aspectos, y asistimos a la incipiente generación de códigos éticos para la acción policial basada en IA, y hay quien entiende que sería posible solventar muchos de los problemas aplicativos que genera esta amenazante predicción policial "person-based" extrapolando a ella los principales principios que se extraen de esos códigos, de forma que, al menos, se le debería aplicar tres reglas: A) debe ejecutarse en un contexto de "red de seguridad social", quiere decirse que, dado que los antecedentes penales a menudo vinculan a personas con desventajas socioeconómicas, los gobiernos deben ayudar a mejorar su bienestar social, lo que se ajusta a los principios (3) y (4). B) hay que garantizar que los seres humanos sean los máximos responsables de la toma de decisiones: la responsabilidad y la rendición de cuentas son cruciales en la aplicación de la ley, lo que también se ajusta a los principios (1) y (2). C). trato respetuoso para todas las partes implicadas para garantizar que

la vigilancia de la IA no sea abusada ni se vuelva contra (parte de) las personas, lo cual es especialmente crucial en el caso de la lucha contra el terrorismo. Esta consideración también se ajusta al principio (5). Aun así, incluso con datos correctos, pueden darse errores y falsos positivos, más si son incorrectos los datos, y por ello, la decisión humana debe estar siempre garantizada como control de la decisión de la máquina[50].

4. EN COMÚN: ÉTICA DE LOS DATOS Y DE LOS ALGORITMOS

Intentaré, a continuación, sintetizar las principales preguntas que debemos hacernos en relación con los datos y los algoritmos que están detrás de la policía predictiva, para tratar de concluir apuntando que la solución es, además de técnica y jurídica, ética. Es decir, hay que mejorar continuamente los procedimientos técnicos que afectan a la determinación de los datos y a la programación de los algoritmos (también a su funcionamiento), y hay que establecer regulaciones legales concretas en ambos ámbitos, pero todo ello debe estar revestido por el componente ético, el que nos servirá para ponderar dónde no es posible llegar, aunque pueda hacerse técnica y legislativamente.

Voy a analizar someramente, las cuestiones que recaen sobre los datos, sin ánimo de exhaustividad, porque todo lo que afecte a la correcta determinación de los datos puede contaminar el resultado de las predicciones policiales sobre la criminalidad[51]:

> a) Se dice que la policía predictiva trabaja con "big data", esto es con grandes cantidades de datos, pero es necesario aclarar que no se

50. HUNG, T-W., YEN, C-P., "On the person-based predictive policing of AI", *Ethics and Information Technology*, *cit.*, hacen un análisis de los sistemas policiales predictivos "person-based", pp. 166 y ss., y concluye que pese a las dificultades y riesgos, se necesitan principios morales y consideraciones más profundas para dar un cierto amortiguamiento del riesgo que representan, pero si se dan esa condiciones puede ser un instrumento útil en la policía comunitaria. Es en esa línea que alude a los diferentes códigos éticos que se van generando, p. 168, y los resume en cinco principios, p. 168: (1) Respeto por la autonomía, las decisiones de la IA no pueden minar la libertad y control humano; (2) transparencia y responsabilidad de las decisiones de la máquina, explicabilidad; (3) integridad y seguridad de los datos en todo su ciclo de vida; (4) gestión de riesgos o manejo adecuado de los riesgos e impactos negativos que la IA produce sobre todo en colectivos vulnerables; (5) la IA debe servir para ayudar y mejorar el desempeño humano, el humano en el centro. Los números entre paréntesis del texto se corresponden con los de cada uno de estos principios.

51. De una u otra forma, en la exposición que sigue, se reflejan las cuatro características básicas de los datos: volumen, variedad, velocidad y veracidad, que marcan la calidad y eficiencia del proceso de aprendizaje de la máquina, véase con más extensión SCHERER, M., "Artificial Intelligence and Legal Decision-Making: The Wide Open?

trata de acumular datos en gran medida, aunque estén relacionados con el objetivo que se pretende alcanzar. Debe haber una medición cuantitativa, pero sobre todo cualitativa, de los datos, huyendo de la obsesión por recopilar la mayor cantidad posible de datos sobre actividad criminal, poniendo el acento en la calidad de los datos, en su relevancia y pertinencia, así como obviar los datos no utilizables para el caso[52]. Todo esto implica una labor selectiva que requiere capacitación y cualificación y que no suele hacerse.

b) Sobre el uso de datos de criminalidad ya existentes, datos del pasado, surgen diversas cuestiones: primera, debería discriminarse entre los datos que provienen de casos resueltos y los que no[53] (por ejemplo, puede haber datos sobre frecuencia de tiroteos en una zona, pero estar siempre resueltos los casos); segunda, debería poder saberse si se usan bases de datos que están completas, es decir, que no hay supresión de datos, o que no se usan de forma incompleta[54].

c) En relación con cantidad y la calidad de los datos[55], aquí surgirán problemas que tienen que ver con lo que se denomina en general "black data" y el "dirty data". Para la cantidad y relevancia de los

---

A Study Examining International Arbitration", *Journal Of International Arbitration, cit.*, pp. 544 y ss.

52. Es algo que se predica en general en materia de IA, WENFEI, F., "Making big data small", Proceedings of the Royal Society A, 8 de mayo de 2019, https://royalsocietypublishing.org/doi/full/10.1098/rspa.2019.0034; y que aplica en el campo de la lucha contra el crimen, LEE, J., "Making Big Data Small: The Importance of Relevant Data Collection for Crime-fighting", 8 de abril de 2019, accesible en https://www.police1.com/police-products/investigation/investigative-software/articles/making-big-data-small-the-importance-of-relevant-data-collection-for-crime-fighting-oJhlz9TsRnMuH5vV/.

53. Así, BLOUNT, K., "Applying the presumption of innocence to policing with IA", International Review of Penal Law, volumen 92, Issue 1, noviembre 2021, p. 43, "as established, police records are not often updated to reflect the disposition of legal processes and this creates an inaccuracy as regards the disposition of charges. When risk assessments are used to generate suspicion and induce police action, acquitted or otherwise cleared individuals may become subject of police scrutiny based on disposed of charges. In this case, the Presumption of Innocence has been violated".

54. LINDENMUTH, K., "Prevention or Self-Fulfilling Prophecy? Predictive Policing's Erosion of the Presumption of Innocence", *Law School Student Scholarship, cit.*, pp. 18-19, señala la dificultad de disponer de datos completos por la policía, sus registros no son comprensivos de todos los crímenes cometidos, es difícil obtener datos completos y, además, es caro.

55. MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.*, p. 10-11, hablan de mejorar la calidad de los datos, su autenticidad y exactitud, eliminando los datos sucios ("dirty data"), con un primer filtro policial de los datos antes de introducirlos al programa. Sobre los "datos

datos es conveniente saber las fuentes de donde se obtienen (judiciales, policiales, administrativas, etc.) que a su vez exige determinar qué sistema de recogida tiene cada una de esas fuentes, qué sistema de clasificación emplean, y, sobre todo, qué grado de interoperabilidad hay entre ellas (por ejemplo, si en un determinado territorio confluyen distintas fuerzas policiales, nacional y autonómica, nacional y local, si las distintas bases de datos están conectadas para permitir sumar correctamente todos los datos sobre delincuencia, o si, por el contrario, están fragmentadas y desconectadas). Y también dónde y cómo están almacenadas y con qué medidas de seguridad, por ejemplo, pueden estar en un mismo servidor, en servidores diferentes, en el mismo país, en países diferentes, todo lo cual redunda en cómo pueden relacionarse unos datos con otros[56].

d) Uno de los principales problemas que afectan a los datos es el de su posible sesgo o carácter discriminatorio, porque eso determina resultados predictivos sesgados y discriminatorios a su vez. Por ello, conviene indagar en el origen de esos sesgos y discriminaciones, en el proceso de recogida y tratamiento de los datos, y saber si hay intervención humana responsable de esos defectos que, en ocasiones, puede ser voluntaria o buscada[57].

e) Los datos en tiempo real obtenidos por la vigilancia policial continuada, pueden ser datos sobre criminalidad o no, porque también se recopilan datos que cedemos voluntaria o inevitablemente (datos de geolocalización al andar por la calle, al circular con un vehículo, por ejemplo), que ya no son datos estrictos sobre delincuencia o sobre hechos criminales. Se genera un histórico de datos que se

---

oscuros" ("black data"), faltos de transparencia, FERGUSON, A. G., "Illuminating black data policing", *Ohio State Journal of Criminal Law,* volumen 15, 2018, 31 pp.

56. MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.,* p. 9, aluden a la necesidad de bases de datos policiales de alta calidad y seguridad.

57. ALIKHADEMI, K., DROBINA, E., PRIOLEAU, D., RICHARDSON, B., PURVES, D., GILBERT, J. E., "A review of predictive policing from the perspective of fairness", *Artificial Intelligence and Law*, *cit.,* pp. 6-7, se refiere a que los datos sesgados, que existen como se puede comprobar en la práctica, pueden afectar al proceso de autoaprendizaje de la máquina; LINDENMUTH, K., *op. cit.,* pp. 18-19, señala que pueden estar sesgados pero que muchas veces es un sesgo de origen humano porque son los humanos los que han recolectado y catalogado esos datos pudiendo haber incluido en ellos sesgos humanos; MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.,* abundan en esta línea p. 9.

analizan para ver si tienen relación con posibles hechos criminales o personas relacionadas con esos posibles hechos criminales. Además de ser preocupante, porque a través de los datos que se generan al realizar actividades cotidianas se produce un monitoreo tendente a extraer patrones que puede terminar sirviendo para predecir criminales o hechos delictivos (redes sociales, por ejemplo), esta la cuestión de que todo análisis implica obtención de información: ¿cómo estamos seguros de que esa información que puede finalmente ser descartada a efectos criminales no tiene otros usos o no resulta destruida? Y la misma pregunta cabe hacerse para el caso de que se descubra una posible vinculación criminal, pero ésta no se actualice, porque hay ahí una potencial criminalidad que queda difusa y que puede tener repercusión en otros momentos.

f) Y esta el espinoso tema de que, en caso de que la conducta criminal predicha no se pueda evitar, los datos ya obtenidos previamente deben tener un régimen de control y validación para su entrada en un proceso penal y para asignarles un valor siempre en atención a la vigencia del derecho de defensa efectivo. Debe poder saberse si el traspaso de datos es íntegro, transparente, o si está modulado o sesgado, porque todo eso es vital para las garantías del proceso penal.

En cuanto a los algoritmos, son dos los principales motivos de preocupación expresados por la doctrina: que al igual que los datos, pueden producir resultados discriminatorios y sesgados, y que, los produzcan o no, funcionan como cajas negras, "black boxes", en el sentido de que no pueden explicarse, o pueden argumentar los resultados y eso las hace incontrolables, también en relación con el proceso seguido. Ambas cuestiones tienen relación.

La doctrina, aunque en forma casi unánime, reconoce que los algoritmos pueden ofrecer, y de hecho ofrecen en bastantes ocasiones, predicciones policiales sesgadas hacia grupos, razas, o concretos individuos, incluso localizaciones geográficas[58], también señala que determinar el sesgo o discriminación del algoritmo no es cuestión fácil y que, en todo caso y teniendo en cuenta los diversos instrumentos para medirlos y evitarlos, se recuerda que las decisiones humanas también pueden estar sesgadas o ser discriminatorias[59]. En todo esto puede influir decisivamente

58. Con un análisis doctrinal sobre la cuestión, MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.*, pp. 9-10.

59. Sobre estos aspectos, y el análisis de los estudios doctrinales, ALIKHADEMI, K., DROBINA, E., PRIOLEAU, D., RICHARDSON, B., PURVES, D., GILBERT, J. E.,

el hecho de que el trabajo de estas herramientas es mediante tratamiento automatizado, de forma que se propone una intervención humana de control ajena a los programadores del algoritmo[60].

En todo caso, hay que diferenciar. Si se producen resultados sesgados en la predicción policial, lo normal es que eso se deba a que se han utilizado datos sesgados, tal y como se ha visto, o bien a que el algoritmo ha incorporado sesgos que pertenecen al programador, y que se deslizan en el código de funcionamiento, bien de forma intencional, bien de forma inadvertida, y ello lleva a que se cometan errores o a que se repliquen, como se acaba de decir, prejuicios y discriminaciones humanas; en definitiva, ofrece resultados no completamente fiables, pero este problema no es ajeno al trabajo humano de policías, jueces, fiscales, etc.[61].

Por otro lado, se suele establecer que los algoritmos funcionan como "cajas negras" ("black boxes"), porque no se puede saber el proceso mediante el cual, a unos determinados "inputs", en forma de datos que son analizados, le corresponde un concreto resultado, "output", predictivo, y se atribuye a la incapacidad del algoritmo para ofrecer una motivación, un razonamiento, una argumentación[62]. Que los algoritmos pueden funcionar como cajas negras en muchas ocasiones, pero no en otras, tiene que ver con muy diversos factores, el que interesa resaltar ahora es que puede deberse a nuestra limitada capacidad cognitiva que impide interpretarlo correctamente; y puede recordarse que propio cerebro humano funciona como una "caja negra" en cuanto a la decisión[63], uno de los temas que

"A review of predictive policing from the perspective of fairness", *Artificial Intelligence and Law*, *cit.*, p. 10.

60. MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences*, *cit.*, pp. 9-10.

61. HUNG, T-W., YEN, C-P., "On the person-based predictive policing of AI", *Ethics and Information Technology*, *cit.*, pp. 166 y 168.

62. Entre la abundante literatura en este sentido, puede citarse ahora, FERGUSON, A. G., "Illuminating black data policing", *Ohio State Journal of Criminal Law, cit.*, 31 pp.; JOH, E. E., "Feeding the Machine: Policing, Crime Data, & Algorithms", William & Mary Bill of Rights Journal, volumen 26, issue 2, article 3, 287 (2017), http://scholarship.law.wm.edu/wmborj/vol26/iss2/3; ULENAERS, J., "The Impact of Artificial Intelligence on the Right to a Fair Trial: Towards a Robot Judge?", *Asian Journal of Law and Economics*, volumen 11, Issue 2, 2020, pp. 16-17 y 27-28; MARROW, P. B., KAROL, M., KUYAN, S., "Artificial Intelligence and Arbitration: The Computer as an Arbitrator. Are We There Yet?", *Dispute Resolution Journal, volumen 74,* number 4, october 2020, pp. 58-59.

63. Sobre estos aspectos, HUNG, T-W., YEN, C-P., "On the person-based predictive policing of AI", *Ethics and Information Technology*, *cit.*, pp. 166-168, quiénes añaden que todo esto ocasiona problemas con la responsabilidad por las decisiones que, desde luego, todavía no recae en la máquina.

sigue siendo objeto de investigación, pero en cambio tiene la capacidad, y así se exige en Derecho Procesal, de motivar, argumentar, razonar, esa decisión y, puede decirse, así "blanquearla". El problema es más agudo en el caso de los algoritmos que auto aprenden y que pueden evolucionar hacia la obtención de resultados no esperados o fuera del rango previsto[64].

Pero, como se ha dicho, la IA, el algoritmo subyacente, no tiene todavía esa capacidad de razonar, argumentar o motivar el resultado obtenido, ya que funciona bajo técnicas de probabilidades inferidas de los datos, pero no puede, todavía, combinar procesos tales como la deducción, la inducción, abducción, ni tiene capacidad heurística, como sí tiene el cerebro humano[65]. Así, las IA, en su proceso de decisión simulada, lo que emplean son razonamientos que sólo pueden ser calificados como mecánicos, estadísticos o probabilísticos, es decir, la IA alcanza una concreta decisión de un caso porque, tras el análisis de datos y la extracción de patrones, concluye que esa decisión era la más adecuada porque era la que resultaba más probable, o más estadísticamente posible, de acuerdo con los datos y patrones. Por supuesto, esto no implica ningún razonamiento, motivación, argumentación o justificación propia, ni aceptable, en principio, para el ser humano[66].

Bien es cierto que hay una preocupación por resolver el problema de la explicabilidad y razonabilidad de las decisiones de la IA, que lleva al desarrollo de modelos llamados *Explainable Artificial Intelligence* (XIA), mediante el cual se pretende poder localizar los elementos que permiten entender la decisión de la IA, lo que no es siempre fácil porque a veces esos elementos no son realmente explicativos, no tienen valor justificativo[67]. Pero por otro lado, puede sostenerse que cabría operar de otro

64. Sobre estas cuestiones puede verse también un anterior trabajo, GUZMÁN FLUJA, V., "Arbitraje y soluciones técnicas inteligentes", *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*/Silvia Barona Vilar (ed. lit.), 2021, pp. 553-609.

65. HUNG, T-W., YEN, C-P., "On the person-based predictive policing of AI", *Ethics and Information Technology*, *cit*., p. 168.

66. SCHERER, M., "Artificial Intelligence and Legal Decision-Making: The Wide Open? A Study Examining International Arbitration", *Journal Of International Arbitration*, vol. 36, Issue 5, 2019, pp. 542-545.

67. No termina de ver que estas iniciativas vayan a tener éxito SOLAR CAYÓN, J., I., "La codificación predictiva: inteligencia artificial en la averiguación procesal de los hechos relevantes", *Anuario Facultad de Derecho, Universidad de Alcalá*, volumen XI, 2018, p. 14. En concreto, concluye que "La complejidad que dimana de la argumentación jurídica e las decisiones judiciales resulta evidente, y no debe soslayarse que se han propuesto diferentes sistemas de IA tendentes a realizar esta labor (QUESTAMP, ARGUMED o CATO). Sin embargo, son a todas luces insuficientes, mecanizando imprudentemente semejante proceso, que constituye además uno de los aspectos cruciales dentro del capítulo de motivación de la sentencia".

modo, sin descartar el anterior, y es reconociendo que en muchos casos no es posible saber cómo y bajo qué argumentos, ha decidido el algoritmo, por más esfuerzos que se hagan, y entonces lo que se debe hacer es determinar si el resultado ofrecido es consistente con los datos utilizados y si es aceptable o no, en comparación a los estándares de aceptabilidad fijados para el humano, aunque esto no obvia todos los problemas (por ejemplo, no habría razones o argumentos a los asirse en caso de querer recurrir el resultado).

La preocupación doctrinal lleva a establecer la necesidad de superar estos problemas, en cuanto se considera que la policía predictiva tiene utilidad, pero sólo es ética y jurídicamente admisible si se eliminan, y para ello una constante es la reclamación de una mayor transparencia, fiabilidad, control, exactitud y responsabilidad en cuanto al uso de datos y algoritmos, siendo recurrente el tema de la certificación de calidad, mediante evaluación por agencias o personas independientes, necesitándose la elaboración de indicadores adecuados[68], así como la debida capacitación y acreditación de estas agencias o personas[69].

Uno de los principales obstáculos que se presentan es el referido a la consideración de los algoritmos como propiedad intelectual y por lo tanto la resistencia de las empresas propietarias y programadores a desvelar los códigos correspondientes, teniendo en cuenta que la gran mayoría de desarrollos de herramientas de policía predictiva están hechos por empresas privadas[70]. Hay un fuerte debate sobre esta cuestión, porque, en definitiva, esta opacidad del algoritmo afecta al ejercicio del derecho de defensa si se llega al proceso penal, y al ejercicio del derecho a conocer las razones de la decisión de la autoridad en los demás casos. Por eso, se propone encontrar las vías que permitan armonizar ambas necesidades de protección, partiendo del hecho de que, aunque los desarrolladores privados siempre pueden invocar el derecho de propiedad intelectual (o también el "trade secret"); por un lado, son contratados en muchas

68. ALIKHADEMI, K., DROBINA, E., PRIOLEAU, D., RICHARDSON, B., PURVES, D., GILBERT, J. E., "A review of predictive policing from the perspective of fairness", *Artificial Intelligence and Law*, *cit.*, p. 10-11.

69. Con toda la doctrina que citan en este sentido, véase ALIKHADEMI, K., DROBINA, E., PRIOLEAU, D., RICHARDSON, B., PURVES, D., GILBERT, J. E., "A review of predictive policing from the perspective of fairness", *Artificial Intelligence and Law*, *cit.*, p. 8-9; MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.*, pp. 10-11.

70. Por todos, MUGARI, I., OBIOHA, E. E., "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", *Social Sciences, cit.*, pp. 10 y ss.

ocasiones por autoridades públicas, y por ello deben estar sometidos a un deber de revelación en lo que sea necesario, y, por otro, se afectan derechos fundamentales de las personas y debe posibilitarse que éstos se puedan ejercer debidamente, lo que será imposible sin esa revelación total o al menos en lo imprescindible para ese ejercicio debido[71]. Alguna solución concreta se propone, como la introducción en el sistema de justicia criminal de USA de la llamada "missing algorithm instruction" (trasunto de la "missing witness" evindentiary rule), sobre todo en la fase de juicio oral, pero también en la fase de investigación, porque siendo fuente de investigación y/o fuente de prueba, tiene un tratamiento diferente al que tiene el humano que también lo es: el humano es confrontado adversarialmente pero el algoritmo, sobre la base del "trade secret", no, y esto debe corregirse[72].

En definitiva, sobre la base de las ideas anteriores, se proponen tres técnicas para mejorar la policía predictiva, que serían: a) el necesario preprocesamiento de los datos, es decir, tratar los datos brutos para

71. Entre otros muchos, CARLSON, A. M., "The Need for Transparency in the Age of Predictive Sentencing Algorithms", Iowa Law Review, volumen 103, 2017, pp. 303-329; MICHAEL BRENNER, M., GERSEN, J. S., MICHAEL HALEY, M., LIN, M., MERCHANT, A., JAGDISHWAR MILLETT, R., SARKAR, S. K., WEGNER D., "Constitutional Dimensions of Predictive Algorithms in Criminal Justice", *Harvard Civil Rights-Civil Liberties Law Review*, volumen 55, 2020, pp. 267-310; TSCHIDER, C. A., "Beyond the "Black Box" 98 Denver Law Review, volumen 98, 2021, pp. 683-723.

72. Véase WON, D., "The Missing Algorithm: Safeguarding Brady Against the Rise of Trade Secrecy in Policing", Michigan Law Review, volumen 120, 2021, pp. 157-193, en las que señala que produce perplejidad esta alta protección del algoritmo porque la protección que el derecho al proceso justo proporciona al acusado no debería cambiar sólo porque la naturaleza de la fuente de investigación es digital y no humana. Señala que esto choca con la doctrina Brady, establecida por la Sentencia de la Corte Suprema de USA en Brady v. Maryland 373 U.S. 83 (1963), conforme a la cual la Fiscalía, en el marco de la vigencia de un proceso justo bajo la cláusula del debido proceso, debe revelar cualquier información favorable al acusado que obre en su poder si tiene relevancia material para el caso del acusado. Es un deber de la Fiscalía que alcanza también a la búsqueda activa de la información que obre en el equipo de dicha fiscalía. Sostiene y justifica en su artículo, es que el algoritmo debe tener el mismo trato que el humano cuando es fuente de investigación o fuente de prueba contra el acusado, por efecto del derecho al proceso justo. Por ello, cuando se invoque el secreto comercial del algoritmo, propone que, en el juicio oral, se establezca una cláusula llamada "missing algorithm instruction", una regla que permitiría a los jurados hacer inferencias razonables y limitadas para salvaguardar los derechos al debido proceso de los acusados cuando su acceso está limitado por las protecciones de propiedad intelectual. Sería un remedio que permitiría salvaguardar el proceso justo sin violar el secreto comercial y son necesitar soluciones extraordinarias como excluir la prueba algorítmica. Se trata de que el jurado infiera las consecuencias que entienda lógicas y razonables de la no revelación del algoritmo por la Fiscalía, sobre todo cuando hay sospechas de funcionamiento erróneo o discriminatorio.

convertirlos en utilizables a efectos de la policía predictiva, previniendo los sesgos y discriminaciones que puedan ocultar, y debe ser realizado por expertos; b) la necesidad de establecer métodos materiales efectivos en el diseño de los algoritmos para evitar sesgos y discriminaciones y, además, establecer sistemas de detección y eliminación de posibles sesgos o discriminaciones en el funcionamiento de los algoritmos; c) hacer un post-procesamiento de los resultados para garantizar que son justos, siendo un ejemplo el trabajo de Lohia *et alii*, según el cual "los resultados se dividen en dos grupos: privilegiados y no privilegiados. Todas las muestras del grupo no privilegiado se analizan en busca de sesgo individual según un método que los autores desarrollaron en un artículo anterior; si obtienen una puntuación alta, se les asigna el resultado que habrían recibido si formaran parte del grupo privilegiado. Todas las demás muestras se dejan sin cambios. Los autores encontraron que su método reducía constantemente el sesgo y el impacto dispar mientras mantenía la precisión, pero es un algoritmo simple que solo parece funcionar para categorías binarias"[73].

V. DERECHOS Y GARANTÍAS PROCESALES PENALES. EN ESPECIAL, LA PRESUNCIÓN DE INOCENCIA

Se acaba de exponer que la ética es un elemento imprescindible para la evaluación del impacto de la inteligencia artificial en cualquier sector de la actividad humana y, en nuestro caso, en el terreno de las decisiones judiciales penales. Se ha podido comprobar que es un tema con muchas ramificaciones porque lo que podríamos denominar "constante ética" forma parte de las ecuaciones referidas a los datos, a los algoritmos, a los programadores, a los decisores, a los legisladores, etc., y sin tener en cuenta los aspectos éticos, la solución a esas ecuaciones no podrá ser nunca correcta. La ética funciona tanto como conjunto de principios que inspiran la regulación de una tarea, cuanto como conjunto de principios que determinan la actuación de las personas que las realizan, señalando las valores que integran el estándar de aceptabilidad.

En el terreno del Derecho debemos acudir a la ética jurídica, entendiendo ahora que se trata de ver los valores que integran los estándares de aceptabilidad de las normas procesales. En este sentido, una primera

73. ALIKHADEMI, K., DROBINA, E., PRIOLEAU, D., RICHARDSON, B., PURVES, D., GILBERT, J. E., "A review of predictive policing from the perspective of fairness", *Artificial Intelligence and Law*, *cit.*, pp. 9-10. El trabajo citado en cuestión es LOHIA, P. K., RAMAMURTHY K. N., BHIDE, M., SAHA, D., VARSHNEY K. R., PURI, R., "Bias mitigation post-process-ness", In: ICASSP 2019-2019 IEEE International Conference on Acoustics, Nal Processing (ICASSP), IEEE, 2019, pp. 2847-2851.

premisa ética que tener en cuenta, desde la perspectiva jurídica, es la referida a la obligación de respetar las bases esenciales del Derecho Procesal, del proceso y, en nuestro caso concreto, del proceso penal, como irrenunciables varas de medir, apreciar y, en su caso, validar, los impactos de la IA en la predictibilidad de las decisiones judiciales penales.

El derecho procesal, el proceso, por supuesto el proceso penal, sólo tienen razón de ser en cuanto se integran por un conjunto de principios y garantías sustanciales e identificadores cuyo menoscabo, desconocimiento, desnaturalización, vulneración o ausencia determinan la imposibilidad de reconocer no ya el resultado o solución del conflicto sino la existencia del propio método procesal (es bien sabido que el proceso judicial se integra por dos principios estructurales: igualdad de armas y contradicción). Por supuesto, no se trata de mantener una posición inmovilista, desmentida por la propia evolución histórica de los derechos y garantías inherentes al proceso judicial, o tan absoluta que pueda hacer inoperante o inocuo el impacto del uso de la IA en el campo del derecho procesal, que, por otro lado, lo que no puede ser es inicuo. Dicho uso, recuérdese que se trata de herramientas, de medios, no de fines en sí mismos, debe propiciar un proceso de adecuación y evolución mutua con el objetivo de llevar, en todo caso, a que el proceso judicial sea un método de solución de conflictos cada vez mejor, más eficiente, que avance en la justicia de las decisiones y que siga basado irrenunciablemente en la igualdad y la contradicción como bases del método y de la solución. La relación del derecho procesal y del proceso judicial con la IA seguramente nos enfrentará a un nuevo entendimiento de la disciplina y el método, lo que no puede resolverse en una rebaja, mucho menos en una renuncia, de los principios, derechos y garantías que son la esencia. También con seguridad, las cuestiones a las que nos enfrentemos tendrán más posibilidades de ser resueltas con éxito si el enfoque y el trabajo se hace de forma interdisciplinar (juristas, técnicos, administradores de tribunales, ingenieros informáticos, también políticos) y desde diferentes perspectivas[74].

74. Si nos centramos en el proceso penal, enseguida aparece que éste no es sino un elemento del más complejo Sistema de Justicia Criminal. La inteligencia artificial afecta no sólo a cada uno de sus elementos (proceso penal, criminalística, criminología, derecho penal, sociología, psicología, etc.,) sino al sistema en su conjunto. La Universidad de Harvard, a través del Berkman Klein Center for Internet & Society, y el Massachusetts Institute of Technology, a través del MIT Media Lab han generado un proyecto denominado "AI: Algorithms and Justice" (https://cyber.harvard.edu/projects/ai-algorithms-and-justice), uno de cuyos puntos de partida es la propia complejidad del Sistema de Justicia Criminal desde la prevención hasta la sanción y su cumplimiento, incluyendo el propio estudio de qué causa la conducta criminal; la utilización de herramientas tecnológicas en cada uno de los diferentes componentes del sistema hace surgir preguntas esenciales que demandan, para su respuesta,

No es fácil trabajar de forma que haya un provecho mutuo como resultado de esta interacción, y no lo es por la sencilla razón de que resultará difícil compaginar evolución con intangibilidad de la esencia garantista del derecho procesal, del proceso judicial y, en concreto, del proceso penal. Se ha planteado el interrogante, según la autora "bastante provocativo", de si estamos ante un momento en el que decidir si resulta deseable reformular los derechos humanos o, por el contrario, regular mejor el uso de la tecnología[75]. Entiendo que lo segundo es ineludible, y esa mejor regulación significa no anteponer eficacia o eficiencia a derechos, para así minimizar los efectos negativos que pueden sufrir individuos concretos, y que lo primero seguramente sucederá, si no está sucediendo ya, pero sólo dentro de unos límites aceptables (exigiendo que se atienda al papel que el consentimiento puede jugar en la redefinición de algunos derechos humanos en el entendido de que, por mucha renuncia voluntaria que pueda haber a determinados ámbitos de privacidad, eso no puede desdibujar el contenido esencial del derecho, desde luego no en su conceptuación como categoría general).

Así, los llamados principios estructurales del proceso, los principios de igualdad y de contradicción, deben mantener su significado pleno y configurarse como reglas obligatorias a seguir en la programación de las IA aplicables al proceso judicial, y deben ser respetados en los resultados que se obtengan de esa aplicación. Por otro lado, los derechos fundamentales a la tutela judicial efectiva (con el derecho de acceso a los tribunales de justicia) y al debido proceso no pueden verse menoscabados o desnaturalizados como consecuencia del uso de las inteligencias artificiales. En este sentido, y ocupándonos en concreto del proceso penal, el derecho

múltiples enfoques: "As its name suggests, the criminal justice system is not a unified construct but a series of interconnected processes, with multiple entry points and stages of evaluation. Technology may help to balance among goals of deterrence, incapacitation, rehabilitation, restitution, and retribution, shedding light on what causes criminal behavior and appropriate responses thereto. Each stage in the development, procurement, deployment, and assessment of each technological tool raises distinct and essential questions that demand a multiplicity of approaches".

75. GALETTA, A, "The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?" *European Journal of Law and Technology*, Vol. 4, No. 2, 2013, http://ejlt.org/article/view/221/377. La respuesta de GALETTA apunta a que ambas partes de la ecuación deben cambiar, así los derechos humanos deben ser redefinidos, en este caso el derecho a la presunción de inocencia debe alcanzar también a la fase de la investigación criminal y al estado de sospechoso (no sólo al juicio oral donde ya se tiene el status de acusado), además de que debería tener también un alcance moral y no sólo legal, mientras que las tecnologías deben regularse más estrictamente cuando afectan a derechos humanos. Nótese que un análisis desde la perspectiva del *common law*, en el *civil law*, generalmente, se considera que la presunción de inocencia rige a lo largo de todo el proceso penal.

fundamental a la presunción de inocencia no puede verse comprometido en ningún caso, lo mismo que el derecho de defensa que asiste a la parte pasiva del proceso penal. La irrupción de la IA en el proceso penal no puede derivar en posiciones de ventaja para la parte acusadora o en privación o limitación de derecho a la contradicción por parte del acusado haciendo inefectiva su defensa ante la acusación. Ya hemos visto, al hablar de los datos y los algoritmos que con su inadecuado manejo se corre el riesgo de subvertir las garantías y derechos que conforman la esencia del proceso judicial.

Se puede ver cómo el análisis de datos, el uso de algoritmos, de programas robóticos, de sistemas expertos legales, de inteligencia artificial, afecta ya a distintos elementos del proceso penal (aunque en muchos casos pueden extrapolarse al proceso judicial en general), muchas veces de forma inadvertida, y cómo, aunque pudiera parecer que no suponen más que avances que no encierran ningún peligro, al profundizar un poco vemos que se ponen en riesgo gravemente, cuando no se vulneran, principios, derechos y garantías conformadores del derecho procesal, en especial del proceso penal.

Tratándose del proceso penal, es obligada una referencia al derecho fundamental al proceso debido, con los variados derechos y garantías que lo integran que no pueden verse desnaturalizados por su relación con la IA. En general, puede afirmarse que la tecnología tiene capacidad para cambiar y alterar el contenido y el funcionamiento del derecho al debido proceso, derecho consolidado a través de siglos, de ahí el debate necesario sobre cómo y hasta qué punto es admisible o debe resolverse ese cambio que puede conducir a una auténtica crisis existencial del sistema judicial y del proceso penal[76]. De esta forma, la configuración de los acontecimientos y la conjunción de diversos actores en el cambio tecnológico son elementos de tensión para los derechos y garantías procesales: el proyecto "AI: Algorithms and Justice" identifica al menos tres grupos de intereses que están en conflicto, el de los intereses comerciales de quienes construyen y venden tecnología, el de los intereses de gestión de costes del sistema de justicia, tanto en funcionarios como en adquisición de herramientas tecnológicas, y el de los intereses de los ciudadanos que buscan preservar las normas y valores en torno a la equidad, la justicia y la responsabilidad[77].

76. Aunque estas afirmaciones pueden considerarse como una conclusión diáfana a la que puede llegar cualquier persona con capacidad reflexiva, sigo en este punto el discurso plasmado en el proyecto "AI: Algorithms and Justice", porque me parece que resume bastante bien tanto la dialéctica co o sus posibles consecuencias y me remito a la nota siguiente para la cita textual.

77. El proyecto "AI: Algorithms and Justice", https://cyber.harvard.edu/projects/ai-algorithms-and-justice, ya citado, de la Universidad de Harvard, a tavés del Berkman

En mi opinión, teniendo en cuenta que los intereses comerciales citados se residencian en el sector privado, y sabiendo que la gestión de los costes del sistema de justicia tiende a estar cada vez más condicionada por la obtención de resultados ligados a la eficacia y a la eficiencia por encima de otros valores, el grupo de interés al que debe atenderse primordialmente para resolver este conflicto es el de los intereses de las personas, de los ciudadanos, cuyos derechos procesales (también los materiales) deben ser preservados en cuanto garantes de esa equidad, justicia y uso responsable de los recursos. Pero, debe advertirse también, la amenaza de una afectación esencial a estos principios y derechos es, cada vez, menos fantasma, y lo es mediante la invocación de la anteposición del valor justicia a la pervivencia de una noción clásica de los mismos; se entiende que mantener una concepción clásica del derecho a un proceso debido o a un proceso justo ("fair trial") no es una opción cuando hacerlo implica renunciar a incorporar las nuevas tecnologías que prometen el logro de un sistema judicial con resultados más justos al tener la capacidad de incrementar la "objetividad" de las decisiones judiciales[78].

Klein Center for Internet & Society, y el Massachusetts Institute of Technology, a través del MIT Media Lab, al entrar en los aspectos de la afectación del derecho al debido proceso ("due process") afirma: "Use of technology in the criminal justice system has the potential to upend centuries-old conceptions of due process and force debates about adapting norms to suit the digital age. The outcome of those debates will hinge on whether new challenges are analogous to past ones (from which we can learn), or whether they represent an existential crisis for the judicial system (demanding a reimagining of criminal liability and punishment)". Y continúa diciendo: "Undeniable tensions exist among commercial interests of those that build and sell technology; cost-management interests of government officers that procure tech tools; and societal interests of citizens seeking to preserve norms and values around fairness, justice, and accountability".

78. Todo ello en el marco de una reflexión sobre los modelos de decisión y argumentación judicial, especialmente en el terreno penal, y de los beneficiosos aportes que le pueden implicar los sistemas expertos legales. Básicamente, lo que se sostiene es que la IA, los sistemas expertos legales aplicados al proceso judicial, en combinación con los avances tecnológicos, permiten, cada vez en mayor medida, reducir las incertidumbres, la discrecionalidad, las dudas, sobre la fijación de los elementos fácticos del proceso y, por ello, también las que puede tener el juez a la hora de decidir. Siendo así, sería posible mejorar el resultado del valor justicia de la decisión judicial y a ello no debe oponerse la vigencia de los principios del derecho al proceso justo, más bien éstos deben modificarse y adaptarse al nuevo escenario. En esta línea, CHANDA, J., "A Scientific Judicial Perspective can solve many hurdles of practical application of AI 'expert system' for judicial decision making", *Nirma University Law Journal, Volume– 8*, Issue 2, July 2019, http://dspace.jgu.edu.in:8080/xmlui/bitstream/handle/10739/2375/A%20Scientific%20Judicial%20Perspective.pdf?sequence=3&isAllowed=y, critica decisiones de la Corte Suprema de la India que anteponen el proceso debido y la privacidad sobre el empleo de los avances científicos, apuesta por revisar garantías como la del derecho a la no auto-incriminación, y afirma sin vacilar ""The principle of fair trial, public hearing, natural justice, though passed through

En realidad, estamos ante un reto apasionante, el de determinar hasta qué punto es posible acompasar la irrupción de la IA en el proceso penal con la vigencia de los principios del proceso debido. No cabe ser apriorísticos en este tema, lo que corresponde es entender que este encuentro generará beneficios a la vez que implicará graves riesgos para las garantías procesales, así como una renovación de su entendimiento en algunos casos. Sólo desde la investigación rigurosa será posible retener los primeros, erradicar los segundos y dimensionar adecuadamente los terceros, una tarea que no será sencilla y que exigirá un trabajo continuo ante el avance de la llamada "justicia automática" o "justicia automatizada"[79].

Dicho lo anterior[80], entiendo necesario el análisis de la relación entre la policía predictiva y la presunción de inocencia. La idea básica es que

---

the acid test of time, may not fit in a world ruled by AI because the principle of fair trial is a cultural export and not universal by nature.41 In the context of our algorithmic future, the need for some of these rules to uphold justice is questionable".

79. Sobre este emergente fenómeno, así como el reto que supone, baste citar ahora el interesante artículo de MARKS, A., BOWLING, B., KEENAN, C., "Automatic justice? Technology, Crime and Social Control", R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology, OUP, Forthcoming Queen Mary School of Law Legal Studies Research Paper No. 211/2015, available on SSRN: https://ssrn.com/abstract=2676154, en cuya página 17 se dice "the challenge is how to ensure that 'automatic justice' retains the characteristics of 'justice' and is in accordance with fair trial rights". Como expongo en el texto, esta retención de las características no se entenderá sin asumir cambios dentro de los límites admisibles.

80. En un plano diferente, pero que guarda una razonable relación con el protagonismo del derecho al proceso debido, merece la pena resaltar que la garantías inherentes a dicho derecho, tal y como han sido configuradas históricamente, pueden ser usadas para reforzar la protección de la privacidad ante el auge de los análisis predictivos del comportamiento de una persona, no sólo de su predecible acción criminal sino también de su predecible comportamiento social, como consumidor, o en cualquier otra faceta de su vida. El uso por parte de empresas privadas (también por el sector público) del "big data" para crear perfiles personales, muchas veces generados únicamente de forma automática, pone en alto riesgo la privacidad de tales personas, situación ante la que hay quien propone que la aproximación más eficaz para la solución del problema es utilizar las garantías del debido proceso (en este caso en su formulación de la tradición del sistema legal angloamericano) y proyectarlas a modo de escudo que otorga protección a las personas afectadas contra el perfilado derivado del uso del "big data". En este sentido véase CRAWFORD, K., SCHULTZ, J., "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", Boston College Law Review, 55, 2014, pp. 93-128, http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4 donde se afirma "By examining due process's role in the Anglo-American legal system and building on previous scholarship about due process for public administrative computer systems, this Article argues that individuals affected by Big Data should have similar rights to those in the legal system with respect to how their personal data is used in such adjudications. Using these principles, this Article analogizes a system of regulation that would provide such rights against private Big Data actors".

la aplicación de las técnicas de IA, así como de otras disciplinas distintas pero que combinan con ella, en el marco de la investigación y enjuiciamiento del hecho criminal está contribuyendo a difuminar la vigencia del derecho a la presunción de inocencia, así como a abrir debates sobre cómo evitar esta situación y cómo fortalecer dicho derecho fundamental.

A mi entender, la policía predictiva ha abierto dos líneas de impacto que pueden causar alteraciones indebidas en el fundamental derecho a la presunción de inocencia:

> a) de un lado, las técnicas de policía predictiva, con sus vertientes proactiva y preventiva, nos sitúa en un momento pre-procesal pero que en muchas ocasiones será la semilla de un proceso penal. Aquí surge el debate sobre el alcance de la presunción de inocencia: sabemos que se trata de un derecho fundamental que protege al acusado y que despliega toda su eficacia en el juicio oral, en la prueba y en la sentencia, y que también debe estar presente en la fase de instrucción, porque el investigado también debe ser considerado inocente hasta que no se pruebe lo contrario, lo que no impide que se pueden decretar medidas cautelares personales y medidas restrictivas de derechos en la investigación del delito; desde una perspectiva amplia del derecho a la presunción de inocencia se ha establecido que su alcance no es estrictamente legal, también social, incluso ético o moral, de forma que vincula a cualquier autoridad pública, por tanto no sólo a jueces y magistrados, también autoridades del gobierno o administración, y a la propia policía en cuanto investigadora material de los delitos[81]. Nótese que, por más amplitud que se quiera dar, la presunción de inocencia se considera dentro de un

81. La presunción de inocencia es una regla probatoria, una regla de juicio y una regla de tratamiento, en ambos casos representa uno de los valores que deben salvaguardarse al máximo, véase, entre otros, DE HOYOS SANCHO, M., "La presunción de inocencia en el Anteproyecto de Ley de Enjuiciamiento Criminal de noviembre de 2020" *Revista de derecho y proceso penal*, n.° 63, 2021, pp. 153-186. Por ello, resulta reconocido como derecho fundamental en los textos internacionales de Derechos Humanos, en las Constituciones nacionales, y en el plano supranacional, siendo ejemplo el caso de la Directiva (UE) 2016/343 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por la que se refuerzan en el proceso penal determinados aspectos de la presunción de inocencia y el derecho a estar presente en el juicio (que no es el único texto de la UE en la que se muestra la preocupación y necesidad de la protección de la presunción de inocencia). Una exposición detallada de todos estos aspectos, incluyendo la jurisprudencia del TEDH, puede verse en MARTÍN DIZ, F., "Presunción de inocencia en procesos penales por violencia de género", *Ius et Praxis*, vol. 24, núm. 3, 2018, pp. 19-66; también en GALETTA, A, "The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?", *European Journal…, cit.*, pp. 5-7.

proceso penal iniciado y en curso, con sus diversos matices, pero lo que aquí se plantea es algo diferente: siendo la actividad predictiva policial anterior a la incoación de proceso penal alguno ¿es posible ampliar la esfera protectora de la presunción de inocencia fuera del estricto proceso penal sin desvirtuar su propio contenido esencial? La pregunta se formula desde la perspectiva de que los datos acopiados no ingresan finalmente en proceso penal alguno.

b) de otro lado, se ha dicho reiteradamente, gracias a la vigilancia policial predictiva, a la policía predictiva, se recaban una serie de datos que, en algunos supuestos, tendrán vocación de ingresar al proceso penal que pueda incoarse al actualizarse la predicción de comisión del crimen. Aquí nos enfrentamos al problema del efectivo ejercicio del derecho de defensa (como elemento llamado a desvirtuar la acusación y preservar la presunción de inocencia), sobre datos obtenidos pre-procesalmente pero que se incorporan al proceso penal, que serán fuente de investigación y que podrán terminar siendo fuente de prueba en el juicio oral; se habla de la espinosa tarea de cómo incorporar toda esa información, adquirida sin "notitia criminis", a un proceso penal que se abre por actualización de esa vigilancia preventiva. Recuérdese que la policía predictiva puede recoger datos sin que ni siquiera estemos ante una sospecha concreta de futura comisión de un hecho delictivo, simplemente como parte de una tarea de vigilancia genérica preventiva.

Visto lo anterior, trataré algunas de las principales vertientes de interferencia entre presunción de inocencia y policía predictiva. Aunque adelanto mi parecer: en primer lugar, parece lógico entenderlo así, las interferencias surgen en relación con la policía predictiva "person-based", es decir cuando la predicción de probable futura comisión de un crimen se dirige sobre una persona concreta; en segundo lugar, debe recordarse que la Directiva UE 680/2016, sobre tratamiento de datos personales en el proceso penal, admite que puedan ser tratados en términos de prevención del hechos delictivo y que puede afectar a personas que han cometido o que van a cometer una infracción penal, siempre que haya motivos fundados para ello, por ello la policía predictiva tiene una importante vertiente de análisis desde la perspectiva de la protección de datos; en tercer lugar, aunque son loables los esfuerzos para fortalecer la vigencia de la presunción de inocencia y ampliar su efecto protector, con las limitaciones que se quiera, a todo el proceso penal, no creo que la cuestión esté en extender la vigencia de la presunción de inocencia a la policía predictiva, algo que podría desnaturalizar la esencia de este derecho, sino más bien debemos preocuparnos de cómo tratar las informaciones recogidas en relación a un

posible sospechoso de cometer un posible crimen, cuando esas informaciones tengan acceso a un proceso penal dirigido contra ese sospechoso, y como esas informaciones deben ser tratadas desde la vigencia de la presunción de inocencia. No se olvide que no estamos en el terreno del proceso penal, aunque podamos llegar a él, sino en el terreno de la prevención, de la previsión de probabilidad de comisión de crímenes para evitarlos, para disuadir de su perpetración, y esto es más policía de seguridad ciudadana o pública, y la afectación de derechos debe enfocarse con otra perspectiva. Claro está que, si finalmente se comete el crimen, se estará en mejores condiciones de investigarlo y resolverlo, y como esto debe hacerse en el marco del proceso penal, ahí es cuando habrá que evaluar cómo encajan esas mejores condiciones obtenidas vía policía predictiva con los derechos y garantías del proceso penal y con la presunción de inocencia. Esto dicho sin perjuicio de algunos matices que se dirán a continuación.

Lo cierto es que estamos ante una cuestión compleja, que tiene muchas aristas, algunas de ellas surgidas del diferente funcionamiento de la presunción de inocencia en *"civil law"* y en *"common law"*, y de la "miríada de concepciones y matices que se atribuyen a este derecho"[82]. Pero una primera conclusión que se puede establecer es que se puede asistir a una modificación del funcionamiento del proceso penal, y de las etapas anteriores, en la que se puede ir pasando de sospechoso a investigado, imputado, acusado y condenado, dando lugar a una confusión entre todos estos estados, limitando las posibilidades de defensa, y deteriorando la presunción de inocencia, no sólo para el caso concreto, sino como categoría garantista.

En cuanto a la afectación que puede sufrir la presunción de inocencia una vez que la información recopilada bajo técnicas de policía predictiva termina ingresando a un proceso penal concreto, referido a una persona concreta, por comisión del delito objeto de predicción, tendrá una diferente dimensión según estemos en la fase de investigación, en la fase de juicio oral o en la determinación de las medidas cautelares personales aplicables, y habrá que ver caso por caso la gravedad de esa afectación[83]. Lo primero que habría que hacer sería salvar la legalidad de la incorporación de dicha información al proceso, porque normalmente ha sido

82. BLOUNT, K., "Applying the presumption of innocence to policing with IA", *International Review of Penal Law, cit.*, pp. 33-48, en concfeto, 35-40.

83. Que podrá darse, además, por problemas inherentes a los datos o inherentes al algoritmo, puede verse, SCHUMANN BARRAGÁN, G., "La inteligencia artificial aplicada al proceso penal desde la perspectiva de la UE" en Pereira Puigvert, S., Ordóñez Ponz, F. (dirs.), Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos, Aranzadi, Cizur Menor, 2021, pp. 517-539.

obtenida sin estar referenciada a un delito ya cometido y esto significa que no se han aplicado las reglas que rigen en la fase de investigación del proceso penal, que están pensadas para investigar delitos ya cometidos, es decir, funcionan en el ámbito reactivo y no preventivo o predictivo. Esa información, atinente al crimen cometido, pero obtenida en gran parte antes de su comisión, debería ser filtrada conforme a los parámetros de la contradicción y del control judicial posterior, y si las supera, entonces podrían incorporarse al proceso penal y, en su momento, llegar a ser fuentes de prueba. Pero ese es sólo el aspecto inicial de la cuestión porque, incluso así, se enfrenta una segunda amenaza a la presunción de inocencia: la que consiste en ver si realmente el acusado está en condiciones reales de ejercer un derecho de defensa efectivo frente a esas fuentes de prueba originadas en la información obtenida en la labor de vigilancia, prevención o predicción, y, en este sentido, hay quien habla, incluso, de una inversión de la carga de la prueba que pasa del acusador al acusado quien tendría que la tarea de contradecir y vencer todas esas pruebas[84] recopiladas en origen de espaldas completas a su conocimiento y sin haber sido informado de la sospecha que recaía sobre él (recuérdese que es una sospecha de posible o probable comisión del hecho delictivo. Esto mismo es aplicable ya durante la fase de instrucción, ya que el investigado se podrá encontrar con que la investigación ya está realizada en un gran porcentaje, y le va a ser muy difícil poder defenderse de forma adecuada. Todo esto, erosiona, en diverso grado, la presunción de inocencia[85], y se empieza a correr el riesgo de que el sistema acepte errores que afectan a su esencia considerándolos como simples errores de coste operacional, que funcionaría como una especie de impuesto sobre los individuos inocentes[86].

A la actividad policial de vigilancia-predicción, que todavía no supone la existencia de un proceso penal, no le son aplicables las garantías del derecho fundamental al proceso justo, pero desde el momento en que las informaciones recogidas puede derivar en la incoación de un proceso penal con una fase de investigación en la que esas informaciones pueden determinar la incriminación de una persona concreta, y una fase de juicio

84. GALETTA, A, "The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?" *European Journal…, cit.,* p. 4.

85. AMBER, M., BOWLING, B., KEENAN, C., "Automatic Justice? Technology, Crime and Social Control", 2015, pp. 24-25. Previamente, en la pp. 18-19, señalan que la ubicuidad de la nueva vigilancia debe llevar a preguntarse el significado, ahora, de la palabra "sospechoso".

86. LOGAN, W. A., FERGUSON, A. G., "Policing Criminal Justice Data", 101 Minnessota Law Review, volumen 101, 2016, p. 615.

oral en la que puede resultar acusado, también puede convenirse que no es tan fácil separar la labor policial de vigilancia-predicción de su posterior incidencia procesal y de la aplicación, ahora sí, del derecho al proceso debido[87]. Debo puntualizar que la no aplicación de las reglas del proceso debido a la fase de vigilancia-predicción policial, no significa que ésta no deba tener como límites el respeto de los derechos fundamentales de la persona, pero quizá frente a la idea de que la presunción de inocencia debe desplegar sus efectos de forma cada vez más extensiva y, por ello, llegando también a la policía predictiva, sea mejor explorar otras vías de protección, aunque no toda la doctrina coincide en este punto como se ve a continuación, habiendo expresado mi postura un poco más arriba.

Así, hay quien sostiene, tras un análisis de la jurisprudencia del TEDH[88], que la vigilancia predictiva debe estar sujeta a la presunción de inocencia por tres razones: primero, porque el uso de antecedentes penales como fuente principal de datos en las evaluaciones de riesgo es problemático porque no extrae adecuadamente los registros de las personas cuyo arresto no fue seguido por una condena; segundo, porque la policía actúa como autoridad pública con la capacidad de perjudicar la imparcialidad de un juicio si hace una declaración o actúa de una manera que provoque el prejuzgamiento de un sospechoso; tercero, porque la vigilancia predictiva con la ayuda de evaluaciones de riesgo es un uso de facto de técnicas de investigación para prevenir el crimen, de forma que este

87. BLOUNT, K., "Applying the presumption of innocence to policing with IA", *International Review of Penal Law, cit.*, pp. 33-48, en concreto p. 35.

88. BLOUNT, K., "Applying the presumption of innocence to policing with IA", *International Review of Penal Law, cit.*, pp. 33-48, p. 39, señala que "el TEDH ha ido ampliando, no sin algunas dudas, la aplicación de la presunción de inocencia a todo lo largo del juicio penal, no sólo el juicio oral, y a los casos en los que, habiendo absolución, las autoridades estatales hacen manifestaciones y acciones que dan a entender que de facto es culpable, y que determinadas actuaciones policiales pueden ser también dañinas para la presunción de inocencia, pero finalmente "no ha llegado a extender la Presunción a las manifestaciones informales de sospecha, pero ha reconocido el poder de una etiqueta o categorización de sospechoso por los efectos prácticos que tiene sobre los derechos de un individuo. En su razonamiento, que fue en gran medida una justificación apoyada por la Presunción, sostuvo que tales actos son ilegales según el artículo 8 de la CEDH. La categoría de sospechoso, o incluso acusado, trae consigo algún grado de privación de libertad así como otras variedades inevitables de trato a las que no se someterá a una persona inocente. De manera similar, una persona que se considera que pertenece a una clase de personas que pueden cometer un delito, queda sujeta a un tipo de trato diferente al de la persona considerada inocente. El estigma de un arresto etiqueta y separa de facto a los culpables del resto de la sociedad. En consecuencia, el Tribunal en S. and Marper v The United Kingdom apoyó el valor del derecho de un individuo a ser visto como inocente y afirmó que existe un aspecto de "reputación" de la presunción, de modo que la determinación de inocencia no debe verse socavada por un estigma de culpabilidad".

nivel de intrusión en el individuo sin sospecha dirigida es paralelo en el proceso a una investigación penal previa al juicio posterior a un cargo y, por lo tanto, también debe requerir el mismo nivel de protección procesal que se encuentra en la Presunción[89].

En un punto intermedio se sitúan otros autores que reconocen que el derecho penal (y el proceso penal) no "ocupa el campo" de tal manera que impida la justicia preventiva, por lo que lo que se debe preguntar es si es posible hacer una invocación de aplicación simétrica de las garantías del proceso penal, incluida presunción de inocencia, a la policía predictiva, dejando entrever que: a) es una cuestión que depende de los matices de lo que se quiera conseguir, porque no es lo mismo la lucha contra el terrorismo, que la lucha contra delincuencia leve, o que preocuparse de personas peligrosas y mentalmente enfermas; b) también depende, dado que considera que nos movemos en un terreno de derechos y garantías civiles, de hasta dónde se entienda que el régimen civil debe tener garantías simétricas a las penales. Y, aunque según las conclusiones a las que se llegue, no descarta esta aplicación extensiva, concluye que, finalmente, lo que importa no es la calificación de un sistema como criminal ni la invocación de la presunción de inocencia, sino más bien, que el Estado otorgue a sus ciudadanos el debido respeto, es decir, debe protegerlos de las amenazas externas, pero debe protegerlos contra la posibilidad de que el propio Estado infrinja la libertad de los ciudadanos por miedo, lo que reputa como cierto independientemente de lo que finalmente decidamos que significa la presunción de inocencia[90].

Por último, están los que consideran[91] que la policía predictiva no actúa bajo el requerimiento constitucional de la razonable sospecha que

89. Todos estos argumentos en BLOUNT, K., "Applying the presumption of innocence to policing with IA", *International Review of Penal Law, cit.* pp. 39-40, argumentos que reitera en pp. 43-44, "Mientras que formas anteriores de técnicas sofisticadas, o tecnología forense de primera generación, se usaban para confirmar o negar sospechas, la segunda generación puede usarse para investigaciones proactivas, perfectamente ilustradas por evaluaciones de riesgo. La principal diferencia entre los dos métodos es la comisión de un delito, un lugar temporal en el que se puede presentar un cargo y las protecciones previas al juicio se otorgan al sospechoso. Sin el delito no hay cargos y el sospechoso potencial, así tratado por la policía, no puede obtener también las protecciones del proceso legal. Como se mencionó anteriormente, esto tiene efectos perjudiciales reales sobre los derechos de las personas. Se argumenta que a medida que la acción contra el individuo se ejecuta cada vez más en un contexto preventivo, las protecciones contra la acción arbitraria del estado deben seguir en consecuencia".

90. Véase KESSLER FERZAN, K., "Preventive Justice and the Presumption of Innocence", Crim Law and Philos (2014) 8:505–525, especialmente pp. 516 y ss.

91. LINDENMUTH, K., "Prevention or Self-Fulfilling Prophecy? Predictive Policing's Erosion of the Presumption of Innocence", *Law School Student Scholarship*, *cit*., pp. 23-25, 2019, 1018, 28 páginas, https://scholarship.shu.edu/student_scholarship/1018.

exige aplicarse sobre hechos concretos actuales o pasados pero ciertos, ya cometidos y que pueden razonablemente atribuirse a. un sujeto, por lo que no cabe hablar de razonable sospecha respecto de hechos futuros que no se han cometido y que no se sabe si se van a cometer o no, y de ahí es difícil establecer que se pueda vulnerar la presunción de inocencia en este estado de la cuestión. Y, también sería así incluso si se considerase aplicable el requerimiento de la sospecha razonable, porque ésta, por sí misma no supone una violación de la presunción de inocencia[92]. Esto conduce a que la defensa ante los excesos de la policía predictiva debe centrarse en las cuestiones referidas a la protección de datos, a la evitación de los tratamientos automatizados, y a la invocación de la invasión de otros derechos fundamentales como la privacidad o la intimidad, que resultan amenazados, sobre todo por el uso de los mecanismos de vigilancia masiva.

92. Yen, C. P., Hung, T-W., "Achieving Equity with Predictive Policing Algorithms: A Social Safety Net Perspective", *Science and Engineering Ethics*, volumen 27, 2021, 16 pp.

Registros biométricos y su aplicación al proceso penal en España e Italia[1]

Inés Celia Iglesias Canle

Catedrática de Derecho Procesal
Universidad de Vigo

SUMARIO: I. INTRODUCCIÓN. II. LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO EN MATERIA DE INTELIGENCIA ARTIFICIAL. III. SISTEMAS DE RECONOCIMIENTO Y USO DE DATOS BIOMÉTRICOS EN ESPAÑA. IV. SISTEMAS DE RECONOCIMIENTO Y DATOS BIOMÉTRICOS EN ITALIA: EL INFORME DEL GARANTE *PRIVACY* SOBRE SARI. V. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

La Comisión Europea ha presentado sus ideas y medidas para una transformación digital que redunde en beneficio de todos. Desde el punto de vista de la estrategia destinada a garantizar el desarrollo de la Inteligencia Artificial centrada en el ser humano, la estrategia europea parte de que en Europa tenemos todo lo necesario para convertirnos en líderes en sistemas de inteligencia artificial.

La Comisión en su Libro Blanco propone un marco para la Inteligencia Artificial fiable basado en la excelencia y la confianza. Es esencial crear confianza con normas claras que aborden los sistemas de Inteligencia Artificial con un elevado nivel de riesgo. Se busca crear un verdadero espacio europeo de datos, un mercado único de datos permitiendo que

1. Trabajo de investigación realizado con motivo de una estancia como Visiting Professor en la Università degli Studi di Roma "La Sapienza", en noviembre de 2021, en el Dipartimento di Studi Giuridici ed Economici.

fluyan libremente por la UE. El Libro Blanco sobre la Inteligencia Artificial se abrió a consulta pública hasta el 19 de mayo de 2020[2].

Últimamente asistimos a una nueva era en la Justicia en la que se proliferan aplicaciones y *startups* dirigidas a operadores jurídicos que estudian las decisiones judiciales con un fin apriorístico, de justicia predictiva, o elaboran perfiles de jueces a partir de sus previas decisiones judiciales. Existen también otras aplicaciones dirigidas a obtener información jurídica. Estos sistemas de toma de decisión se basan en algoritmos y en el uso automatizado de gran cantidad de datos, que persiguen la rapidez y certeza jurídica en la aplicación del Derecho, la seguridad en el resultado, esto es, en el sentido de la decisión judicial. La Inteligencia artificial la podemos definir como la capacidad de un sistema tecnológico de ofrecer prestaciones asimilables a las de la inteligencia humana, o sea la habilidad de resolver problemas o desarrollar actividades humanas, y en los sistemas más avanzados presupone la capacidad de tratar una gran cantidad de datos –la denominada big data– y de ofrecer respuestas para las cuales está programada usando diversos tipos de algoritmos (López, 2019).

De hecho, se están utilizando en determinados sistemas penales algoritmos predictivos que ayudan al juez en la toma de determinadas decisiones judiciales, así como sistemas de identificación biométricos con fines de diversa índole[3].

Si bien se está extendiendo su uso, la aplicación de estas herramientas por parte de los jueces no es pacífica. Desde el pronunciamiento del 13 de julio de 2016 de la Corte Suprema de apelación de Wisconsin sobre la admisibilidad de los algoritmos de predicción del comportamiento humano a la hora de adoptar decisiones judiciales en el proceso penal, se utiliza de forma habitual por parte de los tribunales norteamericanos el software a la hora de evaluar el riesgo de reincidencia del acusado y aconseja a los jueces sobre el tipo de pena y número de años a imponer como pena privativa de libertad, o sobre el establecimiento, o no, de fianzas, libertad condicional… (COMPAS).

El problema es que este tipo de algoritmos no es algo estático, sino que autoevolucionan y además es un pensamiento opaco, lo que impide que

2. Publicado el 19 de febrero de 2020, disponible en https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (última consulta el 27/02/2020).
3. V. en este sentido el trabajo de FORMICI, G. (2019), Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le Corti, *DPCE*, 2 [http://www.dpceonline.it/index.php/dpceonline/article/view/729], pp. 1107 y ss.

un juez pueda decidir completamente informado, lo que afecta a la imparcialidad judicial e incide en el derecho de defensa.

Ello genera serias dudas en cuanto a su aplicación al proceso penal al poderse ver afectado el derecho a un proceso público y con todas las garantías y el derecho de defensa del encausado.

Los algoritmos son "*series de actuaciones matemáticas que se entrelazan para proporcionar un resultado*". Toma como base para ello una gran cantidad de información concentrada en una gran base de datos (*Smart Data*) en la que elige los datos de manera aleatoria, para anticipar una conducta. Los algoritmos pueden usar datos sensibles (como los que se refieren a la religión, género, raza, nacionalidad, salud, genéticos o biométricos, creencias religiosas e ideológicas…), incluso sin que se le hayan aportado estos datos, lo que se denominan "datos inferidos", de modo que sin que se haya autorizado su uso por la persona, finalmente, se hayan utilizado sin que haya otorgado su consentimiento la titular de estos datos (Pérez Estrada, 2019).

En el momento actual el avance tecnológico genera serios riesgos en cuanto a la privacidad y a la comunicación u obtención involuntaria de datos personales. En la Era de la información el verdadero cambio llega con la Web 2.0 o Web colaboracionista ya que otorga a los usuarios un papel más activo que puede publicar información mediante blogs, redes sociales… En la web 3.0, en la que nos encontramos ahora mismo, lo más relevante son las nuevas herramientas tecnológicas como las cookies o las direcciones IP ya que, aun siendo distintas, si se conjuga ambas herramientas, se puede obtener un perfil detallado del usuario y sus preferencias.

En este sentido, el tema que se trata de examinar suscita serias dudas puesto que supone la utilización de los datos o registros biométricos de una persona con fines de prevención, investigación y represión penal, lo que ya es una realidad en algunos países[4].

4. FORMICI, G. (2019) se refieren las experiencias sobre la utilización de datos biométricos en la India, con el sistema *Aadhaar Project,* que es un sistema nacional dirigido a individualizar la identidad de los ciudadanos hindúes mediante la atribución de un *Aadhaar number*, código que es esencial y en el que consta información demográfica y datos biométricos tales como la huella digital, escáner de iris y una foto del rostro). Tal información y código se puede usar también con fines de investigación penal y garantía de la seguridad nacional, y ha sido declarado constitucionalmente legítimo por la Corte Suprema, salvo para determinadas disposiciones que no superaron la regla de la proporcionalidad, cuando la utilización de datos biométricos no tiene como objetivo la garantía de la dignidad humana, supuestos en los que considera que la obligatoriedad del uso del Código resulta desproporcionada por invadir la esfera de derechos de la persona sin justificación suficiente dada la naturaleza especialmente sensible de los datos biométricos.

   Otros países, como Francia también han participado de esta misma idea con la propuesta de modificación de la *Loi relativa à la protection de l'identité,* que se refiere a

El EDP (European Data Protection Board) emitió un informe el 10 de junio de 2020 en el que afirma que la utilización de estos datos biométricos por parte de los Estados miembros o de la propia Unión Europea le suscita duda, en el actual marco normativo. La observancia del principio de proporcionalidad, la protección de los derechos humanos, particularmente, del derecho a la vida privada y a la tutela de los datos personales, de acuerdo con la Jurisprudencia del Tribunal de Justicia de la Unión Europea, determina que su uso sólo se justifica cuando resulta absolutamente imprescindible[5].

No obstante, este órgano concluye que es un tema abierto que sigue siendo objeto de estudio en el seno de la Unión Europea para informar futuras legislaciones a nivel europeo o nacional, que permita en el futuro la utilización de los registros faciales y biométricos con fines de prevención y represión penal, una vez el debate se ha abierto por parte de la Unión Europea, con motivo del Libro Blanco de la Inteligencia Artificial, con vistas a determinar los casos en los que el reconocimiento facial es aceptable y necesario en el contexto de una sociedad democrática y los casos en los que no se justifica.

II. LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO EN MATERIA DE INTELIGENCIA ARTIFICIAL

En la Unión Europea, tal y como se ha comentado en el epígrafe anterior, hay una preocupación clara en relación a la tutela y protección de los usuarios y del derecho a la privacidad. No obstante, todavía no se ha aprobado el reglamento que desarrolla el contenido del artículo 7 del CDHUE, Reglamento que se refiere a la privacidad de las comunicaciones electrónicas. La propuesta de Reglamento de la UE sobre Inteligencia

---

la regulación del documento de identidad, incluyendo en el mismo datos biométricos. En este caso, un pronunciamiento preventivo del *Conseil Constitutionnel, de 22 de marzo de 2012*, consideraron desproporcionadas tales modificaciones, dada la especial naturaleza de los datos biométricos y las posibles finalidades para los que tales datos podrían llegar a ser utilizados, razón por la cual finalmente la reforma se limitó a incluir la huella digital en el chip del carnet de identidad, sin que se crease la base de datos y excluyendo la posibilidad de acceso a los datos biométricos si no es sólo a fines de validar o controlar el documento de identidad.

En Bélgica, desde el año 2019 se incluye en el documento de identidad electrónico dos huellas digitales y fotos del sujeto, sin que se haya previsto la creación de una base de datos nacional a estos efectos, si bien ello ha provocado un informe desfavorable por parte de la autoridad Garante nacional de la privacy belga por no respetar el principio de proporcionalidad.

5. V. a estos efectos Sentencias de 8 de abril de 2014 y de 21 de abril de 2016, así como el caso Marper contra U.K, de 4 de diciembre de 2008.

Artificial incide en la especialidad de la materia y trata de establecer límites a la obtención y distribución indiscriminada de los datos obtenidos.

La propuesta de Reglamento sobre el marco jurídico aplicable a los sistemas de Inteligencia Artificial, regula los sistemas de Inteligencia Artificial de alto riesgo y contiene reglas de transparencia armonizadas para aquellos sistemas dirigidos a interactuar con personas físicas para generar o manipular imágenes, sonidos o contenidos de videos.

La Comisión Europea intenta promover el uso de la Inteligencia Artificial de forma segura y ética, al establecer una serie de reglas con la finalidad de evitar riesgos y consecuencias negativas.

A los efectos que nos interesan, es evidente que tal información podrá ser utilizada por parte de los algoritmos sin que se haya cedido su utilización, de ahí que consideramos necesaria su regulación para establecer un nivel de protección homogéneo en el ámbito europeo tanto a efectos de su conservación y cesión, como en relación a su utilización a través de la justicia predictiva (González Mendoza, 2019).

El Reglamento propone un ámbito de aplicación subjetivo y territorial amplio que comprendería a todos los actores dentro de la cadena de IA, esto es proveedores, importadores, distribuidores, y alcanzaría tanto a los ubicados en la UE, como los empleados en terceros países, cuando desplieguen sus efectos en la UE y propone la división de los sistemas de Inteligencia Artificial en cuatro categorías o niveles de riesgo, la los que le impone más o menos obligaciones en función de su categorización:

1. Sistemas de Inteligencia Artificial prohibidos: se recogen sistemas de IA, listados de forma tasada y periódicamente revisados, cuyo uso está prohibido por implicar un riesgo inadmisible para la seguridad, la vida y los derechos fundamentales. Dicho listado incluye sistemas **que permitan manipular el comportamiento humano, predecir información respecto a colectivos o grupos para identificar sus vulnerabilidades, o los que impliquen registros biométricos o vigilancia masiva en directo por parte de las autoridades en espacios públicos**. Solo se permiten para el cumplimiento de la ley, bajo autorización judicial o administrativa. En casos de urgencia, esta autorización puede ser obtenida a posteriori en casos de extrema urgencia, lo que puede ser polémico.
2. Sistemas de Inteligencia Artificial de alto riesgo: Se listan otros sistemas de Inteligencia Artificial que no están prohibidos, pero implican alto riesgo para los derechos y libertades

fundamentales de los individuos por lo que deben estar sujetos a ciertas obligaciones que garanticen su uso legal y ético. Los sistemas comprendidos en estas categorías incluyen componentes de seguridad aplicables a sectores regulados o infraestructuras críticas tales como el transporte aéreo, vigilancia de vehículos a motor, trasporte ferroviario**. También se incluirían sistemas de categorización o identificación biométrica,** selección de personal, control de fronteras o sistemas que tratan de comprobar el cumplimiento de la ley o la evaluación de la situación crediticia de las personas.

3. Sistemas de Inteligencia Artificial de riesgo medio/bajo: Sistemas que no suponen un alto riesgo para los derechos y libertades, comprenden tecnologías de menor sofisticación.
4. Resto de sistemas de Inteligencia Artificial: Estos últimos en principio no estarían sujetos a ninguna obligación en particular, pudiendo los agentes de la cadena elegir si desean adherirse a sistemas voluntarios de cumplimiento. Por consiguiente, estos sistemas quedarían fuera del ámbito de aplicación del Reglamento.

Las principales obligaciones para cada de estas categorías de sistemas de Inteligencia Artificial son:

1. Sistemas de Inteligencia Artificial prohibidos (art. 5.): Implican un riesgo inadmisible. No obstante, **los consistentes en sistemas de identificación biométrica en remoto y en tiempo real en espacios públicos se permitirían excepcionalmente para el cumplimiento de la ley y, en este caso, bajo autorización judicial o administrativa.** Dicha autorización debe ser solicitada con anterioridad, pero, excepcionalmente, en casos de urgencia, podría solicitarse *a posteriori*.

   El uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de ley, por tanto, están prohibidos, salvo que sea estrictamente necesario, bajo las anteriores premisas, para alcanzar alguno de los siguientes objetivos:

   a) La búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos.

   b) La prevención de una amenaza específica, importante e inminente para la vida, la seguridad física de las personas o de un atentado terrorista.

c) La detección, localización, identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el art. 2, apartado 2 de la Decisión Marco 2002/584/JAI del Consejo, para el que la normativa en vigor en el Estado Miembro implicado imponga una pena o medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado Miembro.

2. Sistemas de Alto riego de Inteligencia Artificial (art. 6 y ss.): Podrían permitirse siempre que sean sometidos a una evaluación de conformidad y gestión del riesgo que suponen durante toda su vida útil. Cada operador de la cadena de valor estaría sometido a una serie de obligaciones específicas:

   a) Gobernanza de datos: es decir, que los datos empleados revistan ciertos estándares de calidad, supervisión y examinación de sesgos…

   b) Seguridad y supervisión humana: En última instancia siempre tendrá que haber una persona con capacidad de control para mitigar eventuales riesgos.

   c) Deberes de transparencia: es decir, que se describan las características del funcionamiento del sistema y la identidad de datos del proveedor.

   d) Inscripción en una base de datos a nivel europeo: la inscripción deberá llevarse a cabo con carácter previo a la puesta en disposición del mercado.

   e) Superación de test de conformidad y obtención de la certificación correspondiente: serán aprobadas especificaciones técnicas con las que habrá que cumplir.

3. Sistemas de Inteligencia Artificial de riesgo medio/bajo: Estos sistemas solo estarán sometidos a un conjunto de normas de transparencia dirigidas a garantizar que su funcionamiento y características son conocidas por los usuarios, así como las implicaciones derivadas del empleo de las mismas.

4. Resto de sistemas de Inteligencia Artificial: Estos sistemas sólo estarían sometidos a sistemas voluntarios de autorregulación.

– RÉGIMEN SANCIONADOR:

De no cumplirse con las anteriores obligaciones se prevén multas que oscilan entre los siguientes límites:

1. Incumplimiento relativo a prácticas prohibidas y las obligaciones de gobernanza de datos de alto riesgo: Hasta 30 millones de euros o el 6 por ciento del volumen de negocio anual total a escala mundial del ejercicio financiero anterior.
2. Incumplimiento de cualquier otro requisito u obligación: hasta 20 millones de euros o el 4 por ciento de negocio anual total a escala mundial del ejercicio financiero anterior.
3. Suministro de información incorrecta, incompleta o engañosa a los organismos y/o autoridades nacionales: hasta 10 millones de euros o el 2 por ciento de negocio anual total a escala mundial del ejercicio financiero anterior.

Esta propuesta de reglamento será revisada y debatida por el Parlamento Europeo y el Consejo. Una vez aprobado será de aplicación directa a todos los países miembros de la Unión Europea. Tiene en cuenta las recomendaciones del Parlamento Europeo del 20 de octubre de 2020, consistente en tres resoluciones de la Comisión Europea.

De hecho, este Reglamento parte del trabajo de la Comisión Europea que ha presentado sus ideas y medidas para una transformación digital que redunde en beneficio de todos. Desde el punto de vista de la estrategia destinada a garantizar el desarrollo de la Inteligencia Artificial centrada en el ser humano, la estrategia europea parte de que en Europa tenemos todo lo necesario para convertirnos en líderes en sistemas de Inteligencia Artificial.

No obstante, es esencial crear confianza con normas claras que aborden los sistemas de Inteligencia Artificial con un elevado nivel de riesgo. Se busca crear un verdadero espacio europeo de datos, un mercado único de datos permitiendo que fluyan libremente por la Unión Europea con las debidas garantías y sin que ello implique una infracción desproporcionada y no justificada de los derechos y libertades fundamentales en el seno de una sociedad democrática.

La utilización de estos sistemas de identificación y reconocimiento para la prevención, investigación y determinación judicial de los delitos tiene sus defensores y críticos. Entre los primeros se encuentran aquellos que enfatizan su efectividad en el control del delito, así como la objetividad con la que obligaría a operar a las fuerzas policiales. Los críticos ponen el acento en ética y en los posibles prejuicios que pueden interferir

en el proceso y que finalmente suponen discriminaciones en relación a determinadas personas o grupos de personas (Scalzini, 2019)[6].

Ciertamente, con la instalación de dispositivos que permiten vigilar personas casi en cualquier lugar, se abre el debate sobre hasta qué punto se puede estar violando el derecho a la privacidad. En este sentido, la Unión Europea ha pedido a los Estados miembros establecer protocolos para realizar un control a las conexiones 5G, a pesar de haber ya establecido el Reglamento General de Protección de Datos y seguir fortaleciendo la regulación. Todo ello da una idea del difícil equilibrio al que nos enfrentamos en este terreno. Seguridad pública versus derecho a la privacidad de todo ser humano.

Como toda problemática que está a caballo entre diferentes ciencias relacionadas con la Justicia penal, se han de abordar los principios y fundamentos de la intervención del Derecho Penal; aspectos procesales que abarcan el respeto a las garantías o derechos fundamentales de las partes en el proceso tanto en fase de investigación, como en la fase de prueba; los derechos fundamentales que, desde el punto de vista constitucional pueden verse afectados o aspectos de la propia ciencia social criminológica.

Si bien es cierto, como hemos dicho anteriormente, que la utilización de la Inteligencia Artificial y las nuevas técnicas investigativas que proporciona son una realidad, también lo es que debe hacerse de acuerdo con los principios y postulados del proceso penal en el actual estado constitucional.

Nadie duda de la incidencia en las garantías procesales de tales técnicas, el derecho a un proceso con todas las garantías y el derecho de defensa, la imparcialidad judicial y la igualdad de armas, gozan de contenido

6. Concretamente, el mismo autor los sistemas de inteligencia artificial están dirigidos y orientados a encontrar correlaciones entre datos, de forma que, si la selección de datos no es en origen representativa o si hay prejuicios de fondo, la decisión final estará viciada por tales prejuicios.

   En tal sentido se pueden distinguir distintas situaciones: Por ejemplo, de un lado, el caso de un sistema de reconocimiento facial que sólo reconocía rasgos de personas de piel clara y que no funcionaba adecuadamente para personas de rasgos de piel oscura, en tales casos las decisiones erróneas se deben a un límite en la selección de la información con la cual cuenta el algoritmo, la selección de datos no era bastante representativa de la realidad y el resultado no era satisfactorio; y, de otro lado, situaciones en las que en el 2015 con motivo de una investigación en la Universidad de Carnegie se demostró que una plataforma publicitaria de Google producía decisiones erróneas que implicaban una discriminación de género, en este caso concreto, se le proponían a las mujeres ofertas de empleo con una remuneración menor respecto a los colegas hombres, en iguales condiciones de titulación y experiencia. En este caso seguramente el problema se debió a los datos seleccionados por el algoritmo de manera que el resultado puede haber sencillamente reproducido una situación real, de objetiva desigualdad, si bien, el resultado final, el envío de ofertas de trabajo menos remuneradas a las mujeres implica una situación de discriminación.

y dimensión constitucional en el art. 24.2 CE y en el reconocimiento del Estado de Derecho que rige en España. Consiguientemente, la incorporación al proceso de estas técnicas novedosas, requiere un estudio detenido sobre en qué medida la afección del derecho fundamental no implica su quebrantamiento, huyendo del Derecho Penal de autor. Sin embargo, ello no puede ser óbice para su utilización puesto que, debemos asegurar la tutela de la víctima, particularmente las víctimas especialmente vulnerables (discapacitados, menores y víctimas de violencia de género). La utilización de los **registros biométricos, por medio de la identificación biométrica,** contribuirán de un modo eficiente a la consecución de tales objetivos.

Por "**datos biométricos"** se entienden los "**datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos [huella dactilar]"** [artículo 3, apartado 13 de la Directiva sobre protección de datos en el ámbito penal; artículo 4, apartado 14, del RGPD; artículo 3, apartado 18, del Reglamento (UE) 2018/1725][7].

No obstante, como establece el Libro Blanco de la Inteligencia Artificial y la propuesta de Reglamento, la recopilación y el uso datos biométricos para la identificación remota, por ejemplo, mediante la instalación de sistemas de reconocimiento facial en lugares públicos, entraña riesgos específicos para los derechos fundamentales, de ahí que, con carácter general, su utilización indiscriminada y generalizada debe estar prohibida.

Las repercusiones de la utilización de sistemas de Inteligencia Artificial de identificación biométrica remota en los derechos fundamentales pueden variar considerablemente en función del objetivo, el contexto y el alcance de dicho uso.

Las normas de protección de datos de la Unión Europea ya prohíben, en principio, el tratamiento de datos biométricos dirigido a identificar de manera unívoca a una persona física, excepto en condiciones específicas.

En concreto, con arreglo al Reglamento General de Protección de Datos Personales, este tratamiento solo puede tener lugar en un número limitado de situaciones, principalmente por motivos de interés público significativo. En este caso, el tratamiento debe tener lugar sobre la base del Derecho nacional o de la Unión Europea, estar sujeto al requisito de

7. Sobre las distintas acepciones y definiciones del término de datos biométricos y su diferenciación con la categoría de los datos genéticos v. IANNUZZI, A., FILOSA, F. (2019), Il tratamento del dati genetici e biometrici, *Dirittifondamentali.it*, 2 [http://dirittifondamentali.it/wp-content/uploads/2019/07/Iannuzzi-Filosa-Il-trattamento-dei-dati-genetici-e-biometrici.pdf].

proporcionalidad, al respeto del derecho a la protección de los datos y a garantías adecuadas. Con arreglo a la Directiva sobre protección de datos en el ámbito penal, para efectuar dicho tratamiento debe existir una necesidad estricta al respecto; en principio, una autorización de la legislación nacional o de la Unión Europea y garantías adecuadas. Puesto que todo tratamiento de datos biométricos dirigido a identificar a una persona física de manera unívoca estaría vinculado con una excepción a una prohibición establecida en la legislación de la UE, **dicho tratamiento ha de atenerse a la Carta de Derechos Fundamentales de la Unión Europea.**

Por consiguiente, de conformidad con las normas vigentes en materia de protección de datos y con la Carta de Derechos Fundamentales de la Unión Europea, la Inteligencia Artificial solo puede utilizarse con fines de identificación biométrica remota **cuando dicho uso esté debidamente justificado, sea proporcionado y esté sujeto a garantías adecuadas**.

Además, el 28 de enero el Comité Consultivo de la Convención sobre la protección de las personas respeto al tratamiento automatizado de caracteres personales 108/1981 (Convención 108) ha adoptado las denominadas *"Guidelines on Facial Recognition"* y establece y aconseja a los Gobiernos que utilicen estos sistemas biométricos de reconocimiento facial que adopten las medidas necesarias para proteger los derechos y la libertad de los interesados.

Finalmente, a fin de abordar las posibles preocupaciones sociales con relación al uso de la Inteligencia Artificial y los datos y registros biométricos para tales fines en lugares públicos, y con el objetivo de evitar la fragmentación del mercado interior, la Comisión abrirá un debate europeo sobre las circunstancias específicas, si las hubiera, que puedan justificar dicho uso, así como sobre las garantías comunes.

Según el artículo 4 del Reglamento General de datos personales de la UE: "datos biométricos": *"datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos"*. También comprende la identificación mediante el iris, geometría de la mano, imagen facial, de voz, de firma, corporal o de ADN o huella genética. El tratamiento de estos datos, en tanto que datos personales, debe hacerse según dijimos de acuerdo con el Reglamento de datos personales.

Los sistemas biométricos dependen de algoritmos computacionales y se les puede definir como un conjunto preescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permiten realizar una actividad, mediante pasos sucesivos que no generen dudas.

La utilización de estos sistemas resulta útil particularmente en pasos fronterizos puesto que facilitan el trámite en aeropuertos y terminales concurridas. El DNI electrónico permite con los datos personales inscritos en un chip facilita el acceso y después se podría realizar el proceso de identificación biométrica, mediante la verificación de huellas digitales, escaneo del iris, comprobación de voz y del rostro, geometría de la mano… con ello se permitiría el paso si el trámite se completa con éxito, ya que los sistemas estarían conectados a su vez con bases de datos de Servicios de control que tienen la capacidad para comprobar la legalidad del pasaporte, chequear la legitimidad de la entrada, cotejar huellas y datos biométricos, etc.

Esta posibilidad es un medio de control de delitos internacionales como el terrorismo y el blanqueo de capitales, narcotráfico y delincuencia transfronteriza en general. La interconexión con las bases de datos de Interpol hará posible la cooperación con todas las organizaciones que trabajan en la prevención y represión delictiva.

Por tanto, también resulta posible su uso de cara a la vigilancia policial predictiva, si bien, como vimos en el marco de la actual propuesta de Reglamento no resulta viable, salvo en determinadas situaciones bajo control judicial o administrativo, lo que ya de por sí suscita dudas, y en casos debidamente justificados y autorizados por la normativa interna de cada Estado Miembro, previo el correspondiente juicio de proporcionalidad del caso concreto, salvo urgencia debidamente justificada.

Debemos no obstante analizar la situación actual más allá de la normativa europea vigente o de la propuesta de Reglamento, porque en tanto en cuanto la misma no sea aprobada no deja de ser una orientación o una mera declaración de intenciones que no da respuesta a la entrada en el proceso penal de los registros biométricos como medio de investigación y prueba. La respuesta europea será tardía porque los distintos ordenamientos jurídicos de la Unión Europea están resolviendo ya la entrada de los registros biométricos en el proceso penal. En tal sentido tomaremos como referencia dos países de la Unión Europea: España e Italia.

III. SISTEMAS DE RECONOCIMIENTO Y USO DE DATOS BIOMÉTRICOS EN ESPAÑA

En nuestro Estado constitucional la norma de referencia actual es la que establece la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones

penales, a falta de una regulación definida sobre la materia. Con ello se trata de transponer la Directiva de la Unión Europea 2016/680 de 27 de abril de 2016, sobre el tratamiento de datos personales en el espacio de cooperación policial y judicial penal[8].

En esta norma española de reciente aprobación asume la finalidad declarada en su preámbulo de establecer un nivel adecuado de protección de los derechos de la ciudadanía, y, en general, de sus datos personales, homologable al resto de los Estados Miembros de la Unión Europea, incorporando para ello las reglas de la directiva de la que trae causa. Con ello se establece un marco jurídico consistente que proporciona seguridad jurídica en el contexto de la cooperación policial y judicial penal, con lo que se proporciona una mayor eficacia a la actuación de las Fuerzas y Cuerpos de Seguridad y al propio sistema judicial penal.

En relación al tema que nos ocupa, se considera de forma clara que el tratamiento de datos genéticos o biométricos sólo puede tener lugar cuando sea estrictamente necesario y se cumplan ciertas condiciones[9].

8. No obstante, como reconoce ORTIZ PRADILLO (2021) la cobertura legal para la incorporación al proceso penal de las imágenes captadas por medio de sistemas de videovigilancia es mucho más amplia y se contiene en más normas. Concretamente dice: "*El régimen legal que ampara esas fuentes videográficas de las que pueden servirse las autoridades varía en virtud del momento y finalidad con que se hayan efectuado tales filmaciones. Aquellas filmaciones videográficas efectuadas en el marco de una investigación penal concreta quedarían encuadrables en el actual régimen del art. 588 quinquies a LECrim (SSTS núm. 272/2017, de 18 de abril, ECLI:ES:TS:2017:1594 y 569/2020, de 30 de octubre, ECLI:ES:TS:2020:3772) y, por tanto, sin ponderación judicial previa. Por el contrario, las filmaciones videográficas anteriores a la investigación del hecho delictivo, ejecutadas con fines muy distintos –prevención, control y seguridad de personas, bienes y dependencias, grabaciones periodísticas o videos domésticos, etc.– quedan amparadas en una normativa legal muy heterogénea y distinta a la Ley de Enjuiciamiento Criminal, referida a la protección de datos personales, como son la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales; la Ley 5/2014, de 4 de abril, de Seguridad Privada; la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, así como su Reglamento de desarrollo, cuando se trate de videograbaciones en instalaciones deportivas; o la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, cuando la grabación videográfica documente la sesión de un órgano colegiado de las distintas Administraciones Públicas*".

9. Los datos genéticos han sido objeto de regulación detenida en nuestro ordenamiento jurídico y, aunque participan claramente de la naturaleza de datos biométricos al facilitar y permitir la identificación de una persona, no son objeto de estudio en el presente trabajo, dado que la regulación, tanto a nivel europeo como nacional, ha despejado las dudas existentes, en relación a su admisibilidad y a los requisitos para su obtención, incluso de forma coercitiva, física o jurídicamente, en el contexto de un proceso penal, facilitando la persecución delictiva y la cooperación jurisdiccional y policial en el ámbito europeo; V. en este sentido nuestro trabajo sobre *La obtención de*

Los datos biométricos, como las huellas dactilares y la imagen facial, se consideran incluidos en esta categoría especial cuando su tratamiento está dirigido a identificar de manera unívoca a una persona física. Esta necesidad de identificación surge en el contexto de la actuación delictiva y a estos efectos en la norma que se analiza se incluye, como veremos, de forma expresa la habilitación legal que facilite una respuesta rápida y adecuada en el uso de estos datos de identificación biométrica, con el objetivo final de garantizar los derechos de los ciudadanos y de la sociedad española.

Por ello, con tal propósito, se prohíbe la adopción de forma expresa de decisiones individuales automatizadas, incluida la elaboración de perfiles en este ámbito, salvo que esté autorizado por una norma con rango de ley del ordenamiento jurídico español o europeo.

A estos efectos, la regulación concreta establece en el art. 5. l) la definición de dato biométricos como "*datos personales obtenidos a partir de un tratamiento técnico especializado, relativo a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*".

El tratamiento de las categorías especiales de datos personales, entre los que se incluyen los datos biométricos, con fines de identificación unívoca de una persona, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:

a) Se encuentren previsto por una norma con rango de ley o por el Derecho de la Unión Europea;

b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física;

c) Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

Las autoridades competentes, sigue diciendo el apartado 2 del art. 13 de esta norma, en el marco de las respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y prevención

perfiles genéticos de ADN a través de la Orden Europea de Investigación, Posada Pérez, José Antonio. Coordinador, Llorente Sánchez-Arjona, Mercedes, "ESTUDIOS PROCESALES SOBRE EL ESPACIO EUROPEO DE JUSTICIA PENAL", Aranzadi, Pamplona, 2021, ISBN: 978-84-1391-169-4.

frente a amenazas contra la seguridad pública. No obstante, los datos de menores y de personas con capacidad modificada judicialmente o incursos en procesos de esta esta naturaleza, según el apartado 3, se tratarán garantizando el interés superior de los mismos y con el nivel de seguridad adecuado.

En el art. 14 se prohíben, como hemos adelantado, las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades, incluyendo el derecho a la supervisión humana. Tales decisiones no pueden basarse en categorías especiales de datos personales del artículo anterior, salvo que se hayan tomado las medidas necesarias para garantizar los derechos y libertades e intereses legítimos del interesado. Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la del base de una de las categorías especiales de datos personales del artículo 13.

En los artículos siguientes se regula el tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad. Concretamente, el art. 15 establece y reconoce la licitud de los sistemas de grabación de imágenes y sonidos por las Fuerzas y Cuerpos de Seguridad, de forma que la captación, reproducción y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad no se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, siempre que se traten tales datos conforme al principio de proporcionalidad y para alguna de las finalidades definidas a continuación: asegurar la protección de edificios e instituciones públicas, propias, o vinculadas a la protección de la seguridad nacional, o finalmente, para prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.

El precepto siguiente se refiere a la instalación de sistemas fijos de videovigilancia o videocámara y en el art. 17 a la utilización de los dispositivos de toma de imágenes y sonido de carácter móvil por parte de las Fuerzas y Cuerpos de Seguridad, estableciendo unas garantías previas para su utilización en el posterior proceso penal.

Por su parte, el art. 18 define el tratamiento y conservación de imágenes de forma que, realizada la filmación de acuerdo con los requisitos de la presente ley orgánica, si la grabación captara la comisión de hechos

que pudieran ser constitutivos de delito, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición de la autoridad judicial, a la mayor brevedad posible, y en todo caso en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

Si se captaran hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad pública, se remitirán al órgano competente, de inmediato, para el inicio del oportuno expediente sancionador.

Las grabaciones serán destruidas en el plazo máximo de tres meses desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

Esta norma resulta consonante con la doctrina de nuestro Tribunal Supremo, de la que se hace eco ORTIZ PRADILLO (2021) y que critica severamente, de forma que convalida la práctica jurisprudencial que ampara la legitimidad de todo tipo de grabaciones que se realicen por las Fuerzas y Cuerpos de Seguridad, siempre que se cumplan los anteriores requisitos y se realicen en el marco de una actividad policial de seguimiento o vigilancia y no sean supuestos encuadrables dentro del art. 588 quinquies a) y b), en los que, salvo urgencia, es preceptiva autorización judicial previa.

Cabe por último plantearse, como hace este autor, sino debieran sujetarse, al igual que cualquier sistema de reconocimiento biométrico para su incorporación como prueba en el proceso penal al régimen legal del art. 588 bis de la LECrim y, consiguientemente, a la regla de la proporcionalidad desde el primer momento, con una autorización judicial previa[10].

10. V. ORTIZ PRADILLO (2021), en palabras de este autor: *"Pero lo que interesa ahora destacar es que la actual jurisprudencia del Tribunal Supremo sostiene que, en las labores policiales de vigilancia u observación de lugares o personas que pudieran estar relacionadas con el hecho que es objeto de la investigación, 'se pueden utilizar toda clase de medios que permitan constatar la realidad sospechada y que sean aptos para perfilar o construir un material probatorio que después pueda ser utilizado para concretar una denuncia ante la autoridad judicial (STS, Sala 2.ª, de 6 de mayo de 1993, ECLI:ES:TS:1993:2828)' y habilita el empleo policial de sistemas mecánicos de grabación de imágenes, sin necesidad de una previa ponderación judicial sobre su necesidad y proporcionalidad, dentro de los márgenes marcados por el respeto a la intimidad y a la inviolabilidad del domicilio, pues estas vigilancias y seguimientos 'no afectan al núcleo esencial del Derecho Fundamental a la intimidad del investigado porque ningún derecho fundamental vulnera el agente que percibe con sus ojos lo que está al alcance de cualquiera. El*

La cuestión a nuestro juicio es más compleja y, como estamos analizando, requiere de un régimen legal nacional o supranacional que permita su utilización como medio de investigación y prueba en los casos en que estamos refiriéndonos, ya no a la mera captación de imágenes por cámaras de videovigilancia o por mecanismos de seguimiento o vigilancia, temas resueltos en la LECrim o en las normas antes referidas, si no hay una investigación judicial abierta (por tanto, no parece operativa la solución propuesta por este autor), sino a mecanismos de captación y registro de datos biométricos, en diferido o en tiempo real, a gran escala para su utilización con fines preventivos o de enjuiciamiento en el proceso penal.

Por su parte se regula en el art. 19 de esta norma el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad, de conformidad con lo dispuesto en relación a las infracciones en materia de protección de datos de carácter personal y según lo establecido en esta ley orgánica, al margen de las responsabilidades penales en que pudieren incurrir.

En cuanto a los derechos de los interesados incursos en causa penal, el art. 26 de esta norma dispone que *"el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento a los que se hace referencia en los artículos anteriores se llevará a cabo de conformidad con las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales.*

2. Cuando los datos sean objeto de tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional penal, o el Ministerio Fiscal, el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento se realizará de conformidad con lo previsto en la Ley Orgánica 6/1985, de 1 de julio, en las normas procesales y, en su caso, el Estatuto Orgánico del Ministerio Fiscal.

---

agente de policía puede narrar como testigo cuanto vio y observó cuando realizaba tareas de vigilancia y seguimiento. Nuestro sistema constitucional no alza ningún obstáculo para llevar a cabo, en el marco de una investigación penal, observaciones y seguimientos en recintos públicos (SSTS núm. 433/2012 de 1 de junio, ECLI:ES:TS:2012:3884; 67/2014 de 28 de enero, ECLI:ES:TS:2014:558; 409/2014 de 21 de mayo, ECLI:ES:TS:2014:2209; 200/2017 de 27 de marzo, ECLI:ES:TS:2017:1069 y 329/2016 de 20 de abril, ECLI:ES:TS:2016:1709)'".

Y concluye: *"La utilización de sistemas de filmación en espacios públicos, a los legítimos fines de prevención, detección, investigación y enjuiciamiento de infracciones penales (y su sometimiento a técnicas de identificación biométrica en diferido o en tiempo real), deberían considerarse igualmente medidas limitadoras de derechos fundamentales, y por ende, someterse a una autorización previa –salvo supuestos de urgencia– que efectúe el conocido 'juicio de proporcionalidad' como test de constitucionalidad de la injerencia de conformidad con los principios rectores del art. 588 bis LECrim".*

3. En defecto de regulación del ejercicio de estos derechos en dichas normas, se aplicará lo dispuesto en esta Ley Orgánica".

Por tanto, además de lo dispuesto en esta norma, de aplicación supletoria, debemos atender al régimen establecido en los arts. 234, 235, 235 bis, 235 ter y 236 bis a 236 decies, cuya reforma se introdujo en la disposición final tercera de esta ley, que remiten al Reglamento UE 2016/679 y a la Ley Orgánica 3/2018 y su normativa de desarrollo, al margen de lo dispuesto en la propia Ley Orgánica. Estos preceptos establecen un régimen de tratamiento de los datos de carácter personal en el ámbito de la Administración de Justicia, y, concretamente, en lo que se refiere al proceso penal, remiten a la norma que estamos analizando y al Estatuto Orgánico del Ministerio Fiscal.

Con carácter general el art. 234 LOPJ establece que los letrados de la Administración de Justicia y los funcionarios competentes de la oficina judicial facilitarán a los interesados cuanta información soliciten sobre el estado de las actuaciones procesales, que podrán examinar y conocer, salvo que hubieren sido declaradas secretas o reservadas conforme a la ley. Este es el criterio general, con independencia de las concretas previsiones para garantizar la privacidad de los datos personales que se contemplan en los siguientes preceptos, en función del momento procesal y de la categoría o situación del interesado y clase de proceso y acto procesal de que se trate.

En la LO 7/2012, de 26 de mayo se regula también el régimen de transferencia de datos personales por las autoridades competentes españolas a un Estado no miembro de la Unión Europea y a una Organización Internacional, incluidas las transferencias ulteriores a otro Estado que no pertenezca a la Unión Europea o a otra organización internacional, siempre que se den las siguientes condiciones:

a) Que la transferencia sea necesaria.

b) Que los datos personales sean transferidos a un responsable del tratamiento competente para los fines mencionados en el art. 1.

c) Que, en caso de que los datos personales hayan sido transferidos a la autoridad competente española procedentes de otro Estado de la Unión Europea, dicho Estado miembro autorice la transferencia ulterior de conformidad con su Derecho Nacional.

d) Que la Comisión Europea haya adoptado una decisión de adecuación de acuerdo con el art. 44 o, a falta de dicha decisión, cuando se hayan aportado evidencias o existan garantías adecuadas de conformidad con el art. 45, o a falta de ambas, cuando resulten de

aplicación las excepciones para situaciones específicas de acuerdo con el art. 46.

e) Cuando se trate de una transferencia ulterior a un Estado que no sea miembro de la Unión Europea u organización internacional, de datos transferidos inicialmente por una autoridad competente española, esta autorizará la transferencia ulterior, una vez considerados todos los factores pertinentes, entre estos, la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales y el nivel de protección existente en ese Estado u organización internacional a los que se transfieran ulteriormente los datos personales.

2. Las transferencias de datos personales por las autoridades españolas sin autorización previa de otro Estado miembro, conforme al párrafo 1c), sólo se permitirán si la transferencia de datos personales resulta necesaria para prevenir una amenaza inminente y grave para la seguridad pública, tanto de un Estado miembro de la Unión Europea como no perteneciente a la misma, o para los intereses fundamentales de un Estado miembro de la Unión Europea y cuando la autorización previa no pueda conseguirse a su debido tiempo.

Las autoridades españolas informarán sin dilación a la autoridad responsable de conceder la autorización previa, y en todo caso en el plazo máximo de diez días a contar desde que se haya producido la transferencia.

Por último, de conformidad con el párrafo 3 de esta norma se impulsará el establecimiento de mecanismos de cooperación internacional y asistencia mutua con los Estados no miembros de la Unión Europea y con organizaciones internacionales, de manera que se facilite la aplicación de la legislación sobre protección de datos personales, inclusive en el ámbito de la resolución de conflictos jurisdiccionales.

De acuerdo con lo dispuesto en la normativa europea de aplicación, concretamente la Directiva UE 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, que transpone la norma contemplada en la LO 7/2021, de 26 de mayo, el régimen de protección y transferencia de datos personales entre Estados miembros de la Unión Europea y a terceros países u Organizaciones Internacionales con niveles de garantías adecuados, se rige por tanto por una norma que establece un marco jurídico que aporta seguridad jurídica para facilitar la cooperación policial y judicial penal y, por tanto, mayor eficacia en el ámbito de la actuación de las Fuerzas y Cuerpos de Seguridad y del propio sistema penal.

Los mecanismos de cooperación policial y judicial, particularmente la Orden Europea de Investigación, proporcionan un instrumento adicional

para permitir la persecución delictiva transfronteriza en el ámbito de la Unión Europea, con el debido umbral mínimo de garantías y tutela de los derechos fundamentales concernidos. La Orden Europea de Investigación constituye un instrumento único para llevar a cabo una o varias medidas de investigación en otro Estado miembro (Estado de ejecución) con vistas a la ulterior obtención de pruebas o para recabar pruebas que ya obran en poder de las autoridades del Estado de ejecución, con el objeto de que las pruebas obtenidas a través de la Orden Europea de Investigación en el Estado de ejecución, surtan efectos en un proceso penal que se sigue en el Estado que emite la OEI. En este sentido, la Orden Europea de Investigación incluye también la adopción de medidas cautelares para el aseguramiento de esta prueba[11].

IV. SISTEMAS DE RECONOCIMIENTO Y DATOS BIOMÉTRICOS EN ITALIA: EL INFORME DEL GARANTE *PRIVACY* SOBRE SARI

Por su parte, el legislador italiano ha llevado a cabo la transposición de la misma directiva mediante el DECRETO LEGISLATIVO de 18 maggio 2018, n. 51 di Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonchè alla libera circolazione di tali dati e che abroga ladecisione quadro 2008/977/GAI del Consiglio.

En esta norma establece en su art. 1, el objeto y ámbito de aplicación de esta norma, esto es, al tratamiento de datos personales con fines de prevención y persecución delictiva y, en el art. 2. apartados n) y o), las definiciones de datos genéticos y biométricos en términos coincidentes con la legislación española:

> *n) dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*

11. V. GONZÁLEZ FERNÁNDEZ, A. I. (2021), La admisibilidad de la prueba obtenida mediante la orden europea de investigación en el proceso penal español*, Revista General de Derecho Procesal*, 54; IGLESIAS CANLE, I.C., GONZÁLEZ FERNÁNDEZ, A.I. (2021).

o) dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

Según el art. 6 de esta norma *"I dati personali raccolti per le finalità di cui all'articolo 1, comma 2, non possono essere trattati per finalità diverse, salvo che tale trattamento sia consentito dal diritto dell'Unione europea o dalla legge"*, con lo que se cumple el principio general de que los datos deben ser tratados en principio para la finalidad para el que se han recogido, al margen de la posibilidad de que su transmisión se permita por la legislación europea, como hemos tenido ocasión ya de comentar respecto a los datos genéticos.

Por su parte, el art. 7, respecto al tratamiento de categorías especiales de datos personales, establece que *"Il trattamento di dati di cui all'articolo 9 del regolamento UE é autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione Europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato"*.

Esta norma habilitante no contempla a mi modo de ver, y como finalmente reconoce el órgano de control encargado de supervisar la tutela y protección de derechos y libertades de los interesados afectadas por el tratamiento de datos personales con fines de investigación criminal, denominado como veremos Garante, la habilitación legal respecto a los datos biométricos, por lo que debemos examinar la legislación italiana puesto que en la Unión Europea por el momento no se permite su utilización, antes bien al contrario, como hemos visto, la intención del legislador comunitario es la de prohibir su utilización indiscriminada con fines prospectivos, salvo en casos muy concretos en los que se justifica la invasión en la esfera de los derechos personales ligados a su obtención y utilización.

En efecto, el Codice della Procedura Italiano en el art. 349 contempla la posibilidad de identificación dactiloscópica, fotográfica o antropométrica, así como de "otros medios", dice literalmente, si no son válidos los primeros.

Ello supone una apertura a cualquier opción o medio de identificación personal que las nuevas tecnologías permiten, como reconocen expresamente algunos autores italianos al analizar el precepto en cuestión. Por tanto, se permite que la policía pueda proceder, según dispone el art. 349.2 CPP, previa autorización escrita del Ministerio Público, a obtener coactivamente el perfil genético (disposición introducida en el año 2005 por el

D. ley 144/2015, convertido en ley 55/2005, de medidas urgentes para la lucha contra el terrorismo internacional), mediante la extracción de cabellos o un frotis bucal para la obtención de saliva.

Se debe hacer, en todo caso, una lectura rigurosa de las posibilidades que contempla la norma en cuanto al tipo de material biológico que se puede obtener, por aplicación del art. 13 de la Constitución Italiana. Se critica doctrinalmente la falta de reserva judicial para la autorización de la intervención corporal previa a la obtención de la muestra biológica, dado el tenor literal del art. 13.2 de la Constitución Italiana que exige reserva jurisdiccional para este tipo de actuaciones que afectan a derechos fundamentales (SPANGHER *et al.*, 2015).

Por su parte el art. 8 del Decreto legislativo de 18 de mayo de 2028, número 51, establece la prohibición expresa de que se tomen decisiones basadas únicamente en un tratamiento automatizado de datos personales, que produzcan efectos negativos al interesado, salvo que estén autorizadas por el Derecho de la Unión Europea o de específicas disposiciones de ley (art. 5).

El art. 7, como ya hemos visto, determina que el tratamiento de datos personales del art. 9, entre los que se encuentran los datos biométricos, con fines de prevención o persecución delictiva o ejecución de sanciones penales, solo puede ser efectuado si es estrictamente necesario y asistido de las garantías adecuadas para los derechos y libertad de los interesados, si es necesario para salvaguardar un interés vital del interesado o de otra persona física o si tiene por objeto datos manifiestamente hechos públicos por el interesado.

En ningún caso estas decisiones se pueden basar en la categoría de datos personales del art. 9 del Reglamento de la Unión Europea, salvo que se adopten las medidas adecuadas para salvaguardar los derechos, la libertad y legítimos intereses del interesado. Además, sigue diciendo este precepto, que las disposiciones de ley deben prever en todo caso garantías adecuadas para los derechos y libertades del interesado. En todo caso, se garantiza el derecho a obtener la intervención humana por parte del titular del tratamiento.

Se regulan en los artículos siguientes los derechos del interesado, particularmente, el derecho a ser informado por parte del titular del tratamiento en relación a la finalidad del tratamiento de los datos personales, así como los derechos de acceso, rectificación o cancelación de los mismos. Deberá informar también del título jurídico del tratamiento, el período de conservación y la categoría de destinatarios de los datos personales, incluidos terceros Países u Organizaciones Internacionales.

Por su parte en el art. 23 de esta norma prevé expresamente que si el tratamiento, por el uso de las nuevas tecnologías, por el ámbito de aplicación, por el contexto o por la finalidad, presenta un riesgo elevado para los derechos y la libertad de las personas físicas, el titular del tratamiento, antes de proceder al mismo, efectúa una valoración del impacto sobre la protección de los datos personales. La referida valoración contiene una descripción general de los tratamientos previstos, una valoración de los riesgos para los derechos y las libertades de los interesados, las medidas previstas para afrontar tales riesgos, las garantías, las medidas de seguridad y los mecanismos que garantizan la protección de los datos personales y el respeto de las normas del presente decreto.

Según el art. 37 la autoridad de control es el Garante, que es la encargada de vigilar la aplicación de las normas del presente decreto, con el fin de tutelar los derechos y las libertades fundamentales de las personas físicas con relación al tratamiento de los datos personales y facilitar la libertad de circulación de los datos dentro de la Unión Europea. A tales fines se le atribuyen al Garante, entre otras, las siguientes funciones, que consideramos más relevantes:

a) La promoción del conocimiento y la consciencia de los riesgos, las normas, garantías y derechos en relación al tratamiento.

b) La promoción de la consciencia entre los titulares y responsables del tratamiento de la importancia de las obligaciones previstas en el presente decreto.

c) Expresión de su opinión en los casos previstos en la ley.

d) Informar, a petición de los interesados, sobre el ejercicio de los derechos previstos en el presente decreto y, si es el caso, cooperar, a tales fines, con la autoridad de control de los otros Estados Miembros.

e) Tratamiento de las reclamaciones presentadas por los interesados, por un organismo, una organización o una asociación en el sentido previsto en el art. 40 en cumplimiento de las averiguaciones sobre el objeto de la reclamación, informando al reclamante del Estado y del resultado de la averiguación dentro de plazos razonables, particularmente cuando sean necesarias ulteriores averiguaciones o una coordinación con otra autoridad de control[12].

12. El art. 40 de este decreto establece que el interesado puede dar una orden a un ente del tercer sector sujeto a la disciplina del decreto de 3 de julio de 2017, núm. 117, que esté activo en el sector de la tutela de los derechos fundamentales y de las libertades de los interesados con relación a la protección de los datos personales, al fin de ejercitar por su cuenta los derechos del art. 39 (que prevé que los interesados que

f) Apoyo a los interesados en las reclamaciones.

g) Respuesta sobre la licitud del tratamiento en el sentido del art. 13 e información a los interesados dentro de los plazos previstos en la ley y de los motivos de su licitud.

h) Colaboración, también trámite intercambio de información, con las otras autoridades de control y de asistencia recíproca con la finalidad de garantizar la aplicación y actuación del presente decreto.

i) Verificar los desarrollo tecnológicos y sociales cuando incidan sobre la protección de los datos personales, en particular la evolución de las tecnologías de la información y de la comunicación.

j) Presentar consultas a los fines del art. 24.

Concretamente, el art. 24 se refiere a las consultas preventivas al Garante sobre tratamiento de datos personales que figuran en un nuevo archivo de próxima creación siempre que la evaluación del impacto sobre la protección de los datos personales presente un riesgo elevado, a los efectos del art. 23, en ausencia de medidas adoptadas por el titular del tratamiento para evitar tales riesgos; o bien porque el tipo de tratamiento presenta un riesgo elevado para los derechos y las libertades de los interesados también en razón de la utilización de las nuevas tecnologías, procedimientos o mecanismos nuevos o bien de los datos genéticos o biométricos. En tal sentido, sigue diciendo este precepto, el Garante puede establecer un elenco de tratamientos sujetos a consulta y el titular del tratamiento debe transmitir al Garante la evaluación del impacto sobre la protección de los datos en el sentido del art. 23 y, a petición, otras informaciones, a fin de consentir a tal autoridad efectuar una evaluación de la conformidad del tratamiento de los riesgos para la protección de los datos personales del interesado o de las relativas garantías.

El Garante dispone de un plazo de seis semanas para emitir su opinión, previa la consulta de su parecer, a los fines de la evaluación prevista en el apartado primero de la presente norma, plazo que se puede prorrogar un mes en el caso de un tratamiento complejo.

Para el desarrollo de sus competencias el Garante tiene reconocidos una serie de potestades, tal y como reconoce el art. 37.3:

a) Desarrollar a petición de los interesados averiguaciones sobre la aplicación del presente decreto.

---

vean afectados sus derechos fundamentales con motivo de un proceso penal y que entiendan que se violan las disposiciones del presente decreto, pueden presentar una reclamación al Garante), en consonancia con las disposiciones de patrocinio previstas en Código de Proceso Civil.

b) Obtener del titular y del responsable del tratamiento el acceso a todos los datos personales objeto de tratamiento.

c) Advertir al encargado del tratamiento en orden a la posible violación de las disposiciones del presente decreto.

d) Exigir al responsable del tratamiento de conformar el tratamiento a las disposiciones del presente decreto, con especifica modalidad de trato y dentro de un plazo determinado, ordenando en particular la rectificación o la cancelación de los datos personales o la limitación del tratamiento en el sentido del art. 12 (que prevé el derecho de rectificación o cancelación por los interesados de los datos personales, así como la limitación temporal de su tratamiento, con las excepciones expresamente previstas, entre las que queremos destacar su posible utilización a efectos probatorios ex. Apartado 3).

e) Imponer una limitación provisional o definitiva al tratamiento, incluso su prohibición o el bloqueo.

f) Promover la consideración de violación del presente decreto.

g) Denunciar los delitos de los que conozca con motivo del ejercicio de sus funciones.

h) Realizar anualmente una relación sobre su actividad, que debe transmitir al Parlamento y al Gobierno, el sentido del art. 154.1 del Código y poner a disposición pública, de la Comisión europea y del Comité en el sentido del art. 68 del Reglamento de la UE, donde debe figurar un elenco de las tipologías de violaciones notificadas y de las sanciones impuestas.

En el ámbito de tales competencias y desarrollo de sus funciones, la Autoridad Garante (que denominaremos "Garante") ha emitido un informe desfavorable, con fecha de 25 de marzo de 2021, en relación a la utilización del SARI Real Time, o sistema de reconocimiento facial implementado por el Ministerio de Interior –Departamento de Seguridad Pública– con el fin de coadyuvar con la actividad de las fuerzas de la Policía o de la Policía Judicial (Borgia, 2021). De hecho, según el art. 47 del Decreto Legislativo de 18 de mayo de 2018, se permite la consulta telemática de datos personales por parte de las fuerzas de policía y seguridad, con respeto a las disposiciones de esa norma y con las limitaciones ahí expresadas.

El informe emitido por el Garante al que hacemos alusión se refiere expresamente a la utilización de datos biométricos y, particularmente, a los sistemas de reconocimiento facial que se usan en la lucha contra la criminalidad, terrorismo y, en general, en el ámbito de la tutela de la defensa

de la Seguridad Nacional. En efecto, en una sociedad en la cual la criminalidad se vale de las nuevas tecnologías, surge la exigencia de identificar a los sujetos que acceden a los lugares públicos.

En tal contexto los controles masivos y sistemáticos de personas son estratégicos para las autoridades públicas y un instrumento fundamental para la seguridad ciudadana y los registros biométricos son un medio adecuado para la individualización de sujetos potencialmente peligrosos, midiendo, mediante metodologías matemáticas y estadísticas, las variables fisiológicas y de conducta propias de la persona.

Dentro de los sistemas biométricos, los sistemas de reconocimiento facial representan por tanto parte de la biometría fisiológica que se ocupa de desarrollar algoritmos capaces de comparar dos imágenes de un rostro humano. Según el *Working Party 29*, el reconocimiento facial puede ser definido como un tratamiento automático de imágenes digitales que contienen las caras de las personas con fines de identificación, autenticación, verificación o categorización de tales personas y consta de varias fases:

- adquisición de imágenes, o sea el proceso de tratamiento de revelar el rostro de una persona y la conversión en formato digital.
- individualización de la presencia de un rostro al interno de la imagen digital.
- atenuación de las variaciones dentro del rostro individual.
- extracción de las características de la imagen digital de una persona.
- registro de imágenes o de modelos de referencia para un control y comparación sucesiva.
- medida de las semejanzas entre una serie de características del modelo con las que están registradas en el sistema.

Sigue diciendo el Garante en su informe, que tales tecnologías pueden ser muy útiles para las Fuerzas de la Policía, a quienes se les exige identificar a un sujeto en los casos en que haya dudas sobre su identidad. Todo ello comporta un tratamiento de datos personales, concretamente, de datos biométricos, esto es, de datos relativos a características físicas, fisiológicas o de comportamiento de una persona, consiguientemente el Garante dirige su mirada a la normativa europea vigente ya analizada. Concretamente, cita el art. 6 de la Convención 108 que explica, en la línea de lo que ya hemos comentado, que el tratamiento de especiales categorías de datos biométricos solo puede ser realizado si se legitima por una base jurídica y si en el Derecho del Estado Miembro en el cual se implementa están previstas garantías adecuadas en relación al respeto a los riegos de los interesados,

de forma que la base jurídica sea suficiente para que el uso de tales tecnologías responda a los principios de legalidad y proporcionalidad.

El Decreto Legislativo 51/2018, que transpone la Directiva UE 680/2016 al ordenamiento jurídico italiano, a juicio del Garante evidencia que el tratamiento de datos personales con fines de investigación delictiva impone una interferencia importante en la vida de las personas que debe estar debidamente justificada, según los arts. 5 y 7, mediante una disposición de rango de ley o de reglamento.

En febrero de 2017 el Ministerio del Interior Italiano, Departamento de Seguridad Pública, había iniciado la puesta en marcha de un sistema automático de reconocimiento de imágenes (SARI), destinado a ser utilizado en dos escenarios operativos distintos. En el sistema SARI el tratamiento de datos está orientado a la identificación biométrica mediante el sistema de comparación de imágenes existentes en la base de datos.

De un lado, el Ministerio había previsto un escenario *Enterprise* (*SARI Enterprise)* con un sistema que permita buscar un rostro presente en una imagen en modo automático, por medio de algoritmos de reconocimiento facial, dentro de una base de datos de sujetos (la base de datos *Automatic Fingerprint Identification System, AFIS*). Se busca una solución aplicativa única, para articular una búsqueda sobre un triple nivel: sobre la base del rostro, esto es, en base a la imagen de la cara; sobre la base descriptiva, es decir, teniendo en cuenta las informaciones descriptivas asociadas a la imagen en la base de datos; y, sobre la base combinada, en cuanto elaborada a partir de la información combinada de ambos datos.

De otro lado, dentro de un escenario *real time (SARI Real time)*, en el que el sistema analiza en tiempo real los rostros de los sujetos tomados de las cámaras instaladas en un área geográfica circunscrita y señalada. Los rostros captados mediante fotogramas de *stream video* son comparados mediante un algoritmo de reconocimiento que tiene en cuenta los elementos de comparación de una *watch list*, o sea una base de datos de importancia con cientos de miles de sujetos, con la generación de una alerta para los operadores en caso de que haya una comparación que dé positivo. El algoritmo realiza una lista de candidatos con una puntuación en función de la probabilidad basado sobre el grado de similitud respecto de las imágenes de los sujetos a individualizar.

El informe del Garante en relación, en primer lugar, al SARI Enterprise, en septiembre de 2018 ha observado, en su informe con número 440/2018, que el tratamiento de datos personales mediante este sistema no presenta críticas desde un punto de vista de la privacidad, ya que se limita a automatizar las operaciones que permiten la elaboración automática de la búsqueda en la base de datos de sujetos fotografiados, por lo que constituye

un tratamiento de datos personales previsto en las normas, concretamente, en el Decreto del Ministerio del Interior de 24 de mayo de 2017, referido a la individualización del tratamiento de datos personales efectuados por el Centro de elaboración de datos del Departamento de seguridad pública o de las fuerzas de la Policía efectuado con instrumentos electrónicos, en desarrollo del art. 53.3 del Decreto legislativo 196/2003.

Además, el requisito de necesidad de tratamiento resulta confirmado por la conexión de tales sistemas respecto a la actividad de identificación desarrollada por las fuerzas de la policía, constituyendo un mero auxilio a la actividad humana, con el fin de agilizar la identificación por parte de la Policía de un sujeto buscado del cual se disponga la imagen facial, queda por tanto sólo la exigencia de la intervención del operador para verificar el resultado producido por el sistema automatizado.

En conclusión, con referencia al tratamiento de imágenes faciales por medio del sistema SARI Enterprise, el requisito de la necesaria previsión normativa del tratamiento del art. 7 del Decreto legislativo debe considerarse satisfecho por las numerosas disposiciones legislativas y reglamentarias que contemplan las necesarias garantías para el interesado.

Pero el parecer del Garante respecto al SARI Real Time es desfavorable en relación al impacto en el sentido del art. 23 del Decreto legislativo. Este precepto se refiere al titular del tratamiento y le carga con el deber de efectuar una evaluación del impacto sobre la protección de los datos personales cuando el tratamiento, por el uso de las nuevas tecnologías e por su naturaleza, presenta un riesgo elevado para los derechos y las libertades de la persona física. En particular, el apartado segundo requiere que su evaluación contenga una descripción general del tratamiento previsto, una evaluación de los riesgos para los derechos y las libertades de los interesados, las medidas previstas para enfrentar tales riesgos y las garantías, medidas de seguridad y los mecanismos para garantizar la protección de los datos personales y el respeto al Decreto.

De la descripción del tratamiento que permitiría el SARI Real Time, que todavía no está en uso, consentiría, de un lado, analizar los rostros de los sujetos captados y, de otro lado, registrar los videos de las cámaras de video. Pero el Garante advierte en su informe que la normativa vigente no realiza referencia concreta alguna a los datos biométricos conforme a la legalidad y proporcionalidad de tales medidas y a la necesidad del control preventivo de un Juez o de una autoridad administrativa independiente (Borgia, 2021).

Concretamente, el art. 134.4 del Código del Proceso penal, relativo a la documentación de los actos para su reproducción audiovisual, la adquisición de documentos mediante fotografías y otros medios de

interceptación de comunicaciones telemáticas no pueden constituir base jurídica suficiente para el tratamiento de datos biométricos que permitan la identificación personal. Tampoco los arts. 55, 348, 354 y 370 del mismo Código procesal constituyen base legal suficiente ya que se refieren a las funciones de la Policía Judicial para asegurar las fuentes de prueba y su conducta respecto al aseguramiento de lugares o personas, sin que aludan a los datos biométricos. Finalmente, el DPR 15/2018 que prevé el tratamiento de datos por medio de los sistemas de videovigilancia que permiten la obtención de fotografías, videos y audio que son sistemas ontológicamente diversos de los datos biométricos.

Por tanto, las fuentes normativas no son suficientes, a juicio del Garante, para el tratamiento de datos biométricos para la finalidad de seguridad pública e represión delictiva, que no puede considerarse fuente normativa suficiente e idónea para legitimar el uso de este sistema de identificación biométrica, a falta de una norma del Derecho de la Unión Europea o del Estado Italiano que lo autorice específicamente.

En conclusión, no es posible encontrar actualmente base jurídica que consienta el tratamiento de datos biométricos para esta finalidad por parte del SARI Real Time, a diferencia de lo que acontece con el SARI Enterprise. No obstante, los riesgos en ambos sistemas son evidentes ya que, como advierte la doctrina que se ha ocupado del tema, no parece del todo claro el funcionamiento de ambos sistemas y las imágenes captadas no tienen todas ellas la misma calidad lo que puede arrojar falsos resultados.

La utilización de las cámaras de videovigilancia y otras técnicas de reconocimiento facial para la finalidad de seguridad, policía y represión de delitos se regula, como hemos comentado, por el Decreto legislativo de 10 de agosto de 2018, que contempla garantías para el tratamiento de datos personales conservados en registros públicos, permite obtener una imagen, la cual se introduce en el sistema SARI a efectos de identificar al sujeto (Borgia, 2021, Fonsi, 2021, López, 2019).

La complejidad deriva de su falta de previsión en el código procesal penal y la necesidad de darle entrada en el proceso como un medio de identificación del posible autor de los hechos, teniendo en cuenta además la necesidad de hacer posible el ejercicio del derecho de defensa. Cabe plantearse si tiene cabida por medio de la previsión normativa de la identificación fotográfica del art. 361 CPP, lo que parece poco garantista a la vista de la falta de asistencia letrada del sujeto identificado y la dudosa garantía que supone la comparación realizada entre el sujeto y la máquina que arroja el resultado. Apunta la doctrina la conveniencia de acudir a un informe pericial para contestar la coincidencia realizada por el sistema,

sobre todo cuando la correspondencia entre los rostros se haya tenido en cuenta por parte de la policía a partir del grado de similitud que ellos consideran que existe. Otros autores como Borgia (2021) plantean la posibilidad de reconducirlo al art. 189 CPP[13], siempre y cuando no implique el uso probatorio de tales resultados obtenidos al margen de la legalidad, considerada prueba atípica, una violación de los derechos previstos constitucionalmente. Por tanto, el mismo autor, duda si tal previsión legal del art. 189 satisface el principio de legalidad y proporcionalidad que deben observarse en cualquier injerencia del derecho a la intimidad.

Otro de los problemas a los que nos enfrentamos tienen que ver con la aparente repetibilidad del acto de identificación que siempre que se realiza por parte del software y controlado por el operador que lo controlo e interpreta el resultado a partir de las coincidencias existentes en los rasgos físicos de las imágenes que se comparan.

Por tanto, los sistemas de identificación que usen datos biométricos deben ser suficientemente seguros, fiables y transparentes, como exige la normativa europea que hemos comentado, lo que a todas luces no sucede en el sistema que estamos comentando, valga como referencia los supuestos de errores en la identificación de autores de los delitos o de falsos positivos que arrojan tales sistemas de identificación, como evidencia la experiencia de Estados Unidos y Reino Unido, que se deben a que la mayor parte de los algoritmos son construidos sobre la base de *datasets* que se componen principalmente de rostros de hombres blancos y adultos, lo que determina que los falsos positivos pertenecen normalmente a minorías étnicas y a personas de sexo femenino (Borgia, 2021; López, 2019).

V. BIBLIOGRAFÍA

FLOR, R., Riforma Orlando: riprese fraudolente, intercettazioni, archivazione e impugnazioni. La diffusioni di riprese e registrazione di comunicazione effettuate fraudolentemente: abusus non tollit usum, *Amministrazione Publica*, in genere, htpps://pluris-cedam.utetgiuridica.it/cgi-bin/DocPrint, fecha de última consulta 07/11/2021.

FONSI, A. (2021), Prevenzione dei reati e riconoscimento faccciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time, *Rivista Penale, Diritto e procedura* [https://www.penaledp.it/prevenzione-dei-

13. Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.

reati-e-riconoscimento-facciale-il-parere-sfavorevole-del-garante-privacy-sul-sistema-sari-real-time/].

FORMICI, G. (2019), Sistemi di riconoscimento e dati biometrici: una nova sfida per i Legislatori e le Corti¸ *DPCE*, 2, pp. 1107-1132.

GEMMA, M. (2016), Tullio Delogu e la criminología, *Archivio Penale*, 1, pp. 188-193.

GONZÁLEZ FERNÁNDEZ, A. I. (2021), La admisibilidad de la prueba obtenida mediante la orden europea de investigación en el proceso penal español, *Revista General de Derecho Procesal*, 54, 2021.

IGLESIAS CANLE, I. C., GONZÁLEZ FERNÁNDEZ, A. I. (2021), La obtención de perfiles genéticos de ADN a través de la Orden Europea de Investigación. En Posada Pérez, José Antonio. Coordinador, Llorente Sánchez-Arjona, Mercedes (Directora), *Estudios procesales sobre el espacio europeo de justicia penal*, Aranzadi, Pamplona.

IANNUZZI, A., FILOSA, F. (2019), Il tratamento dei dati genetici e biometrici, Dirittifondamentali.it., 2, pp. 1-24 [http://dirittifondamentali.it/wp-content/uploads/2019/07/Iannuzzi-Filosa-Il-trattamento-dei-dati-genetici-e-biometrici.pdf].

LOPEZ, R. *et al.* (2019), La rappresentazione facciale tramite software. En SCALFATI, A. (Directora), *Le indagini atipiche*, G. Giappichelli Editore, Torino, pp. 239-257.

MARANDOLA, A., BENE, T. (2018), *La reforma della Giustizia Penalek, Modifiche al codice penale e all'ordinamento penitenziario (L. 103/2017),* Giuffrè, Milano.

MAROTTO, G. (2016), *Il contributo de Grispigni alla Criminologia*¸ Archivio Penale, pp. 194-203.

ORTIZ PRADILLO, J. C. (2021), Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal, *Diario La Ley*, 9955.

SCALZINI, S. (2019), Alcune questioni a propósito di algoritmi, dati, etica e ricerca, *Riv. It. Med. Legal*, 1, pp. 169-178.

VV.AA., SPANGHER, G., MARANDOLA, A., GARUTI, H., KALB, L (Directores) (2015), *Misure cautelari. Indagini preliminari. Giudizio,* vol. II. En "Procedura Penale, Teoria e Pratica de proceso", Wolters Kluwer, pp. 550 y ss.

Inteligencia Artificial, valoración del riesgo y derecho al debido proceso

Mercedes Llorente Sánchez-Arjona

Profesora Titular de Derecho Procesal
Universidad de Sevilla

SUMARIO: I. HACIA UN NUEVO PARADIGMA DE PROCESO PENAL. II. DE LA PELIGROSIDAD CRIMINAL A LA VALORACIÓN DEL RIESGO. III. LA VALORACIÓN DEL RIESGO POR LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL. 1. *Análisis del riesgo por las herramientas de Inteligencia Artificial en las medidas cautelares*. 2. *Inteligencia Artificial en fase de ejecución de la pena. Especial referencia a* RisCanvi. IV. LA INCIDENCIA DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO AL DEBIDO PROCESO. V. BIBLIOGRAFÍA.

I. HACIA UN NUEVO PARADIGMA DE PROCESO PENAL

La evolución, los cambios y las transformaciones sociales han tenido su reflejo, como no podía ser de otro modo, en el modelo de Justicia imperante. La sociedad del Siglo XXI es una sociedad global, dinámica, que avanza a una velocidad inusitada provocando cambios en el terreno social, político, económico, cultural, sociológico y, por supuesto, jurídico. La Justicia, como actor fundamental de esta nueva realidad, no puede permanecer anclada en el pasado, en una justicia analógica, lenta, con papel, fundamentada exclusivamente en los Tribunales y en el proceso judicial, sino que ha de mutar hacia una justicia moderna, digitalizada, con una política de papel 0, ágil, supranacional, que fomente los métodos adecuados de solución de conflictos, una justicia más humana que detenga su mirada con especial atención sobre los más vulnerables[1]. Por consiguiente,

1. BARONA VILAR, S., Prólogo de *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad),* Ed. Tirant lo Blanch, Valencia, 2022, pp. 23-31.

nos encontramos ante una nueva realidad que ha llegado para quedarse, que trasciende a todos los ámbitos de la sociedad y afecta, como no podía ser de otra forma, al Derecho y a la Justicia. En lo que hace al sector justicia, esta realidad nos sitúa en un paso más avanzado a la justicia electrónica, la *eJustice,* que implica aceptar la tecnología como un cauce de realización de actos procesales, con la incorporación de pruebas electrónicas, notificaciones electrónicas, toma de declaración por videoconferencia o la posibilidad de dictar resoluciones judiciales electrónicas. Se busca un cambio en el *modus operandi* en sede judicial revestido de mayor agilidad, tecnológico y digital que venga a sustituir a un modelo lento, escrito y presencial[2] que trasciende ya los márgenes de la digitalización y nos sitúa en el marco de la cuarta revolución industrial con sistemas tecnológicos de última generación. Ciertamente, la digitalización de la Justicia es ya una realidad y su algoritmización comienza a serlo.

Este contexto de cambio, de transformación digital y algorítmica, nos abre un nuevo escenario, plagado de nuevos retos y desafíos, que emergen en sede procesal salpicando a los propios cimientos sobre los que se asienta el proceso, incidiendo en numerosas materias, propias de nuestro ámbito, como medidas cautelares, prueba, motivación de resoluciones, recursos o ejecución e incorporando nuevos conceptos como algoritmos, *Big Data,* o Inteligencia Artificial. Estamos asistiendo a un nuevo escenario que, desde finales del siglo XX, transciende la tercera revolución industrial, abriendo una nueva etapa a la que se le ha denominado como industria del 4.0 o cuarta revolución industrial que "no se define por un conjunto de tecnologías emergentes en sí mismas, sino por la transición hacia nuevos sistemas que están construidos sobre la infraestructura de la revolución digital anterior". En esta revolución 4.0 la confluencia de avances tecnológicos está evidenciando cambios profundos que nos hacen hablar de un cambio de paradigma en términos de magnitud, velocidad y alcance en el que mundo físico y digital se fusionan[3], siendo su irrupción en el marco jurídico una realidad ya incuestionable.

2. BARONA VILAR, S., *Inteligencia artificial o la algoritmización de la vida y de la justicia ¿solución o problema?,* Revista Boliviana de Derecho, núm. 28, julio 2019, p. 39.

3. Para SCHWAB, K., *La cuarta revolución industrial,* Ed. Debate, Barcelona, 2016, p. 9, los cambios que se originarán "son tan profundos que, desde la perspectiva de la historia humana, nunca ha habido una época de mayor promesa o potencial peligro". Para el fundador del Foro Económico Mundial hay tres razones que avalan que nos encontramos con una nueva revolución industrial que no forma parte de la Tercera; estas tres razones se identifican, en primer lugar, con la velocidad que hace que su expansión se produzca a un ritmo exponencial, más que lineal; en segundo lugar, la amplitud y profundidad ya que no solo se está cambiando el que y el cómo hacer las cosas, sino el quienes somos y, en tercer lugar, el impacto de los sistemas al tratarse de la transformación de sistemas complejos entre países, empresas, industrias y sociedad en su conjunto.

Por consiguiente, el nuevo paradigma de proceso hacia el que nos encaminamos viene de la mano de la irrupción de las nuevas tecnologías que hace que podamos hablar de una nueva era en la Justicia en la que, junto a la progresiva digitalización del proceso, comienzan a emerger nuevos conceptos que cada vez nos resultan más familiares. *Big Data,* Inteligencia Artificial y algoritmos no son nociones ya desconocidas en el mundo jurídico y, si bien la Inteligencia Artificial viene ya desde hace tiempo aplicándose al proceso, lo cierto es que el avance que su utilización irá experimentando, en sintonía con los tiempos que corren, comienza a llamar la atención, cada vez con mayor intensidad, de la Doctrina adentrándose en un mundo desconocido que necesita de conocimientos transversales[4]. La aplicación de la Inteligencia Artificial al proceso plantea múltiples interrogantes sobre lo que puede ser en el futuro la función del juez, la obtención de datos para la investigación criminal, la prueba algorítmica, la valoración probatoria, o la misma motivación de la sentencia. En el presente trabajo abordaremos los sistemas predictivos de valoración del riesgo en la justicia penal, en concreto, aquellas herramientas que asisten a los jueces en sede cautelar y de ejecución de la pena por estimar que son fases en las que resulta viable su empleo de cara a evaluar bien el riesgo de reincidencia, bien el riesgo de fuga o el de ocultación de pruebas obviando, por razones de extensión, la predicción en el ámbito policial o *predictive policing* y un tema verdaderamente inquietante cual es la aplicación del juicio predictivo en el momento de dictado de la sentencia de forma tal que el riesgo de reincidencia determine una pena de mayor o menor intensidad[5].

II. DE LA PELIGROSIDAD CRIMINAL A LA VALORACIÓN DEL RIESGO

La noción de peligrosidad criminal es un concepto jurídico-legal que presenta una estrecha conexión con las ciencias del comportamiento y con la criminología[6] constituyendo una referencia esencial en la aplicación de

4. LLORENTE SÁNCHEZ-ARJONA, M., "Prueba e Inteligencia Artificial ¿buen maridaje?" en *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad),* Ed. Tirant lo Blanch, Valencia, 2022, p. 483.

5. *Vid.* sobre este particular, MONTESINOS GARCÍA, A., "Justicia penal predictiva" en *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad), cit.,* pp. 442-447, que, acertadamente, alerta del riesgo de sancionar a un sujeto por la posibilidad de delinquir en un futuro y del grave quebranto que ello supondría al principio de presunción de inocencia.

6. ANDRÉS-PUEYO, A., "Peligrosidad criminal: análisis crítico de un concepto polisémico" en *Neurociencias y derecho penal: Nuevas perspectivas en el ámbito de la culpabilidad y tratamiento jurídico-penal de la peligrosidad,* DEMETRIO CRESPO, E., (Dir.), 2020, pp. 483-504.

las medidas cautelares, las medidas de seguridad, la prevención de delitos o la misma fase de ejecución de sentencias. Este concepto, nacido al calor del Positivismo criminológico de finales del siglo XIX y principios del XX, se identificaba con una tendencia que analizaba la predisposición del sujeto a cometer delitos en un futuro pudiendo distinguirse dos dimensiones, una subjetiva, que se identifica con la capacidad criminal que porta un sujeto, y una objetiva, relativa a los delitos ya cometidos y los que se espera cometa en un futuro[7]. Pero este concepto de peligrosidad, que fue contemplado con no poco escepticismo por buena parte de la doctrina penal[8], ha dado paso, progresivamente, a un nuevo movimiento que sustituye esta noción de peligrosidad por la de valoración del riesgo de reincidencia o de violencia (*violence risk assessment*), centrado no en determinar si el individuo posee o no la cualidad subjetiva de peligroso, sino en la valoración de un conjunto de factores, no ya solo personales sino también ambientales, variables en el tiempo, que resultan propicios al mayor o menor grado de comisión de nuevos delitos y que posibilitan contar con pronósticos que determinen la reincidencia futura en términos de probabilidad[9].

No obstante, y aun cuando este concepto está siendo remplazado, lo cierto es que la peligrosidad criminal constituye todavía, a día de hoy, el presupuesto y fundamento de las medidas de seguridad en nuestro ordenamiento jurídico[10], de hecho, su correcta comprensión exige de la vinculación de ambos conceptos. Como es bien sabido, las consecuencias jurídicas que derivan de la perpetración de un hecho típico y antijurídico son las penas y las medidas de seguridad, teniendo su fundamento la primera de ellas en la culpabilidad del autor y la segunda en la peligrosidad[11]. Pero este sencillo esquema que pasaba por imponer penas en atención al

7. LEAL MEDINA, J., "El concepto de peligrosidad en el Derecho penal español: proyección legal y alcance jurisprudencial. Perspectivas actuales y de futuro", *Diario La Ley*, núm. 7870.
8. Sobre el progresivo incremento del Derecho Penal de la peligrosidad *vid.* entre otros, ACALE SÁNCHEZ, M.J., *Medición de la respuesta punitiva y Estado de Derecho,* Pamplona, 2010; ALONSO RIMO, A., "Medidas de seguridad y proporcionalidad con el hecho cometido (a propósito de la peligrosa expansión del Derecho penal de la peligrosidad)", *Estudios Penales y Criminológicos*, XXIX, 2009, pp. 109 y ss.
9. MARTÍNEZ GARAY, L., "Peligrosidad, algoritmos y due process: el caso State v Loomis", *Revista de Derecho Penal y Criminología*, 3.ª época, núm. 20, julio 2018, p. 487.
10. ROMEO CASABONA, C. M., *Peligrosidad y Derecho penal preventivo,* Ed. Bosch, Barcelona, 1986, pp. 20 y ss.; ARMAZA ARMAZA, E. J., *El tratamiento penal del delincuente imputable peligroso,* Ed. Comares, Granada, 2013, pp. 77 y ss.
11. BORJA JIMÉNEZ, E., "Peligrosidad criminal e individualización judicial de la pena" en *Peligrosidad criminal y Estado de Derecho,* ORTS BERENGUER, E., ALONSO RIMO, A., ROIG TORRES, M., Ed. Tirant lo Blanch, Valencia, 2017, p. 13.

hecho cometido por los imputables, medidas de seguridad a los inimputables, cuando se constatase su criminalidad, o la imposición de ambas, pena y medida, en el caso de los sujetos semi imputables siguiendo el llamado sistema vicarial, varía con la entrada en vigor de la Ley Orgánica 5/2010, de 22 de junio[12], que pasa a prever medidas de seguridad para los sujetos plenamente imputables "agotada la dimensión retributiva de la pena" con la que se pretende dar respuesta a la peligrosidad subsistente del sujeto huyendo de una prolongación indiscriminada de la privación de libertad contraria a los principios elementales del Derecho Penal amparados constitucionalmente. Aun cuando donde adquiere mayor relevancia el concepto de peligrosidad es en el contexto de las medidas de seguridad y para sujetos inimputables y semi imputables, se pasa a incorporar para su cumplimiento posterior a la pena privativa de libertad con la finalidad de contrarrestar la peligrosidad de los sujetos una vez que se ha cumplido la pena impuesta por el delito.

En este contexto, el juicio de peligrosidad tiene un componente intuitivo y las tablas de pronósticos no sirven al juez de punto de apoyo seguro al enjuiciar la peligrosidad de un sujeto[13]. El método tradicional clínico[14] de valoración de la peligrosidad del sujeto se considera poco fiable, y adolece de una insuficiente base empírica, son instrumentos relativamente subjetivos, que incluyen entrevistas, observación del comportamiento o el uso de inventarios o escalas. Frente a ellos, los métodos actuariales son objetivos, explícitos y no requieren de ningún juicio de valor por parte del evaluador[15], potenciando la eficacia de las valoraciones clínicas al predecir

12. BOE núm. 152, de 23 de junio de 2010.
13. CEREZO MIR, J, *Curso de Derecho Penal Español,* I, Ed. Tecnos, 6.ª ed., Madrid, 2004, p. 170.
14. *Cfr.* ESBEC RODRÍGUEZ, E., FERNÁNDEZ SASTRÓN, O., "Valoración de la peligrosidad criminal (riesgo-violencia) en psicología forense. Instrumentos de evaluación y perspectivas", *Psicopatología Clínica Legal y Forense*, Vol. 3, núm. 2, 2003, pp. 77-82, que efectúan un análisis riguroso sobre diversas medidas clínicas estructuradas como el *Psychopathy Checklist-Revised PCL-R,* considerado como un método fiable para identificar a aquellos delincuentes varones y pacientes psiquiátricos con mayor probabilidad de reincidencia, el *HCR-20 Violence Risk Assessment Scheme,* que consiste en una guía sistemática para la evaluación clínica de la peligrosidad constando de 20 items divididos en tres categorías, cuales son, Histórica, Clínica y de Riesgo.
15. Ejemplos de medidas actuariales son la Guía para la Valoración de Violencia (*Violence Risk Appraissal Guide VRAG)*, desarrollado en 1994 como un instrumento de valoración de la peligrosidad criminal de los varones de alto riesgo, conteniendo diversas variables cuya puntuación individual se suma dando un resultado para cada individuo que posteriormente se contrasta con tablas actuariales con objeto de obtener la probabilidad de reincidencia en cada caso; variación de este instrumento es el *Sex Offender Risk Appraisal Guide (SORAG)* dirigida a valorar el riesgo de reincidencia en delitos de naturaleza sexual; con esta misma finalidad se desarrolló el instrumento

conductas violentas a medio y largo plazo[16]. No obstante, no nos encontramos con métodos excluyentes ya que en múltiples casos los elementos clínicos utilizan métodos estadísticos como apoyo de sus decisiones y viceversa. Estos diferentes enfoques se adaptan mejor a los ya señalados presupuestos de peligrosidad y de riesgo, respectivamente, de forma tal que la determinación de la peligrosidad criminal ha solido recurrir a métodos científicos basados en informes de expertos, mientras que el análisis del riesgo de delinquir se ha valido de procedimientos estadísticos o actuariales que fomentan la despersonalización del análisis, respondiendo a enfoques muy diversos que pueden llevar a resultados diferentes sobre la decisión de aplicar o no una determinada medida de seguridad[17].

Este cambio de paradigma, que sustituye el concepto de peligrosidad por la valoración del riesgo, ha venido acompañado de una nueva metodología en la forma de medir ese riesgo que se basa en la observación empírica de grandes grupos de sujetos y en una combinación estadística de variables que concurren en ellos y que demuestran estar asociadas a la aparición de conductas violentas o delictivas, o lo que es lo mismo, a factores de riesgo[18]. En estos procedimientos actuariales la evaluación recae en aspectos objetivos, como pueden ser la edad en que cometió el primer delito, el número de condenas previas, si padece o no adiciones…, eliminando los componentes subjetivos que se puedan proyectar sobre la citada evaluación. Estos juicios de predicción de riesgo se sirven de herramientas que utilizan unas tablas de pronóstico basadas en cuestionarios a cuyas respuestas se les otorga una determinada puntuación según el valor que se les ha adjudicado previamente, permitiendo cuantificar y medir el nivel de riesgo delictivo[19] en base a la aplicación de modelos matemáticos. No se pretende el llegar a una individualización precisa del sujeto sobre el pronóstico de su reiteración delictiva personal, sino que lo que se

---

Rapid Risk Assessment for Sexual Offence Recidivism (RRASOR), el *Stanic 99,* llamado así porque incluye exclusivamente variables estáticas o el Árbol de Clasificación Iterativa (*ICT)* que clasifica a los sujetos en bajo o alto riesgo. Para un desarrollo más exhaustivo *vid.* ESBEC RODRÍGUEZ, E., FERNÁNDEZ SASTRÓN, O., *Valoración de la peligrosidad criminal (riesgo-violencia) en psicología forense. Instrumentos de evaluación y perspectivas, cit.,* pp. 70-76.

16. ESBEC RODRÍGUEZ, E., FERNÁNDEZ SASTRÓN, O., *Valoración de la peligrosidad criminal (riesgo-violencia) en psicología forense. Instrumentos de evaluación y perspectivas, cit.,* p. 66.
17. ROMEO CASABONA, C.M., "Riesgo, procedimientos actuariales basados en Inteligencia Artificial y medidas de seguridad", *R.E.D.S.*, núm. 13, julio-diciembre 2018, p. 40.
18. MARTÍNEZ GARAY, L., *Peligrosidad, algoritmos y due process: el caso State v Loomis, cit.,* p. 487.
19. SANZ MORAN, "La peligrosidad criminal. Problemas actuales" en *Delincuentes peligrosos,* Ed. Trotta, Madrid, 2014, p. 75.

persigue alcanzar es su clasificación en grupos prototípicos a los que se les ha asignado un determinado nivel de riesgo estableciendo sobre estos parámetros previsiones sobre el riesgo de reincidencia delictiva[20].

Actualmente, las herramientas más recientes de evaluación del riesgo se valen de algoritmos para emitir un pronóstico recurriendo a sistemas de Inteligencia Artificial. Se parte de una base actuarial utilizando un conjunto de datos que cruza siguiendo un esquema llamado algoritmo que ofrece diversas perspectivas de solución basándose en criterios estadísticos de forma automática y objetiva. El cambio no viene motivado por acudir a un nuevo método sino porque se usa una herramienta tecnológica que procesa de forma "inteligente" los algoritmos que sirven de base al procedimiento actuarial[21].

III. LA VALORACIÓN DEL RIESGO POR LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

El nuevo paradigma de proceso penal hacia el que nos encaminamos viene de la mano de la irrupción de las nuevas tecnologías que hace que podamos hablar de una nueva era en la Justicia en la que, junto a la progresiva digitalización del proceso, comienzan a emerger nuevos conceptos que cada vez nos resultan más familiares. Estos nuevos conceptos se identifican con la era 4.0, con los sistemas de Inteligencia Artificial, que aun cuando vienen ya desde hace tiempo aplicándose al proceso, lo cierto es que el avance que su utilización irá experimentando, en sintonía con los tiempos que corren, está abriendo nuevos retos para los diversos ordenamientos jurídicos comportando una importante innovación, en lo que a este trabajo atañe, para el Derecho Procesal y el Derecho Penal. Esta nueva era tecnológica propicia la aparición de nuevos métodos de investigación que vienen caracterizados por una mayor eficacia pero que, al mismo tiempo, pueden llegar a provocar un grave quebranto de los derechos fundamentales de las personas[22]. Ciertamente, el uso de estos recursos tecnológicos se extiende a una ya infinidad de actividades que enmarcan la vida de las personas como pueden ser con las decisiones que están relacionadas con la concesión de un préstamo, la contratación de un seguro privado de vida, el reconocimiento de un crédito, la automatización y mejora de la productividad del tejido empresarial, en el ámbito

20. SANZ MORAN, "La peligrosidad criminal. Problemas actuales", *cit.*, p. 75.
21. ROMEO CASABONA, C.M., *Riesgo, procedimientos actuariales basados en Inteligencia Artificial y medidas de seguridad*, *cit.*, p. 47.
22. BORGES BLÁZQUEZ, R., *Inteligencia Artificial y proceso penal,* Ed. Aranzadi, Pamplona, 2021, p. 111.

sanitario… llegando incluso en países como China a establecer un sistema que clasifica el civismo de sus ciudadanos a través de un sistema de crédito social en el que ganan o pierden puntos en función de las normas establecidas y de su comportamiento en sociedad y todo ello en base a las acciones que quedan registradas en red.

En lo que hace al ámbito judicial, y más en concreto al proceso penal, estas herramientas de valoración del riesgo vienen experimentando un crecimiento exponencial introduciéndose plenamente en la práctica forense, especialmente en los sistemas del *Common Law,* en donde se utilizan para decidir cuestiones tales como la suspensión de la pena (*probation)*[23], la libertad condicional (*parole),* el nivel de supervisión que debe acompañar a ambas, la imposición o no del *civil commitment* a los *sexual violent predators*[24]*,* incorporándose también en la fase de determinación de la pena *(evidence-based sentencing o smart sentencing)*, al incorporar valoraciones de riesgo como uno de los criterios a tener en cuenta a la hora de establecer el tipo y la cuantía de la pena, con la finalidad de reducir la reincidencia[25]. Para los defensores de este tipo de herramientas de valoración del riesgo, su utilización en fase de sentencia contribuye a evitar el riesgo de reiteración delictiva en base, no a una impresión subjetiva del juez sobre el grado de peligro que presenta un sujeto, sino fundamentándose en conocimientos rigurosos y empíricamente motivados sobre la existencia de dicho riesgo. Además, se abre un nuevo panorama que nos enfrenta a nuevas metodologías aplicables a los procesos actuariales que van a tener una notable influencia en el marco del proceso penal al incorporar sistemas de Inteligencia Artificial en la valoración de riesgos cuyos

23. *Aproximación al sistema de probation como alternativa a la prisión,* www.vidalabogados.eu.com. "El término *probation* alude al método que se utiliza para el tratamiento de determinados delincuentes seleccionados, al que voluntariamente se someten, y que consiste en la suspensión de la persecución del delito o de la ejecución de la condena o de la pena impuesta, durante un plazo de prueba en el que, con o sin condiciones, el sujeto queda en libertad bajo la vigilancia y asistencia de una persona que se encarga de orientarle y tutelarle, de manera que superado el plazo de prueba y cumplidas las condiciones, obtiene como beneficio bien la extinción de la acción penal y el archivo del proceso, bien la remisión definitiva de la condena, bien de la pena impuesta". *Vid.* sobre ese sistema, LAFARGE TURPIN, C., *La figura de la suspensión de la ejecución de la pena en las legislaciones europeas. Especial referencia a la pena de probation,* IUS, Vol. I, núm. 1, julio 2019; MAQUEDA ABREU, M.L., *Suspensión condicional de la pena y probation,* Ed. Autor Editor, 2012; CID MOLINE, J., *La elección del castigo: suspensión de la pena o probation versus prisión,* Ed. Bosch, 2009.

24. Proceso por el cual si se determina por el Tribunal que se es una persona peligrosa sexualmente o que tiene una personalidad sexual psicopática, se confinara por un tiempo de periodo indeterminado en un centro de tratamiento estatal previa evaluación por un equipo que decidirá sobre proceder o no al confinamiento.

25. MARTÍNEZ GARAY, L., *Peligrosidad, algoritmos y due process: el caso State v Loomis, cit.,* pp. 488 y ss.

resultados resultarán determinantes para valorar aspectos tan cruciales como imposición o no de programas de rehabilitación, régimen de libertad condicional o prisión provisional, imposición de medidas de seguridad e, inclusive, servir de fundamentación a la condena de una pena de prisión de larga duración. Estas herramientas que pueden ayudar a determinar el peligro de reincidencia delictiva, de revictimización e, inclusive, de comisión de un ilícito penal, se basan en la utilización de un gran número de datos, tanto de carácter personal como de otro tipo, que procesados a través de algoritmos pueden llegar a proporcionar unos resultados que servirán para predecir el posible comportamiento futuro de una persona en diversos ámbitos[26].

Por consiguiente, numerosas instituciones jurídicas como la libertad condicional, las medidas de seguridad o la suspensión de la pena, entre otras, exigen del juez un pronunciamiento en función de estimaciones sobre como el sujeto va a comportarse en el futuro y, especialmente, sobre si existe riesgo de reincidencia delictiva. Tal como ha quedado expuesto, la necesidad de dar satisfacción a estas demandas legales ha traído como consecuencia una investigación exhaustiva sobre los factores asociados a un mayor riesgo de violencia, multiplicando los instrumentos diseñados para evaluar dicho riesgo, al tiempo que el tradicional concepto de peligrosidad iba siendo sustituido por el de valoración de riesgo[27]. En las siguientes líneas analizaremos algunas de estas herramientas que, valiéndose de sistemas de Inteligencia Artificial, se encaminan a determinar los factores de riesgo en fase de ejecución de sentencias y para la adopción de medidas cautelares.

1. ANÁLISIS DEL RIESGO POR LAS HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL EN LAS MEDIDAS CAUTELARES

Si hay algo que caracteriza a las medidas cautelares de naturaleza personal es el fuerte impacto que destilan en la esfera de los derechos fundamentales de las personas, impacto que es sin duda más prominente cuando nos referimos a la prisión provisional. Sabido es que el fundamento de las medidas cautelares viene estrechamente vinculado al tiempo que transcurre desde que se inicia el proceso hasta que este finaliza por

26. DE HOYOS SANCHO, M., "El uso jurisdiccional de los sistemas de Inteligencia Artificial y la necesidad de su armonización en el contexto de la Unión Europea", *Revista General de Derecho Procesal*, núm. 55, 2021, p. 3.

27. MARTÍNEZ GARAY, L., "Problemas conceptuales y de comunicación en la evaluación del riesgo de reincidencia y su aplicación al sistema penal: el ejemplo de RisCanvi" en *Peligrosidad criminal y Estado de Derecho,* ORTS BERENGUER, E., ALONSO RIMO, A., ROIG TORRES, M., Ed. Tirant lo Blanch, Valencia, 2017, p. 342.

sentencia firme, tiempo que puede ser utilizado para hacer peligrar una posible sentencia de condena. La decisión judicial que se pronuncia sobre la adopción de una medida cautelar parte de una doble premisa que atiende, en primer lugar, a la probabilidad de que contra el investigado se emita una sentencia condenatoria *(fumus boni iuris),* esto es, indicios suficientes que permitan mantener la imputación de un hecho delictivo al sujeto afectado por las medidas en caso de medidas personales o la responsabilidad civil del mismo, y, en segundo lugar, a la probabilidad de que la libertad del imputado entrañe una grave afectación del proceso, bien por riesgo de fuga, bien por desaparición de pruebas, o, en el caso de medidas patrimoniales, riesgo de ocultación de la cosa o de insolvencia *(periculum in mora)*. En este contexto, se trata de dilucidar si la concurrencia de riesgos-peligros que pueden justificar la adopción de una u otra medida cautelar puede experimentar una mayor objetividad con la incorporación de estos sistemas algorítmicos[28].

La probabilidad de que el proceso culmine con una sentencia condenatoria contra el imputado, trasladado a la órbita procesal penal *fumus commissi delicti,* así como la peligrosidad o peligro de fuga, *periculum libertatis,* se efectúa por el juez de manera prospectiva, esto es, se trata de una hipótesis sobre hechos futuros[29], adoptándose decisiones en un contexto de relativa incertidumbre, en el que resulta esencial efectuar una adecuada valoración de los riesgos. La utilización de herramientas tecnológicas en esta fase del proceso puede resultar especialmente controvertida ya que buena parte de las medidas que pueden acordarse son restrictivas del derecho a la libertad y se aplican a un sujeto que aún no ha sido enjuiciado ni condenado[30] y que resulta amparado por el principio de presunción de inocencia. Además, estas circunstancias se tornan especialmente complejas cuando hacemos referencia a la prisión provisional al ser la medida cautelar personal más gravosa y restrictiva de los derechos del encausado al suponer la privación de libertad del sujeto que la padece.

Cuando un juez adopta una medida cautelar aplica un proceso cognitivo complejo "que viaja desde las estructuras teóricas basadas en la experiencia, la memoria y los cálculos estadísticos, hasta la adopción de

28. GÓMEZ COLOMER, J.L., BARONA VILAR, S., *Proceso Penal. Derecho Procesal III,* Ed. Tirant lo Blanch, Valencia, 2021, p. 324.
29. VALENZUELA SALDIAS, J., "Hacia un estándar de prueba cautelar en materia penal: algunos apuntes para el caso de la prisión preventiva", *Política Criminal*, vol. 13, núm. 26, diciembre 2018, p. 841-842.
30. NEIRA PENA, A.M., "Inteligencia Artificial y tutela cautelar. Especial referencia a la prisión provisional", *Revista Brasileña de Direito Processual Penal*, vol. 7, núm. 3, septiembre-diciembre, 2021, p. 1900.

una medida o decisión congruente con el precedente"[31]. En ningún caso estas medidas pueden considerarse una pena anticipada, sino que responden a la necesidad de enervar o mitigar un determinado riesgo bien de fuga, bien de reiteración delictiva o bien de destrucción de pruebas, en ocasiones en una fase muy incipiente del proceso en la que deben adoptarse decisiones de extraordinaria relevancia en base a indicios no siempre suficientemente sólidos. El proceso mental que sigue un juez a la hora de tomar una determinada decisión parte de unos apoyos que se conocen como heurísticos[32], o lo que es lo mismo, directrices generales que se siguen por las personas para tomar una determinada decisión[33], produciéndose, en múltiples ocasiones, una suerte de automatismo en la toma de decisiones en relación con casos parecidos o análogos que han sido resueltos con anterioridad que, en buena parte, encuentra su justificación en la sobrecarga de trabajo a la que se ven expuestos nuestros jueces. Centrándonos en la prisión provisional, por ser la medida cautelar más invasiva[34], la Ley de Enjuiciamiento Criminal apunta que tan solo habrá de adoptarse "cuando objetivamente sea necesaria y cuando no existan otras medidas menos gravosas" (art. 502.2 LECR), estando sometida al principio de legalidad, y siendo una medida excepcional, subsidiaria, provisional y proporcionada al logro de fines constitucionalmente legítimos[35]. Pues bien, la carga de trabajo y las consecuencias que se pueden derivar de una indebida denegación son las razones que motivan a muchos jueces a no apartarse de la petición del Ministerio Fiscal, reforzándose "el anclaje basado en la comodidad y la necesaria reducción de carga de trabajo, la accesibilidad y la disponibilidad en relación con aquellos argumentos que

31. SIMÓN CASTELLANO, P., *Justicia cautelar e Inteligencia Artificial: la alternativa a los atávicos heurísticos judiciales,* Ed. Bosch, 2021, p. 120.

32. En relación a esta cuestión, el estudio pionero se debe a los psicólogos israelíes TVERSKY y KAHNEMANN, *Judgement under uncertainty: Heuristics and Biases,* Revista Science, 1974. Estos autores procedieron a relacionar y sistematizar estas reglas heurísticas definiéndolas como aquellas reglas cognitivas que, inconscientemente, todo ser humano aplica al procesar la información que recibe del exterior y que permiten "reducir las tareas complejas de asignar probabilidad y predecir valores a operaciones de juicio mas simples".

33. NIEVA FENOLL, J., *Inteligencia Artificial y Proceso Judicial, cit.,* pp. 45-60, que distingue entre heurístico de representatividad, de accesibilidad, de anclaje y ajuste y de afección.

34. MORENO CATENA, V., CORTÉS DOMÍNGUEZ, V., *Derecho Procesal Penal,* Ed. Tirant lo Blanch, Valencia, 2019, p. 331, apunta que la prisión provisional "se sitúa desde luego en el campo de tensión entre el deber estatal de perseguir eficazmente el delito y el deber, también estatal, de asegurar el ámbito de libertad del ciudadano, de modo que en esta medida cautelar se refleja, más que en ninguna otra institución jurídica –más incluso que en la propia pena–, la ideología política que subyace a un determinado ordenamiento".

35. SSTC 127/1984, 241/1994 o 147/2000.

el juzgador tiene más cerca, esto es, lo que solicita o interesa la medida, es decir, el Ministerio Fiscal y la representatividad"[36]. Como se ha señalado en diversos estudios empíricos, dentro del campo de las decisiones judiciales el anclaje ha resultado ser el heurístico por excelencia en la jurisdicción penal y, en concreto, el anclaje considerado como la superposición de la condena impuesta por el Juez en relación a la petición del Ministerio Fiscal alcanza un impacto aproximadamente del 60% de las resoluciones[37]. Pero, además, conviene no olvidar que estos procesos mentales empleados por el juez no están exentos de sesgos y que estos, junto a los ya referidos automatismos, se producen en el proceso cautelar con una probabilidad mayor que en la sentencia cuya base la constituyen las pruebas que se practican en fase de juicio oral[38].

En este contexto, la valoración del *periculum* o riesgos concretos que las medidas cautelares tratan de precaver por herramientas de Inteligencia Artificial pueden llegar a resultar especialmente útiles habiendo alcanzado, a día de hoy, un elevado grado de complejidad al emplear algoritmos de aprendizaje automático que generan modelos de riesgos en base a ingentes cantidades de datos. Así, si lo que se trata de evitar es el riesgo de fuga, la propia Ley de Enjuiciamiento Criminal aporta en su artículo 503.3 un conjunto de indicadores que atienden a la naturaleza del hecho, a la gravedad de la pena que pueda llegar a imponerse al investigado o encausado, su situación familiar, laboral y económica, así como la inminente celebración del juicio oral. De igual forma la jurisprudencia hace referencia a la posibilidad de una pena alta, a la existencia de fugas anteriores, a la resistencia en el momento de la detención, a la pertenencia a banda organizada, a la tenencia de domicilio fijo o de medios económicos de que disponga el reo[39].

Si lo que se busca es mayor objetividad a la hora de evaluar los peligros por los sistemas de Inteligencia Artificial habrá que partir de la materia prima, esto es, de las bases de datos de las que se nutre el algoritmo que

36. SIMÓN CASTELLANO, P., *Justicia cautelar e Inteligencia Artificial: la alternativa a los atávicos heurísticos judiciales, cit.*, p. 122.

37. FARIÑA, F., ARCE, R., NOVO, M., "Heurístico de anclaje en las decisiones judiciales", *Psicothema,* vol. 14, núm. 1, 2002, estudio en el que se analizaron un total de 555 sentencias dictadas por los Juzgados de lo Penal y las Audiencias Provinciales de la Comunidad Autónoma Gallega entre los años 1980 a 1995, midiendo el efecto de anclaje en relación a la fijación de la pena, tomando como referencia la previa calificación de la Fiscalía, resultando que un porcentaje superior al 60% de las sentencias estaban guiadas por un efecto de anclaje en relación a la petición del MF.

38. SIMÓN CASTELLANO, P., *Justicia cautelar e Inteligencia Artificial: la alternativa a los atávicos heurísticos judiciales, cit.*, p. 131.

39. NIEVA FENOLL, J., *Inteligencia Artificial…, cit.*, pp. 75-76, en las que enumera diversos autos de Juzgados de Instrucción relativos a esta materia.

aplicados en esta contexto han de tener en cuenta los datos del precedente, el análisis de la jurisprudencia anterior, así como toda la información que obra en la causa que contribuyen a proporcionar al juez resultados estadísticos sobre la posibilidad de que el investigado se acabe sustrayendo a la acción de la justicia. No obstante, se corre el riesgo de caer en el automatismo de una forma más acusada que si la decisión emanara de un órgano judicial, ya que, al reproducir los patrones de decisión en base a resoluciones ya acordadas, se evita el entrar a conocer de una forma verdaderamente individualizada y atendiendo a las particularidades del caso concreto[40], por lo que resulta de todo punto esencial que el sistema maneje datos no solo referidos a casos anteriores, sino también al caso concreto a través del volcado de toda la información que obra en la causa.

Junto con evitar el peligro de fuga, otra de las finalidades de la prisión provisional prevista en la Ley de Enjuiciamiento Criminal es la de evitar el riesgo de reiteración delictiva, finalidad esta particularmente delicada cuando se acoge en fase de medidas cautelares ya que nos encontramos con un sujeto amparado por el principio de la presunción de inocencia, cosa muy distinta de cuando se utiliza este mismo parámetro respecto de un reo condenado del que ya se ha probado su responsabilidad delictiva. Aplicar algoritmos utilizando el riesgo de reincidencia delictiva en fase de medidas cautelares o, inclusive, para determinar la pena en las sentencias ha merecido fuertes críticas por parte de un amplio sector doctrinal que alerta, no sin razón, de los peligros que entraña el que una máquina pueda llegar a decidir automáticamente la libertad o prisión de las personas basado en un elemento de justicia predictiva. Distinto es que este riesgo de reincidencia delictiva se utilice en fase de ejecución de sentencia, ya que aquí partimos de posibilidades más altas de acierto refrendadas por una sentencia firme de condena.

Ahora bien, lo cierto es que en nuestro ordenamiento procesal la legitimidad de la reiteración delictiva como finalidad de la prisión provisional ha venido refrendada tanto por nuestro Tribunal Constitucional[41], como por el Tribunal Europeo de Derechos Humanos que, conforme a los artículos 5.1 c) y 5.3 del CEDH, permite a los Estados mantener una privación cautelar de libertad con carácter previo al juicio como medio de prevención de una concreta y específica infracción penal, fundamentada en hechos o informaciones concretas basadas en datos objetivos[42]. Por consiguiente, si

40. NEIRA PENA, A.M., *Inteligencia Artificial y tutela cautelar. Especial referencia a la prisión provisional, cit.*, p. 1912.
41. SSTC 128/1995, de 26 de julio y 27/2008, de 11 de febrero.
42. SSTEDH de 6 de noviembre de 1980, caso *Guzzardi c. Italia;* de 7 de marzo de 2013, caso *Ostendorf c. Alemania* y de 28 de octubre de 2014, caso *Urtans c. Letonia.*

se admite este juicio de peligrosidad de un sujeto cuando aún tiene a su favor la presunción de inocencia por la vía de las máximas de experiencia en el razonamiento judicial, se cuestiona por algunos autores el motivo por el que no podrán ser usadas las herramientas de Inteligencia Artificial si revisten las suficientes garantías. Hay que partir que estas herramientas almacenan más datos que la propia experiencia del Juez por lo que puede convertirse en un valioso punto de apoyo a la actuación judicial en la toma de estas decisiones siempre que sea transparente y no discriminatoria[43].

Sobre este particular, es necesario hacer referencia al caso *Eric Loomis* y a la correspondiente resolución emanada de la Corte de Wisconsin en el año 2016, por suponer un claro ejemplo de aplicación práctica de las herramientas de Inteligencia Artificial que se utilizan para predecir comportamientos futuros, así como de los riesgos que su utilización puede conllevar si no se observan las garantías suficientes. Dicha sentencia fue dictada haciendo uso del algoritmo predictivo contenido en el *software* denominado COMPAS concebido para determinar el grado de peligrosidad de una persona, el riesgo de reincidencia delictiva y como herramienta para ayudar a los jueces en la determinación de la pena. En la fase de investigación preliminar se redactó un informe que incluía una valoración del riesgo de reincidencia, *risk assessment*, ofreciendo una puntuación, conforme a la cual el Tribunal le condenó a la pena de seis años a la vista de los resultados de la aplicación del algoritmo. Tras esta condena el Sr. Loomis interpuso el correspondiente recurso al considerar que se le había vulnerado el derecho a un proceso justo al haber sido condenado en base a datos suministrados por el programa y no en informaciones precisas sobre su persona, ya que COMPAS, aparte de estar amparado por el secreto comercial, suministra datos por grupos de individuos. El recurso fue desestimado por considerar la Corte Suprema de Wisconsin la legitimidad del uso del algoritmo predictivo para valorar el riesgo de reincidencia, si bien declara que no puede ser el único elemento que fundamente la sentencia condenatoria. Finalmente, la Corte Suprema de Estados Unidos confirmó esta resolución[44].

43. DE HOYOS SANCHO, M., "El Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: Reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo", *Revista Española de Derecho Europeo*, *cit*., nota 60, p. 32.

44. Un estudio exhaustivo de este caso puede verse en DE HOYOS SANCHO, M., "El Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: Reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo", *Revista Española de Derecho Europeo*, núm. 79, octubre-diciembre, 2020, pp. 25 y ss., concluye la autora que "en consecuencia, a pesar de la aparente neutralidad y objetividad de este tipo de algoritmos predictivos, tal y como está concebido el *software COMPAS* se puede concluir que su utilización vulnera el derecho de defensa, la igualdad de partes y la necesaria transparencia en los sistemas utilizados en la adopción de decisiones

La trascendencia de este caso se explica por apuntalar los principales problemas a los que se enfrentan este tipo de algoritmos predictivos, a saber, en primer lugar, la imposibilidad de conocer los datos de los que se nutre el sistema y si estos están o no sesgados y, en segundo lugar, el carácter opaco de estos sistemas para los operadores jurídicos, una suerte de caja negra, *black box*, que, conforme a un resultado numérico, ofrece una puntuación determinada que marca la adopción de una medida cautelar, de un permiso penitenciario o el contenido de una sentencia, entre otros. Referido a este programa concreto, una de las principales críticas que se han vertido sobre el mismo viene referido a que los indicadores de riesgo son marcadamente racistas al multiplicarse notablemente la puntuación del algoritmo por el mero hecho de ser el investigado o acusado de origen afroamericano. La necesidad de contar con la intervención del Juez en la decisión final es, a día de hoy, una premisa indubitada; estas herramientas han de servir como instrumentos de apoyo o asesoramiento en la toma de decisiones judiciales ya que una resolución fundada exclusivamente en el resultado de la aplicación de un algoritmo no puede estimarse respetuosa con las garantías del debido proceso[45].

Finalmente, otra de las finalidades justificativas de la prisión provisional hace referencia a la necesidad de evitar el riesgo de destrucción de pruebas, resultando de nuevo necesario de cara a su valoración la combinación de datos del caso concreto junto a los datos análogos de casos pasados. La jurisprudencia suele tomar en consideración actuaciones del reo encaminadas a preparar coartadas o eliminar o manipular vestigios del delito[46], la peligrosidad de la actuación delictiva en su conjunto[47], la posición de poder que ejerza el reo en una organización[48], la posibilidad de colaboración en la destrucción de pruebas por un entorno cercano al reo[49], o el carácter reciente de los hechos que puede aumentar la voluntad

judiciales; por mucho que, como indicó la Corte Suprema de Wisconsin, no pueda ser el único elemento que fundamente la sentencia condenatoria".

45. COTINO HUESO, L., "¿A quién sanciono? Garantías frente al uso de la Inteligencia Artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", *La Ley Privacidad*, núm. 4, 2020.
46. NIEVA FENOLL, J., *Inteligencia Artificial y Proceso Judicial, cit.,* p. 65, citando en nota 10 el auto del Juzgado de Instrucción núm. 7 de Alicante, de 10 de febrero de 2017, núm. rec., 2526/2016.
47. NIEVA FENOLL, J., *Inteligencia Artificial y Proceso Judicial, cit.,* p. 65, citando en nota 12 el Auto Juzgado de Instrucción núm. 3 de Pamplona, de 27 de noviembre de 2012, núm. rec. 2708/2012.
48. NIEVA FENOLL, J., *Inteligencia Artificial y Proceso Judicial, cit.,* p. 65, citando en nota 13 el Auto Juzgado de Instrucción núm. 3, de 9 de marzo de 2018, núm. rec. 82/2017.
49. NIEVA FENOLL, J., *Inteligencia Artificial y Proceso Judicial, cit.,* p. 65, citando en nota 14 el Auto Juzgado de Instrucción núm. 6, de 5 de octubre de 2016, núm. rec. 85/2014.

de destruir las pruebas[50]. En este escenario, los sistemas de Inteligencia Artificial si pueden ser útiles para valorar cual es la probabilidad real de que el investigado pueda obstaculizar la investigación ocultando o destruyendo pruebas ofreciendo un cálculo basado en ingentes capacidades de almacenamiento y procesamiento de información[51], si bien para huir del automatismo resulta esencial conectarla con las circunstancias del caso concreto.

2. INTELIGENCIA ARTIFICIAL EN FASE DE EJECUCIÓN DE LA PENA. ESPECIAL REFERENCIA A *RISCANVI*

Los permisos de salida penitenciarios juegan un papel esencial en los procesos de reinserción y rehabilitación de los internos ya que sirven para preparar la vida en libertad contribuyendo a reducir el riesgo de reincidencia futura en la comisión de nuevos delitos. A día de hoy, se considera que los permisos de salida resultan una herramienta esencial en la intervención penitenciaria y forman parte del programa individualizado de tratamiento para cada interno[52]. Si bien resultan ser un instrumento muy relevante para la rehabilitación de los internos, lo cierto es que la concesión de estos permisos comporta unos peligros asociados al incumplimiento de las obligaciones que de ellos dimanan, así como un aumento de las posibilidades de que se cometan nuevos delitos[53].

En este contexto, la valoración del riesgo de quebrantamiento de permisos de salida resulta extremadamente útil en el proceso de toma de decisiones que llevan a cabo los funcionarios penitenciarios a la hora de decidir la concesión o no de un permiso de salida. Tal como se desprende del artículo 6 del Reglamento Penitenciario "ninguna decisión de la Administración penitenciaria que implique la apreciación del comportamiento humano de los reclusos podrá fundamentarse, exclusivamente, en un tratamiento automatizado de datos o informaciones que ofrezcan una definición del perfil o de la personalidad del interno". De su lectura parece colegirse que, si bien es cierto que la normativa impide que estos

50. NIEVA FENOLL, J., *Inteligencia Artificial y Proceso Judicial, cit.,* p. 65, citando en nota 15 el Auto Juzgado de Instrucción núm. 6, de 27 de julio de 2017, núm. rec. 91/2016.
51. SIMÓN CASTELLANO, P., *Justicia cautelar e Inteligencia Artificial: la alternativa a los atávicos heurísticos judiciales, cit.,* p. 156.
52. FÉREZ-MANGAS, D., ANDRÉS-PUEYO, A., *Predicción y prevención del quebrantamiento de los permisos penitenciarios,* Revista Española de Investigación Criminológica, núm. 13, 2015, p. 3.
53. FÉREZ-MANGAS, D., ANDRÉS-PUEYO, A., *Eficacia predictiva en la valoración del riesgo del quebrantamiento de permisos penitenciarios,* La Ley Penal, núm. 134, septiembre-octubre, 2018, p. 2.

instrumentos de valoración y gestión del riesgo ocupen una posición hegemónica, son conformes a Derecho siempre y cuando no resulten ser exclusivos, esto es, que no monopolicen la decisión judicial.

En nuestro país se utilizan dos instrumentos específicos de valoración de riesgo; así, en primer lugar, las Tablas de Variables de Riesgos (TVR) y de Concurrencia de Circunstancias Peculiares (CCP) en todas las prisiones gestionadas por la Secretaría General de Instituciones Penitenciarias y, en segundo lugar, el protocolo *RisCanvi* en los centros penitenciarios ubicados en la comunidad autónoma catalana, consecuencia de la transferencia de competencias en materia penitenciaria a favor de esta autonomía.

Comenzando por las Tablas de Variables de Riesgo y de Circunstancias Peculiares fueron las primeras herramientas de naturaleza actuarial del sistema penitenciario español[54], residiendo su finalidad en analizar el riesgo que supone otorgar un permiso de salida ordinario a un determinado sujeto. La Tabla de Variables de Riesgo consta de diez factores de riesgo que atienden a extranjería, drogodependencia, profesionalidad delictiva, reincidencia, quebrantamientos, ausencia de permisos, artículo 10 de la LOGP, deficiencia convivencial, lejanía o presiones internas a las que puede haber estado sometido. Una vez obtenida una puntuación en cada una de las variables se emplea una fórmula matemática, denominada ecuación de riesgo, para determinar la puntuación global o final del riesgo en cada supuesto. Esta valoración se complementa con la Tabla de Concurrencia de Circunstancias Peculiares compuesta por otras variables que deben ser tenidas en cuenta a la hora de valorar o no la concesión de un permiso y que atienden, entre otras, a circunstancias como si el condenado pertenece a una organización delictiva, la transcendencia social del delito, el tiempo que le resta al interno para cumplir las ¾ partes de la condena, o si presenta alteraciones psicopatológicas. La Tabla de Variables de Riesgo es un dato a valorar en conjunto con el resto de circunstancias peculiares, siendo la presencia y el grado de cada una de estas variables determinada por los profesionales de la Junta de tratamiento.

En relación a la eficacia predictiva de ambas Tablas no existen datos empíricos que demuestren su capacidad predictiva, salvo uno realizado en el año 1993 en relación a la Tabla de Valoración de Riesgo, si bien son utilizadas frecuentemente en la toma de decisiones para la concesión o no de un permiso penitenciario aun cuando ambas tablas contienen fallos y no deben ser tomadas como algo totalmente fiable. Además, estas Tablas, que en su momento supusieron un hito al colocar a nuestro sistema penitenciario en la vanguardia en lo que hace a la gestión y predicción del

54. Estas Tablas entraron en vigor por Instrucción 22/1996, de 16 de diciembre.

riesgo de quebrantamientos de permisos penitenciarios, no ha venido acompañada de la necesaria revisión de sus *ítems* en cerca ya de tres décadas necesitando de una revisión en profundidad[55].

Por su parte, el protocolo *RisCanvi* es una herramienta desarrollada por el Grupo de Estudios Avanzados en Violencia de la Universidad de Barcelona y los Servicios Penitenciarios de la Generalitat de Cataluña para gestionar no solo la valoración del riesgo, sino los programas más adecuados para influir en los factores de riesgo presentes en cada sujeto con el objetivo de mejorar la reinserción social de los condenados. *RisCanvi* permite estimar la probabilidad de ocurrencia de cuatro tipos de riesgos diferentes, en concreto, el quebrantamiento de condena, la violencia intrainstitucional, la reincidencia violenta y la violencia autodirigida. Este protocolo se administra por medio de un programa informático, el *eRisCanvi,* que consta de dos formatos, el denominado *Screening*[56] o de cribado, con diez factores de riesgo, y el Completo, con cuarenta y tres factores de riesgo[57] cuyas versiones se complementan con otras variables de clasificación que pueden ser tenidas en cuenta como factores de riesgo y que hacen referencia al sexo, edad, nacionalidad y situación procesal, clasificando a los penados en niveles de riesgo obtenidos mediante un procedimiento actuarial.

En relación a la eficacia predictiva del protocolo *RisCanvi,* la configuración actual de la versión *Screening* presenta, a juicio de los expertos, deficiencias atribuibles al algoritmo y a la combinación de factores de riesgo que indican la conveniencia de sustitución de aquellos factores que no se asocien al quebrantamiento y su sustitución por otros que permitan mejorar su capacidad predictiva. Por su parte, la versión Completa utiliza factores de riesgo que no se asocian al quebrantamiento de permiso limitando e influyendo de forma negativa en la valoración futura del riesgo de quebrantamiento[58]. De este modo, cada interno es monitorizado por la Junta de Tratamiento a través de psicólogos, trabajadores sociales,

55. FÉREZ-MANGAS, D., ANDRÉS-PUEYO, A., *Eficacia predictiva en la valoración del riesgo del quebrantamiento de permisos penitenciarios*, *cit*., pp. 9 y ss.
56. Los factores de riesgo son: inicio de la actividad delictiva, historia de violencia, problemas con conducta penitenciaria, quebrantamientos o incumplimientos, drogodependencia o alcoholismo, respuesta al tratamiento psicológico o psiquiátrico, intentos de autolesión, falta de recursos económicos, falta de apoyo familiar o social y valores pro-criminales.
57. A título ilustrativo, algunos de los factores de riesgo son: edad en el momento de la comisión del hecho delictivo, delito violento, duración de la pena, conflictos con internos, expedientes disciplinarios, regresión en grado, falta de planes de futuro, falta de apoyo familiar…
58. FÉREZ-MANGAS, D., ANDRÉS-PUEYO, A., *Eficacia predictiva en la valoración del riesgo del quebrantamiento de permisos penitenciarios*, *cit*., p. 10.

juristas… siendo la encargada de realizar las valoraciones a través de una lista de factores de riesgo que son analizados con la ayuda de un programa informático al que se aplican unos algoritmos que permiten efectuar un pronóstico. Antes de la aparición de estos programas el análisis de la posibilidad de quebrantamiento se hacía a partir del juicio clínico y la experiencia, imperando la intuición en unos resultados que adolecían de falta de seguridad. Por esta razón, el uso de herramientas o protocolos diseñados con esta finalidad que utilizan sistemas de valoración más precisos y contrastados, resultan esenciales de cara a determinar la probabilidad futura de no retorno o incumplimiento.

Ciertamente, ningún pronóstico resulta infalible y más cuando se trata de comportamientos humanos. No obstante, tal como se afirma en el Auto 498/2018 de la Audiencia Provincial de Barcelona[59] a través del protocolo *RisCanvi,* junto con la valoración efectuada de forma individualizada por los profesionales que están en contacto directo con el interno, "se hacen predicciones rigurosas. De ahí que cuando el resultado, tanto del *RisCanvi* como de los miembros del equipo de tratamiento, sea de riesgo bajo, no existen motivos razonables para denegar el permiso, con independencia de la naturaleza del delito y gravedad de la pena, ya que se han valorado todos los factores de riesgo, incluyendo especialmente la clase y gravedad del delito, y se ha concluido que el riesgo de reiteración delictiva o de quebrantamiento de condena es bajo, y por tanto existe base fundada para considerar que el interno hará un buen uso del permiso. Como ya se ha dicho, es imposible asegurar ese extremo ya que nos movemos en el campo de las predicciones de comportamiento a futuro". En los supuestos de disconformidad entre la valoración de la junta de tratamiento, que defienda el permiso, y el protocolo *RisCanvi* que estime un riesgo alto o medio, la práctica demuestra que el Juez de Vigilancia Penitenciaria se vale más de este pronóstico, tal como se deduce de los datos que apunta como desde 2009 solo un 3,2% de las 89.638 veces que se ha aplicado *RisCanvi* se ha contradicho lo dispuesto por el algoritmo. A ello se une la alta tasa de falsos positivos presos que el algoritmo predice erróneamente que reincidirán, sobreestimando sistemáticamente la peligrosidad; en concreto, conforme al informe realizado por el Centro de Estudios Jurídicos de la Generalitat el 82% de los presos que *RisCanvi* tacho de peligrosos no volvieron a delinquir, si bien, como la otra cara de la moneda, tan solo dio un 4,6% de falsos negativos, esto es, de presos que clasificó de riesgo bajo y luego reincidieron, detectando correctamente como de alto o moderado riesgo al 77% de los reincidentes.

59. Auto que conoce de la concesión de un permiso tras la comisión de delito cometido en otro permiso hace 20 años. Sección 21.ª de 15 de marzo de 2018.

Con todo, este sistema tiene a su favor el haber sido diseñado merced a la colaboración de dos instituciones públicas, a diferencia de lo que viene siendo común en la mayor parte de los países, que es el comprar la tecnología a una empresa privada con todos los problemas que ello acarrea de falta de transparencia. No obstante, resulta ciertamente llamativo que tras casi doce años de su utilización en las prisiones catalanas no exista ningún mecanismo público que proceda a su evaluación permitiendo conocer el peso que tiene cada uno de los factores de riesgo que cambian según el género, edad u origen del preso. Por tanto, aun cuando el resultado sea público la información del peso de cada una de las variables no la conocen ni los jueces de vigilancia penitenciaria que aceptan o deniegan los permisos, ni los abogados, ni los funcionarios de prisión. Paradójicamente se repite el problema que impera cuando estas herramientas nacen de empresas privadas en la que la falta de trasparencia merma el derecho de defensa del condenado desconocedor de los motivos que justifican la eficacia predictiva del algoritmo. Transparencia algorítmica y auditoría pública siguen brillando por su ausencia aun cuando nos encontremos con una herramienta que nace de instituciones públicas.

IV. LA INCIDENCIA DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO AL DEBIDO PROCESO

Llegados a este punto, el dilema al que nos enfrentamos es si estas herramientas algorítmicas de valoración del riesgo resultan compatibles con el derecho al debido proceso. Ciertamente, la utilización de la Inteligencia Artificial en el proceso penal incide directamente en las garantías procesales alterando el modo de actuación de la policía y de los jueces y removiendo los cimientos del proceso, amén de hacer peligrar garantías y derechos básicos[60]. Y es que la línea roja en la incorporación de cualesquiera Inteligencia Artificial en el marco de la justicia penal se halla en el respeto a los derechos y garantías del sujeto investigado, acusado y de la víctima. El resultado algorítmico debe pasar un filtro de control anterior y posterior humano, habrá que garantizar transparencia tanto en su funcionamiento, como respecto a las personas que programan y supervisan. Para ello, lo óptimo sería que las personas encargadas de trabajar con estos sistemas pertenezcan al sector público con objeto de garantizar una mayor transparencia de estas herramientas que pueden llegar a afectar a la vida diaria de los ciudadanos; mientras ello no resulte posible lo ideal sería conseguir una cooperación cada vez más estrecha entre el

60. BARONA VILAR, S., *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Ed. Tirant lo Blanch, Valencia, 2021, p. 511.

sector privado y el sector público. Además, resultaría conveniente que se crearan equipos interdisciplinares constituidos por juristas, psicólogos, sociólogos, criminólogos e ingenieros, para evitar sesgos y que la información emane con las mayores dosis de objetividad posibles.

Es común que los algoritmos funcionen siguiendo un modelo de caja negra, es decir, el usuario tras introducir los datos en el modelo obtiene unos resultados, pero no sabe cuál es el camino por el que se ha llegado a los mismos. Otro de los problemas se deriva del hecho de que estas herramientas se basan en delitos conocidos y esclarecidos por los departamentos policiales. Si los datos que se introducen en el modelo presentan algún tipo de sesgo, se podría provocar la estigmatización de individuos o zonas que presenten las características que los algoritmos identifican como indicadores de riesgo. Los problemas basados en la falta de transparencia y la posible estigmatización si se trabaja con datos sesgados, han hecho que se llame la atención sobre las implicaciones éticas derivadas de estas herramientas y de cómo pueden vulnerar derechos como la intimidad y la protección de datos. Así, los detractores de estas herramientas se plantean si es ético actuar de alguna forma contra alguien que no ha cometido un delito aún, o si estuviese justificado monitorizar las acciones de determinados individuos para determinar su peligrosidad[61].

Pero, además, no podemos perder de vista que nos encontramos con un sistema algorítmico que no es infalible por lo que ha de ser siempre un apoyo a la labor policial o judicial pero no ha de tomarse como fundamento absoluto en la toma de decisiones; en todo caso, el control humano es necesario, así como la ratificación por otros elementos probatorios o por otras fuentes de información. Los sistemas algorítmicos predictivos pueden justificarse como colaboradores policiales y para proteger a determinadas víctimas, si bien su expansión general favorece la consolidación del modelo político del Estado policial, por lo que se ha de lograr un adecuado equilibro entre tecnología y derechos fundamentales, salvaguardando el derecho al debido proceso y con todas las garantías. Y es que alcanzar la seguridad a toda costa y potenciar un Derecho Penal cada vez más expansivo no han de ser los objetivos a alcanzar. La Inteligencia Artificial se ha de convertir en un poderoso aliado de la Justicia, pero no en la Justicia misma[62]. La adopción de tales sistemas puede contribuir a que los procedimientos legales sean más claros y rápidos, y también, en algunos aspectos, más fiables, pero estos sistemas de prevención de delitos,

61. GONZÁLEZ ÁLVAREZ, J. L., SANTOS HERMOSO, J., CAMACHO-COLLADOS, M., "Policía predictiva en España. Aplicación y retos futuros", *cit.*, p. 29.
62. LLORENTE SÁNCHEZ-ARJONA, M., "Big Data, Inteligencia Artificial y Violencia de Género", *Diario La Ley, Sección Ciberderecho*, 25 de marzo de 2021.

que pueden ser muy beneficiosos para la sociedad, deben ser legalmente controlados para evitar que lleguen a vulnerar derechos fundamentales de las personas.

El dilema se centra en el binomio seguridad pública *versus* derechos fundamentales, corriendo el peligro de seguir propiciando un Derecho Penal de la Seguridad cada vez más expansivo. Por tanto, sin duda alguna, el impacto del uso de la Inteligencia Artificial en los derechos humanos es el capítulo central de cara al futuro[63]. Conviene recordar que la Inteligencia Artificial es una creación humana, fruto de una actividad previa de datificación, automatización y robotización llevada a cabo por personas que diseñan e implementan su uso y sujeta en su funcionamiento y aplicación a las normas de derechos humanos y exigencia de responsabilidad[64]. Resulta incontestable que la Inteligencia Artificial tiene impacto, tanto positivo como negativo, en el ejercicio de los derechos humanos, en el funcionamiento de las sociedades democráticas y en el Estado de Derecho[65]. Por consiguiente, el principio de igualdad, la presunción de inocencia, el derecho de defensa, la protección de los datos personales y el derecho a un proceso justo no pueden verse afectados en ningún caso.

Comenzando con el derecho de defensa, este puede verse lesionado por no conocer los litigantes los algoritmos que la herramienta utiliza en la toma de sus decisiones, o más bien, como la máquina ha llegado a ese determinado resultado. Por tanto, resulta fundamental la desclasificación de los algoritmos, ya que si no se pueden rebatir los resultados por desconocer el *iter* que se ha seguido y el porqué de una concreta decisión el derecho de defensa podría dejar de existir[66]. Así mismo, se puede ver afectado el derecho a la intimidad, ya que para la investigación de los delitos no queda otra opción que restringir la intimidad de las personas para averiguar datos de su vida privada. Como hemos visto, para identificar posibles situaciones de reiteración delictiva se trabaja con millones de datos almacenados de forma aleatoria, para establecer patrones estadísticos, estableciéndose un perfil a las personas a las que se les atribuye un determinado patrón de tendencias.

63. NIEVA FENOLL, J., *Inteligencia Artificial y proceso judicial, cit.,* pp. 127.
64. MARTÍN DIZ, F., "Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial" en *Derecho Procesal. Retos y transformaciones,* BUJOSA VADELL, L., (Dir.), Ed. Atelier, Barcelona, 2021, p. 298.
65. Conclusiones de la Conferencia de Helsinki del Consejo de Europa el *Impacto del desarrollo de la Inteligencia Artificial en los derechos humanos, la democracia y el Estado de Derecho,* febrero de 2019.
66. *Vid.* sobre este particular, NIEVA FENOLL, J., *Inteligencia Artificial y proceso judicial, cit.,* pp. 139-150.

De igual forma, estas herramientas predictivas pueden poner en serio peligro al derecho fundamental de la presunción de inocencia. Ciertamente, el que las características de un sospechoso coincidan con un perfil de riesgo sin haber realizado una mínima actividad probatoria ya pone en serio peligro la presunción de inocencia[67]. Así, este derecho puede verse condicionado cuando una herramienta de inteligencia artificial utiliza cánones discriminatorios y sesgados en relación a determinados perfiles de personas por su origen, condición, raza, género, lugar de residencia o antecedentes penales.

Finalmente, puede verse afectado el principio de igualdad de armas entre partes por el uso de datos generados automáticamente a través de algoritmos que, generalmente, están protegidos por el derecho a la propiedad intelectual y que provocan la imposibilidad de acceder al "código fuente" del algoritmo que gobierna el sistema de Inteligencia Artificial y que hace prácticamente imposible impugnar los resultados que proporciona el sistema y que pueden ser utilizados en un proceso penal. Nos encontraríamos inmersos en un proceso caracterizado por una "asimetría o desequilibrio cognoscitivo"[68], ya que la parte pública y las grandes corporaciones tendrían acceso a la tecnología más moderna al disponer, por regla general, de más medios económicos de los que no gozan los particulares que no dispondrán de verdaderas opciones para rebatir o impugnar los resultados que emanen de los sistemas de Inteligencia Artificial. Sin transparencia, derechos fundamentales como el contradictorio y la paridad de armas entre partes pueden poner en grave peligro el derecho al debido proceso.

La Inteligencia Artificial va a cambiar el concepto y la práctica del Derecho, es más, podemos decir que ya lo está cambiando, pero a lo que no se puede renunciar, en aras a una mayor eficiencia, es al conjunto de derechos fundamentales y garantías procesales que han costado tanto esfuerzo conquistar. Además, la Inteligencia Artificial no puede contextualizar, por lo que la interpretación de la ley no podrá ser desempeñada de forma automatizada por un programa de *software*. En todo caso, estos sistemas han de verse como una ayuda a la actuación policial y judicial pero la automatización no debe suplir el factor humano que han de aprender a convivir en justo equilibrio, siempre con el horizonte del respeto a los derechos fundamentales de todo ser humano.

67. NIEVA FENOLL, J., *Inteligencia Artificial y proceso judicial, cit.*, pp. 150-154.
68. QUATTROCOLO, S., "Equita del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell uomo", *Revista italo-española de Derecho Procesal*, vol. 2, 2019, p. 12.

V. BIBLIOGRAFÍA

ACALE SÁNCHEZ, M. J., *Medición de la respuesta punitiva y Estado de Derecho,* Pamplona, 2010; ALONSO RIMO, A., *Medidas de seguridad y proporcionalidad con el hecho cometido (a propósito de la peligrosa expansión del Derecho penal de la peligrosidad),* Estudios Penales y Criminológicos, XXIX, 2009.

ANDRÉS-PUEYO, A., "Peligrosidad criminal: análisis crítico de un concepto polisémico" en *Neurociencias y derecho penal: Nuevas perspectivas en el ámbito de la culpabilidad y tratamiento jurídico-penal de la peligrosidad,* DEMETRIO CRESPO, E., (Dir.), 2020.

ARMAZA ARMAZA, E. J., *El tratamiento penal del delincuente imputable peligroso,* Ed. Comares, Granada, 2013.

BARONA VILAR, S., *Inteligencia artificial o la algoritmización de la vida y de la justicia ¿solución o problema?,* Revista Boliviana de Derecho, núm. 28, julio 2019.

– *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Ed. Tirant lo Blanch, Valencia, 2021.

– Prólogo de *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad),* Ed. Tirant lo Blanch, Valencia, 2022.

BORGES BLÁZQUEZ, R., *Inteligencia Artificial y proceso penal,* Ed. Aranzadi, Pamplona, 2021.

BORJA JIMÉNEZ, E., "Peligrosidad criminal e individualización judicial de la pena" en *Peligrosidad criminal y Estado de Derecho,* ORTS BERENGUER, E., ALONSO RIMO, A., ROIG TORRES, M., Ed. Tirant lo Blanch, Valencia, 2017.

CEREZO MIR, J, *Curso de Derecho Penal Español,* I, Ed. Tecnos, 6.ª ed., Madrid, 2004.

CID MOLINE, J., *La elección del castigo: suspensión de la pena o probation versus prisión,* Ed. Bosch, 2009.

COTINO HUESO, L., *¿A quién sanciono? Garantías frente al uso de la Inteligencia Artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020,* La Ley Privacidad, núm. 4, 2020.

DE HOYOS SANCHO, M., "El Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: Reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo", *Revista Española de Derecho Europeo*, núm. 79, octubre-diciembre, 2020.

– "El uso jurisdiccional de los sistemas de Inteligencia Artificial y la necesidad de su armonización en el contexto de la Unión Europea", *Revista General de Derecho Procesal*, núm. 55, 2021.

ESBEC RODRÍGUEZ, E., FERNÁNDEZ SASTRÓN, O., *Valoración de la peligrosidad criminal (riesgo-violencia) en psicología forense. Instrumentos de evaluación y perspectivas,* Psicopatología Clínica Legal y Forense, Vol. 3, núm. 2, 2003.

FARIÑA, F., ARCE, R., NOVO, M., *Heurístico de anclaje en las decisiones judiciales,* Psicothema, vol. 14, núm. 1, 2002.

FÉREZ-MANGAS, D., ANDRÉS-PUEYO, A., *Predicción y prevención del quebrantamiento de los permisos penitenciarios,* Revista Española de Investigación Criminológica, núm. 13, 2015.

– *Eficacia predictiva en la valoración del riesgo del quebrantamiento de permisos penitenciarios,* La Ley Penal, núm. 134, septiembre-octubre, 2018.

GÓMEZ COLOMER, J. L., BARONA VILAR, S., *Proceso Penal. Derecho Procesal III,* Ed. Tirant lo Blanch, Valencia, 2021.

GONZÁLEZ ÁLVAREZ, J. L., SANTOS HERMOSO, J., CAMACHO-COLLADOS, M., *Policía predictiva en España. Aplicación y retos futuros*, Behavior & Law Journal, vol. 6, núm. 1, 2020.

LAFARGE TURPIN, C., *La figura de la suspensión de la ejecución de la pena en las legislaciones europeas. Especial referencia a la pena de probation,* IUS, Vol. I, núm. 1, julio 2019.

LEAL MEDINA, J., *El concepto de peligrosidad en el Derecho penal español: proyección legal y alcance jurisprudencial. Perspectivas actuales y de futuro,* Diario La Ley, núm. 7870.

LLORENTE SÁNCHEZ-ARJONA, M., "Big Data, Inteligencia Artificial y Violencia de Género", *Diario La Ley, Sección Ciberderecho,* 25 de marzo de 2021.

– "Prueba e Inteligencia Artificial ¿buen maridaje?" en *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad),* Ed. Tirant lo Blanch, Valencia, 2022.

MAQUEDA ABREU, M. L., *Suspensión condicional de la pena y probation*, Ed. Autor Editor, 2012.

MARTÍN DIZ, F., "Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial" en *Derecho Procesal. Retos y transformaciones*, BUJOSA VADELL, L., (Dir.), Ed. Atelier, Barcelona, 2021.

MARTÍNEZ GARAY, L., *Peligrosidad, algoritmos y due process: el caso State v Loomis,* Revista de Derecho Penal y Criminología, 3.ª época, núm. 20, julio 2018.

– "Problemas conceptuales y de comunicación en la evaluación del riesgo de reincidencia y su aplicación al sistema penal: el ejemplo de RisCanvi" en *Peligrosidad criminal y Estado de Derecho,* ORTS BERENGUER, E., ALONSO RIMO, A., ROIG TORRES, M., Ed. Tirant lo Blanch, Valencia, 2017.

MONTESINOS GARCÍA, A., "Justicia penal predictiva" en *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad),* Ed. Tirant lo Blanch, Valencia, 2022.

MORENO CATENA, V., CORTÉS DOMÍNGUEZ, V., *Derecho Procesal Penal,* Ed. Tirant lo Blanch, Valencia, 2019.

NEIRA PENA, A. M., *Inteligencia Artificial y tutela cautelar. Especial referencia a la prisión provisional,* Revista Brasileña de Direito Processual Penal, vol. 7, núm. 3, septiembre-diciembre, 2021.

QUATTROCOLO, S., "Equita del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell uomo", *Revista italo-española de Derecho Procesal*, vol. 2, 2019.

ROMEO CASABONA, C. M., *Peligrosidad y Derecho penal preventivo,* Ed. Bosch, Barcelona, 1986.

– *Riesgo, procedimientos actuariales basados en Inteligencia Artificial y medidas de seguridad,* R.E.D.S., núm. 13, julio-diciembre 2018.

SANZ MORÁN, "La peligrosidad criminal. Problemas actuales" en *Delincuentes peligrosos,* Ed. Trotta, Madrid, 2014.

SCHWAB, K., *La cuarta revolución industrial,* Ed. Debate, Barcelona, 2016.

SIMÓN CASTELLANO, P., *Justicia cautelar e Inteligencia Artificial: la alternativa a los atávicos heurísticos judiciales,* Ed. Bosch, 2021.

TVERSKY y KAHNEMANN, *Judgement under uncertainty: Heuristics and Biases,* Revista Science, 1974.

VALENZUELA SALDIAS, J., *Hacia un estándar de prueba cautelar en materia penal: algunos apuntes para el caso de la prisión preventiva,* Política Criminal, vol. 13, núm. 26, diciembre 2018.

La inteligencia artificial para mejorar la lucha contra la violencia de género

Vicente Magro Servet

Magistrado de la Sala de lo Penal del Tribunal Supremo
Doctor en Derecho

SUMARIO: I. INTRODUCCIÓN. II. LA INTELIGENCIA ARTIFICIAL ANTE LA VIOLENCIA DE GÉNERO Y EL DICTADO DE MEDIDAS CAUTELARES. 1. *Para el dictado de la orden de protección respecto al alejamiento, dispositivos electrónicos, o posible control y protección policial*. 2. *Sobre la suspensión del régimen de visitas ex art. 544 ter 7 LECrim (LO 8/2021, de 4 de junio)*. 3. *Suspensión cautelar de la patria potestad*. III. LA INTELIGENCIA DE ARTIFICIAL NO RESUELVE, PERO AYUDA A RESOLVER. 1. *El mimetismo conductual de la violencia de género y su aprovechamiento por la IA*. 2. *La ampliación de la violencia de género*. 3. *El objetivo de la IA no es buscar la verdad de lo ocurrido, sino la procesal*. 4. *La búsqueda ágil de la IA de la Jurisprudencia aplicable*. 5. *La IA no es la que decide. Ayuda al jurista. No le sustituye*. 6. *La IA nos permite ganar en efectividad*. 7. *No debe haber recelos en la justicia en admitir la ayuda de la IA*. 8. *El libro Blanco de la IA y la europeización*.

I. INTRODUCCIÓN

Dentro del amplio abanico de medidas que podemos encontrar para luchar contra la violencia de género exponemos en las presentes líneas las ventajas que puede suponer introducir entre aquellas a la inteligencia artificial. Una herramienta de tanta actualidad en nuestros días y con un amplio espectro de opciones de abarcar muchas materias en donde sacarle el fruto que esta posibilidad tecnológica potente nos puede aportar.

Así las cosas, resulta evidente que la inteligencia artificial tiene un largo recorrido y aplicación en la lucha contra la violencia de género, porque puede incidir de forma muy positiva en la predictibilidad, como vamos a analizar, y en la adopción de medidas cautelares a la hora de proteger a las víctimas.

La determinación y acierto de los algoritmos que constituyen la información de la Inteligencia artificial para actuar sobre lo que ha ocurrido en hechos semejantes y lo que puede ocurrir es un factor trascendental en la eficacia que puede esperarse de esta herramienta tecnológica de utilización todavía muy reducida en la justicia.

Así, el análisis comparativo entre lo que ha ocurrido y lo que puede ocurrir tiene en los algoritmos introducidos en materia de violencia de género un extenso campo de aplicación, habida cuenta que nos encontramos en un fenómeno claramente repetitivo, que se constata sobre todo en los reiterados informes elaborados por el Observatorio de Violencia doméstica y de género del CGPJ y con un aspecto conductual que se reproduce en el tiempo. Porque se trata de actuaciones comunes y formas de actuar ancladas en el espíritu de dominación y machismo del hombre sobre la mujer, según se refleja en la Exposición de Motivos de la LO 1/2004, y que tiene unos parámetros de actuación homogéneos en la mayoría de los casos y con un carácter predecible en cuanto a los hechos que han ocurrido y a la protección a las víctimas de lo que pueda ocurrir.

Resulta, así, evidente que una de las materias claves en la lucha contra la violencia de género es actuar desde el campo de la prevención, porque desde el punto de vista de la pena a imponer ante un hecho concreto, este mismo ya ha ocurrido, y la respuesta es la del Estado de derecho contra el autor. Pero los avances tienen que producirse en la protección de las víctimas para evitar que se vuelvan a repetir los hechos de maltrato, así como que se pueda producir otro más grave que se tiene que predecir y prevenir. Y todo ello puede hacerse por la inteligencia artificial (IA en adelante).

En este sentido, si hay un campo importante donde se puede trabajar en materia de ciencias del comportamiento es en la violencia de género Y los denominados cazadores dementes criminales a los que ya nos referíamos en otro artículo en esta misma revista[1] pueden ir recogiendo y fijando lo datos que, luego, por los expertos en esta herramienta se introducen como algoritmos en la base de la IA y pueda servir de ayuda a jueces, fiscales y fuerzas y cuerpos de seguridad del Estado para prevenir la forma más grave de ejecución de la violencia de género que es el crimen.

1. Los "Mindhunter" o la introducción de la ciencia del comportamiento criminal para el éxito de la investigación policial, MAGRO SERVET, V. *Diario La Ley,* N.° 9874, 18 de Junio de 2021, Wolters Kluwer.

No estamos utilizando la tecnología todo lo que esta nos permite para dar respuesta a muchos de los problemas que tiene la sociedad. Y, además, cuando lo hacemos es muy lentamente, dando pie y paso a quienes infringen la norma para que se aprovechen de esta lentitud. Resulta necesario que la tecnología se ejecute ágilmente ante los problemas de la violencia, porque cómo actuar desde el punto de vista de la IA es perfectamente posible ante el aprendizaje de la misma "de lo que ha ocurrido" y cómo y qué puede hacer para evitar que vuelva a darse la conducta violenta, o, al menos, ser previsible y advertir de lo que no se puede hacer desde el punto de vista de la víctima, al alertar del riesgo, y de lo que se debe hacer con el autor, tales como medidas cautelares a imponer con el análisis de la predictibilidad.

La IA tiene la ventaja de que con los datos que le da la intervención humana, ella actúa en un periodo de "aprendizaje", como señala BONET NAVARRO[2], "porque le permite perfeccionarse en su funcionamiento y de ese modo evolucionar". Y es que la IA ante la violencia de género recibirá los datos como algoritmos y ella misma llegará a conclusiones y respuestas ante los propios datos, primero almacenados, para, luego, efectuar las deducciones más apropiadas ante el caso concreto. Aprende de lo que ha ocurrido y prevé lo que puede ocurrir con una *aproximación de previsibilidad* ciertamente muy exacta y real. Y es que crear y desarrollar un algoritmo supone no resolver ejerciendo función jurisdiccional, evidentemente, pero sí ayudar con datos y fuentes relevantes para que el juez pueda resolver con aproximación científica gracias a la IA.

La ayuda que le puede proporcionar al juez de violencia contra la mujer la IA en violencia de género es muy importante al momento de actuar en el dictado de las medidas cautelares, sobre todo, ya que la sentencia, tras el juicio y la prueba, o resolver recursos frente a la sentencia es hacerlo del caso concreto, en donde también puede resultar muy útil al sacar el criterio uniforme que existe ante supuestos semejantes con exactitud, pero adaptado a las particularidades y circunstancias del mismo que se le hayan introducido para que nos dé la respuesta. Pero en el caso de las cautelares es donde la efectividad de la IA puede ser mayor.

Recordemos la cita que hace BONET NAVARRO del "famoso abogado artificialmente inteligente llamado Ross, contratado por el bufete Baker & Hostetler, basado en Watson, plataforma de computación cognitiva

2. BONET NAVARRO, J. Doctor en Derecho. Catedrático de Derecho Procesal en la Universidad de Valencia (España). Algunas consideraciones acerca del poder configurador de la inteligencia artificial sobre el proceso. En *Debates contemporáneos del Proceso en un mundo que se transforma,* Colección Jurídica | ISBN (Libro versión digital): 978-958-8943-60-2. Universidad Católica Luis Amigó.

desarrollada por IBM, que, según se dice, es capaz de leer y comprender, generar hipótesis cuando se le pregunta y responder con referencias y citas para respaldar sus conclusiones. Es apto para encontrar normas y jurisprudencia y es capaz de aprender y ofrecer respuestas estructuradas".

En cualquier caso, también puede ser de interés la IA en materia de violencia de género para ayudar en la investigación criminal, ya que destaca este autor su utilidad en dos vías:

"a. *Investigación criminal:*

El sistema *Valcri* (Visual Analytics for Sense-making in Criminal Intelligence Analysis) "para detectar patrones sospechosos y reconstrucción de escenas para plantear nuevas líneas de investigación como ayuda para generar ideas sobre la dinámica el tiempo y las razones por las que se cometió un crimen, así como su posible autor.

b. *Medidas cautelares:*

Destaca este autor la influencia de la IA en métodos o sistemas preventivos del delito o de evaluación de riesgos como Hart o Compas.

Sistema hat: Es la Herramienta de Evaluación de Riesgo de Daños (Harm Assessment Risk Tool). Se destina a predecir la posibilidad de cometer delitos. Fue desarrollada en colaboración con la Universidad de Cambridge y se encuentra en fase de prueba en el Reino Unido. Se basa en el aprendizaje automático y se entrenó en los archivos de la Policía de Durham entre 2008 a 2012. Partiendo de estos, de si ciertos sospechosos reincidieron y con base en diversos factores no siempre relacionados con el delito cometido, se pretende que el sistema evalúe el riesgo como bajo, medio o alto en los sospechosos reincidentes.

Como resultado, sus predicciones se afirma que han sido del 98% efectivas para predecir bajo riesgo y del 88% efectivas con alto riesgo de reincidencia. Al menos, por el momento, solo tendrá utilidad para el asesoramiento de quien deba juzgar, al tiempo se prevén auditorías sistemáticas como su funcionamiento y fiabilidad de sus conclusiones.

Sistema Compas: Trabaja sobre perfiles de gestión de delincuentes correccionales para sanciones alternativas y pretende evaluar el riesgo de reincidencia. Se trata de un algoritmo desarrollado por una empresa privada, a pesar de que será utilizado en el sistema judicial de algunos estados de USA. Incluye 137 preguntas de contenido muy variado y respondidas por el investigado o acusado, así como información extraída de diversos registros. El algoritmo clasifica a la persona en una escala de uno (riesgo bajo) a diez (riesgo alto). Sus predicciones no son vinculantes, pero sirven como ayuda para la toma de decisiones judiciales".

La ventaja de la IA en materia de darnos información acerca de cómo resolver ante hechos de violencia de género, en la fase de investigación criminal, en las medidas cautelares a adoptar por el juez y en el dictado de la sentencia tras el juicio para aplicar el criterio correcto es tal que, como recuerdan RAMÍREZ, FRANCO Y JARAMILLO[3] "la maquina dirigida por IA combina enormes cantidades de datos, siguiendo la estructura del algoritmo, y evoluciona sobre sí misma a velocidades cada vez mayores. Científicamente se ha comprobado que los procesos mentales del cerebro humano se mueven a 120 metros por segundo, mientras que en los circuitos electrónicos de una maquina la información puede llegar a viajar a la velocidad de la luz (Narváez, 2018). Esto implica que la información que un humano procesaría en veinte mil años de trabajo intelectual, la maquina lo haría en poco más de una semana".

Sin embargo, hay que tener en cuenta y dejar claro que cuando el juez tenga estas herramientas para resolver no estaría actuando como si fuera la voz de la IA, y que la máquina fuera la que, en el fondo, resolviera. No es así. Lo que ocurre es que la IA le suministra al juez la información necesaria y suficiente para ayudarle en su resolución. Pero ni pone el auto, ni la sentencia. Suministra la información relevante para que el juez la recoja y con ella y su formación y valoración resuelva. Esto es importante para rebajar las críticas ante la introducción del sistema de la IA ejerciendo una especie de función cuasi judicial.

Sobre esta misma idea de que la IA ayuda al juez *y no es el juez* se pronuncian SUÁREZ MANRIQUE Y DE LEÓN VARGAS[4] al señalar que "Se ha debatido mucho sobre el juez artificial, la posibilidad de que sea un programa, y no una persona humana, quien dicte sentencia. Estas discusiones por lo general apuntan a direcciones equivocadas. Pues, este tipo de programas sobre el "juez autómata", no se refieren, especialmente, a que sea una maquina la que remplace la labor del juez, sino que se refiere a que existan programas de ayuden o que hagan más eficiente la toma de decisiones judiciales. Esta labor puede enfocarse desde diversas direcciones".

Esta es una puntualización importante, porque los críticos ante la IA en justicia minimizan su intervención ante la posibilidad de que se acabe confiando la capacidad de decidir en la máquina, y no en el ser humano.

3. Reflexiones en torno a la inteligencia artificial, el proceso judicial y la educación de los abogados. Diana RAMÍREZ CARVAJAL, Vanessa FRANCO, Daniel JARAMILLO. En *Debates contemporáneos del Proceso en un mundo que se transforma* Colección Jurídica | ISBN (Libro versión digital): 978-958-8943-60-2. Universidad Católica Luis Amigó.

4. Inteligencia artificial y su aplicación en la administración de justicia. Wilson Yesid SUÁREZ MANRIQUE y Georgina Isabel DE LEÓN VARGAS. *Revista jurídica.* Nov 2019. Vol. 11.

II. LA INTELIGENCIA ARTIFICIAL ANTE LA VIOLENCIA DE GÉNERO Y EL DICTADO DE MEDIDAS CAUTELARES

1. PARA EL DICTADO DE LA ORDEN DE PROTECCIÓN RESPECTO AL ALEJAMIENTO, DISPOSITIVOS ELECTRÓNICOS, O POSIBLE CONTROL Y PROTECCIÓN POLICIAL

Como estamos apuntando, la IA en violencia de género puede actuar de forma muy positiva a las medidas cautelares que sepan adoptar en la orden de protección del artículo 544 ter LECrim, ya que el análisis de la valoración del riesgo se puede realizar con la información que suministra la IA y, en ese sentido, el informe de valoración del riesgo basado en esta ciencia le servirá también al juez y al fiscal para tomar la decisión que proceda con arreglo a derecho, pero basado en IA con los datos de los que se dispone y que son importantes para que la IA "auxilie" al juez.

Sobre la importancia de tener el juez base suficiente para el dictado de la medida cautelar dentro de la orden de protección podemos recordar que sobre ello ya se ha pronunciado el Tribunal Supremo en Sentencia 371/2018 de 19 Jul. 2018, Rec. 10067/2018, donde señala que: "necesidad de llevar a cabo un esfuerzo en la valoración de la presencia de incremento del riesgo en las víctimas con una especial atención en su detección en las denuncias que presentan las víctimas, y que se debe acompañar en la denuncia policial al estudio que al efecto se elabore, así como en los institutos de medicina legal en la valoración forense, como consta en el Protocolo médico-forense de valoración urgente del riesgo de violencia de género del Ministerio de Justicia, donde se marcan las pautas de la detección del riesgo. Ello supone actuar desde el campo de la prevención en la evitación de la reiteración de estos hechos, y alertando a la víctima del riesgo concurrente, así como pudiendo articularse instrumentos de ayuda social y económica a las víctimas de malos tratos que así puedan entrar en ese arco de víctimas en situación de riesgo, pudiendo individualizarse las situaciones en aras a evitar la agravación de conductas que acaben con el crimen de género".

La IA conformará una propuesta ante los datos que tiene de hechos semejantes, de los que constan del caso, y de la propia automatización de la misma por su aprendizaje, ya que la esencia de la IA es que aprende de lo que se le da, que es lo que eleva su nivel de simple máquina y sirve de ayuda al juez.

La antes citada sentencia incide, también, en "la conformación del denominado S.A.R.A (Spouse Assault Risk Assessment) en cuanto a las entrevistas que permitirán la evaluación de la existencia del riesgo, clave

para elaborar el informe que sirva para adoptar las medidas conducentes a evitar el riesgo en la víctima, desaconsejando, en su caso, la reanudación de la convivencia, incluso aunque se extinga la pena de alejamiento que se pueda acordar por la concurrencia del factor de previsibilidad de la reiteración de las conductas, y que puedan acabar con el crimen de género, consecuencia demostrada en los casos que ofrecen las estadísticas en estos casos".

Los errores acerca de la incorrecta valoración del riesgo y las consecuencias que de ello se pueden derivar fueron destacados en la sentencia de la Audiencia Nacional de 30 Sep. 2020, Rec. 2187/2019, al destacar que:

"La valoración policial y gestión del riesgo de violencia por las Fuerzas y Cuerpos de Seguridad permite clasificar y proteger a las víctimas en función del riesgo, así como informar a las autoridades judiciales de sus estimaciones. Los agentes actuantes rellenan el formulario del sistema Viogén (formulario VPR), que contiene una serie de indicadores, y el sistema asigna automáticamente un nivel de riesgo a la víctima conforme a los datos introducidos en el formulario, aunque permite la modificación al alza por los agentes si consideran que resulta necesario asignar un nivel de riesgo más alto para una mejor protección de la víctima.

El resultado de la valoración se hace constar por diligencia en el atestado en informe automatizado. Se informará a la víctima de las medidas de autoprotección, según el nivel de riesgo, y habrá un seguimiento de la evolución del nivel de riesgo mediante formulario de evolución del nivel de riesgo (formulario VPER). En caso de riesgo 'no apreciado', como este caso, el nivel de información es el mismo que al de cualquier denunciante, información de derechos y recursos a su disposición, recomendaciones de autoprotección y facilitar teléfonos de emergencias y atención especializada, no estando previsto plazo de nueva valoración si no hay orden de protección judicial pudiendo cambiar el caso a situación de 'inactivo'.

Es indudable que el sistema de medición de la intensidad del nivel de riesgo, aunque se trate de la evaluación inicial, da una predicción no sólo para aplicar las medidas de protección policial adecuadas a cada nivel de riesgo, sino que proporciona información relevante a la autoridad judicial que tiene que adoptar la orden de protección. La medición policial del riesgo no es decisiva para el juez, pero es información especializada de asesoramiento útil para la valoración judicial de la 'situación objetiva de riesgo para la víctima' que exige la ley procesal en la adopción de medidas cautelares de protección, junto con otros instrumentos de valoración".

En este caso, la víctima fue asesinada tras denunciar cuando había datos para prevenir este hecho, por lo que no se aplicó el protocolo para la valoración del nivel de riesgo de violencia de género y la inacción e incumplimiento del protocolo dio lugar a que las actuaciones realizadas desde el punto de igualdad municipal no fueran tenidas en cuenta ni suscitaran una elevación de la valoración del riesgo, que se consideró como "no apreciado". Con ello, se declaró la responsabilidad patrimonial del Estado por defectuosa valoración del riesgo.

2. SOBRE LA SUSPENSIÓN DEL RÉGIMEN DE VISITAS EX ART. 544 TER 7 LECRIM (LO 8/2021, DE 4 DE JUNIO)

También es posible utilizar la IA para adoptar las medidas del artículo 544 ter. 7 LECrim en cuanto a la suspensión del régimen de visitas, habida cuenta que si ahora se ha establecido por la Ley de protección de la infancia 8/2021, de 4 de Junio la suspensión preceptiva cautelar del mismo ante un hecho de violencia de género, la defensa podría articular la vía excepcional que ha sido introducida en el precepto de no acordar la suspensión por existir datos que aporta que permiten lo que ahora es excepcional, que es la no suspensión del régimen de visitas ante procedimiento de violencia de género.

Recordemos que, dados los casos que ha habido de la denominada *violencia vicaria* por la que se mata a los menores para hacer daño a la madre, resulta importante la IA para poder tener información suficiente en estos casos a la hora de resolver. Y, así, para decidir el juez podría basarse en los datos suministrados por la IA para adoptar, bien la regla general que ahora se incluye de la suspensión, o bien la vía excepcional de la no suspensión del régimen de visitas.

3. SUSPENSIÓN CAUTELAR DE LA PATRIA POTESTAD

Por otro lado, también es posible que con arreglo lo dispuesto en el artículo 544 quinquies 1, a) LECrim se pueda suspender la privación de la patria potestad en base también a los datos que suministra la IA, ya que si es sabido que la LO 8/2021, de 4 de Junio de protección de la infancia ha introducido la privación de la patria potestad de forma preceptiva en el artículo 140 bis.2 CP como pena, es posible hacerlo como vía preventiva con la medida cautelar de la suspensión de la patria potestad ante un hecho grave de violencia de género, y, en consecuencia, la posibilidad de adoptar esta medida cautelar por esta vía también estará basada en los algoritmos que suministra la IA.

III. LA INTELIGENCIA DE ARTIFICIAL NO RESUELVE, PERO AYUDA A RESOLVER

1. EL MIMETISMO CONDUCTUAL DE LA VIOLENCIA DE GÉNERO Y SU APROVECHAMIENTO POR LA IA

Son muchos los estudios que se están haciendo sobre la forma en que se llevan a cabo los actos de violencia de género, y la experiencia profesional nos indica el carácter repetitivo y secuencial de estas agresiones de violencia de género, lo que facilita y favorece que la IA pueda aportar mecanismos suficientes de ayuda a los profesionales para actuar de forma cautelar, como decimos, ante los mismos patrones de conducta, por ejemplo, a la hora de acordar medidas cautelares de alejamiento, el uso de la vivienda familiar, prohibición de aproximación a víctimas y sus familiares, uso de armas y expulsión del hogar familiar, y otras medidas que están ancladas en la información que suministra la inteligencia artificial.

Resulta evidente, por ello, que pocas materias existen en la actualidad en donde el *mimetismo conductual* se reproduce con tanta repetición como en la violencia de género, ya que la base y la raíz de las acciones está basada en los principios y bases que se recogen en la LO 1/2004 de protección integral contra la violencia que sufren las mujeres, enraizado en la dominación y machismo del hombre sobre la mujer, y en las bases referenciales que fija el Convenio de Estambul. Pero no solamente anclado en la relación de pareja o ex pareja, sino en los ataques a cualquier mujer por el hecho de ser mujer, ya que no podemos circunscribir la lucha contra la violencia de género al ámbito del artículo 173.2 CP, sino otorgándole un carácter mucho más amplio y ambicioso de la agresión, por el hecho de que la víctima sea mujer, enraizado en un comportamiento machista que es el enfoque debe dársele a los estudios de IA para tomar medidas contra la violencia de género. Y no solamente circunscrito a la violencia que se ejerce en el hogar, que es una de las manifestaciones de la violencia de género, pero que no se acota a este círculo interno familiar, sino que se extiende a todo comportamiento de dominación del hombre sobre la mujer.

2. LA AMPLIACIÓN DE LA VIOLENCIA DE GÉNERO

Son acertados, pues, los estudios que se están realizando ahora en el Consejo General del Poder Judicial, por medio de su observatorio de violencia doméstica y de género, ya que está ampliando el concepto de violencia de género a la que se ejerce sobre la mujer para reconocer con

exactitud la estadística real que existe, por ejemplo, en los crímenes de género, no circunscritas las cifras solamente a las que se producen en el hogar, sino fuera de él sin círculo de relación de pareja o ex pareja, lo que nos daría y nos dará una realidad más ajustada que la disfuncionalidad que existe en la actualidad al sujetar estas cifras al ámbito del 173.2 CP.

En los casos de crímenes o violaciones a mujeres pueden darse connotaciones afectantes a la violencia de género cuando la conducta lleva consigo el ataque a la mujer por el hecho de ser mujer, de tal manera que la IA puede verse reforzada y alimentada por los algoritmos suministrados por toda la información que se le va dando acerca de los modos de comportamiento y patrones a seguir por los autores de este tipo de hechos, lo que puede ser de indudable ayuda en la fase de la investigación policial, analizando perfiles y cuadrando la información de la que se dispone en el caso con la que la IA dispone de casos semejantes.

Por ello, el círculo de la violencia de género da un paso más allá para situarse en el ámbito de los ataques a las mujeres por el hecho de ser mujeres vía Convenio de Estambul, y por encima del marco de sujetos del art. 173.2 CP en la relación de pareja y ex pareja hombre-mujer, aunque extendiéndolo a los menores dentro del marco de la denominada *violencia vicaria*, como se ha contemplado ahora en la LO 8/2021, de 4 de junio en la Disposición final décima, que lleva por rúbrica Modificación de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. Se añade, así, un apartado nuevo 4 al artículo 1, con la siguiente redacción:

"4. La violencia de género a que se refiere esta Ley también comprende la violencia que con el objetivo de causar perjuicio o daño a las mujeres se ejerza sobre sus familiares o allegados menores de edad por parte de las personas indicadas en el apartado primero".

Con ello, el campo de juego de la IA se multiplica para permitir abarcar un amplio espectro de situaciones y ayudar en la investigación policial, en la fase de instrucción con la resolución en las medidas cautelares, y, luego, en la decisión que se adopte recogiendo y reflejando la jurisprudencia más actualizad y aplicable según los hechos que han sucedido y se han declarado probados.

En este último aspecto la IA es donde también despliega un largo recorrido en su ayuda, porque nos facilita una búsqueda rápida de la respuesta de los tribunales al caso concreto, concentrando mucho mejor la selección de lo que se quiere buscar ante el potente banco de datos de los que dispone la IA y su capacidad de aprendizaje y de saber y percibir lo que está buscando el jurista. Además, ayuda tanto en la fase de

celebración del juicio como en la del dictado de la sentencia, ya que el uso de la IA en juicio oral, por su rapidez de respuesta y de acierto le da al jurista lo que este no puede recordar en ese momento del juicio, por lo que la IA puede resultar de suma utilidad en el propio desarrollo del juicio a la hora de tomar decisiones el letrado/a de la defensa o acusación, así como el Ministerio Fiscal, e, incluso, el propio Tribunal, por ejemplo, a la hora de dar respuesta a las cuestiones previas que se plantean al inicio del juicio, y que podría dar lugar a su resolución *in voce* al comienzo del mismo, por ejemplo, en el campo del planteamiento de la prueba ilícita y la conexión de antijuridicidad con las pruebas obtenidas si se declara la ilicitud de una prueba. Ello permite el adelantamiento de la decisión antes del dictado de la sentencia.

3. EL OBJETIVO DE LA IA NO ES BUSCAR LA VERDAD DE LO OCURRIDO, SINO LA PROCESAL

Ahora bien, lo que está claro es que la IA no pretende buscar, ni el sistema judicial, lo que ha ocurrido en un caso concreto sino la "verdad en base a lo que se ha probado". Señalan a estos efectos SUÁREZ MANRIQUE y DE LEÓN VARGAS que "no se sabe ni se sabrá lo que a ciencia cierta acontece en cada caso, ya que conocer la verdad no es la naturaleza de la administración de justicia, simplemente creerla, esto refleja la imposibilidad del conocimiento de la verdad real y a cambio solo la formación de una aceptada verdad procesal. En tal sentido, Luna (2019) plantea lo siguiente: Con el estudio de las nociones analizadas ha quedado claro que la búsqueda de la verdad en el proceso judicial es un objetivo difícil de satisfacer en modo pleno, por lo cual se plantea que frente al proceso lo que se tiene es una verdad con carácter de validez.

Así, para el proceso los hechos son conforme se han probado y no como ocurrieron en la realidad". Recuerdo sobre este punto que en un intercambio de jueces internacional que recibimos en España me preguntaba un Magistrado extranjero si aquí buscábamos la verdad de lo que había ocurrido en el caso concreto, siendo la respuesta la misma señalada antes, en el sentido de que ese no es el objeto del proceso, sino la decisión en base a la prueba que se había practicado, que no es otra que la función judicial a la hora de dictar la sentencia en esto, y solo en esto, y no en su percepción o idea de lo "podría haber ocurrido".

La IA nos permite, pues, un amplísimo abanico de soluciones que van a dar muchas posibilidades a los juristas en sede de juicio oral, como estamos puntualizando, ya que el conocimiento tan amplio y el *razonamiento* de la IA en cuestión de segundos es imposible que lo tenga la mente

humana, por lo que la inmediatez de la respuesta es lo que le va a dar más juego a la IA para el jurista. Así, en los juicios ante casos de violencia de género permitirá la búsqueda y respuesta de la jurisprudencia inmediata según se desarrolle el mismo y sea necesario hacer mención a la doctrina jurisprudencial más reciente aplicable en el turno de informe, o si existe un Acuerdo de Pleno del Tribunal Supremo sobre el elemento concreto que ha surgido en el juicio y es preciso indicar el letrado/a, o el Fiscal en el momento en el que está informando ante el Tribunal al concluir la práctica de la prueba.

4. LA BÚSQUEDA ÁGIL DE LA IA DE LA JURISPRUDENCIA APLICABLE

Más tarde, la IA desempeña un papel fundamental para el juez que va a resolver al facilitarle de forma ágil la jurisprudencia aplicable al caso concreto, e, incluso, la solución dada a casos idénticos, una vez introducidos los datos, aunque reservándose, evidentemente, el juez el papel que le queda de valoración de esos datos que le suministra la IA, ya que esta no dicta la sentencia. Pero sí que ayuda, y mucho, al juzgador a dictarla, porque lo que le da al juez es *información* rápida y selectiva para el caso concreto.

Esta rapidez en la obtención de información jurídica relevante supone un salto cualitativo en la Administración de Justicia, porque donde se pierde muchísimo tiempo es, precisamente, en la búsqueda de la información, del precedente judicial aplicable al caso concreto. Y aquí es donde los juristas dan mucho valor a las amplias posibilidades que tiene la IA en la justicia a la hora de facilitarnos información que, en ocasiones, tardamos en conseguir. Bien porque no se realizan con exactitud las labores de búsqueda, o porque no se le ha suministrado la debida información actualizada al máximo en el aspecto temporal. Y esto es importante, porque una vez implementada la IA en la Administración de justicia debería conseguirse una rapidez en el traslado de la información contenida en la sentencia a la IA para que ésta pueda añadir el dato y procesarlo con la información de la que ya dispone para complementarla con la nueva sentencia dictada.

Lo mismo cabe decir de la trascendencia de los Acuerdos de Pleno del Tribunal Supremo y su traslación a la IA para su uso por todos los juristas con la rapidez e inmediatez que merece que el Alto Tribunal haya aprobado un acuerdo de Pleno en un caso concreto que puede ser de suma utilidad para todos los juristas que en el momento de la adopción del Acuerdo de pleno puedan estar barajando un caso en el que puede y debe aplicarse ese Acuerdo.

La abundante jurisprudencia que se está dando en la materia que estamos tratando de la violencia de género puede servir de gran ayuda con la IA para adelantar trabajo y obtener soluciones inmediatas, analizando lo que se reclama de ella con una agilidad y concreción y acierto en la búsqueda que es lo que se solicita y espera de la misma por el jurista.

Por ello, destaca MARTÍNEZ GUTIÉRREZ[5] la ayuda de la IA en materia de jurisprudencia se basa en la existencia de "potentes bases de datos de búsqueda de jurisprudencia al modo de sistemas expertos que puedan preseleccionar jurisprudencia aplicable, o, incluso, dando al juez o magistrado la posibilidad de elegir entre diferentes opciones predeterminadas por el sistema. Se trataría, pues, de la aplicación de técnicas de jurimetría a la labor jurisdiccional".

5. LA IA NO ES LA QUE DECIDE. AYUDA AL JURISTA. NO LE SUSTITUYE

De todos modos, cierto y verdad es que a la IA se le está pidiendo algo más, y mucho más, de ahí que exista un cierto recelo en algunos juristas, y es que se comporte como un ser inteligente capaz de decidir. Así, recuerda GUTIÉRREZ RODRIGUEZ que "el término "inteligencia artificial" fue introducido por John McCarthy en 1956, a propósito de un taller que organizó junto con un grupo de investigadores en Dartmouth College y que buscaba explorar el trabajo de Alan Turing sobre aprendizaje automatizado (machine learning) (Ertel, 2017; Kelleher & Tierney, 2018; Mitchell, 2019; Webb, 2019). Una de las primeras definiciones de IA fue propuesta por McCarthy: "El objetivo de la IA es desarrollar máquinas que se comportan como si fueran inteligentes" (Ertel, 2017)".

Añade, por ello, que "la IA es como un sistema que toma decisiones automatizadas y que imita la inteligencia humana (Webb, 2019). En términos similares, la Comisión Europea recientemente definió la IA como "sistemas que muestran un comportamiento inteligente al analizar su entorno y tomar acciones, con cierto grado de autonomía, para lograr objetivos específicos" (European Commission, 2018, p. 2)".

Ahora bien, no se trata de darle a la IA unas prerrogativas y responsabilidades que solo tiene el jurista cuando decide cómo resuelve, sino de aprovecharse de las excelencias de este sistema para cuando llegue la hora

5. Inteligencia artificial, algoritmos y automatización en la Justicia. Propuestas para su efectiva implantación. Rubén MARTÍNEZ GUTIÉRREZ, Profesor Titular de Derecho Administrativo Universidad de Alicante, *Práctica de Tribunales,* N.° 149, Sección Estudios, Marzo-Abril 2021, Wolters Kluwer.

decidir. Pero, por ejemplo, para el letrado/a que prepara un caso, que le ayuda a saber cómo enfocarlo, que le permite saber y conocer cómo se ha resuelto otros semejantes, y lo que es más increíble, cómo podría resolverse el que tiene en sus manos si se cumplen determinados parámetros.

Con ello, el *enfoque correcto del caso* es lo que le sirve de ayuda al letrado/a y que a la hora de decidir el juez, éste tome como referencias lo que le suministra la IA como propuestas razonadas, lo que no es algo negativo, o que desapodere a la justicia de su verdadera autonomía y *sustituya en el papel de decidir al juez por la máquina.* En modo alguno. El enfoque correcto es el de la magnífica ayuda que aporta la IA y la sensación que se tiene de "ganarle tiempo al tiempo". Porque lo que da, sobre todo, es la amplísima información que selecciona y ofrece la IA al jurista, y que éste solo conseguiría invirtiendo mucho tiempo en la búsqueda.

6. LA IA NOS PERMITE GANAR EN EFECTIVIDAD

La IA nos permite ganar en efectividad, que es la concentración de la eficacia y la eficiencia en un sistema que nos lo da todo: buena información, segura y acertada, y en un tiempo muy breve y directo, que son el complemento perfecto que ayuda en la toma final de decisiones en unos tiempos más cortos y con una información segura adaptada al caso concreto que se está analizando.

No puede verse con miedo en la justicia, pues, que la IA tenga una amplia capacidad de automatización y de razonar o de pensar, porque la decisión final es humana, no de la máquina. El aporte de información y propuesta de soluciones al caso es una ayuda incalculable, y obtenerlo en el tiempo que lo da la IA algo inimaginable cuando nos teníamos que ir a una biblioteca a buscar información, pero empezando por saber lo que estábamos buscando y dónde podríamos obtenerlo. Todo eso lo da la IA al instante, con lo que la multiplicidad de los resultados en el trabajo determina la alta rentabilidad de la IA. Y, sobre todo, en una materia como la que estamos tratando, tan sensible, y tan necesitada de una respuesta ágil, segura y resolutiva.

Porque nótese que, como destaca GUTIÉRREZ RODRÍGUEZ[6] "entenderemos las herramientas con tecnología de IA como aquellas que cuenta con sistemas de toma decisiones automatizadas, que imitan la inteligencia humana y que – en algunos casos – están dotadas de la capacidad de aprender por sí mismas vía procesos iterativos de ensayo y error. En

6. Retos éticos de la inteligencia artificial en el proceso judicial Por: Juan David GUTIÉRREZ RODRÍGUEZ, 21 de agosto de 2020.

el contexto de la IA, el término "aprendizaje automatizado" (machine learning) fue usado inicialmente para describir aquellos "programas que le dan a un computador la habilidad de aprender de los datos"(Kelleher & Tierney, 2018, p. 13). Lo que distingue a los aparatos dotados de esta capacidad es que sus "algoritmos son capaces de analizar automáticamente una gran cantidad de conjuntos de datos para extraer patrones que potencialmente son interesantes y útiles".

7. NO DEBE HABER RECELOS EN LA JUSTICIA EN ADMITIR LA AYUDA DE LA IA

Pero cierto es que el recelo en la justicia existe, de ahí que se deba llevar a cabo un esfuerzo para clarificar que la IA es una ayuda, no el "nuevo juez-robot". Incide también en esta preocupación MARTÍNEZ GUTIÉRREZ señalando que: "la utilización de técnicas de IA en la Administración de Justicia ha sido un ámbito en el que la doctrina ha dudado más a la hora de valorar positivamente su aplicación, quizá por tratarse de un ámbito en el que existe una clara y lógica discrecionalidad por parte de los jueces y magistrados en la adopción de sus decisiones, y esta circunstancia genera una cierta incertidumbre: ¿será adecuado, acertado o justo que un sistema informático o software resuelva por si solo un problema jurídico que ha sido objeto de un conflicto judicial?".

8. EL LIBRO BLANCO DE LA IA Y LA EUROPEIZACIÓN

Por otro lado, si se apuesta por la IA en la lucha contra la violencia de género debe adoptarse una posición en la UE al respecto uniforme con métodos implantados de forma global, porque estamos tratando de un problema globalizado que afecta a todos los Estados de la UE, por lo que es precisa la suficiente inversión que acomode la gran idea que es utilizar IA en la lucha contra la violencia de género, pero hacerlo en condiciones óptimas.

Debemos recordar la reciente publicación el 19 de Febrero de 2020 del LIBRO BLANCO sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza por la Comisión Europea de la UE, donde se destaca a este respecto que: "En 2016, se invirtieron unos 3 200 millones EUR en inteligencia artificial en Europa, frente a los cerca de 12 100 millones EUR en América del Norte y 6 500 millones EUR en Asia. Ante este hecho, Europa debe aumentar significativamente sus niveles de inversión. El Plan coordinado sobre inteligencia artificial desarrollado

con los Estados miembros está demostrando ser un buen punto de partida para estrechar la cooperación en materia de inteligencia artificial en Europa y crear sinergias que optimicen la inversión en la cadena de valor correspondiente". Es decir, que si se quiere apostar por la IA debe serlo con la inversión suficiente. Si apostamos por ella, lo es en la mejor de las condiciones técnicas posibles, porque, como expusimos recientemente[7]. *No se trata de implantar nuevas tecnologías, sino de implantar buenas tecnologías.*

Continuando sobre la posición de Europa acerca de cómo se puede implementar la IA en la justicia destaca MARTÍNEZ GUTIÉRREZ la Resolución del Parlamento Europeo, de 20 de enero de 2021, sobre inteligencia artificial: cuestiones de interpretación y de aplicación del Derecho internacional. Recuerda que interesa destacar cuatro de los planteamientos de este documento en materia de IA en el ámbito de la justicia, a saber:

"(1) Señala el documento 'que el uso de la IA en el ámbito de la justicia podría mejorar el análisis y la recogida de datos y la protección de las víctimas, y que esta posibilidad podría estudiarse en investigación y desarrollo e ir acompañada de evaluaciones de impacto, en particular en relación con las salvaguardias para la tutela judicial efectiva y frente a los sesgos y la discriminación, aplicándose para ello el principio de precaución; recuerda, no obstante, que no puede ocupar el lugar de un ser humano a la hora de dictar sentencia o tomar decisiones'.

(2) En segundo lugar, 'insta a los Estados miembros a que evalúen los riesgos relacionados con las tecnologías basadas en la IA antes de automatizar las actividades relacionadas con el ejercicio de la autoridad estatal, en particular en el ámbito de la justicia; pide a los Estados miembros que se planteen la necesidad de establecer salvaguardias, como por ejemplo la supervisión por profesionales cualificados y normas relativas a la ética profesional'.

(3) Asimismo, 'solicita que se mantenga informado al público sobre el uso de la IA en el ámbito de la justicia, y que dichos usos no den lugar a discriminación derivada de sesgos de programación; subraya que debe respetarse el derecho de toda persona a tener acceso a un funcionario público, así como el derecho del funcionario responsable a tomar personalmente la decisión y a desviarse de la información recibida de la IA cuando lo considere necesario a la luz de los detalles del asunto en cuestión; recalca el derecho de la persona demandada a recurrir la decisión de conformidad con la legislación nacional, sin que se elimine en ningún caso la responsabilidad final del poder judicial'.

7. La aplicación de la inteligencia artificial en la Administración de Justicia. Vicente MAGRO SERVET, Magistrado del Tribunal Supremo. Doctor en Derecho, *Diario La Ley*, N.° 9268, Sección Doctrina, 27 de Septiembre de 2018, Wolters Kluwer.

Y (4) 'solicita, por tanto, que todos esos usos en el ámbito público y administrativo constituyan información de dominio público y que se evite la discriminación derivada de sesgos de programación'".

Vemos que la citada Resolución incide en que una de las ventajas de la IA en la justicia es el tema que ahora estamos tratando, centrado en la protección de las víctimas, y, en nuestro caso, de violencia de género. Mujeres y menores, como ya hemos expuesto.

Pero otro de los aspectos que se destacan de esta Resolución de 2021 es que un objetivo esencial de la IA en justicia es que se debe aspirar a proporcionar seguridad jurídica a los ciudadanos, y, en concreto, a los juristas, porque la potencialidad que hemos descrito en los usos posibles donde se puede proyectar la IA permite reforzar la seguridad jurídica con ese posicionamiento en el criterio uniforme y su consolidación ante el mismo caso, extraído de la documentación suministrada por la jurisprudencia a la IA, su almacenamiento y orden interno del programa que después se ofrece al jurista que la utiliza.

Por todo ello, frente a los críticos ante el uso de la IA en justicia apunta el autor antes citado, de acuerdo con la tesis que mantenemos, que "un sistema de IA no tiene porqué ser totalmente autónomo o ajeno a la supervisión humana", porque la esta última es la decisoria del juez ante las propuestas del sistema de IA, que no le vincula, pero sí le suministra la información suficiente para ayudarle en esta, que es lo que se destaca en la Resolución de Enero de 2021.

BUENO DE MATA[8], citando a SILVIA BARONA trata de la "algoritmización del derecho", haciendo luego referencia a las dudas y preocupación sobre *los algoritmos sesgados.* Añade, también, la mención del importante tratadista en la materia como NIEVA FENOLL en cuanto hace referencia a la IA como "herramienta de auxilio en materia de procedimiento, prueba, medidas cautelares o argumentación y distinguir esta inclusión de decisiones automatizables en materia de admisión de pruebas, resolución de recursos o posibilidades en materia de ejecución. En relación al objeto de esta investigación, el autor ya se plantea la posibilidad de que, en el caso de que puedan existir herramientas de inteligencia artificial para la investigación policial, será necesario que se "explique su por qué, no solamente será posible descubrir crímenes con mayor eficacia, sino que

8. Protección de datos, investigación de infracciones penales e inteligencia artificial: novedades y desafíos a nivel nacional y europeo en la era postcovid. Por Federico BUENO DE MATA. Profesor Titular de Derecho Procesal. Universidad de Salamanca *La Ley Penal,* N.° 150, Sección Derecho Procesal Penal, Mayo-Junio 2021, Wolters Kluwer.

las motivaciones de los jueces tendrán muy superiores posibilidades de ser más completas y correctas al estar más adecuadamente establecidas las premisas del razonamiento inferencial".

Se cita, asimismo, la importancia de "la Propuesta de Reglamento de 21 de abril de 2021, por la que se establecen normas armonizadas sobre la inteligencia artificial en la Unión, cuestión que también afectará irremediablemente en un futuro próximo a las investigaciones tecnológicas en la era post covid y, por ende, a los procesos penales donde se utilicen datos electrónicos, destacando que "esta propuesta de Reglamento sobre IA proporciona una definición de lo que se debe entender por la misma, indicando que sería 'un software que, mediante el empleo de técnicas matemáticas y de programación, conocidas como 'algoritmos', permiten elaborar resultados que sirven para realizar predicciones, pronósticos de conductas, recomendaciones de decisiones futuras, entre otros fines'".

Destaca este autor, también, con acierto, la mención del art. 485 LECrim del Anteproyecto de la LECrim que se refiere al tema que antes hemos tratado en torno a la valoración del riesgo, que lleva por rúbrica *Instrumentos de valoración del riesgo de violencia o reincidencia* y apunta que:

1. Los instrumentos de valoración del riesgo de violencia o reincidencia deberán incluir todos los parámetros estadísticos que permitan evaluar tanto su fiabilidad como su capacidad predictiva.

2. Dichos instrumentos especificarán el tamaño de la población con la que se han construido, las variables utilizadas como factores de riesgo, los criterios de medición empleados para ponderar dichos factores asignando puntuaciones, y el tiempo de validez de la predicción. También habrán de identificar los estudios de validación realizados.

Con ello, ya el Anteproyecto recoge la plasmación de la IA en materia de actuación predictiva y potenciación de los indicadores tecnológicos de la IA en avanzar la metodología llevada a cabo para la obtención de las conclusiones y que se conozcan los parámetros tenidos en cuenta a la hora de llevar a efecto una acertada valoración conclusiva.

De esta manera, pese a las posibles dudas que a algunos juristas les pueda parecer la introducción de la IA en justicia, BUENO DE MATA asegura que "La doctrina procesalista española es una de las más reconocidas a nivel mundial al tratar el impacto de la inteligencia artificial en diferentes aspectos del proceso. Podemos decir que la inteligencia artificial se está convirtiendo en un tema medular y de especial interés para muchos juristas. Sin duda, estamos ante un tema de presente y futuro que irá acompañado de muchas oscilaciones legales hasta conseguir una

base jurídica sólida y concreta". Y es que lo importante es conocer qué nos puede ofrecer la IA en la justicia y en este caso en la lucha contra la violencia de género, y qué podemos escoger y elegir de sus bondades y obtener el máximo aprovechamiento sin infringir derechos fundamentales ni hacer un uso descontrolado de sus posibilidades, que son muchas, desconectado del preciso control con el que hay que manejar estas herramientas, al punto de que debe ser el jurista el que use a la máquina y no ésta a aquél, porque también se corre el riesgo ante un uso indebido de la IA que haga que esta se pueda acabar apoderando del hombre-mujer-decisor convirtiendo a este en el autómata y a la máquina en lo que antes hacía el ser humano. Con todo ello, concluimos que quien decide al final es el ser humano, pero sin desaprovechar las amplias posibilidades que nos reporta la IA. Y en la lucha contra la violencia de género no podemos "descontar aliados". Y uno muy bueno puede ser la IA… si le sabemos sacar el provecho que merece.

Inteligencia artificial y proceso judicial: perspectivas ante un alto tecnológico en el camino

Jordi Nieva-Fenoll

Catedrático de Derecho Procesal
Universitat de Barcelona

SUMARIO: I. INTRODUCCIÓN: LOS PARONES DE LA CIENCIA. II. AVANCES EN LA AUTOMATIZACIÓN DE PROCEDIMIENTOS. III. USO AMPLIO DE INTELIGENCIA ARTIFICIAL EN LA PREPARACIÓN DE ESCRITOS JUDICIALES. IV. INTELIGENCIA ARTIFICIAL Y PRUEBA. V. INTELIGENCIA ARTIFICIAL Y PREDICCIÓN DEL RIESGO. VI. INTELIGENCIA ARTIFICIAL Y ODR. VII. UN POSIBLE FUTURO.

I. INTRODUCCIÓN: LOS PARONES DE LA CIENCIA

Hace un cierto tiempo que puede detectarse que pese a la enorme expectación suscitada por la posibilidad de introducir la inteligencia artificial en los procesos judiciales[1], el balance es más bien escaso a día de hoy.

1. La literatura científica es hoy ya recurrente sobre el tema. Partiendo de los primeros estudios de BONET NAVARRO, José, "La tutela judicial de los derechos no humanos. De la tramitación electrónica al proceso con robots autónomos", *Revista CEFLegal*, n. 208 (mayo 2018), pp. 77 y ss., y NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial*, Madrid 2018, se han sucedido en los últimos años un sinfín de trabajos sobre la cuestión. Por citar sólo algunos, RE, R. M./SOLOW-NIEDERMAN, A., "Developing Artificially Intelligent Justice", 22 Stan. Tech. L. Rev. 2019, pp. 242 y ss. GIAMPIERO, L., "Regulating (Artificial) Intelligence in Justice: How Normative Frameworks Protect Citizens from the Risks Related to AI Use in the Judiciary", European Quarterly of Political Attitudes and Mentalities, 8(2), 2019, pp. 75 y ss, https://nbn-resolving.org/urn:nbn:de:0168-ssoar-62463-8. RIGANO, C., "Using Artificial Intelligence to Address Criminal Justice Needs", *NIJ Journal*, n. 280 enero 2019, pp. 1 y ss. CUI, Y. Artificial Intelligence and Judicial Modernization, Springer 2020. QUATTROCOLO,

Está costando mucho automatizar los procedimientos, las herramientas de predicción de riesgo funcionan de manera defectuosa[2], las investigaciones policiales con herramientas de reconocimiento facial están arrojando todavía demasiados errores[3] –detectados incluso por Facebook[4]–, los ODR con inteligencia artificial no parecen estar avanzando realmente más allá de respuestas automáticas de algunas plataformas a reclamaciones absolutamente previsibles[5], y no se están aplicando las ventajas de la inteligencia artificial a campos como la prueba, o incluso a fases procedimentales relativamente sencillas en la enorme mayoría de los casos, como la ejecución en el proceso civil.

¿Por qué se está operando con semejante lentitud? La respuesta no es evidente. Desde luego, existen diversos factores que explican el retraso, entre ellos el económico por la falta de inversión debidamente orientada. Pero también cabe detectar las dificultades enormes de poner en contacto a juristas e informáticos a la hora de explicar nuestras necesidades y elaborar los algoritmos de manera conveniente, de modo que no vulneren nuestros derechos fundamentales. Esa es la preocupación principal, muy reiterada, en los diversos documentos que las instituciones de la Unión

S., *Arificial Intelligence, Computational Modelling and Criminal Proceedings*, Springer 2020. SOURDIN, Tania, *Judges, Technology and Artificial Intelligence, The Artificial Judge*, Cheltenham 2021. FORREST, Katherine B., *When Machines Can Be Judge, Jury, and Executioner. Justice in the Age of Artificial Intelligence*, Singapur 2021. SOURDIN, Tania, MEREDITH, Jacqueline, LI, Bin, *Digital Technology and Justice. Justice Apps*, London 2020. SINGH, Nishant, *AI and Justice*, New Delhi 2021.

2. LARSON, Jeff/MATTU, Surya/KIRCHNER, Lauren/ANGWIN, Julia, "How We Analyzed The Compas Recidivism Algorithm", *Propublica*, 23-5-2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. DRESSEL, Julia/FARID, Hany, "The Accuracy, Fairness, And Limits Of Predicted Recidivism", *Science Advances*, 17-1-2018, http://advances.sciencemag.org/content/4/1/eaao5580.full. BERK, R., HEIDARI, H., JABBARI, S., KEARNS, M., ROTH, A., "Fairness in Criminal Justice Risk Assessments: The State of the Art", *Sociological Methods & Research*, feb. 2021, Vol. 50, issue 1, pp. 3 y ss.

3. EDMON, G., WHITE, D., TOWLER, A., SAN ROQUE, M., KEMP, R., "Facial Recognition and Image Comparison Evidence: Identification by Investigators, Familiars, Experts, Super-recognizers ans algorithms", Melbourne University Law review, 2021, 45(1), pp. 47-50. HONG CHEN, LIWEI GENG, HONGDONG ZHAO, CUIJIE ZHAO, AIYONG LIU, "Image recognition algorithm based on artificial intelligence", *Neural Computing and Applications*, 2021.

4. DE CHANT, T. "Facebook to stop using facial recognition, delete data on over 1 billion people", *Ars Technica*, 11-2-2021, https://arstechnica.com/tech-policy/2021/11/after-tagging-people-for-10-years-facebook-to-stop-most-uses-of-facial-recognition/.

5. *Vid.* el errático funcionamiento de la plataforma la resolución de litigios en línea de la Unión Europea: https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=ES. Sobre la misma, Valbuena González, F. "La plataforma europea de resolución de litigios en línea (ODR) en materia de consumo", *Revista de Derecho Comunitario Europeo*, 52, 2015, pp. 987 y ss.

Europea han ido emitiendo sobre este particular desde 2020[6], así como la UNESCO en 2021[7].

A día de hoy, en realidad, sólo parece que los programas que trabajan con selecciones de jurisprudencia y propuestas argumentativas están teniendo un éxito ciertamente remarcable[8], particularmente en algunos despachos grandes de abogados, que han mejorado notablemente su capacidad de trabajo y respuesta de un modo que detectan algunos seres humanos por la rapidez del producto, pero no, y esto es importante, por la calidad intrínseca u originalidad de la argumentación. Con todo, parece que estas herramientas de elaboración de la argumentación y del lenguaje persuasivo, al menos en la parte jurídica, pueden llegar a ser un lugar muy común bastante antes de lo que pensábamos.

Paralelamente, con una observación más detenida cabe detectar también un cierto parón tecnológico nada desdeñable, cuyas causas no son claras, aunque puede estar derivado de las dificultades inmensas en la construcción de los algoritmos y su "entrenamiento". Es cierto que en materia de inteligencia artificial, igual que en otros campos, la evolución de la técnica no ha sido lineal, sino que ha dado saltos seguidos de incomprensibles parones. Puede ser que a veces falte el talento necesario para evolucionar más deprisa, o bien incluso que las empresas estén más centradas en la elaboración de algoritmos para recolectar la mayor cantidad de datos posibles para comerciar con ellos, que no en mejorar la herramienta en sí misma para realizar operaciones más complejas.

Tras el tradicional lenguaje algo falaz en esta materia –*machine learning*, *deep learning*, redes neuronales, etc.– se esconde que lo único que hace la inteligencia artificial es recopilar una enorme cantidad de datos que contrasta con los que ya tiene, pero de manera todavía demasiado defectuosa en su clasificación, sin poder modificar las alternativas de toma de decisión preestablecidas si no es mirando siempre al pasado, a los datos que ya posee. Eso es lo que se denomina "entrenamiento" de la herramienta, y en ese punto radica una de sus principales dificultades. Lo que nos separa a los seres humanos de la máquina no es exactamente nuestra curiosidad,

6. *Vid*. la *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión*. COM/2021/206 final.
7. *Proyecto de texto de la recomendación sobre la ética de la inteligencia artificial*, 41 C/73, pp. 13 y ss.
8. *Vid.,* por ejemplo, https://jurimetria.laleynext.es/content/QueEs.aspx. *Vid.* también el proyecto Bidaraciv: https://www.heraldo.es/noticias/aragon/2020/11/24/la-inteligencia-artificial-saca-argumentos-de-sentencias-con-decenas-de-folios-en-segundos-1406805.html.

puesto que la IA, con su increíble capacidad de absorción de datos, tiene la más ambiciosa "curiosidad" que pueda imaginarse. Sí nos hace diferentes, en cambio, nuestra creatividad –más allá del criticismo, que también–, que aunque no siempre abunda, no depende sistemáticamente –a diferencia de la IA– de los datos que ya conozcamos. Somos capaces de improvisar. Por ello, el único riesgo a día de hoy que ha intuido la literatura, e incluso científicos como Stephen Hawking en 2014[9], no es tanto que la máquina nos sustituya, sino que pongamos los medios necesarios para dejarnos sustituir por la máquina, que es muy diferente[10].

El tema es apasionante, pero en este trabajo me voy a ocupar solamente de la aplicación de la inteligencia artificial en materia judicial, en qué medida está usándose de manera efectiva, cuáles son sus perspectivas de futuro y cómo podría afectar a nuestro quehacer cotidiano próximamente.

II. AVANCES EN LA AUTOMATIZACIÓN DE PROCEDIMIENTOS

La experiencia, tan comentada, de Estonia, está resultando algo decepcionante al estar limitada al enjuiciamiento automatizado de pequeñas reclamaciones de cantidad –7.000 €– y haber evidenciado que no se puede utilizar en casos que se separen de la pauta general y requieran más margen de maniobra[11]. Por su parte, la experiencia en Argentina es muy limitada –por ahora– a algunos sectores del ámbito administrativo[12], igual que la de EE. UU. en materia de infracciones de tráfico[13]. Pese a ello, lo cierto es que la automatización de los procedimientos es el campo en el que la inteligencia artificial tiene hoy por hoy mayor potencial para tener un impacto directo en la vida de los ciudadanos, al acelerar los procesos reduciéndose con ello la litigiosidad. Dicha aceleración no sólo deriva de la rapidez de la máquina y de que pueda trabajar sin descanso, a diferencia de un humano, sino que esa rapidez hará desaparecer los conflictos derivados de la mora dolosa de los muchos deudores que se aprovechaban de las carencias y lentitud del sistema judicial para ganar tiempo.

Como ya se ha detectado en los casos de algunas reclamaciones masivas frente a bancos sobre todo, que han llevado a la discutible decisión de

9. CELLAN-JONES, R., "Stephen Hawking warns artificial intelligence could end mankind", BBC, 2-12-2014, https://www.bbc.com/news/technology-30290540.
10. *Cfr.* DEEKS, A., "The Judicial Demand for Explainable Artificial Intelligence", *Columbia Law Review*, vol. 119, n. 7, 2019, pp. 1829 y ss.
11. LO, D. "Can AI replace a judge in the courtroom?", *UNSW Newswire*, 1-10-2021.
12. TARRICONE, M. "Justicia automatizada, sí o no: cómo funciona el software que ya se usa en CABA", *Perfil*, 30-9-2020.
13. SOURDIN, *Judges, Technology and Artificial Intelligence, The Artificial Judge*, *cit.*, p. 129.

especializar algunos juzgados incluso[14], hay procesos que son idénticos por mucho que cambien las partes, la cuantía de lo reclamado, o incluso algunas circunstancias particulares bastante previsibles en el fondo. Lo mismo sucede con muchos desahucios y otros procedimientos posesorios, y hasta con reclamaciones de cantidad como la práctica totalidad de los procedimientos monitorios.

Se trata de casos que en muchísimas ocasiones carecen de oposición, por lo que pueden ser tramitados de principio a fin de manera automática, como de hecho ya sucede aunque con un increíble dispendio en recursos humanos, usando los tradicionales formularios. Son procedimientos en los que la reclamación es obvia, la falta de respuesta del demandado es sistemática y la resolución del juez absolutamente previsible con la documentación aportada, que prácticamente siempre es la misma o similar. Ocurre casi lo mismo, por cierto, con la ejecución de condenas dinerarias en el ámbito civil. Sólo hay que buscar patrimonio del deudor en las bases de datos, registrales o no, que ya poseemos, y seleccionar de manera automática el bien más realizable en función de los patrones de decisión que le demos al algoritmo, que deben consistir en combinar el máximo provecho para el acreedor con el menor perjuicio posible para el deudor a fin de no dañarle innecesariamente[15], añadiendo un indigente al sistema de manera absurda.

En estas condiciones, no hay razón alguna para que no exista una herramienta de inteligencia artificial que celebre todos esos procedimientos en un tiempo muy reducido, estableciéndose en las leyes una drástica reducción de los plazos y hasta unos patrones de respuesta muy sencillos que ayuden al demandado o incluso a su abogado. Procesos que actualmente tardan meses o años en concluir con éxito –o con victorias pírricas– podrían estar definitivamente resueltos en unos diez días como máximo, al reducirse de manera radical el tiempo de respuesta judicial, convirtiéndose en automática y trabajando la herramienta inteligencia artificial durante las 24 horas del día.

Es cierto que ello no será posible en los procesos en que la documentación aportada no sea tan fácilmente analizable por la herramienta, al no

14. *Vid.* v.g. el Acuerdo de 16 de diciembre de 2020, de la Comisión Permanente del Consejo General del Poder Judicial, por el que se atribuye a determinados juzgados, con competencia territorial indicada para cada uno de los casos, de manera exclusiva y excluyente o no excluyente, según los casos, el conocimiento de la materia relativa a las acciones individuales sobre condiciones generales incluidas en contratos de financiación con garantías reales inmobiliarias cuyo prestatario sea una persona física. BOE 22-12-2020. *Vid.* también el Acuerdo de 23-6-2021, BOE 28-6-2021.
15. *Vid.* este parámetro en NIEVA FENOLL, J., *Derecho Procesal II, Proceso Civil*, Valencia 2019, p. 456.

entrar en los patrones habituales, o bien que sean los propios abogados o sus clientes quienes intentando dilatar el procedimiento, hagan lo imposible por aportar datos o evidencias que se salgan del patrón. Tal actitud chicanosa podría ser corregida con sanciones que en un primer momento amenazarían con colapsar también el sistema, aunque quizá no tanto si ya se plantean desde un primer momento, consiguiéndose tal vez un eficaz efecto disuasorio acompañado de las debidas explicaciones persuasivas para favorecer que todos los actores colaboren con el sistema, en beneficio de una mejor justicia.

El único problema con todo lo anterior, que no es menor, será la bajada del volumen de trabajo de muchos abogados. Se diga lo que se diga en torno a que la inteligencia artificial va a crear nuevos empleos, lo cierto es que suprimirá modos de trabajo habituales en muchos ámbitos, y este es sin duda uno de ellos[16].

III. USO AMPLIO DE INTELIGENCIA ARTIFICIAL EN LA PREPARACIÓN DE ESCRITOS JUDICIALES

Pero como antes indiqué, el campo principal de aplicación de la inteligencia artificial en materia judicial en este momento es el de la elaboración de escritos judiciales, por ahora de los litigantes, pero probablemente en breve también de los tribunales. Igual que ya leemos muchas argumentaciones en las sentencias, perfectamente detectables, fruto del uso abusivo de las bases de datos de jurisprudencia y de la utilización, aún más abusiva, de la herramienta corta–pega, en el futuro vamos a ver una mayor perfección en la elaboración de estas argumentaciones, cada vez con un lenguaje más natural y con redacciones perfectamente correctas desde el punto de vista gramatical.

De momento están funcionando con ayuda humana, tanto en la reconfiguración de los algoritmos como en la selección o alteración de los textos a utilizar en cada caso. Pero aunque así siga siendo durante bastante tiempo, es obvio el salto cualitativo en nuestra labor cotidiana. El avance ha sido posible gracias a los muchos años que llevamos utilizando nuestra primera inteligencia artificial, las bases de datos de jurisprudencia, que constituyen realmente la única experimentación que nosotros les podemos aportar a los informáticos, a diferencia de lo que sucede en otras

16. *Cfr.* SAHOTA, N., "Will A.I. Put Lawyers Out Of Business?", *Forbes*, 9-2-2019. https://www.forbes.com/sites/cognitiveworld/2019/02/09/will-a-i-put-lawyers-out-of-business/?sh=70b953631f00. "Will AI Replace Lawyers & Other Myths: Legal AI Mythbusters", *JDSUPRA*, 5-3-2021, https://www.jdsupra.com/legalnews/will-ai-replace-lawyers-other-myths-1763878/.

ciencias, que justamente por eso avanzan muchísimo más deprisa en esta materia. Disponen de muchísimos datos, que a nosotros se nos hacen inaprehensibles.

¿Puede llegar un momento en que esos datos de nuestros procesos dejen de ser tan resbaladizos? Depende del modelo de juez que pensemos asumir en el futuro, más "humano" o con superior automatismo. Hasta el momento, pese a que la "práctica" sin duda ha usado desde hace incluso siglos un rudimentario sistema de automatismos gracias a los modelos de resolución, la ciencia jurídica procesal ha reservado, de manera bastante inconsciente, un espacio enorme al primer modelo, el humano. Se ha aceptado, por ejemplo, que la valoración de los interrogatorios dependa de la intuición del juez fundándose en la "inmediación"[17], instrumento que casi se ha convertido en una especie de varita mágica para algunas jurisprudencias[18] sin la más mínima referencia a la racionalidad. Sucede algo parecido, en el fondo, con la prueba pericial, dado que el compartir o no las razones del perito, incluso con los criterios Daubert[19], acaba siendo casi una cuestión de fe. Pero no sólo eso, sino que también aceptamos que el juez condene a una persona en un proceso penal cuando su convicción vaya "más allá de toda duda razonable", sin concretar con precisión desde ese punto de vista epistémico cuándo concurra ese parámetro o estándar probatorio[20]. Lo mismo exactamente ha sucedido en el proceso civil con la "probabilidad preponderante"[21]. Al final, el juez decide en la sentencia lo que es capaz de motivar de modo que convenza a una mayoría de

17. HENKE, Host-Eberhard,"Rechtsfrage oder Tatfrage – eine Frage ohne Antwort?" *ZZP*, 81, 3-4, 1968, p. 323 y ss. BACIGALUPO ZAPATER, Enrique, "Presunción de inocencia, 'in dubio pro reo' y recurso de casación", *Anuario de Derecho penal y Ciencias Penales*, 1988, pp. 29 y ss.
18. STC 2/2010, 11-1-2010, FJ 4. STEDH 22-11-2011, as. Lacadena Calero c. España. Aunque algo está cambiando muy poco a poco. *Vid.* STS 957/2021 (Sala II), 9-12-2021.
19. Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993), General Electric Co. v. Joiner, 522 U.S. 136 (1997), Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999). *Vid.* sobre los mismos VÁZQUEZ, Carmen, *De la prueba científica a la prueba pericial*, Madrid 2015. NIEVA FENOLL, "Repensando Daubert: la paradoja de la prueba pericial", en AAVV, Peritaje y prueba pericial, Barcelona 2017, pp. 85 y ss., y antes DONDI, Angelo, "Paradigmi processuali ed 'expert witness testimony' nel diritto statunitense", *Rivista Trimestrale di Diritto e Procedura Civile*, 1996, pp. 261 y ss., AULETTA, Ferruccio, *Il procedimento di istruzione probatoria mediante consulente tecnico*, Padova 2002. ANSANELLI, Vincenzo, *La consulenza tecnica nel processo civile*, Milano 2011, TARUFFO, Michele, "Prova scientifica e giustizia civile", en AAVV, *Giurisprudenza e scienza*, Roma 2017, pp. 241 y ss.
20. LAUDAN, Larry, *Truth, error and criminal law: an essay in legal epistemology*, New York 2006, p. 29 y ss, 61. Trata de ponerle remedio a este problema FERRER BELTRÁN, Jordi, *Prueba sin convicción*, Madrid 2021, pp. 208 y ss.
21. ROSENBERG/SCHWAB/GOTTWALD, *Zivilprozeßrecht*, Munchen 2010, p. 768.

juristas sobre todo, aunque tantas veces la proximidad de esos juristas con esa convicción del juez se sustenta en impresiones no realmente explicables. Simplemente les parece convincente, pero a la mayoría se le hace muy difícil indicar con total precisión científica por qué. Y eso es justamente lo que necesitaría un programador de inteligencia artificial.

Sucede lo mismo incluso con la argumentación jurídica. Confiamos en el juez por la *auctoritas* que le otorga su amplia formación jurídica[22], si la tiene, y le llamamos a todo ello *iura novit curia*, sin más, porque pensamos que el juez, sea más o menos avezado o incluso simplemente más o menos inteligente –de todo hay–, será capaz de encontrar en el ordenamiento jurídico la mejor respuesta para nuestro caso, aunque muchas veces, leyendo las motivaciones percibamos perfectamente que no ha sido así. Pero a pesar de ello, le damos todo el crédito a lo decidido y lo protegemos a ultranza con la cosa juzgada, convirtiendo así al juez en una especie de oráculo infalible[23]. Aceptando incluso, o sabiéndolo perfectamente[24], que el juez muchas veces se deja llevar por su intuición acerca del trasfondo de lo realmente acaecido en un caso, acomodando la motivación para obtener la decisión que le parezca justa teniendo presente el indicado trasfondo.

Y esa determinación de lo que sea la justicia es muy frecuente, y está basada, insisto, demasiadas veces en la intuición judicial pese a las múltiples admoniciones de doctrina e incluso jurisprudencia para no proceder así. Pero una vez elaborada la motivación, si es considerada razonable en un juicio intersubjetivo de los tribunales superiores que revisen el caso, revisión que puede ser igualmente intuitiva para la mayoría, no será atacable la sentencia, aunque en el fondo esté mal fundada.

En definitiva, en materia judicial se le ha dado un recorrido tremendo al "ojo clínico" de los jueces, igual que en otro tiempo se le atribuyó al de los médicos. Sin duda, es urgente salir de dicha situación, igual que lo hizo la medicina a través de la tremenda batería de pruebas diagnósticas que hoy existen y que han partido del conocimiento empírico. Por mucho que tantas veces el paciente lo desearía por comodidad, ningún médico sensato hoy en día se atreve ya a realizar diagnósticos intuitivos tomando los pocos datos de la sintomatología que le suministra el paciente. Esas pruebas diagnósticas le son tan cómodas al médico que incluso se abusa

22. CARRERAS LLANSANA, Jorge, *Las fronteras del Juez*, en: "FENECH/CARRERAS, Estudios de Derecho Procesal", Barcelona 1962, pp. 103 y ss.
23. Así lo debieron imaginar los juristas en época de Hammurabi, cuando impusieron esta invariabilidad de las resoluciones judiciales de manera generalizada. *Vid.* NIEVA FENOLL, *La cosa juzgada*, Barcelona 2006, pp. 25 y ss.
24. FORZA, A., MENEGON, G., RUMIATI, R., *Il giudice emotivo*, Bologna 2017.

de las mismas en casos en que la sintomatología permitiría realizar un diagnóstico no 100% seguro, pero sí probablemente más allá de toda duda razonable.

El día en que los juristas obremos realmente de la misma forma que los médicos –sin incurrir en el citado exceso de comprobaciones utilizando debidamente el concepto de pertinencia de la prueba– y busquemos justificaciones a nuestros razonamientos que se alejen de una vez por todas de los argumentos de autoridad –que hoy resultan predominantes en la ciencia jurídica– de autores y jurisprudencia, la inteligencia artificial podrá ayudarnos igual que lo hace en el ámbito de la medicina. Con todo, en el momento actual ya podría hacerlo de forma relativamente sencilla, buscando esas opiniones pasadas, de doctrina o jurisprudencia, que sustentan los pareceres presentes. Cabe imaginar una herramienta que no sólo proponga argumentaciones, como ya existe, sino que identifique las argumentaciones de abogados y jueces y les suministre automáticamente esos anhelados apoyos en forma de citas automáticas, perfectamente identificadas, a Locke, Montesquieu, Blackstone o a la sentencia X del Tribunal Supremo o del Tribunal Europeo de Derechos Humanos, es decir, todas esas citas que a la mayoría de juristas le hacen pensar –tantísimas veces de manera errónea– que un escrito está bien fundamentado.

Lo anterior sería el sueño –casi ensueño– de muchos abogados, jueces, y hasta de bastantes profesores universitarios, por cierto. El efecto positivo es que se abolirían los plagios y hasta se fomentaría la creatividad si el jurista quiere ir más allá de lo que ya existe. El negativo es que juristas creativos hay realmente pocos y con esas herramientas podría haber incluso menos si no empieza a ponerse en valor de una vez esa creatividad. La ciencia jurídica podría ir cayendo en el anquilosamiento de la profecía autocumplida de escritos de parte razonables con respuestas judiciales absolutamente previsibles, igual que cae la jurisprudencia con la fosilización propia del sistema de precedentes[25]. De hecho, ya ha ocurrido incluso considerando solamente, como ya se indicó, el uso de las herramientas de corta y pega.

Pero es justamente de algo así de lo que debe huirse, salvo en los casos en que el automatismo sea la única alternativa razonable, como sucede en los procesos reiterativos que antes se citaron. La ciencia jurídica debe

25. *Cfr.* PASSANANTE, L., *Il precedente impossibile*, Torino 2018, pp. 185 y ss. KOOPMANS, T., *The future of the Court of Justice of the European Communities*, Yearbook of European Law 1991, p. 29 y ss. CHIARLONI, Sergio, *In difesa della nomofilachia*, Riv. trim. di dir. e proc. civ., 1992, p. 127 y ss. TARUFFO, Michele, *La Corte di cassazione tra legittimità e merito*, Il Foro Italiano, Parte V, Roma 1988, p. 237. CROSS, *Precedent in English Law*, Oxford 196, pp. 4, 30-32.

escapar definitivamente de la intuición y de la pura filosofía, acercándose mucho más al empirismo, disponiendo la aplicación del derecho en función de la *voluntas legislatoris* tras una determinación de los hechos que sea correcta desde el punto de vista empírico, respetando siempre, naturalmente, los derechos fundamentales[26].

Y en ese trance, como veremos seguidamente, sí puede ayudar la inteligencia artificial, señalando y descartando lo que es correcto desde una lectura certera de la realidad. Veámoslo.

IV. INTELIGENCIA ARTIFICIAL Y PRUEBA

En los últimos años, el estudio de la prueba ha experimentado un crecimiento extraordinario que nos está permitiendo sacarlo, como antes se ha indicado, de la simple intuición. Ya no creemos que el juez verá a los testigos y sabrá si mienten recurriendo a su "experiencia"[27], sino que ahora, gracias a la psicología del testimonio[28], es posible establecer parámetros cada vez más fiables de credibilidad. Por desgracia, aún no de veracidad, que será la siguiente frontera que tal vez se alcance algún día. De momento permanece en un terreno todavía demasiado intuitivo.

Pero cada vez menos, igual que sucede, como ya se ha dicho, con la prueba pericial. Mejores o peores, tenemos, como ya se dijo, unos criterios de comprobación de las hipótesis, y ese es el primer paso para conseguir que la prueba entre definitivamente en el campo de la ciencia. Curiosamente, mucho ha ayudado una parte de la filosofía en ello, la

26. Como dejó dicho TARUFFO, M., "Idee per una teoria della decisione giusta·, en *Verso la decisione giusta*, Torino 2020, p. 360, explicando así su concepto de "justicia".

27. Partida III, Tít. XVI, Ley 28: "*Otrosi dezimos, que deven ser preguntados del tiempo en que fue fecho aquello sobre que testiguan, assi como del año, e del mes, e del dia, e del logar en que lo fizieron. Ca si se desacordassen los testigos, diziendo el uno que fuera fecho en un logar, e el otro en otra parte, non valdria su testimonio.* (…) *E aun deven ser preguntados los testigos, quien eran los otros testigos que estavan delante, quando acaescio aquello sobre lo que testiguan: e mas preguntas non han por que fazer al testigo que fuere de buena fama. Mas si fuere ome vil, e sospechoso, que entendiesse el Juez, que anda desvariando en su testimonio, entonce devele fazer otras preguntas por tomarle en palabras, diziendo assi: Quando este fecho sobre que testiguas acaecio, que tiempo fazia? Estava nublado, o fazia sol? o quanto ha que conociste estos omes de quien testiguas? e de que paños eran vestidos, quando acaescio esto que dizes? Ca por lo que respondiere a tales preguntas como estas, e porlas señales que viere en la cara del, tomar ha apercibimiento el Juez si ha de creer lo que dize el testigo, o non*".

28. LOFTUS, *Eyewitness testimony*, Harvard 1996. MAZZONI, *Psicologia della testimonianza*, Roma 2015. MAZZONI, *¿Se puede creer a un testigo?*, Madrid 2010. DIGES, *Los falsos recuerdos*, Barcelona 1997. MANZANERO, *Memoria de testigos*, Madrid 2010. MANZANERO, *Psicología del testimonio*, Madrid 2008. IBABE EROSTARBE, *Psicología del testimonio*, Donostia 2000.

epistemología[29], pero en esto el Derecho no se diferencia de otras ciencias. Simplemente le ha costado muchísimo más ser consecuente con las exigencias del método científico, cuya concepción pertenece enteramente, por cierto, al terreno de la epistemología.

En concreto, la inteligencia artificial ayudará en materia probatoria en tres campos principales: la revisión de los parámetros de valoración de la prueba, la elaboración de hipótesis y, eventualmente, la concreción con menor subjetividad de los llamados "estándares probatorios" como consecuencia del indicado segundo campo, la elaboración de hipótesis.

En cuanto al primer terreno, la inteligencia artificial podría operar, por ahora, en un doble ámbito: el de los interrogatorios y el de la prueba pericial. Con respecto a las tradicionales prueba testifical y prueba de declaración de las partes –que obviamente son interrogatorios–, como se acaba de indicar, la psicología del testimonio[30] ha avanzado mucho con abundante experimentación que ha arrojado datos empíricos que son utilizables por los programadores al diseñar los algoritmos. Se podría crear una herramienta de inteligencia artificial que valorara, por ejemplo, las condiciones ambientales de la observación sobre la que se declara, teniendo en cuenta la herramienta si el interrogado estuvo lejos o cerca de lo observado, si había más o menos luz, si había consumido alguna sustancia o si estuvo en una situación de estrés, entre otros puntos de interés. También, por supuesto, podría analizar la posible presencia de móviles para mentir, aunque esto es más complicado, igual que podría tener en cuenta la corroboración de la declaración con el resultado de otras pruebas, la coherencia interna de lo declarado o incluso la presencia de comentarios oportunistas en la declaración.

En concreto, la herramienta podría ser diseñada, no como una especie de robot de funcionamiento automático, sino como una pauta de alertas para que el juez vaya introduciendo sus valoraciones al respecto, de manera que el resultado final no sea una especie de pronóstico de credibilidad, sino simplemente el resultado de un trabajo del juez guiado por la herramienta, que podría asistirle también en la motivación. De ese modo podríamos evitar, al menos en parte, los errores que ya sabemos que se

29. Hay que agradecer su labor, entre otros, a LAUDAN, Larry, *Truth, error and criminal law: an essay in legal epistemology*, New York 2006. GASCÓN ABELLÁN, Marina, *Los hechos en el derecho. Bases argumentales de la prueba*, Madrid-Barcelona 2004. FERRER BELTRÁN, Jordi, *La valoración racional de la prueba*, Madrid 2007. GONZÁLEZ LAGIER, *Quaestio facti. Ensayos sobre prueba, causalidad y acción*, Lima, 2005 y, por supuesto, a TARUFFO, Michele, *La prueba de los hechos*, trad. de Jordi Ferrer Beltrán de "la prova dei fatti giuridici", Milano 1992, Madrid 2002.

30. *Vid.* las obras ya citadas al respecto.

han detectado en las herramientas de predicción del riesgo y que veremos en el epígrafe siguiente.

El segundo campo interesante en materia probatoria en que puede intervenir la inteligencia artificial es el de la elaboración de hipótesis. En este caso, la herramienta –ya con precedentes en ALIBI[31]– lo que hace es partir de los datos que le va suministrando el juez acerca de la prueba, elaborando hipótesis de qué ha podido suceder. Hasta el momento se ha utilizado para suministrar a los abogados líneas de defensa para la concepción de coartadas para sus clientes, pero se podría utilizar perfectamente para formular una serie de hipótesis de qué ha podido suceder partiendo de los datos de los que el juez dispone. El trabajo de la herramienta tendría como resultado, por ejemplo, la exposición de esas hipótesis, que habrán sido elaboradas partiendo de casos antiguos, lo que supone reunir toda la "experiencia", y mucho más, que pueda tener un juez como fruto de su memoria, pero con dos inconvenientes: la máquina no es creativa, por lo que puede ser esclava de hipótesis de relatos que sucedieron sólo en el pasado, pero que no tienen que ver con el presente; además esos datos, como se ha dicho, serán de procesos antiguos, lo que provocará que si los mismos no fueron juzgados correctamente –y eso difícilmente lo sabremos salvo que se evidencie el error judicial más adelante– se irán arrastrando esos errores y, lo que es peor, su influencia en el presente. Un auténtico desastre.

Ese problema, que en absoluto es menor, lastra el tercer terreno en el que se podría utilizar la IA: la concreción de estándares probatorios[32]. Los mismos otorgan aparentemente una gran seguridad a los operadores jurídicos, que encuentran en ellos una especie de fórmulas mágicas para exponer sus conclusiones probatorias, pero son muchísimas veces sólo intuitivos, pese a que pretendan los contrario. En su versión a mi juicio más depurada[33], parten precisamente de la elaboración de hipótesis propia de la probabilidad inductiva, arrojando conclusiones más o menos seguras en función de si las hipótesis alternativas a la que va alcanzando mayor sustento probatorio, se van descartando, logrando así por fin un grado de confirmación que pretende otorgar más seguridad al juez que toma la decisión.

En ese escenario podría ayudar naturalmente la inteligencia artificial, pero de un modo limitado aunque a mi juicio benéfico. Podría, en concreto, servir de pauta de la conducta probatoria del juez y las partes en el trance de la admisión y la práctica de la prueba. Al exponer esas hipótesis,

31. NISSAN, E., "Legal Evidence, Police Intelligence, Crime Analysis or Detection, Forensic Testing, and Argumentation: An Overview of Computer Tools or Techniques", 17 Int'l J.L. & Info. Tech. 1, 2009, pp. 1 y ss.
32. *Vid.* nuevamente FERRER BELTRÁN, *Prueba sin convicción*, *cit.*, pp. 29 y ss.
33. *Ibidem.*

es más fácil realizar correctamente la labor de admisión de los medios de prueba, y también es más sencillo guiar su práctica, escapando de la tradicional hipótesis única que sólo busca confirmarse o desmentirse, y que puede ser fácilmente víctima del sesgo de confirmación.

Es decir, siendo a mi juicio la mayor utilidad de los estándares la de servir de pauta probatoria a los jueces, la inteligencia artificial sería útil para conseguir guiar aún mejor el uso de esa pauta, ampliando incluso su rango de observación al ser más probable que elabore bastantes más hipótesis que las que se le puedan ocurrir a un juez tomando como única ayuda su imaginación y la de las partes.

Confirmada la hipótesis de que se trate, la herramienta puede incluso ayudar a redactarla, igual que ya se vio que era posible con el juicio de derecho partiendo sobre todo de la jurisprudencia. Y ello no debe sorprender ni causar estupefacción, puesto que hará más sencilla la labor judicial, con la consiguiente ayuda humana del juez para completar la redacción, como es lógico.

V. INTELIGENCIA ARTIFICIAL Y PREDICCIÓN DEL RIESGO

Este ha sido el campo en el que más se ha desarrollado la inteligencia artificial en el ámbito judicial, y con resultados tan espectaculares como controvertidos. En materia procesal penal, en diferentes momentos, los jueces se preguntan si una persona tiene un perfil de riesgo a fin de saber fundamentalmente si volverá a cometer un delito, aunque también para acabar de corroborar pruebas que no les convencen del todo, consiguiendo esa deseada confirmación a través de la averiguación del perfil del reo. Son casos en que el juez tiene ya una convicción razonable acerca de la culpabilidad, pero desea elevar ese nivel de convicción con la indicada determinación del perfil.

Quienes habían perfilado tradicionalmente a los reos, en el mejor de los casos, eran los psicólogos. También los juristas intentaban establecer pareceres –bastante *amateurs*, por cierto– recurriendo a los antecedentes penales del reo e incluso a su comportamiento en la sala de justicia o en el momento de la detención, o incluso acudiendo a trasnochados saberes lombrosianos[34] que pese su carácter vetusto y reiteradamente desacreditado, conservan una sorprendente supervivencia en el imaginario colectivo que también comparten los jueces. Pero todo ello no eran más que prejuicios de quien no es experto en una materia.

34. LOMBROSO, Cesare, *L'uomo delinquente*, Torino 1897.

Al contrario, los psicólogos de la personalidad[35] fueron elaborando a lo largo de los años una serie de criterios para evaluar el riesgo que podían suponer los reos, compilando decenas de dichos criterios que han ido utilizando cotidianamente en las entrevistas cognitivas que han practicado a un sinfín de sujetos pasivos del proceso penal, sobre todo para evaluar los riesgos de la concesión de permisos carcelarios a un reo, o bien para dictaminar acerca de su libertad condicional.

Entre dichos criterios existen fundamentalmente datos que diversos metaanálisis han demostrado que son buenos predictores de futuro comportamiento delictivo, no considerados de forma separada, sino de manera conjunta. Y así se tiene en cuenta, por ejemplo, el consumo abusivo de alcohol u otras sustancias estupefacientes, el nivel atencional de un reo, su capacidad de compromiso, su comportamiento violento en la prisión a través de la revisión de su expediente disciplinario, el hecho de ser capaz de generar un entorno de amistad, etc.[36].

Sin embargo, también se han tenido en cuenta a lo largo de los años datos mucho más sensibles como el nivel de estudios, el lugar de residencia, la tenencia de un domicilio fijo o el número de mudanzas en los últimos años, o también datos definitivamente orientados ideológicamente como las opiniones políticas sobre algunos delitos o incluso la raza, por no hablar de la estética física que el individuo decide atribuirse[37]. No se crea, además, que se recurre solamente –aunque también– a los prejuicios para elaborar esos criterios, sino que habitualmente se identifican todos esos datos en personas enjuiciadas –de manera correcta o errónea, es imposible saberlo– como culpables, y a partir de ahí se van elaborando datos estadísticos de incidencia de esos criterios en cada reo que sirven para reforzar o disminuir la relevancia de los mismos en las evaluaciones.

35. *Vid*. entre otros REDONDO ILLESCAS, Santiago/ANDRÉS PUEYO, Antonio, "Predicción de la violencia: entre la peligrosidad y la valoración del riesgo de violencia", *Papeles del psicólogo: revista del Colegio Oficial de Psicólogos*, vol. 28, n. 3, 2007 (Ejemplar dedicado a: Predicción de la violencia), pp. 157 y ss. REDONDO ILLESCAS, Santiago/ANDRÉS PUEYO, Antonio, "La Psicología de la delincuencia, *Papeles del psicólogo: revista del Colegio Oficial de Psicólogos*, vol. 28, n. 3, 2007 (Ejemplar dedicado a: Predicción de la violencia), pp. 147 y ss. ANDRÉS PUEYO, Antonio/LÓPEZ, S./ÁLVAREZ, E., "Valoración del riesgo de violencia contra la pareja por medio de la SARA", *Papeles del Psicólogo*, 2008. Vol. 29 (1), pp. 107 y ss.

36. NORTHPOINTE, *Practioners Guide to COMPAS*, 17-8-2012, pp. 23 y ss. http://www.northpointeinc.com/files/technical_documents/FieldGuide2_081412.pdf.

37. BORNSTEIN, Aaron M., "Are algorithms building the new infrastructure of racism?", *Nautilus*, 21-12-2017, http://nautil.us/issue/55/trust/are-algorithms-building-the-new-infrastructure-of-racism, y nuevamente NORTHPOINTE, *Practioners Guide to COMPAS*, 17-8-2012, pp. 23 y ss. http://www.northpointeinc.com/files/technical_documents/FieldGuide2_081412.pdf.

Hace ya tiempo que la inteligencia artificial, o mecanismos similares, entraron en estas evaluaciones, en ocasiones de manera menos polémica, como en el caso de RISCANVI[38] o HART[39], a veces de manera extraordinariamente polémica, como ha sucedido y está sucediendo con COMPAS[40], y otras veces de modo un tanto ingenuo, como acontece con Viogén[41] o desde 2018 con Veripol[42]. Por ser bastante reasuntivo y reflejar un nivel máximo de peligro, se explicará solamente lo sucedido con COMPAS en los Estados de EE. UU. que lo utilizan, que por fortuna ni mucho menos son todos.

COMPAS es una auténtica herramienta de inteligencia artificial que asiste –no sustituye– a los jueces en la predicción del riesgo a fin de evaluar este factor en un reo a efectos de imponer medidas cautelares, decisiones de libertad en el ámbito penitenciario o incluso como acompañamiento de veredictos de culpabilidad. Lo que se conoce de la herramienta –sus fabricantes[43] no revelan los entresijos de su funcionamiento por razones de propiedad intelectual– es relativamente poco. Su algoritmo tiene en cuenta 137 criterios[44], entre los cuales están los antes indicados, también los más polémicos. Pero nadie sabe realmente cómo se realiza esa evaluación. Simplemente se ha demostrado ya en varios estudios que la herramienta no es más acertada que un ser humano[45], y

38. ANDRÉS-PUEYO, A./ARBACH-LUCIONI, K./REDONDO, S., "The RisCanvi: A New Tool for Assessing Risk for Violence in Prison and Recidivism", en *Handbook of Recidivism Risk/Needs Assessment Tools*, Chichester 2018, pp. 255 y ss.
39. "Harm Assessment Risk Tool". GIAMPIERO, L., "Regulating (Artificial) Intelligence in Justice: How Normative Frameworks Protect Citizens from the Risks Related to AI Use in the Judiciary", *cit.*, p. 81.
40. "Correctional Offender Management Profiling for Alternative Sanctions". NORTHPOINTE, Practioners Guide to COMPAS, 17-8-2012.
41. http://www.interior.gob.es/web/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen.
42. OFICINA DE TRANSFERENCIA DE RESULTADOS DE INVESTIGACIÓN (OTRI). UNIVERSIDAD COMPLUTENSE DE MADRID, "Veripol, inteligencia artificial a la caza de denuncias falsas", https://www.ucm.es/otri/veripol-inteligencia-artificial-a-la-caza-de-denuncias-falsas.
43. Northpointe, Inc.
44. https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html. NORTHPOINTE, *Practioners Guide to COMPAS*, 17-8-2012, pp. 23 y ss.
45. FARRELL, JAMES, "Humans Beat Popular Algorithm For Spotting Potential Re-Offenders", *SILICONANGLE*, 17-1-2018, https://siliconangle.com/blog/2018/01/17/popular-algorithm-used-spot-potential-reoffenders-sometimes-extend-prison-sentence-doesnt-work-according-researchers/. FUSSELL, Sidney, "Study Finds Crime-Predicting Algorithm Is No Smarter Than Online Poll Takers", *Gizmodo*, 18-1-2018, https://gizmodo.com/study-finds-crime-predicting-algorithm-is-no-smarter-th-1822173965. PEARSON, Jordan, "Bail Algorithms Are As Accurate

que además es indudablemente racista[46]. Se teme incluso que esta última característica ni siquiera sea algo que los fabricantes hayan querido eludir, sino más bien todo lo contrario. Bien parece que han elaborado unos perfiles de población–diana sobre la que se desea deliberadamente actuar, con un resultado final que es claramente escandaloso[47]. De momento esta herramienta no ha llamado la atención –pese a que no ha faltado oportunidad[48]– del Tribunal Supremo Federal de los EE. UU., aunque considerando cuál fuere su composición en un momento determinado, tal vez es mejor que no se fijen demasiado en esta herramienta, a riesgo de bendecir un autoritarismo y arbitrariedad realmente incompatibles con el mantenimiento de la democracia. Lo tristemente sucedido con la benéfica e histórica jurisprudencia de la regla de exclusión[49], podría tener su secuela también en este ámbito.

Con todo ello puede verse cómo la tecnología se puede falsear y poner al servicio de las ideologías, cuando de lo que se trataba en un inicio es de imprimir objetividad y racionalidad al comportamiento judicial. Y es que en realidad, en esta materia puede acabar sucediendo lo mismo que con otros ingenios de inteligencia artificial. Al ir aumentando su enorme base de datos automáticamente con el falazmente llamado *machine learning*, puede llegar un momento en que la máquina sea víctima de la peor versión del sesgo de confirmación, afectando a su funcionamiento de una manera todavía más radical de lo que lo hace con las personas. Quiero decir con ello que la máquina se puede ir haciendo paulatinamente cada vez más discriminadora con determinados grupos de población, a fuerza de ir propiciando cada vez más condenas contra esos colectivos, nutriendo al algoritmo con los datos de dichas condenas.

As Random People Doing An Online Survey", *Motherboard*, 17-1-2018, Https://Motherboard.Vice.Com/En_Us/Article/Paqwmv/Bail-Algorithms-Compas-Recidivism-Are-As-Accurate-As-People-Doing-Online-Survey. YONG, Ed, A Popular Algorithm Is No Better At Predicting Crimes Than Random People, *The Atlantic*, 17-1-2018, https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/.

46. LARSON, Jeff/MATTU, Surya/KIRCHNER, Lauren/ANGWIN, Julia, "How We Analyzed The Compas Recidivism Algorithm", *Propublica*, 23-5-2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.
47. CORBETT-DAVIES, Sam/PIERSON, Emma/FELLER, Avi/GOEL, Sharad, "A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear", *The Washington Post*, 16-10-2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/?noredirect=on&utm_term=.c31b4a5b6bbd.
48. State v. Loomis. 881 N.W.2d 749 (Wis. 2016).
49. *Vid.* MIRANDA ESTRAMPES, Manuel, *Prueba ilícita y regla de exclusión en el sistema estadounidense. Crónica de una muerte anunciada*, Madrid 2019.

Lo que sucede es que estas herramientas descubren lo peor de la inteligencia artificial y la razón principal de su parón. La técnica mira siempre al pasado porque se nutre de los datos provenientes del mismo. Y en lugar de superarlo, como ha sucedido tantas veces en la historia humana, se hunde cada vez más en él. Como ya se anunció al inicio de este artículo, la inteligencia artificial es incapaz de superarse, al menos por el momento. Actúa siempre exactamente igual, y son solamente los humanos que mueven los hilos de sus algoritmos los que pueden alterar esta realidad. Y no es nada fácil, dado que el funcionamiento interno de la máquina es algo similar a un conjunto imbricado de madejas de las que es bastante complicado encontrar los hilos correctos llegados a cierto punto.

En realidad, con frecuencia lo único que puede hacerse es empezar de nuevo y construir otra herramienta, que volverá a tener los mismos problemas que la anterior, especialmente el de la orientación ideológica, que es difícilmente evitable en materia judicial. Al fin y al cabo, los jueces de un país siguen diversos patrones ideológicos, más allá de los valores constitucionales, aunque no debiera ser así. Y dichos patrones, si son mayoritarios, acabarán haciéndose preponderantes gracias a la IA, porque se nutre siempre, como ya se ha indicado, de decisiones judiciales pasadas.

Mientras no se supere este inconveniente tecnológico, el problema se producirá una y otra vez. Tal vez ello impedirá un uso extendido de esta tecnología en este ámbito de la realidad judicial, o tal vez la continuará afectando negativamente. Cualquiera de los dos escenarios es nefasto. Y la única solución es la revisión e influencia constante de juristas con valores democráticos muy consolidados trabajando codo con codo con los programadores, existiendo un control democrático estricto en la elección de ambos grupos de profesionales. Nada de lo indicado es fácil en absoluto, pero acabará siendo imprescindible si se desea –sólo si se desea– evitar el autoritarismo.

VI. INTELIGENCIA ARTIFICIAL Y ODR

Un ámbito en el que ya existe inteligencia artificial funcionando con cierta frecuencia es el de los ODR. Empezaron algunas empresas[50] a utilizarlo, pero ahora ya son los organismos públicos de algunos países[51] los

50. Ebay: https://pages.ebay.com/services/buyandsell/disputeres.html#what; Paypal: https://www.paypal.com/us/webapps/mpp/security/seller-dispute-resolution; Amazon: https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=G9NMDH46UFNMFNKN.

51. Entre otros, Holanda: KISTEMAKER, Laura, "Rechtwijzer and Uitelkaar.nl. Dutch Experiences with ODR for Divorce", *Family Court Review*, abril 2021. *Vid.* otras experiencias de EE. UU. y Canadá en JTC Resource Bulletin, Case Studies in ODR for

que están aplicando –o al menos interesándose– por esta tecnología para resolver sobre todo algunas pequeñas causas, esas grandes olvidadas –salvo excepciones– de los sistemas judiciales de todos los tiempos. Parece que por fin se podría encontrar una manera rapidísima y muy barata de resolver estas controversias ya citadas anteriormente, en particular reclamaciones de cantidad, procesos posesorios, procesos de consumidores y divorcios no demasiado complejos, que son la mayoría, por otra parte, si se huye de la salsa del anecdotario de cualquier abogado matrimonialista.

Ciertamente, a día de hoy ya no cuesta tanto pensar en una app para interponer una solicitud monitoria o para divorciarse. En ambos casos, la app tendría que ir dando opciones al usuario que este debería ir marcando. Sin ánimo alguno de exhaustividad, en el caso de la solicitud monitoria, indicar el nombre completo del deudor, la cantidad debida y subir el documento del que se derive la existencia de la deuda. Los datos del acreedor ya figurarán por defecto en la app, que los habrá pedido al descargarla. Con esos datos, la app emitiría un mandato de pago que el deudor contestaría en el plazo establecido en las leyes, con advertencia de que si hay oposición se generará un proceso jurisdiccional y en caso de perderlo, podría sobrevenir una sanción –debiera concretarse cuál– por uso indebido de la administración de justicia. Con ello, la reclamación quedaría resuelta. Lo mismo sucedería con un divorcio. Se formularía la solicitud, que estaría conectada con los datos de los registros para averiguar la existencia de hijos, bienes en común y capacidad económica. De no haber oposición al divorcio, la propia plataforma lo declararía, calcularía la pensión, y pondría en marcha la división del patrimonio, operaciones que podrían ser moduladas posteriormente por los tribunales, pero con el divorcio ya declarado. Y siempre que esas operaciones sean necesarias, claro está. De hecho, es posible que en el futuro, superando la influencia sobre la legislación civil de la indisolubilidad canónica del vínculo, se simplifiquen bastante las medidas económicas consecuencia de un divorcio, pero esa es otra cuestión.

Los anteriores son solamente dos ejemplos de los muchos que podrían darse – entre otros, las ya citadas reclamaciones de consumidores– acerca de lo que está por venir, que podría llegar a automatizarse aún más en el futuro siguiendo la mecánica de los contratos inteligentes –*smart contracts*–: en caso de impago, se formularía inmediatamente una solicitud monitoria. De ese modo, la resolución de esos conflictos tan frecuentes –los impagos de acreedores– sería tan rápida que probablemente el conflicto, o acabaría desapareciendo o nunca llegaría a los tribunales. De hecho, actualmente alcanzan ese estado judicial, como ya se ha dicho, en

Courts: A view from the front lines. 29-11-2017. https://www.srln.org/system/files/attachments/Case%20Studies%20in%20ODR%20for%20Courts.pdf.

un intento del deudor de mala fe de utilizar en su favor la lentitud de la administración de justicia.

Pero por otra parte, los ODR pueden favorecer una reforma que ya se está empezando a reclamar desde distintos foros: la contundente simplificación de las normas de competencia territorial, y en muchos casos su abolición[52]. Si los litigios se sustancian en su mayoría a distancia con una restricción drástica de la oralidad[53], carece de sentido que deban asignarse a una sola sede y que además esa asignación pueda provocar complicaciones. Al contrario, cuando los procesos son *online*, no tiene absolutamente nada de particular que los resuelva cualquier tribunal de un Estado, sea cual fuere el territorio en que radique, propiciándose de ese modo una más racional distribución de los recursos materiales y humanos de la justicia de un país, al ser asignados los procesos de manera equitativa a los tribunales con menor carga de trabajo. Palabras como "declinatoria" podrían pasar a la historia en esos procesos, que pueden ser muy fácilmente la mayoría.

Por último, como ya se referenció al inicio de este apartado, debe destacarse la presencia de servicios corporativos que resuelven en línea las reclamaciones de los usuarios cuando no son complejas, consiguiéndose así la evitación de un nuevo proceso. Se trata de herramientas de inteligencia artificial que identifican el problema y ofrecen soluciones al consumidor o usuario, resolviendo definitivamente el inconveniente o canalizándolo al departamento correspondiente de la empresa para favorecer su correcta resolución. Con ello, no solamente se evitan procesos, sino que aumenta el nivel de satisfacción de los usuarios. Algunas de esas herramientas formulan incluso propuestas de conciliación, que una vez aceptadas por el usuario, se convierten en un medio alternativo eficaz íntegramente *online*.

VII. UN POSIBLE FUTURO

Es completamente desconocido cómo va a ser el futuro. Lo imaginamos siempre acompañado de una mejora imparable de la tecnología, lo que podría no ser así dependiendo de las circunstancias sociales de cada momento. Las crisis, económicas o incluso bélicas, o las simples faltas de inversión pueden ralentizar los procesos. Ahora mismo, como se dijo al principio del artículo, estamos en un momento evidente de parón derivado

52. *Vid.* NIEVA FENOLL, *Derecho Procesal II, Proceso Civil*, *cit.*, pp. 37-38.

53. *Vid.* NIEVA FENOLL, "La discutible utilidad de los interrogatorios de partes y testigos (algunas reflexiones sobre la oralidad en tiempos de pandemia)", *Ius et Praxis*, vol. 26, n. 3, diciembre 2020. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122020000300157&lng=n&nrm=iso&tlng=n.

de diversas circunstancias, como ya se indicó, no todas claras dejando al margen la dificultad inmensa de configurar correctamente los algoritmos para ser aplicables a situaciones que siempre habían dependido de decisiones con un margen de discrecionalidad elevado el tener en cuenta una multiplicidad de factores, no siempre atribuyéndoles el mismo peso. Ese es el caso de los procesos judiciales. Por mucho que las leyes otorguen más estabilidad a las decisiones de los jueces, al final confiamos en juzgadores que son tan humanos como nosotros para que perciban con empatía el caso que se les plantea, empatía social que no siempre pueden reflejar las leyes con puntualidad.

Con todo, si este *impasse* se supera, la presencia humana en los tribunales menguará, igual que lo hará el número de abogados dedicados a los procesos judiciales. Debe evitarse en cualquier caso caer en experiencias de total automatización que anularían la voluntad de los jueces en beneficio de la imposición de las líneas de actuación del poder ejecutivo[54], que es el que acostumbrará a estar encargado de financiar la tecnología para configurar los algoritmos. Es aceptable la automatización de los procedimientos, pero no del enjuiciamiento salvo en casos realmente reiterativos. Debería ser este un límite ético que nunca debiera superarse, a riesgo de pasar de la justicia de los jueces a la justicia de los programadores y de aquellos que les influyan, lo que sería democráticamente inadmisible.

La clave está, por tanto, en no superar los límites que marcan los derechos fundamentales, anulando el derecho de defensa frente a una máquina que va a juzgar siempre sistemáticamente igual en situaciones que puedan parecer idénticas, pero que no lo son atendidas las muy diferentes circunstancias socioeconómicas de los sujetos concernidos. Tampoco es aceptable no dejar espacio a la presunción de inocencia de personas cuyas características estén ya señaladas de antemano por el algoritmo, y que por ello irremediablemente van a verse sujetas en el mejor de los casos sólo a medidas cautelares, y en el peor de ellos a condenas injustas.

Hay que luchar porque todo lo conseguido gracias al derecho al juez independiente e imparcial, no se pierda si algún día las máquinas influyen en mayor medida en el enjuiciamiento. La independencia judicial y la imparcialidad constituyen un único concepto formulado de manera

54. *Vid.* See "Big Data, AI and China's Justice: Here's What's Happening", *China Justice Observer*, 1-12-2019. https://www.chinajusticeobserver.com/a/big-data-ai-and-chinas-justice-heres-whats-happening. See also Jie-jing YAO/Peng HUI, "Research on the Application of Artificial Intelligence in Judicial Trial: Experience from China", *Journal of Physics: Conference Series*, vol. 1487, 2020. https://iopscience.iop.org/article/10.1088/1742-6596/1487/1/012013/meta.

habitualmente binómica, que intentaba que los jueces estuvieran libres de influencias en su criterio que pudieran activar sus emociones, de manera que su juicio se viera ilegítimamente alterado por las mismas. Como dije, se espera del juez una empatía que refleje el consenso social que intentan reflejar las leyes, pero no hasta el punto de manipular lo que dicen esas leyes hasta acabar pervirtiéndolas, que es lo que puede suceder cuando el juez no es auténticamente independiente. Se trata de que no se caiga en el mismo riesgo derivando la decisión en autoridades de programación que no son independientes, o bien en programadores que no pueden evitar que en el proceso de adquisición de datos y enriquecimiento de la herramienta, se manipule igualmente el proceso de decisión de la herramienta, como está sucediendo con algunas redes sociales, particularmente en el momento actual con Facebook[55].

No hay que alarmarse, no obstante. La incorporación de esta tecnología al proceso de manera decidida va a ser tecnológicamente lenta, al menos de momento. Las advertencias que se han realizado están formuladas para el instante en que esa misma tecnología vuelva a avanzar de nuevo de modo acelerado, cosa que, aunque nada es seguro, siempre puede acabar sucediendo.

55. PLANAS BOU, Carles, "La manipulación política se propaga en Facebook", *El Periódico*, 15-9-2020.

Retos del derecho probatorio ante las nuevas tecnologías[1]

Joan Picó i Junoy

Catedrático de Derecho Procesal
Universitat Pompeu Fabra (Barcelona)

SUMARIO: I. INTRODUCCIÓN. II. LAS NUEVAS TECNOLOGÍAS COMO FUENTES DE PRUEBA. PROBLEMAS QUE PLANTEAN Y SOLUCIONES. III. LAS NUEVAS TECNOLOGÍAS COMO INSTRUMENTOS AL AUXILIO DE LOS TRADICIONALES MEDIOS DE PRUEBA: LA NEUROCIENCIA Y LOS ALGORITMOS DE MICRO-EXPRESIONES FACIALES. 1. *La neurociencia*. 2. *Los algoritmos de micro-expresiones faciales*.

I. INTRODUCCIÓN

Las nuevas tecnologías están presentes en todos los actos de nuestra vida cotidiana. Estamos en plena Cuarta Revolución Industrial, y el derecho probatorio no es ajeno a esta realidad social.

Estas nuevas tecnologías pueden incidir en el derecho probatorio de dos formas distintas: (a) como mecanismos de reproducción de la realidad susceptibles de formar la convicción judicial, esto es, como nuevas fuentes probatorias; y (b) como instrumentos de auxilio de los tradicionales medios de prueba en la medida en que se presentan como herramientas susceptibles de verificar el resultado de las pruebas de interrogatorio de las partes, testigos y declaraciones de peritos.

1. El presente trabajo se enmarca dentro del Proyecto I+D+i "Nuevos retos tecnológicos del derecho probatorio" (PID2020-115304GB-C21) del Plan Estatal de Investigación Científica del Ministerio de Ciencia e Innovación; y del Grupo de Investigación Reconocido, Consolidado y Financiado "Evidence Law" (2017 SGR 1205) de la AGAUR, ambos liderados por Joan Picó Junoy.

II. LAS NUEVAS TECNOLOGÍAS COMO FUENTES DE PRUEBA. PROBLEMAS QUE PLANTEAN Y SOLUCIONES

La Cuarta Revolución Industrial en la que nos encontramos se caracteriza por el uso masivo de las nuevas tecnologías y su intervención en casi todos los actos del hombre. Todo ello constituye una inmensa fuente de elementos probatorios que pueden utilizarse en un proceso judicial. Estas nuevas fuentes de prueba se hayan especialmente en cuatro ámbitos de la sociedad:

a) En la forma de relacionarse las personas, mediante el uso continuo de las redes sociales como Facebook (con cerca de 3.000 millones de usuarios), YouTube (con más de 2.500 millones de usuarios), WhatsApp (con 2.000 millones de usuarios), la reciente TikTok (con 1.000 millones de usuarios); o Twitter (con 350 millones de usuarios)[2]; y el almacenamiento y transmisión de todo tipo de información, datos o contenidos *online* en alguno de los muchos espacios virtuales que hay en el mercado como Google Drive, Dropbox, WeTransfer, Mega, Box, OneDrive, Dataprius, CloudMe, HubiC, Degoo, MediaFire, Weflio Drive, Filesharing24, PlusTransfer, Wimi, etc. Todos estos conceptos han pasado a formar parte de nuestro vocabulario habitual;

b) En la contratación electrónica, especialmente con el desarrollo vertiginoso de grandes empresas multinacionales dedicadas al comercio electrónico de cualquier tipo de producto o servicio, como las estadounidenses Amazon o Ebay; las chinas Alibaba o Tencent, la japonesa Rakuten; o las europeas Vente Privee o Zalando. El auge de la contratación electrónica por internet hace que la facturación del volumen de negocio *online* se acerque cada día más al tradicional en papel;

c) En la interconexión directa de los instrumentos electrónicos habituales en la vida de los ciudadanos a través de internet, esto es, internet de las cosas (IoT). Diferentes estudios indican que hoy en día hay 42.620 millones de dispositivos electrónicos conectados a Internet al objeto de ofrecer servicios y aplicaciones inteligentes útiles para el confort de la sociedad (y esta cifra se duplicará en poco tiempo, hasta llegar a los 75.440 millones en 2025)[3]. Este continuo incremento de IoT está favoreciendo el increíble auge de los *smart contracts* en los que las cosas interactúan autónomamente, esto es, sin intervención directa de las personas, en función del

2. Datos obtenidos de https://blog.hootsuite.com/simon-kemp-social-media/ (fecha de consulta: 3 de abril de 2022).
3. Ver https://www.researchgate.net/figure/Internet-of-Things-IoT-connected-devices-from-2015-to-2025-in-billions_fig1_325645304 (fecha de consulta: 3 de abril de 2022).

programa para el que han sido desarrollados[4]. Sin embargo, lo cierto es que en la actualidad todavía no se han planteado especiales problemas probatorios respecto de los *smart contracts*; y

d) En la forma de comunicarse las personas, sustituyendo las palabras por símbolos o figuras (*emojis* o *emoticons*) que, como destacan GOLDMAN y ABEL FABREGÓ, también tienen su repercusión probatoria, pues cada vez es más frecuente en los tribunales la admisión de dichas figuras para probar los hechos que simbolizan[5].

Lo primero que debemos destacar es que estamos ante una materia en la que, otra vez más, la tecnología va por delante de las leyes, por lo que la práctica de los tribunales intentar afrontar los nuevos problemas tecnológicos con los instrumentos legales clásicos. En este trabajo solo vamos a referirnos a las cuestiones probatorias, por lo que no entraremos a examinar, por ejemplo, la gestión telemática de los procesos o los tribunales electrónicos, o cualquier otra materia que exceda del estrictamente probatorio.

En materia probatoria, en todos los países se plantean problemas similares y muy complejos[6]. Estamos acostumbrados a probar los hechos físicos que resultan fácilmente constatables en la medida en que están en soporte papel, pero todo ello se hace mucho más difícil cuando estamos

4. Un *smart contract*, siguiendo el concepto de su propio creador SZABO (*Foreword to "Smart Contracts": 12 Use Cases for Business & Beyond*, en "Chamber of Digital Commerce, Washington, D.C.", 2016 [*cfr.* http://digitalchamber.org/assets/smart-contracts-12-use-cases-for-business-and-beyond.pdf –fecha de consulta: 1 de febrero de 2022–]; y *Smart Contract*, en "Building Blocks for Digital Markets", 1996 [*cfr.* http://digitalchamber.org/assets/smart-contracts-12-use-cases-for-business-and-beyond.pdf –fecha de consulta: 1 de febrero de 2022–]) es el conjunto de obligaciones, especificadas en forma digital, que incluyen los protocolos de actuación dentro de los cuales las partes cumplen automáticamente sus obligaciones. Su campo de actuación en inmenso: así, por ejemplo, en diciembre de 2016, la *Chamber of Digital Commerce* –la asociación comercial más grande del mundo que representa la industria digital y de *blockchain*, con sede en Washington, D.C., en el documento "Smart Contracts: 12 Use Cases for Business & Beyond" describe doce ejemplos de *smart contracts* para ámbitos tan amplios como identificaciones digitales de las personas, financiación del comercio, gestión de valores, servicios post-comercio, registros de datos financieros, transacciones bancarias e hipotecas, transmisiones de propiedades, cadenas de suministros de cualquier tipo, seguros de automóviles, ensayos clínicos, etc.

5. GOLDMAN, E., *Emojis and the Law*, en "Washington Law Review", vol. 9: 2018, pp. 1227-1291; y ABEL FABREGÓ, A., *Los emojis como fuente de prueba*, en "Revista Jurídica de Catalunya", vol. 120, 2021: 4, pp. 977-1002.

6. Para una visión de derecho comparado me remito a PICÓ I JUNOY, J., *The New Challenges of Evidence Law in the Fourth Industrial Revolution*, a "Technology, the Global Economy and other New Challenges for Civil Justice", K. Miki (ed.), editorial Intersentia, Cambridge, 2021, pp. 477-518.

ante lo que podemos denominar "hechos electrónicos o digitales" (entendiendo por "hecho electrónico" aquel que se realiza de manera virtual o no física, esto es, básicamente a través de Internet). Por ello, el proceso civil tradicional debe adaptarse rápidamente a estos nuevos retos tecnológicos.

Vamos a intentar descubrir cómo está empezando a afectar el mundo tecnológico al ámbito de la prueba judicial, y cuál es el futuro que nos espera. Y se procurará resolver los interrogantes que habitualmente se plantean en todos los tribunales del mundo y que no siempre tienen fácil solución: ¿Cómo accede un dato electrónico al proceso? ¿Qué límites hay en el control de los datos electrónicos? ¿Cómo se impugnan y verifican? ¿Qué precauciones han de tomarse para conservar datos electrónicos? ¿Cuándo es necesario un peritaje informático?, etc.

Cuando las pruebas no están en el mundo real, sino en el virtual o digital, se complica muchísimo su búsqueda y aportación al proceso. Los citados ámbitos de la sociedad en los que las nuevas tecnologías se han desarrollado especialmente, tienen una regulación normativa similar en todo el mundo: las redes sociales y la contratación electrónica tienen su propia regulación en todos los estados democráticos; y IoT suele estar huérfana de una regulación específica en casi todos los países.

Hay dos grandes problemas que suelen estar presentes en la prueba de los hechos electrónicos o digitales, y que son realmente preocupantes: la posible intromisión en la vida privada o esfera más íntima de las personas para lograr acceder a tales hechos, precisamente, porque se mantienen en un ámbito cerrado de privacidad; y la facilidad de manipulación o alteración de su contenido.

Respecto del primer problema, es cierto que la tecnología ha abierto ciertos ámbitos de la esfera íntima de las personas que, con anterioridad, se mantenían privados (así, por ejemplo, puede vulnerarse el derecho al honor, a la imagen o a la intimidad a través de noticias transmitidas mediante redes sociales; pueden exponerse públicamente determinados hechos de contenido familiar, personal o íntimo en un WhatsApp o un SMS; o mediante IoT se puede entrar en el interior de una vivienda a través de cualquier dispositivo que se encuentre en ella y esté conectado a internet). Este mundo tan interconectado digitalmente tiende a "despersonalizar" las relaciones sociales, esto es, a olvidar que detrás de cada uno de los "hechos electrónicos" hay personas cuyos derechos fundamentales deben ser siempre respetados (en especial, el derecho a la intimidad, el derecho al secreto de las comunicaciones, y el derecho a la protección de datos personales, entre otros). En consecuencia, el peligro más importante a evitar es que en la búsqueda y obtención de la prueba del "hecho electrónico" se

vulnere un derecho fundamental. Y en este sentido, tanto el Tribunal Europeo de Derechos Humanos (TEDH) como la Corte Interamericana de Derechos Humanos (CIDH) han tenido ocasión de destacar que en la prueba de los hechos no todo es admisible, siendo uno de sus límites más estrictos el de la ilicitud o ilegalidad en su obtención. Para luchar de la forma más eficaz posible contra este problema es básico que la ley declare con toda rotundidad que cualquier elemento probatorio logrado con vulneración de un derecho constitucional, tanto en el mundo real como el virtual, deberá inadmitirse como prueba en un proceso judicial (y de hecho, en la mayoría de las legislaciones internacionales existe jurisprudencia y normas de exclusión probatoria referentes a las pruebas ilícitamente obtenidas)[7].

Y el segundo problema es el de la facilidad de manipulación del contenido de una red social, un mensaje de e-mail o un documento electrónico. Aunque parezca increíble, es mucho más fácil alterar el contenido de un documento tecnológico que el clásico documento en papel, y así, por ejemplo, respecto de un e-mail, sin necesidad de mucha experiencia es posible modificar su contenido o el destinatario del mismo, así como no parece complicado en una página "html" modificar el código fuente de dicha página y luego imprimirlo, dando la impresión de que el documento así reproducido es el mismo que se encuentra en línea. Sin embargo, estos problemas se superan en la mayoría de los países mediante el uso de algunas herramientas tecnológicas (como la certificación digital a través de empresas de certificación autorizadas públicamente para emitir dicha certificación), diversas prácticas legales (ya sea a través del uso de diferentes tipos de testimonios –especialmente a través de instituciones dedicadas a intermediar en la comunicación entre empresas–, o la redacción de políticas o protocolos de actuación a las que deben sujetarse las partes contratantes), o a través de un peritaje informático.

Una vez resueltos estos dos problemas, la pregunta que inmediatamente debemos hacernos es: ¿Todas estas nuevas fuentes de prueba digitales pueden introducirse en el proceso a través de los clásicos medios probatorios"?

Siguiendo los tres ámbitos de la sociedad en los que se han desarrollado mayoritariamente las nuevas tecnologías, expuestos anteriormente,

7. El problema de la prueba ilícita escapa a los objetivos de este estudio, pero plantea en todos los países una riqueza impresionante de matices: para una primera aproximación del tema me remito a PICÓ I JUNOY, J., *La prueba ilícita: un concepto todavía por definir*, en "La Administración de Justicia en España y en América", dir. Pilar Martín Ríos, edit. Astigi, Sevilla, 2021, pp. 1589-1606 (y en "La Ley Probática", n.° 1, 2020, pp. 1-18); e *idem.*, *El concepto de prueba ilícita en Michele Taruffo*, en "JUSTICIA", 2021:2, pp. 33-52.

los "hechos electrónicos" pueden introducirse en el proceso de la siguiente manera:

a) Con referencia a las redes sociales, su acceso como prueba al proceso puede tener lugar, básicamente, a través de:

– La prueba documental privada: normalmente los datos digitales suelen imprimirse y aportarse como documentos sin que haya habido problema alguno en su admisión probatoria, y ello tanto si constan en un correo electrónico[8], en una red social[9], en un WhatsApp[10], o figuran en la simple imagen de un "pantallazo"[11]. Además, es perfectamente admisible que una parte requiera a la otra la aportación documental de los mensajes cruzados de manera telemática[12], entrando en juego el deber de colaboración entre las partes y la posible *ficta admissio* del contenido del documento en caso de negativa injustificada a aportarlo (prevista en el art. 329.1 de la Ley de Enjuiciamiento Civil española [en adelante LEC]).

– La prueba documental pública: en ocasiones puede acudirse a un fedatario público (especialmente a un notario) para que visualiza un WhatsApp o acceda a determinada red social al objeto de que, en un acta de constatación de hechos, deje fiel reflejo de su contenido para su posterior aportación al proceso[13]. En este punto, debemos ir con suma cautela dada la facilidad de manipular los datos electrónicos que se presentan al fedatario público (tales como efectuar copias fidedignas de páginas web; alterar la identificación del emisor y destinatario de un e-mail, o la fecha en que se realizó el mensaje electrónico).

– Los instrumentos de archivos digitales tales como un USB o *pendrive*, un CD, etc.[14, 15];

8. *Cfr.* la sentencia de la Audiencia Provincial de Madrid, sección 22.ª, 1050/2015, de 10 de diciembre; o la sentencia de la Audiencia Provincial de Barcelona, sección 18.ª, 795/2015, de 5 de noviembre.
9. *Cfr.* la sentencia del Tribunal Supremo español, Sala 1.ª, 300/2015, de 19 de mayo.
10. *Cfr.* la sentencia del Tribunal Supremo español, Sala 1.ª, 115/2016, de 1 de marzo; o la sentencia de la Audiencia Provincial de Madrid, sección 27, 702/2015, de 24 de noviembre.
11. *Cfr.* la sentencia del Tribunal Supremo español, Sala 1.ª, 300/2015, de 19 de mayo; o la sentencia de la Audiencia Provincial de Madrid de 24 de mayo de 2007.
12. *Cfr.* la sentencia de la Audiencia Provincial de Sevilla de 13 de marzo de 2008.
13. *Cfr.* la sentencia de la Audiencia Provincial de Alicante de 13 de noviembre de 2008.
14. *Cfr.* la sentencia del Tribunal Supremo español, Sala 4.ª, de 16 de junio de 2011; la sentencia de la Audiencia Provincial de Barcelona 2 de julio de 2007; o el auto de la Audiencia Provincial de Barcelona de 4 de noviembre de 2008, entre otras muchas resoluciones judiciales.
15. En algunos países estos instrumentos se consideran, a efectos probatorios, como documentos; mientras que en otros tienen su propia regulación autónoma. Curiosamente

– El interrogatorio de las partes o de los testigos: a través de sus declaraciones se puede arrojar luz respecto de los contenidos publicados en una red social o la verdadera participación de la parte en la misma (no olvidemos que, con cierta frecuencia, hay suplantaciones de identidad en las comunicaciones que se producen en las redes sociales), o el contenido de los documentos electrónicos que hayan sido impugnados judicialmente, como puede suceder con un e-mail[16]. En este punto, debo destacar la existencia en el mercado de empresas (terceros de confianza) encargadas de actuar como intermediarias en toda la contratación electrónica y que, en caso de litigio, pueden intervenir en el proceso aportando documentos o declarando como testigos[17].

– Y el dictamen pericial informático: mediante esta prueba se puede acreditar la posible alteración de los datos que figuran en una red social, la manipulación de un e-mail y, en general, adquirir certeza respecto de la autenticidad de los hechos reflejados electrónicamente[18]. Pese a la rotundidad con que se pronuncia cierta jurisprudencia[19], no siempre es necesario aportar este dictamen pericial para dar credibilidad al dato electrónico[20]; y su simple impugnación judicial no comporta la exigencia de tener que aportarse al proceso un dictamen pericial informático, pues para ello deben explicitarse argumentos razonables, explicaciones serias, o cualquier dato o elemento que dote de cierta verosimilitud a dicha impugnación[21].

---

en España si bien tienen una regulación autónoma (arts. 382 a 384 LEC), ésta es muy similar a la propia de la prueba documental.

16. *Cfr.*, respecto al contenido de una red social, la sentencia del Tribunal Supremo español, Sala 1.ª, 300/2015, de 19 de mayo; y de los e-mails, la sentencia de la Audiencia Provincial de Segovia de 31 de julio de 2008, o la sentencia de la Audiencia Provincial de Zaragoza de 14 de enero de 2005.
17. Así, *vid.* el Reglamento (UE) n.° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
18. Cuestión distinta son los numerosos problemas que deben superarse en la práctica judicial, que se inician en la elección de la titulación exigible al perito, los que se originan en la correcta obtención del objeto a peritar y su posterior no contaminación en la "cadena de custodia", costes, etc. Para el tema *vid.* PUIG FAURA, S., *La prueba pericial informática en el procedimiento civil*, edit. Wolters Kluwer, Madrid, 2015.
19. Así, por ejemplo, *vid.* la sentencia del Tribunal Supremo español, Sala 2.ª 300/2015, de 19 de mayo.
20. En este sentido, *vid.* las sentencias del Tribunal Supremo español, Sala 1.ª, 375/2018, de 19 de julio y 754/2015, de 27 de noviembre.
21. *Cfr.* la sentencia del Tribunal Supremo español, Sala 2.ª, 375/2018, de 19 de julio; o la SAP de Madrid 583/2017, de 18 de octubre. En doctrina *vid.* el reciente estudio de FUENTES SORIANO y ARRABAL PLATERO, *Impugnación de la prueba tecnológica: práctica de prueba instrumental y exigencia de un "principio de prueba"*, en "Revista General de Derecho Procesal", núm 47. 2019, pp. 1-21.

b) Respecto a la contratación electrónica, cada país suele tener su propia normativa reguladora de la firma electrónica, por lo que deberemos acudir a estas regulaciones nacionales para conocer los diferentes tipos de firma electrónica, su valor probatorio y su impugnación en el proceso[22]. Además, debo destacar la existencia en el mercado de empresas encargadas de actuar como intermediarias en toda la contratación electrónica para que, en caso de litigio, pueden intervenir en el proceso aportando documentos o declarando como testigos. De igual modo, la propia declaración de las partes es fundamental para conocer su verdadera voluntad negocial.

c) Y finalmente, por lo que hace referencia a IoT, será fundamental la intervención del programador que intervino en las diversas fases de creación y desarrollo del *smart contract*, la declaración que la persona solicitante de dicho contrato, así como la prueba pericial informática para

22. En el caso español, esta regulación se materializa en:

a) la Ley 59/2003, de 19 de diciembre, de firma electrónica, cuyo art. 3 establece: "[…] 4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel […]. 7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable […] 8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica. La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación […]. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil"; y

b) La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, cuyo art. 23.1 establece: "1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez"; y el art. 24 prevé: "1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico. Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. 2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental".

verificar la corrección de los datos aportados por las partes y el citado programador.

En conclusión, como podemos comprobar, los medios tradicionales de prueba todavía sirven para aportar al proceso las nuevas fuentes probatorias digitales que aparecen en las redes sociales, en la contratación electrónica, o en mundo de IoT. Y esta es la respuesta que a nivel mundial está dándose en todos los países.

III. LAS NUEVAS TECNOLOGÍAS COMO INSTRUMENTOS AL AUXILIO DE LOS TRADICIONALES MEDIOS DE PRUEBA: LA NEUROCIENCIA Y LOS ALGORITMOS DE MICRO-EXPRESIONES FACIALES

Como indiqué en la introducción de este estudio, las nuevas tecnologías pueden ser instrumentos de auxilio de los tradicionales medios de prueba en la medida en que se presentan como herramientas susceptibles de verificar el resultado de las pruebas de interrogatorio de las partes, testigos y declaraciones de peritos.

Nos planteamos aquí la posibilidad de si es posible controlar, por vías tecnológicas, las declaraciones personales de los propios litigantes, los testigos y los peritos. Y en concreto, nos centramos en la neurociencia y los algoritmos de micro-expresiones faciales.

1. LA NEUROCIENCIA

La neurología parece ofrecer mecanismos capaces de mesurar la verdad o la mentira de dichas declaraciones como, por ejemplo, mediante las imágenes de resonancia magnética –fMRI–. Sin embargo, lo cierto es que, en la actualidad, la doctrina es muy crítica sobre la eficacia o validez científica de dichos mecanismos.

Desde la neurociencia, día a día, se están aportando nuevas técnicas dirigidas a evidenciar los cambios neuronales del cerebro humano con la ayuda de sofisticadas técnicas de imágenes cerebrales que permiten mostrar concretas regiones cerebrales que ejecutan una función determinada[23]. No obstante, actualmente nos encontramos con limitaciones empíricas

23. En este sentido, *vid.* ya GREELY y WAGNER, *Reference Guide on Neuroscience*, en "Reference Manual on Scientific Evidence", 3.ª edición, The National Academies Press, Washington, 2011, pp. 807-808; y PARDO y PATTERSON, *Philosophical foundations of Law and Neuroscience*, en "University of Illinois Law Review", 2010, p. 1228, notas 91 a 93.

importantes sobre la fiabilidad de estas pruebas científicas de detección de la mentira[24]. Y aunque fuese cierta la posibilidad de detectar cuál es la zona cerebral que tiene por función responder a un interrogatorio, esto es, de modo científico, se pudiera determinar cuando el declarante está conscientemente faltando a la verdad, se abren múltiples interrogantes, pues es posible que el declarante[25]:

a) mienta pero tenga capacidad de control de sus propios estímulos emocionales –innata o adquirida– que evite la activación de la región cerebral de la matriz de la mentira y, en consecuencia, ésta no sea detectada;

b) diga la verdad pero se active la región cerebral que determina el estímulo de la mentira porque su sistema nervioso se ha alterado sobremanera (por ejemplo, al estar declarando respecto a hechos de carácter íntimo, o sobre los que ha mantenido ocultos durante tiempo y quería seguir manteniéndolos así, o con referencia a los que cree que le pueden traer consecuencias especialmente perjudiciales de cualquier tipo –afectivas, personales, profesionales, económicas, etc.–);

c) diga la verdad y "mienta", por ejemplo, porque la declaración se fundamenta en un conocimiento erróneo de los hechos[26];

d) e incluso es posible que diga la verdad ante hechos que formalmente aparezcan como falsos. Tuve ocasión de participar en un caso real en el que unas imágenes radiológicas demostraban una situación en la que objetivamente era lógico pensar en la existencia de dolor cuando, en realidad, éste nunca había existido: se trataba de una mujer anciana, de 89 años, en la que tras un atropello tuvo que ser intervenida quirúrgicamente para colocarle un clavo endomedular por una fractura pertrocantérea en la

24. Así, por ejemplo, suele argumentarse que no todos los cerebros humanos son iguales; que los experimentos todavía son escasos; y que en muchos casos la presunta matriz de la mentira se asocia también a otras actividades cognitivas que van más allá de la mentira –*cfr.* PARDO y PATTERSON (*op. cit.*, p. 1228, nota 95)–. Igualmente crítico se muestra NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial*, edit. Marcial Pons, Madrid, 2018, pp. 89-90.

25. PICÓ I JUNOY, J., *La prueba del dolor*, en "Neurociencia y proceso judicial", edit. Marcial Pons, Madrid, 2013, pp. 91-92.

26. Para simplificar esta afirmación me basta el siguiente ejemplo, supongamos que el Sr. A cree que la Tierra es plana, es decir, para él la afirmación de que la Tierra es plana (1) es verdadera. Ahora supongamos que el Sr. A miente al Sr. B, y le dice que la Tierra tiene forma esférica (2). En este caso, la afirmación 1 es verdadera y la 2 es falsa; pero el Sr. A ha mentido al Sr. B y le ha dicho una mentira que, curiosamente, es una verdad. Es una verdad que se fundamenta en un conocimiento erróneo de la realidad de los hechos. El Sr. A miente –pues dice lo contrario de lo que cree– pero al estar equivocado (creer algo erróneo), le lleva a decir la verdad mintiendo (ejemplo obtenido de http://filosofia.laguia2000.com/creencias/sobre-verdad-y-mentira; fecha de consulta: 1 de febrero de 2022).

cadera derecha. En el seguimiento realizado tras la operación, la paciente, a pesar de que la fractura radiológicamente estaba consolidada, declaraba un fuerte dolor de la cadera derecha durante y tras la rehabilitación, que nunca había tenido antes del accidente, y respecto del cual el doctor de la compañía aseguradora del causante del accidente entendía que ya existía con anterioridad debido a la existencia de una coxartrosis visible en las radiografías previas a la operación. En este caso, la compañía aseguradora se negó a indemnizarla por el dolor (y su tratamiento posterior –que podía comportar, por ejemplo, una nueva intervención quirúrgica para una artroplastia o implantación de una prótesis total de cadera–) debido a que la artrosis es una patología degenerativa no atribuible a un traumatismo (y de hecho, como he indicado, ya se percibía en las imágenes radiográficas prequirúrgicas). Si bien es cierto que las radiografías mostraban la existencia de artrosis, que habitualmente causa dolor, en la comparecencia de la medida cautelar se probó que la anciana nunca se había quejado del dolor en esa zona[27], por lo que se determinó que el accidente fue el desencadenante del dolor, motivo por el cual la compañía aseguradora fue obligada a pagar la intervención quirúrgica requerida por la anciana[28].

En definitiva, todas estas situaciones nos llevan a debates mucho más profundos, como el de la dicotomía entre cerebro y mente, esto es, a si es posible que exista mente más allá del mero elemento fisiológico del cerebro, por lo que el estudio de este órgano humano –por muy profundo y detenido que sea– parecería ser incapaz de detectar la mente del declarante, pero todo ello excede del objetivo del presente estudio[29]. En todo caso, la hipótesis de que es posible mediante las imágenes cerebrales

27. Como se acreditó, entre otras pruebas, mediante la declaración de su médico de familia y un certificado de su historial médico en la que no aparecía ninguna prescripción medicamentosa que guardase relación con el dolor de la cadera, ni ningún ingreso en servicios hospitalarios de urgencia por esta causa.

28. De igual modo, el trabajo de GREELY y WAGNER (*op. cit.*, p. 809) destaca la existencia de estudios por imágenes computarizadas en los que se demuestra que las personas pueden ser hipnotizadas para sentir dolor sin que exista ningún estímulo externo doloroso y, a pesar de ello, se active la "matriz del dolor", por lo que dichas imágenes cerebrales responderán a una realidad falsa de los hechos. Y también podemos pensar en el amputado en una extremidad con dolor de miembro fantasma que declara tener dolor en su extremidad ausente. En este caso, efectivamente es posible que el declarante diga la verdad, esto es, no esté mintiendo, pero ello no coincida con algo que es objetivamente cierto, a saber, que no existe la extremidad de la cual dice partir el dolor que sufre. Como se puede comprobar, en ambos casos, la máquina podrá detectar que el declarante no miente –porque el dolor existirá como percepción subjetiva de la persona afectada– aunque el hecho del origen del dolor es manifiestamente falso.

29. Al respecto, *vid.* PARDO, M. y PATTERSON, D. (*op. cit.*, pp. 1218-1220); y NIEVA FENOLL, J. (*op. cit.*, pp. 169-171).

detectar cuando una persona está mintiendo sigue siendo rebatida en multitud de estudios científicos, por lo que es lógico seguir reflexionando sobre la admisibilidad probatoria de dichas imágenes cerebrales para determinar la mayor o menor credibilidad de las declaraciones judiciales de las partes, testigos y peritos.

En las experiencias del derecho comparado[30], partiendo de que en ningún país se prevé expresamente una regulación sobre este punto, lo que demuestra que el desarrollo tecnológico va siempre por delante del desarrollo normativo, existe una respuesta muy dispar:

a) hay países en los que no se permite su uso, y para ello se formulan muy diversas razones: la falta expresa de previsión normativa, lo que induce a la praxis judicial a no admitirlo –como sucede en Inglaterra, Gales o China–; la expresa prohibición en las leyes de enjuiciamiento –este es el caso, por ejemplo, del Código Procesal Civil japonés–; la desconfianza sobre su confiabilidad (*reliability*) o la falta de carácter científico de estas nuevas tecnologías –esta es la experiencia judicial de USA, Inglaterra y Gales–; o la expresa previsión legal de que el control de la veracidad de los testigos, las partes o peritos se confía en exclusiva al juez o al jurado, quienes con la cuidadosa valoración de la prueba deben llegar al libre convencimiento de dicha veracidad, sin que nada pueda interferir en su libertad de valoración probatoria; y

b) hay países en los que se admite el uso probatorio de las fMRI con determinadas condiciones, por ejemplo, siempre que ello se deba a la propia voluntad de quien desea someterse a estas nuevas tecnologías y no haya un trato denigrante contra su dignidad humana –y así se conocen distintos supuestos jurisprudenciales en Alemania o Perú–. En todo caso, se considera que la ley, al remitirse a la libre valoración judicial de las pruebas, le otorga al juez un amplio margen de discrecionalidad para admitir y valorar cualquier elemento probatorio que estime útil para formar su convicción sobre los hechos litigiosos –como sucede en Taiwán o Ecuador–. Además, hay países en los que abiertamente se admiten las nuevas tecnologías en el ámbito judicial debido al convencimiento general a favor de su eficacia y autenticidad, y a que el uso generalizado que de los mismos efectúa la Administración induce a confiar en todos los avances tecnológicos –como es el caso de Noruega–. Ello comporta que, en el caso de que una parte denuncie la mendacidad en la declaración de la parte contraria o de los testigos, *prima facie*, pueda usarse cualquier medio tecnológico válido para descubrirla.

30. Para las que me remito a PICÓ I JUNOY, J., *The New Challenges of Evidence Law in the Fourth Industrial Revolution, op. cit.,* pp. 487 y ss.

Sin embargo, lo cierto es que en la mayoría de los países no se ha planteado la problemática aquí expuesta debido a que no existen reglas legales o jurisprudencia sobre el tema. En España, a falta de una norma que prohíba el uso la fRMI para detectar la mendacidad en la declaración judicial de los testigos, partes o peritos, no debería haber obstáculo para su admisión siempre que se cumplan las siguientes tres condiciones: (a) que haya sometimiento voluntario de la persona declarante; (b) que se realice siguiendo las pautas que marca la comunidad científica, debiéndose documentar en un informe pericial, que deberá poder ser contradicho por la parte contraria; y (c) que se respete la libre valoración judicial de toda la prueba, esto es, tanto la que se deriva de la propia declaración sometida a fMRI como la del informe pericial, pues al encontrarnos ante un mecanismo no totalmente confiable debe dejarse un margen de discrecionalidad en la valoración del juez. Como es bien sabido, esta libertad de valoración no supone, en ningún caso, la arbitrariedad judicial sino todo lo contrario, la necesidad de motivar los resultados de la prueba en la sentencia, pues solo así se permite al justiciable conocer la verdadera razón del porqué de dicha sentencia. En todo caso, se plantea aquí un problema de difícil solución respecto de los países con jurado (básicamente los del *common law*) pues el enjuiciamiento de los hechos lo realiza el jurado y de forma no motivada, por lo que cabe el peligro ya apuntado por DAMASKA de que el perito venga a sustituir la función del juez[31], esto es, que algo no confiable (la opinión experta de la fMRI) condicione indebidamente algo que pertenece en exclusiva al jurado, como es el otorgar mayor o menor credibilidad a las personas que declaran ante él[32].

2. LOS ALGORITMOS DE MICRO-EXPRESIONES FACIALES

Las nuevas tecnologías nos ofrecen otra posible forma de verificar la veracidad de la declaración de una persona: se trata de los algoritmos referentes a sus micro-expresiones faciales.

En la actualidad existe una parte de la psicología clínica que considera que es posible detectar cuando una persona miente a través de sus micro-expresiones faciales[33]. Partiendo de los estudios de Higgard e Isaacs,

31. DAMASKA, M. *Evidence Law Adrift*, Yale University Press, New Haven & London, 1997, p. 151(existe una versión al español con el título "El derecho probatorio a la deriva", traducción de Joan Picó i Junoy, edit. Marcial Pons, Madrid, 2015).
32. Lo que conduciría a su rechazo. Ello es lo que, como hemos visto, sucede en los USA, donde la Corte Suprema y los tribunales federales no admiten el IRMf, incluso aunque fuese confiable, porque es responsabilidad del jurado evaluar la credibilidad de los testigos y partes.
33. Al respecto, *vid.* PICÓ I JUNOY, J., DE MIRANDA VÁZQUEZ, C. y ANDINO LÓPEZ, J.A., *Examen de un nuevo método de detección judicial de la mentira*, en "La prueba en

siguiendo por los trabajos de Paul Ekman así como los de Porter y Brike, y acabando por los más recientes de Matsumoto –figura destacada en el campo de las micro-expresiones faciales– puede llegarse a la conclusión teórica de que existen determinadas zonas de la cara que, debidamente analizadas, permiten saber cuándo una persona miente o dice la verdad[34]. Para estos autores, cuando las emociones se expresan espontáneamente, las mismas expresiones faciales y movimientos musculares aparecen en el rostro, y esto parece deberse al hecho de que estas expresiones faciales están bajo el control neural de dos áreas distintas del cerebro, una de ellas controla los movimientos voluntarios y la otra los involuntarios. En consecuencia, si una persona trata de controlar sus expresiones, ambos sistemas se involucran en un conflicto neuronal por el control de la cara, lo que produce una expresión facial muy breve que se denomina "micro-expresión", imperceptible a simple vista, pero controlable a través de la reproducción a velocidad muy lenta de la grabación del rostro humano[35]. Basándose en distintas zonas fáciles en las que supuestamente se manifiesta la "micro-expresión" de la mentira, determinadas empresas, aplicando un algoritmo –que no revelan–, son capaces de elaborar informes periciales que se utilizan ante los tribunales como prueba para dar mayor o menor credibilidad a la declaración de una determinada persona[36]. Y en ocasiones en España se han admitido como prueba estos informes de expertos[37].

---

acción. Estrategias procesales en materia probatoria. Libro en homenaje a Luis Muñoz Sabaté", director Joan Picó Junoy, edit. J.M.ª Bosch, Barcelona, 2019, pp. 267 a 275.

34. Para el estudio de esta doctrina *vid.* MATSUMOTO, D. y HWANG, H. C., *Microexpressions differentiate truths from lies about future malicious intent*, en "Frontiers in Psychology" 2018: 9, pp. 1-11 (*cfr.* https://www.frontiersin.org/articles/10.3389/fpsyg.2018.02545/full; fecha de consulta: 1 de febrero de 2022).

35. Estas "micro-expresiones" faciales serían tan efímeras que solo tienen una duración entre 0.04 y 0.20 segundos (*cfr.* MATSUMOTO y HWANG, *op. cit.*, pp. 3-4).

36. Especialmente en el campo del derecho de familia y cuando intervienen menores debido a la facilidad de manipular sus verdaderos sentimientos; y en el ámbito del proceso penal por delitos de violencia de genero, ya que aquí suelen haber solo dos declaraciones contradictorias: la de la víctima y la del presunto agresor.

37. Con carácter general, favorable a la libertad del juez para valorar los gestos o conductas de las partes, la sentencia del Tribunal Supremo español, Sala 2.ª, 119/2019, de 6 de marzo, de manera acrítica llega a afirmar: "Presupuestos en el análisis de la valoración por el Tribunal de la declaración de la víctima […] recordemos que es posible que el Tribunal avale su convicción en la versión de la víctima, ya que la credibilidad y verosimilitud de su declaración se enmarca en la apreciación de una serie de factores a tener en cuenta en el proceso valorativo del Tribunal. Y así podemos citar los siguientes: […] 4. "Lenguaje gestual" de convicción. Este elemento es de gran importancia y se caracteriza por la forma en que la víctima se expresa desde el punto de vista de los "gestos" con los que se acompaña en su declaración ante el Tribunal". Partiendo de este planteamiento jurisprudencial, no es extraño encontrar resoluciones judiciales en primera instancia que admiten el valor probatorio de dichos dictámenes periciales: en este sentido, por ejemplo, me remito a la sentencia

Sin embargo, recientemente, un grupo internacional de expertos en la materia ha publicado un estudio que resulta sumamente significativo sobre el carácter de "pseudo-ciencia" de todos estos métodos de detección de la mentira[38]. Ponen de relieve, entre otras cosas, que quienes tienen experiencia científica con la detección de la mentira coinciden en señalar que no hay comportamientos no verbales que sean propios y exclusivos de las personas sinceras, o de las mendaces. En otras palabras, no existen indicadores objetivos de mentira al estilo del mito de la "nariz de Pinocho". Según expone este panel de expertos, la generalizada obnubilación de los legos por todo lo que salga "de la boca" de los expertos ha provocado que cualquier supuesto conocimiento con apariencia de científico sea asumido acríticamente. En el ámbito judicial tal fenómeno ha sido muy acusado, probablemente motivado por la imperiosa necesidad de encontrar métodos infalibles para detectar el engaño en los procesos jurisdiccionales.

Pero lo cierto es que faltan estudios experimentales que den validez científica a estos métodos de detección de la mentira[39]. Como si de un

del Juzgado de Primera Instancia núm. 18 de Barcelona de 31 de julio de 2018, que admite la validez probatoria de un "informe pericial de Micro-expresiones faciales y lenguaje corporal inconsciente" del hijo en el proceso de divorcio de sus padres, basándose en que las partes no se oponen al mismo y "[…] se han acompañado al mismo avales de distintos organismos oficiales y universitarios que reconocen dicha prueba de utilidad tanto en procedimientos civiles como penales y que consiste en la filmación con una cámara mientras que se formulan distintas preguntas (de control, de indicio, de provocación y de confirmación)".

38. DENAULT, V., *et altri*, *The analysis of nonverbal communication: The dangers of pseudoscience in security and justice contexts*, en "Anuario de Psicología Jurídica", 2020: 30, pp. 1-12 (*cfr.* https://journals.copmadrid.org/apj/art/apj2019a9; fecha de consulta: 1 de febrero de 2022).

39. Por ello, existen resoluciones judiciales que no dan valor probatorio a estas pruebas de expertos. Como buen ejemplo de ello, la sentencia de la Audiencia Provincial de Barcelona, sección 18.ª (especializada en derecho de familia), de 8 de mayo de 2019 (ECLI:ES:APB:2019:5002) establece lo siguiente: "El informe de 22-11-2017 de XX titulado "Investigación y Desarrollo de micro expresiones faciales y lenguaje corporal" afirma […]. Se afirma la credibilidad del relato por las reacciones oculares y la cronología gestual. Tal como recoge la sentencia no se ha aportado publicación científica que avale y contraste la técnica utilizada. En el recurso de apelación se aporta una relación de bibliografía sobre el tema pero no acreditación que avale la cientificidad de la técnica utilizada constando que hay literatura que cuestiona su fundamento científico. No podemos considerar dicha técnica como válida para verificar la credibilidad de las manifestaciones vertidas por la menor […]. La utilización de dicha metodología no está suficientemente contrastada, se desconoce la concreta formación de las personas que la han llevado a cabo y la forma en como ha sido aplicada a la menor se considera por la Sala totalmente inadecuada. Por todo ello se descartan las conclusiones alcanzadas en el informe". En la misma línea, la sentencia de la Audiencia Provincial de Barcelona, sección 12.ª (especializada en derecho de familia), de 18 de diciembre de 2018 (ECLI:ES:APB:2018:12369) mantiene: "[…] En relación a las

medicamento se tratase, es fundamental testar o verificar el grado de efectividad de cualquier método que se ofrezca en el práctica judicial como panacea de la detección de la mentira mediante el control de las micro-expresiones faciales, y ello es básico especialmente cuando algún tribunal puede verse inclinado a otorgar validez científica –y en consecuencia probatoria– a dictámenes periciales en los que presuntamente se afirma que una persona (parte, testigo o perito) miente o dice la verdad.

Uno de estos experimentos es el realizado por la "Asociación de Probática y Derecho Probatorio" (APDP)[40]. A través de ella y una empresa europea que realiza los citados dictámenes periciales de micro-expresiones faciales se ideó un ensayo clínico para verificar el grado de efectividad del sistema en el caso de la declaración de diez mujeres que supuestamente habían sufrido violencia de género. La APDP contactó con dos asociaciones de mujeres maltratadas y dos escuelas de teatro, y escogió para el ensayo clínico cuatro actrices de arte dramático –que debían mentir acerca de un episodio de violencia de género– y seis mujeres que realmente la sufrieron[41]. Para la empresa que debía efectuar los informes periciales se mantuvo el completo anonimato de la identidad de todas las mujeres y el número concreto de las que habían sufrido violencia de género. Las mujeres debían efectuar una exposición oral, de treinta minutos, grabada en video, relatando sus episodios de violencia de género y contestando a preguntas de un psicólogo de la empresa, y su identidad frente a dicha empresa se resumía en un simple número (del uno al diez)[42]. Las grabaciones debían realizarse con presencia de algún miembro de la APDP y la empresa tenía la expresa prohibición de ponerse en contacto posterior con dichas mujeres. La APDP hizo entrevistas individuales previas con

periciales aportadas por la Sra. Gracia para sostener su versión obran en la causa […] un análisis de la empresa XX sobre micro-expresiones faciales y lenguaje corporal inconsciente, análisis al que la Sala no otorga valor científico". Y, por último, la sentencia de la Audiencia Provincial de Barcelona, sección 20.ª (penal), de 13 de septiembre de 2018 afirma: "Así pues, la pericial de micro expresiones faciales resulta completamente innecesaria y nada relevante puede aportar".

40. Ver, PICÓ I JUNOY, J., DE MIRANDA VÁZQUEZ, C. y ANDINO LÓPEZ, J.A., *op. cit.*, pp. 267-275.

41. Las diez mujeres no se conocían entre ellas para evitar el efecto contagio en sus relatos de violencia de género. Por participar en este ensayo clínico, exponiendo el relato de violencia de género, las mujeres que efectivamente la habían sufrido percibían 200 euros, y las actrices 100 euros en el momento de la grabación, y 100 euros más si conseguían que la empresa no detectase su declaración falsa.

42. El correlato del número con la concreta identidad de la persona y la circunstancia de si había sufrido o no violencia de género se mantuvo en secreto para la empresa, y estos datos se guardaron secretos en una plica cerrada custodiada por un notario, quien debía abrirla tras la entrega de los informes periciales de la empresa para así verificar el grado de acierto de los mismos.

todas ellas para explicarles el objeto y finalidad del ensayo clínico, y para que diesen su consentimiento expreso al mismo. Se aprobó un calendario de grabaciones para que en una semana se pudieran efectuar sus declaraciones. En fin, tras más de cuatro meses de preparación del ensayo clínico y doscientas horas de trabajo por parte de los investigadores, siete días antes de empezar las grabaciones la empresa que debía realizar los dictámenes periciales sobre detección de mentira a través de micro-expresiones faciales envió un e-mail en el que expresó su voluntad de no realizar el ensayo clínico justificándose en el volumen de trabajo que tenían[43]. Inmediatamente se les ofreció realizar el mismo ensayo clínico sin limitación de fechas, con el fin de ajustarse al calendario de trabajo que le fuese bien a la empresa, pero la respuesta fue la misma: no querer testar científicamente el método de realización de sus dictámenes periciales alegando un elevado volumen de trabajo. Los hechos son muy elocuentes: que cada uno saque sus propias conclusiones.

43. Literalmente, el e-mail recibido indicó: "Buenos días xxx: te informo que nos hemos reunido de urgencia la Junta Directiva y nos va resultar imposible realizar el ensayo. A fecha de hoy, lamentablemente no nos podemos comprometer a realizar 10 informes simultáneos y cumplir las fechas estipuladas".

La deseable consideración de la IA utilizada en el ámbito tributario como sistema de alto riesgo en la propuesta de Reglamento sobre IA del Parlamento Europeo y el Consejo

Irune Suberbiola Garbizu

Profesora de Derecho Financiero
Universidad del País Vasco-Euskal Herriko Unibertsitatea

SUMARIO: I. CONTEXTUALIZACIÓN. II. APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO TRIBUTARIO. 1. *La IA en la asistencia e información al contribuyente*. 2. *La IA en el control del cumplimiento tributario*. 3. *La IA ante el nuevo modelo de relación entre Administración tributaria y contribuyente*. 4. *La IA en los procedimientos de revisión tributaria y en el procedimiento sancionador*. III. RIESGOS ASOCIADOS A LA UTILIZACIÓN DE LA IA EN EL ÁMBITO TRIBUTARIO Y DERECHOS DEL CONTRIBUYENTE AFECTADOS POR ESE USO. 1. *Características de la IA que entrañan determinados "riesgos"*. 2. *Derechos de los contribuyentes afectados por la utilización de la IA en el ámbito tributario*. 2.1. Derecho a una resolución motivada. 2.2. Derecho a la presunción de inocencia. 2.3. Derecho a la intimidad y la inviolabilidad del domicilio constitucionalmente protegido. 2.4. Derecho a la igualdad y a la no discriminación. IV. LA INTELIGENCIA ARTIFICIAL UTILIZADA EN LOS PROCEDIMIENTOS TRIBUTARIOS COMO SISTEMAS DE ALTO RIESGO. 1. *Los sistemas de alto riesgo en la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión*. 2. *La exclusión de los sistemas de IA utilizados en el ámbito tributario de la categoría de sistemas de*

alto riesgo. 3. *La necesaria reconsideración de la protección de los obligados tributarios de la injerencia de sistemas de inteligencia artificial de alto riesgo en un ámbito fiscal*. V. BIBLIOGRAFÍA.

I. CONTEXTUALIZACIÓN

La inteligencia artificial (IA), ha permanecido hasta hace poco tiempo en el imaginario popular ligada a la ciencia ficción, como un fecundo género que ha dado lugar obras literarias que luego se han convertido en cintas cinematográficas. Philips K. Dick su *El informe de la minoría, ¿Sueñan los Androides con ovejas mecánicas?* y sus homónimas *Minority Report y Blade Runner* son claro ejemplo de ello. Gracias a este tipo de libros y películas, nos imaginamos la IA como parte de un futuro distópico en el que la tiranía de las máquinas gobierna nuestra sociedad; como un mecanismo de un lugar extraño y ajeno a nuestra realidad. Sin embargo, como veremos, la cercanía de esa realidad, su actual existencia, depende de lo que entendamos por IA.

Desde que en 1956 se definiera por primera vez la inteligencia artificial por MacCarthy como "la ciencia y la ingeniería de la fabricación de máquinas inteligentes" son múltiples las definiciones que se han utilizado para delimitar este concepto. La reciente propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión[1], concreta su contenido de forma muy amplia, indicando que un sistema de inteligencia artificial es el software que se desarrolla empleando una o varias técnicas y estrategias que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.

En el terreno jurídico, parece que existen materias que ofrecen una mayor predisposición para las tecnologías sustentadas en esos sistemas de inteligencia artificial. Nos referimos a cuestiones relacionadas con la intendencia judicial (por ejemplo, en el reparto de asuntos, la determinación de cuantías…); al Derecho del seguro; a la mediación electrónica; a actuaciones preventivas en el ámbito penal en determinadas jurisdicciones[2]… También a aquellas relacionadas con el ámbito tributario donde, a

1. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF.
2. COMPAS en Estados Unidos, PROMETEO en Argentina…

pesar de su exclusión expresa del perímetro de los sistemas de IA de alto riego en la referida propuesta de reglamento, la inteligencia artificial es toda una realidad.

En efecto, el considerando 38 de dicha propuesta de reglamento indica que "no debe considerarse que los sistemas de IA destinados específicamente a que las autoridades fiscales y aduaneras los utilicen en procesos administrativos forman parte de los sistemas de IA de alto riesgo usados por las autoridades encargadas de la aplicación de la ley con el fin de prevenir, detectar, investigar y enjuiciar infracciones penales". Lo cual, como veremos, puede acarrear múltiples problemas en relación con la necesidad de conciliar la utilización de la IA con la protección de los derechos fundamentales de los obligados tributarios, habida cuenta de que estos sistemas se utilizan por nuestras Haciendas en todos los procedimientos de aplicación de los tributos (gestión, inspección, y recaudación), en asuntos de mera intendencia, así como en materias más intrusivas que, de alguna manera, pueden estar relacionadas con el derecho a la defensa, la presunción de inocencia, el derecho al proceso debido, la protección de la intimidad o la intromisión en el domicilio constitucionalmente protegido.

En las siguientes líneas comenzaremos con una descripción de la utilización de la inteligencia artificial en el ámbito tributario para, a continuación, incidir en aquellas cuestiones que pueden verse afectadas por el uso de una tecnología que, como veremos, es opaca a los ojos del contribuyente, a los efectos de determinar si la exclusión de la consideración de estos sistemas como sistemas de alto riesgo en la mencionada propuesta de reglamento es, o no, oportuna.

II. APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO TRIBUTARIO

La utilización de la inteligencia artificial en el ámbito tributario es extensa y viene realizándose desde hace décadas. Como indica el plan estratégico de la Agencia Estatal de Administración Tributaria (AEAT) para 2020-2023, esta Administración "siempre ha estado a la vanguardia en la utilización de nuevas tecnologías y esta circunstancia ha experimentado un impulso muy relevante en los últimos años con el desarrollo de nuevas herramientas de selección, obtención y tratamiento de la información y de utilización de inteligencia artificial para la realización de las actuaciones de información y asistencia a los contribuyentes"[3].

3. https://www.agenciatributaria.es/static_files/AEAT/Contenidos_Comunes/La_Agencia_Tributaria/Planificacion/PlanEstrategico2020_2023/PlanEstrategico2020.pdf.

1. LA IA EN LA ASISTENCIA E INFORMACIÓN AL CONTRIBUYENTE

El ámbito natural de la aplicación de la inteligencia artificial en materia tributaria se extiende a todos los procedimientos de aplicación de los tributos. En lo que atañe a los procedimientos de gestión y recaudación, los sistemas de IA se han utilizado en la primera de las funciones que es consustancial a toda Administración tributaria, aquella que consiste en las labores de información y asistencia a los obligados tributarios en tres aspectos concretos:

- La tramitación automatizada, por ejemplo para denegar automáticamente una reclamación, emitir una liquidación, cruzar y triangular datos sobre distintos hechos con trascendencia tributaria… Este tipo de tecnología permite monitorizar y revisar bancos de datos de forma más efectiva y eficaz de suerte que se puedan utilizar los recursos de la Administración tributaria para reformular sus servicios y redirigirlos a áreas más necesitadas de atención.
- La segmentación de contribuyentes, ya que el tratamiento automatizado de datos permite delimitar perfiles de contribuyentes, lo cual facilita no solo que nuestras Haciendas dispongan de un "retrato robot" (nunca mejor dicho) de eventuales defraudadores sino también, que adapten sus servicios a las necesidades de los contribuyentes desde un enfoque centrado en el obligado tributario.
- La puesta en marcha de todo un catálogo de asistentes virtuales que fomentan una relación colaborativa entre Administración y administrado. La práctica tributaria nos ha demostrado la utilidad de este tipo de tecnologías en múltiples aplicaciones: IBM Watson para las dudas que se puedan suscitar en relación con el Suministro Inmediato de Información (SII) en el Impuesto sobre el Valor Añadido; también en lo que atañe a este tributo AVIVA y PRE-303; las Administraciones de asistencia Digital Integral (ADIs), puestas en marcha con el referido plan estratégico 2020-2023 de la AEAT, que pretenden ser mostradores virtuales de asistencia al contribuyente 24/7;…

2. LA IA EN EL CONTROL DEL CUMPLIMIENTO TRIBUTARIO

Por su parte, en lo que afecta a la segunda de las funciones consustanciales a nuestro Fisco, la labor de control del cumplimiento de las obligaciones tributarias y que, pese a realizarse principalmente en los procedimientos de inspección también se lleva a cabo, aunque de forma más sucinta en el procedimiento de gestión, la AEAT viene utilizando distintos

modelos de inteligencia artificial tanto predictivos (que identifican a los contribuyentes que es probable no vayan a cumplir sus obligaciones) como prescriptivos (aquellos que determinan cómo incidir eficazmente en los incumplidores). En este sentido, se utilizan toda una batería de sistemas que usualmente se dan de forma combinada, y que de forma somera podemos resumir en:

- Técnicas estadísticas y econométricas tradicionales, que como tales no podemos considerar estrictamente como inteligencia artificial en los términos definidos en el propuesta de reglamento, pero que sí sirven para la obtención de valores atípicos que crean alertas respecto de precios, valores o proporciones. Nos referimos a sistemas basados en R, SAS…
- Técnicas de inteligencia artificial, basadas en conocimientos expertos y redes neuronales que buscan reproducir la forma en que el cerebro adopta decisiones inteligentes.
- Árboles de decisión: *Support Vector Machine* (SVM), técnicas multivariadas, análisis de conglomerados… que permiten tareas de clasificación y que ofrecen más información que las anteriores respecto a las razones que fundamentan una decisión.
- Recientemente, también se han introducido herramientas de análisis de redes sociales que, si bien en apariencia pueden no tener elementos con trascendencia tributaria aportan datos que, con la triangulación que facilita la IA, sí llegan a tenerla[4].

En este contexto, la AEAT dispone de todo un catálogo de herramientas de inteligencia artificial que le permiten desarrollar labores de control. De forma muy somera, podemos indicar que nuestra Hacienda estatal utiliza los siguientes instrumentos:

- ZÚJAR: se trata de una herramienta de procesamiento analítico en línea multidimensional y *Data Warehousing* que facilita la consulta y el estudio de toda la información existente en el sistema con contenidos cargados desde la base operacional. Igualmente permite visualizar, listar, filtrar, agrupar, ordenar, cruzar, calcular estadísticas, expresiones entre campos, segmentizar, dibujar gráficos, exportar datos…
- PROMETEO, una suerte de ZÚJAR especializado en el análisis de la información aportada en una comprobación de un determinado

4. DORADO FERRER, X. "Redes sociales, metadatos y derecho a la intimidad en los procedimientos tributarios", *Quincena Fiscal*, N.° 12, 2021, pp. 91-103.

contribuyente. Permite hacer una conciliación entre la información contable y el extracto bancario, cruzar con cualquier información de las bases de datos de la propia Hacienda.

- TESEO, un desarrollo propio de la AEAT para analizar, visualizar y editar gráficamente las relaciones entre elementos existentes en el sistema información analítico de la AEAT, ofreciendo funciones analíticas y de representación, tanto para los nodos, como para las relaciones. Gracias a esta herramienta se pueden realizar búsquedas, filtrados, agrupaciones, detección e caminos, almacenar consultas, exportarlas, así como realizar presentaciones en disposiciones jerárquicas, ortogonales, circulares…
- GENIO, herramienta de *reporting* también creada por la propia AEAT que emite informes normalizados en línea que también permite el diseño autónomo y la visualización de informes basados en consultas realizadas en las herramientas de análisis multidimensional ZÚJAR y PROMETEO.
- ELECTRA, tratamiento de multígrafos para detectar patrones de fraude con técnicas como la búsqueda por medio de *k-cores.*
- HERMES, plataforma global de riesgos que analiza las diferencias existentes entre el comportamiento del contribuyente en su declaración y el modo en que debiera haberlo hecho de acuerdo con los datos que obran en poder de la Administración, lo que permite desarrollar y explotar perfiles de riesgo cuando los resultados se separan de los estándares previstos.
- Herramientas comerciales de Business Intelligence (no desarrolladas por la AEAT) con modelos predictivos con entrenamiento enfocados al análisis y el data minigabinete y que al igual que en el caso anterior son utilizados para detectar comportamientos anómalos y patrones de fraude. Usualmente se utilizan como ayuda para tomar decisiones en la tramitación de expedientes. Los resultados obtenidos se llevan a la plataforma analítica y determinados riesgos productivos se vuelcan en el sistema de riesgos global HERMES.

La elección de uno u otro modelo de inteligencia artificial debe ser precisa, pues, en función del objetivo específico que pretenda alcanzarse puede resultar más adecuada una determinada plataforma en detrimento de otra, puede requerirse la combinación de distintos sistemas… En cualquier caso, además de los riegos inherentes a la adecuada elección y diseño de la inteligencia artificial utilizada, existen, también, otros riesgos consustanciales a la utilización de este tipo de tecnologías ya apuntados

por quienes me han precedido en el uso de la palabra y que, en ningún caso debemos olvidar. Volveremos a este extremo en el epígrafe III de este análisis.

3. LA IA ANTE EL NUEVO MODELO DE RELACIÓN ENTRE ADMINISTRACIÓN TRIBUTARIA Y CONTRIBUYENTE

Según se ha expuesto, la inteligencia artificial en el ámbito de los procedimientos de aplicación de los tributos (gestión, inspección y recaudación) ha conocido múltiples utilidades tanto en lo que atañe a las labores de asistencia e información al obligado tributario, como a las que afectan a las labores de control.

No obstante, debemos recordar que estas funciones no son compartimentos estancos y que, en ocasiones, las labores que desarrollan los distintos órganos de aplicación de los tributos se complementan dando lugar a servicios de asistencia-control en los que se imbrican ambos desempeños. Esto es, precisamente, lo que ocurre en lo que la OCDE ha venido a llamar *Compliance by Design*, cumplimiento por diseño, un modelo de Administración tributaria en el que se buscan formas de mejorar la relación con las pequeñas y medianas empresas (PYMES), con la intención de lograr niveles más altos de cumplimiento voluntario a menores costes, tanto para las PYMEs como para la propia Hacienda[5], lo cual es más fácil cuando los asuntos fiscales de una entidad o individuo sean menos complejos, pero incluso es viable cuando los contribuyentes tienen estructuras muy complicadas, como las empresas multinacionales. Con esta filosofía, el concepto C*ompliance by design* describe cómo las Administraciones tributarias pueden explotar los desarrollos tecnológicos y las formas en que las empresas se organizan, para incorporar el cumplimiento tributario en los sistemas operativos y de gestión que utilizan los operadores económicos.

Para ello la OCDE propone una doble aproximación, la *secured chain approach*, la cadena segura de información, y la *centralised data approach*, la centralización de datos. En la primera, la "*secured chain approach*", se crea un flujo de información seguro, desde la captura de transacciones comerciales, hasta la determinación final del monto de la deuda tributaria que se abona por el contribuyente. En este contexto, el papel del organismo fiscal es, principalmente, actuar como facilitador del entorno necesario que asegure que el flujo de información desde el contribuyente

5. OCDE (2014), *Tax Compliance by Design: Achieving Improved SME Tax Compliance by Adopting a System Perspective*, OECD Publishing, 2014. Disponible en: http://dx.doi.org/10.1787/9789264223219-en.

es lo suficientemente seguro, lo cual ahorra la necesidad de realizar auditorías posteriores a la presentación del tributo, por ser la propia Administración tributaria quien canaliza todo el tráfico de información, y las condiciones de trazabilidad, integridad y no repudio. Un ejemplo de cumplimiento tributario basado en este tipo de sistemas lo encontramos en la utilización de cajas registradoras certificadas que proporcionan a las Haciendas información segura sobre las transacciones registradas. La caja registradora se conecta a un sistema de contabilidad en línea que registra automáticamente todas las transacciones. Entre tanto, el resto de transacciones comerciales se capturan a través de apuntes contables derivados de las cuentas existentes en entidades financieras. El sistema contable, obviamente, debe proporcionarse por un proveedor homologado/certificado y debe contener una serie de controles incorporados que aseguren la veracidad y calidad de la información proporcionada. Del mismo modo debe/puede contener todas las medidas necesarias para realizar liquidaciones tributarias en línea de acuerdo con la legislación vigente, (aunque en determinadas circunstancias pueda requerir cierta "ayuda manual", por ejemplo, a la hora de optar o no por una determinada deducción), el contribuyente puede presentar el formulario de declaración de impuestos en el mismo sistema y, en consecuencia, el pago de puede realizarse a través de esa plataforma. El objetivo final es diseñar un sistema en un modo en el que tanto la Administración tributaria como el obligado tributario puedan obtener la deseada certeza sobre el importe de la deuda tributaria, sabiendo que los procesos son seguros, y trabajando en comandita como eslabones de una misma cadena. Las dos partes obtienen beneficios adicionales: la Administración (que actúa como facilitador de los hitos necesarios para el funcionamiento del sistema) dispone de seguridad sobre el alcance de la capacidad económica del obligado tributario y le hace tributar en consonancia; el contribuyente, además de ver salvaguardada su capacidad contributiva, se ahorra o reduce los farragosos trámites de las obligaciones formales. Conviene señalar que el *secured chain approach* lejos de ser una entelequia, una ideación remota en su ejecución, o una forma de relación entre Administración y administrado extraña, propia de jurisdicciones tributarias anglosajonas, es toda una realidad en nuestro país, al menos, en lo que atañe a las Haciendas Forales de Álava, Bizkaia y Gipuzkoa, donde el Proyecto TicketBAI ha comenzado su andadura de forma voluntaria y será obligatorio en todo el territorio de la Comunidad Autónoma del País Vasco en 2024[6]. Por su parte, la filosofía que subyace en el segundo

6. Se trata de un proyecto conjunto desarrollado por las Haciendas Forales, en colaboración con el Gobierno Vasco, que obliga a los contribuyentes afectados (con contadas excepciones, todos aquellos que ejerzan una actividad económica) a adaptar sus

enfoque, el de la centralización de datos o *centralised data approach*, es la de asegurarse que la Administración puede, por sí misma, capturar tantas transacciones comerciales de la fuente como sea posible, para determinar la cantidad correcta de impuestos a pagar con el aporte de una mínima información por parte del contribuyente. En este caso, el papel de la Hacienda se fundamenta en la gestión de todo el proceso y en el manejo y transformación de toda la información, por lo que la necesidad de que el contribuyente brinde información de sus propias transacciones se reduce significativamente limitándose, principalmente, a proporcionar datos sobre terceros. La obtención de datos directamente de la fuente debiera facilitar la consecución de la certeza deseada en cuanto a la delimitación de la capacidad económica del contribuyente porque el groso de los datos no se proporciona por el obligado tributario y, por tanto no es susceptible de ser manipulado u ocultado. Sin embargo, se requieren otros mecanismos que detecten cualquier transacción que quede fuera del marco informativo que se obtiene de terceros.

Como podemos observar, de los dos acercamientos posibles al *compliance by design*, es el primero, el que se conoce como *secured chain approach,* el que de mejor forma implementa una nueva cultura de relación colaborativa entre la Administración tributaria y el contribuyente pero el que, de alguna forma, también puede implicar ciertos riesgos que deben considerarse respecto a la intromisión que, en determinados supuestos pueda suponer la integración de los procedimientos tributarios en la operativa de nuestras empresas y, más concretamente en los sistemas informáticos que, en algunas ocasiones, pueden constituirse, por qué no, como domicilios constitucionalmente protegidos de los contribuyentes[7].

herramientas de facturación, de forma que al momento de emitir la correspondiente factura o documento sustitutivo, la información tributaria asociada a la transacción se recoge en dicho documento y se remite de forma casi simultánea al Fisco. La iniciativa, a diferencia de los ejemplos analizados previamente. En principio TicketBAI es de aplicación a todas las personas físicas y jurídicas que realicen una actividad económica, quienes deben utilizar un software de facturación que cumpla los requisitos técnicos establecidos en la normativa y que permite a las Haciendas Forales controlar los ingresos de los contribuyentes, además de facilitar a los mismos el cumplimiento de sus obligaciones tributarias. En un ámbito estatal, también se está trabajando en el desarrollo de iniciativas que aboquen a la utilización de softwares garantes. En la actualidad se está redactando el reglamento que desarrolle la prohibición del software de doble uso implantado por ley 11/2021, lo cual ha suscitado alguna crítica en la doctrina en cuanto a la imprescriptibilidad de las infracciones que su incumplimiento pudiera suscitar (*Vid.* al respecto PÉREZ TENA, J.R. "La lucha contra el software de doble uso en la Ley General Tributaria: un ensayo de infracciones tributarias permanentes", *Estudios financieros. Revista de contabilidad y tributación: Comentarios, casos prácticos*, N.° 463, 2021, pp. 5-46).

7. *Vid.* al respecto la STS de 24 de abril de 2010 (recurso n.° 3791/2006).

Recordemos, al respecto, que estos sistemas (físicos o incluso virtuales, a través de tecnologías *cloud computing*) pueden contener datos sobre la intimidad de las personas físicas o la vida privada "social" de las personas jurídicas con lo que deben gozar de la misma protección que la ofrecida por el artículo 18.2 de nuestra Constitución (en adelante CE)[8]. Volveremos sobre este extremo más adelante al analizar los derechos de los contribuyentes eventualmente afectados por la utilización de la IA en el ámbito tributario.

4. LA IA EN LOS PROCEDIMIENTOS DE REVISIÓN TRIBUTARIA Y EN EL PROCEDIMIENTO SANCIONADOR

Lo expuesto en epígrafes precedentes da cuenta del desarrollo presente de la inteligencia artificial en los procedimientos de aplicación de los tributos donde, como hemos visto, tanto en lo que atañe a las labores de asistencia-información como a las de control del cumplimiento tributario, o aquellas otras que imbrican ambas cuestiones, los órganos de aplicación de los tributos, a través de los pertinentes procedimientos de gestión, inspección y recaudación hacen uso ya de las vastas utilidades que proporciona.

Sin embargo, en lo que respecta al resto de procedimientos tributarios, a los procedimientos de revisión y al procedimiento sancionador, más allá del fundamento de las decisiones automatizadas, predicciones, previsiones… basadas en la IA y que puedan suscitar el punto de partida de dichos procedimientos (por ser resolutorias en cuestiones de mera intendencia, trámite o numéricas, porque ponen fin a la vía administrativa, porque fundamentan un procedimiento inspector que es paralelo a la incoación de un procedimiento sancionador…), en principio, la inteligencia artificial no despliega en la actualidad en la esfera tributaria todos sus efectos del modo en que pudiera desplegarlos, por ejemplo, adoptando la decisión sobre un recurso, imponiendo una multa concreta, en definitiva, entrando en una materia que, hasta el día de la fecha ha conocido de cierta "reserva de humanidad". Lo cual, obviamente, no significa que no se pueda hacer o que no plantee las mismas dudas que, al respecto, se presentan en un ámbito estrictamente jurisdiccional.

8. FERNÁNDEZ LÓPEZ, R.I., "La autorización judicial para la entrada y registro en el domicilio constitucionalmente protegido del obligado tributario", en MERINO JARA, I. (Dir.) *Prevención y Fraude, nuevas medidas tributarias. Adaptado a la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal*, La Ley, Las Rozas, 2021, p. 253.

III. RIESGOS ASOCIADOS A LA UTILIZACIÓN DE LA IA EN EL ÁMBITO TRIBUTARIO Y DERECHOS DEL CONTRIBUYENTE AFECTADOS POR ESE USO

1. CARACTERÍSTICAS DE LA IA QUE ENTRAÑAN DETERMINADOS "RIESGOS"

Como hemos tenido ocasión de atisbar, la utilización de la inteligencia artificial en el ámbito tributario apunta ciertos "peligros" que necesariamente han de considerarse en la propia configuración y diseño de estas tecnologías. El primero está relacionado con la generación de nueva información de valor agregado que se suscita por el propio algoritmo en el que se basa la inteligencia artificial. Una "nueva información" que va más allá del mero metadato o el "dato sobre el dato", que, en cierta manera, ayuda a sistematizar la información existente de forma que facilita la estandarización de la misma y permite realizar búsquedas y sistematizaciones. Ciertamente, el poder de relación de datos que tiene la IA, puede crear un nuevo conocimiento a través de reglas proporcionadas por un experto (SBR) o a través del análisis de casos previamente acaecidos (SBC) que, simplemente, trasciendan la información de la que de forma previa dispone el Fisco.

La base de este nuevo conocimiento está, según se ha comentado por alguno de los autores que me acompañan en esta obra, en el *machine learning* que crea una nueva realidad aparente que funciona a modo de presunción *iuris tantum* y que sirve para tomar decisiones por parte de las Administraciones, en el caso que nos ocupa, la Administración tributaria. Esta realidad se imbrica a la perfección con la apuntada importancia de la elección de la IA más pertinente según el objetivo perseguido, pues, podemos encontrarnos con modelos entrenados a partir de patrones, lo cual perfecciona y automatiza la comprensión actual del riesgo fiscal existente en un determinado contexto, reduciendo el número de casos mal seleccionados para su intervención (lo cual ahorra tiempo al Fisco y carga tributaria a contribuyentes cumplidores), pero no ayuda a identificar nuevos perfiles de riesgo o riesgos fiscales desconocidos (para lo sí son buenos los modelos no supervisados). Sin embargo, no debemos desconocer que en el "programa" (aparente o expreso) de esa inteligencia artificial que aprende de las reglas o casos que lo alimentan, pueden existir sesgos (voluntarios o involuntarios, conscientes o inconscientes) que atenten contra el principio de igualdad tributaria contenido en el artículo 31.1 de la Constitución.

Igualmente, debemos destacar que, en el proceso de generación de esta información de valor agregado, debe primar la transparencia y que,

lamentablemente, en ocasiones, más de las deseables, la opacidad derivada de las "cajas negras" (*black boxes*) en las que se convierten los algoritmos que sustentan la inteligencia artificial hace imposible discernir los motivos que fundamentan una determinada decisión[9], todo lo cual puede suscitar una manifiesta indefensión, además de convertir en *iuris et de iure* presunciones que, *a priori*, debieran admitir prueba en contrario. Lo mismo ocurre para algunos autores[10] que consideran los algoritmos que subyacen en la inteligencia artificial como verdaderos reglamentos que, en consecuencia, debieran ser publicados o publicitados de alguna manera. En primer lugar, en aplicación del principio de transparencia, en relación con su código fuente[11]. En segundo lugar, porque operan como verdaderos códigos jurídicos[12], en el entendimiento de que al igual que los reglamentos se utilizan para la evaluación de las circunstancias que conciernen a un caso concreto, siguiendo una inferencia lógica que fija las consecuencias jurídicas que le son predicables, cuando los algoritmos sean utilizados para evaluar las condiciones que afectan a un supuesto determinado, o para prescribir cuál debe ser la respuesta jurídica al mismo, materialmente debiéramos considerarlos como esos reglamentos tradicionalmente utilizados por la Administración. En este sentido, los algoritmos

9. *Vid*. al respecto SERRANO ANTÓN, F. "La Inteligencia artificial y administración tributaria. Especial referencia al procedimiento de inspección tributaria" en SERRANO ANTÓN, F. (Dir.) *Inteligencia artificial y Administración tributaria: eficiencia administrativa y defensa de los derechos de los contribuyentes*, Thomson Reuters Aranzadi, Cizur Menor, 2021, pp. 149-189.

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

11. *Vid*. al respecto OLIVARES OLIVARES, B. "Transparencia y aplicaciones informáticas en la Administración Tributaria", Crónica Tributaria, N.° 174, 2020, pp. 89-112.

12. Entre otros, además de BOIX PALOP, Andrés, "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", Ob. Cit.; YEUNG, K. y LODGE, M., *Algorithmic regulation*, Oxford University Press, Oxford, 2019; DE LA CUEVA GONZÁLEZ-COTERA, J., "Código fuente, algoritmos y fuentes del Derecho", *El Notario del Siglo XXI*, N.° 77, enero/febrero 2018, pp. 36-39; en relación con la participación de los ciudadanos en el proceso normativa NADAL SÁNCHEZ, H., DE LA CUEVA GONZÁLEZ-COTERA, J., "Redefiniendo la isegoría: open data ciudadanos", en CERRILLO I MARTÍNEZ, A., PEGUERA, M., PEÑA-LÓPEZ, I., PIFARRÉ DE MONER, M. J., VILASAU SOLANA, M. (coords.), *Retos y oportunidades del entretenimiento en línea. Actas del VIII Congreso Internacional, Internet, Derecho y Política*, Universitat Oberta de Catalunya, Barcelona 9-10 julio, 2012, UOC-Huygens Editorial, Barcelona, pp. 283-300. Documento disponible en línea: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/15121/6/IDP_2012.pdf (04/07/20), *Vid.*, igualmente, HASSAN, S. y DE FILIPPI, P. "The Expansion of Algorithmic Governance: From Code is Law to Law is Code", *Journal of Field Actions*, N.° 17, 2018, pp. 88-90, disponible en https://journals.openedition.org/factsreports/4518.

empleados, en la medida en que aplican reglas[13], preordenan la decisión final que ésta pueda adoptar, y limitan su ámbito de discreción a partir de los postulados contenidos en su programación, lo que los convierte en reglamentos en un sentido jurídico material[14].

Según vemos, esa realidad a la que Philip K. Dick hacía referencia en su *Informe de la minoría* no es ni tan distópica ni tan lejana: la imposibilidad de acceder a la motivación de la toma de decisiones de determinadas inteligencias artificiales puede llevar a una suerte de "profecía autocumplida" en la que al obligado tributario le resulta del todo imposible escapar del sino que le ha sido determinado por el algoritmo.

De lo expuesto hasta ahora se deduce que, si bien la utilización de la inteligencia artificial por las administraciones tributarias ha supuesto un gran adelanto en los procesos de automatización en el ámbito de los procedimientos de gestión, así como en las facultades prospectivas de los órganos de inspección, también presenta determinadas flaquezas que pudieran afectar a sus los derechos de los contribuyentes. Por ello resulta imprescindible analizar aquellos derechos se pueden ver, de hecho son, más afectados de suerte que, a continuación, podamos analizar la protección que debiera serles conferida desde el prisma de la propuesta de reglamento.

2. DERECHOS DE LOS CONTRIBUYENTES AFECTADOS POR LA UTILIZACIÓN DE LA IA EN EL ÁMBITO TRIBUTARIO

Como hemos tenido ocasión de apuntar, la utilización de la inteligencia artificial por nuestras Administraciones tributarias puede afectar a distintos derechos del contribuyente. Desde un punto de vista procesal, alguno de ellos, como el derecho a una resolución motivada o el derecho a la presunción de inocencia, se englobarían dentro del derecho a la tutela judicial efectiva; otros dentro del derecho a la igualdad del artículo 14 CE o el derecho a la intimidad personal y familiar o la inviolabilidad del domicilio del artículo 18 CE, obviamente desde el prisma y las limitaciones que les confiere el Derecho Tributario.

En las siguientes líneas señalaremos las cuestiones más relevantes que afectan al uso de la IA en este ámbito y, en su caso, mencionaremos los pronunciamientos jurisprudenciales que pueden perfilar el futuro de esta

13. Bien porque, como veremos se utilizan Sistemas Basados en Reglas o porque la aplicación las infiere de una serie histórica de supuestos con la que se alimenta a la herramienta.

14. BOIX PALOP, Andrés, "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", *op. cit.*, p. 237.

tecnología en los procedimientos tributarios, al menos en los que atañe a los procedimientos de aplicación de los tributos, a la gestión, a la inspección y a la recaudación.

2.1. Derecho a una resolución motivada

La motivación de los actos administrativos en el ámbito tributario viene referida en distintos puntos a lo largo de la Ley General Tributaria (LGT): en el artículo 81 LGT respecto de la adopción de medidas cautelares en el artículo 102 LGT en relación con las liquidaciones, en el artículo 103 LGT para los actos de liquidación, los de comprobación de valor, los que impongan una obligación, los que denieguen un beneficio fiscal o la suspensión de la ejecución de actos de aplicación de los tributos; en el artículo 113 LGT para la autorización judicial para la entrada en el domicilio de los obligados tributarios; en los artículos 132 y 133 LGT para el procedimiento de verificación de datos; artículo 134 LGT para la comprobación de valores; en el artículo 142 LGT en lo que se refiere a las facultades de los órganos de inspección; artículo 146 LGT en lo que atañe a la adopción de medidas cautelares en el procedimiento de inspección; en el 150 LGT respecto a la suspensión del plazo de este procedimiento; el artículo 159 LGT sobre el plazo para la emisión del informe preceptivo para la declaración del conflicto en la aplicación de la norma tributaria; el artículo 208 y 210 LGT para el procedimiento sancionador; en los artículos 215, 217, 225, 230, 233, 238, 241 LGT en los distintos procedimientos de revisión; y, finalmente, en el artículo 251 LGT sobre las excepciones a la práctica de liquidaciones en caso de existencia de indicios de delito contra la Hacienda Pública.

La obligatoriedad de la motivación en todos los procedimientos mencionados no es, en absoluto, baladí: justifica las decisiones adoptadas en relación con la fijación de la intensidad con que un determinado obligado tributario debe contribuir al sostenimiento de los gastos públicos; limita su derecho a la propiedad privada y, en determinadas ocasiones puede estar relacionado con supuestos en los que se perfilan no sólo infracciones tributarias sino, incluso, delitos.

Como sabemos el ámbito penal, el derecho a un debido proceso, contenido implícitamente en el artículo 24 CE, se plantea como un derecho consustancial al mismo, que, por su parte, y en aplicación de los principios penales al derecho punitivo tributario puede, también, tener reflejo en el ámbito que nos ocupa. Así lo entendió nuestro Tribunal Constitucional en fecha temprana en su Sentencia 18/1981, al indicar que "los principios inspiradores del orden penal son de aplicación, con ciertos matices al Derecho Administrativo sancionador, dado que ambos son manifestaciones del

ordenamiento punitivo del Estado tal y como refleja la propia Constitución y una muy reiterada jurisprudencia del Tribunal Supremo, hasta tal punto que un mismo bien jurídico puede ser protegido con técnicas administrativas o penales, si bien en el primer caso con el límite que establece el propio artículo 25, en su n.° 3, al señalar que la Administración Civil no podrá imponer penas que directa o subsidiariamente impliquen la privación de libertad" (fundamento jurídico 2.°), precisando que "los principios esenciales reflejados en el artículo 24 de la Constitución en materia de procedimiento han de ser aplicados a la actividad sancionadora de la Administración, en la medida necesaria para preservar los valores esenciales que se encuentran en la base del precepto, y la seguridad jurídica que garantiza el artículo 9 de la Constitución. No se trata, por tanto, de una aplicación literal dadas las diferencias apuntadas, sino con el alcance que requiere la finalidad que justifica la previsión constitucional".

Como indica ROMERO FLOR, lo anterior invita a señalar que existe "un único sistema de garantías frente a un único poder punitivo que posee una variante penal y otra administrativa sancionadora"[15], por lo que debemos aceptar la aplicación y, por ende, el respeto a los principios constitucionales comunes a toda contención de conductas derivadas de la inobservancia de las normas jurídicas, entre ellas, también, las tributarias. En otras palabras, si bien este derecho al debido proceso, del que forma parte el derecho a que las decisiones judiciales sean motivadas, no se aplica en toda su extensión en el Derecho Administrativo, a su procedimiento, como consecuencia de las prebendas inherentes a la Administración, la necesidad de que las resoluciones que culminan el mismo estén motivadas está contemplada en el artículo 35 de la Ley 39/2015, que expresamente señala que las propuestas de resolución en los procedimientos de carácter sancionador, así como los actos que resuelvan procedimientos de carácter sancionador o de responsabilidad patrimonial, deben estar motivadas.

Fuera del ámbito sancionador, este último artículo exige que deban motivarse los actos que limiten derechos subjetivos o intereses legítimos; los actos que resuelvan procedimientos de revisión de oficio de disposiciones o actos administrativos, recursos administrativos y procedimientos de arbitraje y los que declaren su inadmisión; los que se separen del criterio seguido en actuaciones precedentes o del dictamen de órganos consultivos; los acuerdos de suspensión de actos, cualquiera que sea el motivo de ésta; la adopción de medidas provisionales; los acuerdos de aplicación de la tramitación de urgencia, de ampliación de plazos y de realización

15. Literal ROMERO FLOR, Luis M.ª, "Deberes Tributarios Vs Derechos Humanos: El Derecho a No Autoinculparse en el Procedimiento Tributario", *Papeles el Tiempo de los Derechos*, n.° 5, 2014, p. 5.

de actuaciones complementarias; los que rechacen pruebas propuestas por los interesados; los que acuerden la terminación del procedimiento por la imposibilidad material de continuarlo por causas sobrevenidas, así como los que acuerden el desistimiento por la Administración en procedimientos iniciados de oficio; y, finalmente, los actos que se dicten en el ejercicio de potestades discrecionales, así como los que deban serlo en virtud de disposición legal o reglamentaria expresa. En definitiva, la motivación debe estar presente en todo un catálogo de actos administrativos que, como no podía ser de otra forma, también tienen sus reminiscencias en el ámbito tributario. Por ello, los artículos de la LGT antes referidos exigen que los actos que deriven de las actuaciones de la Administración Tributaria deban, en cualquier caso, motivarse.

La segunda acepción del verbo motivar en la RAE indica que consiste en "dar o explicar la razón o motivo que se ha tenido para hacer algo". Ciertamente, esta acción no consiste únicamente en señalar una concatenación de hechos y fundamentos jurídicos, sino que debe reflejar el proceso de injerencia racional que une los primeros con los segundos, y las consecuencias que de esta relación se infieren y anudan desde un punto de vista jurídico. Como ha venido a indicar desde antiguo el Tribunal Supremo en numerosas ocasiones[16], ha de darse razón del proceso lógico y jurídico que determina la decisión, es necesario que se dé a conocer a los interesados las razones de la decisión administrativa para que haga posible la defensa de sus derechos e intereses, ya que sólo conociéndolas podrá después alegar cuanto convenga a su defensa, sin verse sumidos en la indefensión que prohíbe el artículo 24.1 de nuestra Constitución.

Pues bien, es aquí, precisamente, donde determinados sistemas de inteligencia artificial pueden llegar a conculcar el derecho a un acto administrativo motivado, principalmente por dos razones. Por un lado, porque esos procesos de injerencia lógica en ocasiones escapan a la propia programación diseñada por los constructores de la IA. En efecto, cuando nos encontramos ante sistemas que aprenden de sus experiencias, construyendo a partir de las mismas las reglas que aplicarán a futuros supuestos, las razones que impulsan esas decisiones venideras quedan fuera del alcance de los parámetros que inicialmente se les hayan podido dar por parte de los programadores. Ni siquiera está en sus manos explicar los motivos que las impulsan, sus programas "han cobrado vida propia" adoptando decisiones autónomas.

La cuestión no es, según decíamos, en absoluto trivial. El Tribunal Constitucional y el Tribunal Supremo han señalado en distintas sentencias que

16. Tomamos por todas ellas una, la ya antigua STS de 12 de enero de 1998.

la motivación constituye una garantía frente a la arbitrariedad que pueda darse en la decisión de actos administrativos, en el entendimiento de que es consecuencia de una exégesis racional del ordenamiento[17]. Por ello, no puede consistir en una "mera declaración de conocimiento y menos aún en una manifestación de voluntad que sería una proposición apodíctica, sino que ésta –en su caso– ha de ser la conclusión de una argumentación ajustada al tema o temas en litigio, para que el interesado, destinatario inmediato pero no único, y los demás, los órganos judiciales superiores y también los ciudadanos, puedan conocer el fundamento, la *ratio decidendi* de las resoluciones"[18]. Por otro lado, incluso en aquellos casos en los que los fundamentos que motivan las decisiones de la IA puedan explicarse por no ser opacos, por no estar dentro de esas cajas negras (aquellas *black boxes)* en las que derivan los sistemas de *machine learning*, nos encontramos con dos problemas: el primero, la (ausencia de) publicidad que se les dé a los algoritmos que subyacen en los términos antedichos en epígrafes precedentes; el segundo, la eventual ininteligibilidad de los mismos para el común administrados, que carece de los conocimientos técnicos necesarios para su comprensión cabal,incluso, en el caso de que sean publicados.

En cualquiera de los supuestos, bien porque se trata de algoritmos que adoptan sus decisiones en *black boxes*, bien porque el contenido del algoritmo y su código fuente no se publica, o simplemente porque es ininteligible, el resultado puede ser el mismo, la anulación o en su caso la anulabilidad del acto administrativo. A tenor de lo dispuesto en el artículo 47 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAPAC), y en lo que atañe a la materia tributaria, en el artículo 217 LGT, la anulación del acto sólo sería viable si entendiéramos que la opacidad de los motivos de la decisión equivale a la ausencia total y absoluta del procedimiento del que emana, algo que no parece predicable en estos supuestos.

Sin embargo, entendemos que esta opacidad sí puede derivar en la anulabilidad de dicho procedimiento. En efecto, la ausencia de motivación, o su equivalente algorítmico cuando las razones que motivan una decisión automatizada permanecen opacas al administrado, puede ser constitutiva de anulabilidad si éste último se ha visto imposibilitado a la hora de conocer las razones que conducen a la Administración a dictar el acto en cuestión, ya que podría generar indefensión, o un mera irregularidad no invalidante si es que el "velo" impuesto al algoritmo no ha producido ese

17. Por todas como muestra de una jurisprudencia ya consolidada, la STC 77/2000, de 22 de marzo o la STC 311/2005, de 12 de diciembre. También la STS 1688/2017, de 29 de noviembre.
18. STC 77/2000, FJ 1.

desconocimiento de los motivos y razones que fundamentan la decisión. En consecuencia, para determinar la extensión de esta anulabilidad va a ser necesario fijar si el administrado, el obligado tributario, ha podido llegar a conocer las razones de la decisión que adopta la Administración: sólo en ese caso podremos alegar la indefensión referida en el artículo 48.2 LRJAPAC o en el artículo 219 LGT para los casos de revocación de los actos de aplicación de los tributos y de imposición de sanciones.

2.2. Derecho a la presunción de inocencia

Señalábamos en líneas precedentes cómo los principios del Derecho Penal son aplicables, con matizaciones, en el Derecho Tributario sancionador, lo cual implica que el principio de presunción de inocencia no puede reducirse al estricto campo del enjuiciamiento de conductas presuntamente delictivas, debemos colegir que igualmente preside la adopción de cualquier resolución tanto administrativa como jurisdiccional que se fundamente en la condición o conducta de las personas de cuya apreciación derive un resultado sancionatorio o limitativo de sus derechos.

Partiendo de esta premisa, y obviando las críticas que se puedan hacer respecto a la progresiva objetivización de la responsabilidad en el ámbito tributario desde la práctica administrativa, el modelo en el que nos enmarcamos se origina en la idea de que debiera sancionarse (penal o administrativamente) sólo a aquellos sujetos que más allá de toda duda razonable son culpables. Sin embargo, la introducción de la informática decisional, bien en la resolución de conflictos (entendidos en sentido amplio, no en lo que estrictamente atañe a los procedimientos de revisión), bien aportando fundamentos para que el funcionario encargado de resolver adopte la decisión que considere oportuna, implica que las decisiones respecto a la culpabilidad dependen de un cálculo de probabilidades en el que confiamos para concluir en tal o cual sentido. Debemos ser conscientes de que los algoritmos, el código fuente que subyace en la IA decisional, cuantifican el umbral de probabilidad a partir del cual una persona es "culpable" y de que, admitiendo el uso de estos mecanismos también asumimos como aceptable (e incluso inevitable) que probabilísticamente se sanciona a inocentes, algo a todas luces poco ético y contrario a los principios inherentes a todo Estado de Derecho.

2.3. Derecho a la intimidad y la inviolabilidad del domicilio constitucionalmente protegido

En nuestro entorno más cercano, el Tribunal Supremo ha tenido ocasión de expresar su opinión respecto al alcance del poder decisorio de la

inteligencia artificial en el ámbito tributario. En efecto, el Auto del Tribunal Supremo 9821/2019, de 3 de octubre, admite a trámite un recurso de casación contra la sentencia del Tribunal Superior de Justicia de Andalucía que desestima el recurso de apelación en relación con una petición de la Administración Tributaria para entrar en el domicilio constitucionalmente protegido de un sujeto con un perfil de alto riesgo según lo determinado por los programas y aplicaciones de la AEAT.

Tras la admisión a trámite del recurso de casación en el entendimiento de que debe ponderarse si los requisitos para la entrada son proporcionados cuando se basan únicamente en la información que proporcionan este tipo de sistemas, con lo que se cuestiona, al menos, la necesaria ponderación entre el derecho a la intimidad y la utilización de instrumentos de IA, en la STS 3023/2020, de 1 de octubre, nuestro Alto Tribunal indica que "no pueden servir de base, para autorizar la entrada, los datos o informaciones generales o indefinidos procedentes de estadísticas, cálculos o, en general, de la comparación de la situación supuesta del titular del domicilio con la de otros indeterminados contribuyentes o grupos de estos, o con la media de sectores de actividad en todo el territorio nacional, sin especificación o segmentación detallada alguna que avale la seriedad de tales fuentes. Tal análisis, de hacerse excepcionalmente, debe atender a todas las circunstancias concurrentes y, muy en particular, a que de tales indicios, vestigios o datos generales y relativos –verificado su origen, seriedad y la situación concreta del interesado respecto a ellos– sea rigurosamente necesaria la entrada, lo que exige valorar la existencia de otros factores circunstanciales y, en particular, la conducta previa del titular en respuesta a actuaciones o requerimientos de información efectuados por la Administración". Toda una declaración de intenciones que marca el camino de lo que en un futuro se vaya a exigir en relación con los actos administrativos automatizados y que, de alguna manera, ha pretendido mitigarse mediante la modificación introducida en la LGT (artículos 113 y 142.2) mediante la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal que, como bien ha apuntado algún autor afectan a determinados contenidos del derecho a la inviolabilidad del domicilio[19].

Otro ejemplo de lo que la jurisprudencia puede hacer a la hora de delimitar el perímetro de la injerencia con la que la IA en el ámbito tributario puede afectar al derecho a la intimidad, lo encontramos fuera de nuestras fronteras, concretamente en los Países Bajos, un ordenamiento que, entre

19. *Vid.* FERNÁNDEZ LÓPEZ, R.I., "La autorización judicial para la entrada y registro en el domicilio constitucionalmente protegido del obligado tributario", en MERINO JARA, I. (Dir.) *Prevención y Fraude, nuevas medidas tributarias. Adaptado a la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal*, *op. cit.*, p. 222.

otros, ha implementado un modelo de aprendizaje sin supervisión, el *System Risk Indication,* más conocido como SyRI, que traducido al español podríamos denominar Indicación de Riesgo del Sistema. SyRI es un instrumento legal que el gobierno holandés utiliza para prevenir y combatir el fraude en el ámbito de la Seguridad Social y la Administración Tributaria en el que, a través de su infraestructura técnica y procedimientos asociados, se pueden vincular y analizar datos de forma anónima en un entorno seguro, para generar informes de riesgo. De este modo, SyRI permite a las autoridades gubernamentales centrales y locales combinar amplias categorías de datos previamente almacenados por separado, analizarlos utilizando un "modelo de riesgo" no revelado, e identificar a algunas personas con más probabilidades de cometer fraude fiscal. Conviene apuntar, como adelanto de la eventual discriminación que en ocasiones acompaña a estas herramientas, que según indica el Relator Especial sobre Pobreza Extrema y Derechos Humanos de la ONU, es un sistema que, desde su introducción, se ha utilizado exclusivamente en áreas con una alta proporción de residentes de bajos ingresos, migrantes y minorías étnicas[20], lo cual, no deja de ser llamativo en un país que, habiendo recibido en alguna ocasión el calificativo de paraíso fiscal, no utiliza estas herramientas para los grandes contribuyentes en atención a su derecho a la intimidad.

Precisamente, es el derecho a la vida privada el argumento utilizado por el Tribunal que estudia el caso para refutar la legalidad de la herramienta. En efecto, el Tribunal de la Haya que dicta sentencia[21], en una apuesta valiente que se aparta precedentes judiciales de otras jurisdicciones[22], recuerda que de conformidad con el artículo 8 del CEDH, los Países Bajos, como Estado miembro, tienen una responsabilidad especial en la aplicación de nuevas tecnologías para encontrar el equilibrio adecuado al sopesar, por un lado, las ventajas asociadas con el uso de esas tecnologías en el contexto de la prevención y el control, el fraude y, por otro lado, la injerencia que pueda suponer en el ejercicio del derecho al respeto de la vida privada. Desde el punto de vista de la protección del derecho al respeto de la vida privada, que incluye el derecho a la protección de los datos

20. ALSTON, Philip, *Brief in the case NJCM c.s./ De Staat Der Nederlander (SyRi) before the District Court of The Hague,* ONU, 2019.
Disponible en: https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf.
Último acceso: 28/07/2020.

21. Sentencia de 5 de febrero de 2020, caso número C-09-550982-HA ZA 18-388.

22. *Loomis vs. Wisconsin* en Estados Unidos. *Vid.,* para un examen de esta y similares sentencias en tribunales norteamericanos HALL, Claire, "Challenging Automated Decision-making by Public Bodies: Selected Case Studies from other jurisdictions", *Judicial Review*, N.° 1, 2020, pp. 8-20.

personales, la legislación debe proporcionar un marco suficientemente eficaz con el que todos los intereses en juego puedan sopesarse de forma perspicaz y verificable entre sí. Sobre la base de la legislación, todos deben poder tener la expectativa razonable de que, en el caso del uso de SyRI, se respetará suficientemente su vida privada, algo que, lamentablemente, no se puede garantizar.

A juicio del Tribunal, la herramienta no cumple el requisito establecido en el artículo 8, apartado 2, del CEDH de que la injerencia en el ejercicio del derecho al respeto de la vida privada debe ser necesaria, proporcionada y subsidiaria en relación con a su propósito previsto. Para llegar a esta conclusión contrasta el contenido de SyRI a la luz de los propósitos que persigue, con la invasión de la privacidad que su uso implica, y opina que la legislación no cumple con el "equilibrio justo" (la relación razonable) que debe existir en el CEDH, entre el interés social al que sirve la legislación, y la violación de la vida privada que crea, para poder hablar de una invasión de la privacidad suficientemente justificada. Al hacerlo, el tribunal tiene en cuenta, también, los principios fundamentales que subyacen en la protección de datos en virtud de la legislación de la UE (la Carta de los Derechos Fundamentales y el Reglamento General de Protección de Datos), en particular, los principios de transparencia, el principio de limitación de la finalidad y el principio de minimización de datos.

2.4. Derecho a la igualdad y a la no discriminación

La opacidad a la que venimos haciendo referencia exige, igualmente, la salvaguardia de los principios fundamentales de igualdad y de no discriminación frente a las decisiones o predicciones realizadas por inteligencias artificiales, que, lamentablemente, no siempre son neutras. En efecto, los sesgos implícitos, voluntarios o involuntarios, predeterminados o adquiridos por el propio sistema, que subyacen en estas potentes herramientas pueden provocar discriminaciones algorítmicas estructurales que son, del todo, inadmisibles[23].

Si los sistemas de IA beben indefectiblemente de fuentes que abocan a inspeccionar ciertas cuestiones sobre un determinado segmento poblacional, social, profesional… en forma de bucle, porque los resultados obtenidos a partir de ciertos datos se convierten en datos que alimentan, de

23. CORVALÁN, Juan G., "El peligro de la inteligencia artificial como oráculo del sistema penal". *Diario Infobae*, 30 de agosto 2017. Disponible:http://www.infobae.com/opinion/2017/08/30/el-peligro-de-la-inteligencia-artificial-como-oraculo-delsistema-penal/.

nuevo, el sistema, podemos encontrarnos con graves problemas de desigualdad en el tratamiento tributario de determinados grupos de obligados tributarios sin causa que razonablemente lo justifique. De hecho, tal distinción pudiera ser constitutiva de una vulneración del artículo 21 de la Carta Europea de Derechos Fundamentales, en la medida en vulnera la prohibición de toda discriminación, y, en particular en estos casos, la ejercida por raza, orígenes sociales o patrimonio.

Desde otro punto de vista, si aceptamos como algún autor, que los algoritmos son reglamentos[24], los sesgos y discriminación implícita en los mismos podrían llegar a conculcar, no ya la igualdad tributaria del artículo 31 CE, sino más aún, la igualdad del artículo 14, con las implicaciones procesales que esta circunstancia supone en cuanto a la defensa de los intereses de los contribuyentes en el ámbito de la utilización del recurso de amparo. En este plano, si los algoritmos son reglamentos, es decir normas jurídicas, les es aplicable el axioma de igualdad ante la (ley) contenido en este último artículo, lo que, de suyo, podría plantear problemas de constitucionalidad respecto de aquellos sistemas de inteligencia artificial que implícita o explícitamente están contaminados con sesgos discriminatorios en atención a circunstancias específicas como la actividad ejercida, el origen geográfico, el ser (o no) destinatario de ayudas públicas…

Sin llegar a estas últimas posiciones, entendemos que la retroalimentación de los sistemas de *machine learning*, cuando sus resultados se emplean para adoptar decisiones que afectan, en la generalidad de los casos, a un acotado e idéntico grupo de contribuyentes pudieran llegar a producir, en la práctica, discriminaciones que atenten contra lo dispuestos tanto en la referida Carta Europea de Derechos Fundamentales como en el artículo 1 del Protocolo 12 del Convenio Europeo de Derechos Humanos.

La utilización de herramientas de inteligencia artificial, debiera, en principio, robustecer este derecho a la igualdad, en la medida en que el procedimiento se hace más objetivo, y, por ende, menos susceptible de caer en las involuntarias discrecionalidades del funcionario encargado de realizar el control. Sin embargo, como hemos tenido ocasión de comprobar, este *desiderátum* no se corresponde con la realidad. Sabemos que estas aplicaciones no son asépticas y que cuando su aprendizaje se basa en reglas, aquellas que les proporcionan sus programadores, estas reglas pueden contener sesgos que produzcan discriminaciones entre contribuyentes. En estas circunstancias debiera preocuparnos, y mucho, que el conjunto de herramientas de *Business Intelligence* que se utilizan por la

24. BOIX PALOP, Andrés, "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", *op. cit.*

Hacienda española no hayan sido desarrollados por los servicios informáticos de la AEAT. No es sólo que estos sistemas estén sesgados, sino que, además, esos sesgos provienen de programadores que ni siquiera son parte de la Administración, esto es, pueden ser sesgos mercantilizados. Más aún, incluso en aquellos desarrollos SBC en los que los algoritmos pudieran estar libres de sesgos, la discriminación puede derivar del propio aprendizaje del sistema, que se nutre de datos históricos de forma casi tautológica. Si la herramienta se alimenta de una base de datos en la que se parte del estudio de unos casos concretos, el algoritmo subyacente va a interiorizar la serie histórica proyectándola a futuro. Es fácil hacer el paralelismo entre Tay, el robot racista y misógino creado por Microsoft para Twitter[25] y lo que puede pasar con este tipo de herramientas en el ámbito tributario. Si en la serie histórica partimos de una base en la que, por ejemplo, actores, presentadores de televisión, y artistas varios son más proclives a defraudar, el sistema decide investigarlos más, y por tanto, encuentra aún más fraude en este segmento, abundando en una hipótesis de salida que entra en bucle, sin solución de continuidad[26]. Esto es, entre otros fenómenos, lo que se achacaba a SyRI en Holanda, que, al tratarse de una herramienta alimentada con datos de clases sociales depauperadas, los análisis futuros incidían principalmente en estos segmentos sociales en forma de bucle.

De suyo, en la medida en que disponen de una memoria infinita, estas discriminaciones a las que venimos haciendo referencia responden al propio ADN de los algoritmos, que se basan es estimaciones matemáticas que bien pudieran socavar principios tan arraigados en nuestro ordenamiento como el de justicia, equidad, rehabilitación, … ¿Por qué el hecho de que un contribuyente haya cometido una vez un ilícito tributario lo convierte, a efectos de estos sistemas, potencialmente en defraudador de forma perenne? ¿Dónde queda el derecho a la autodeterminación personal, el derecho a cambiar de opinión, el derecho a no volver a equivocarse? Como indica GONZÁLEZ DE FRUTOS[27], "la memoria de las tecnologías es infinita y está en conflicto con la propensión humana al olvido, al perdón y con el derecho de rehabilitarse".

25. https://www.publico.es/ciencias/inteligencia-artificial-internet-tay-robot-microsoft-nazi-machista.html.

26. Recordemos que SyRI se utilizaba principalmente para emitir informes sobre estratos sociales de bajos ingresos, y que, en cierta manera, esto le ayudaba a crear perfiles de eventuales defraudadores que, a su vez, alimentaban el sistema ahondando en el caladero de contribuyentes pobres sobre los que emitir nuevos informes.

27. GONZÁLEZ DE FRUTOS, Ubaldo, Inteligencia Artificial y Administración Tributaria", en SERRANO ANTÓN, Fernando, *Fiscalidad e inteligencia artificial: Administración Tributaria y contribuyentes en la era digital*, Thomson Reuters Aranzadi, Cizur Menor, 2020, p. 157, literal.

IV. LA INTELIGENCIA ARTIFICIAL UTILIZADA EN LOS PROCEDIMIENTOS TRIBUTARIOS COMO SISTEMAS DE ALTO RIESGO

1. LOS SISTEMAS DE ALTO RIESGO EN LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN

La propuesta de reglamento a la que venimos haciendo referencia en epígrafes precedentes reconoce la existencia de una sólida protección de los derechos fundamentales en el ámbito europeo que, ello no obstante, se pone en cuestión por la opacidad y falta de transparencia de algunas aplicaciones de IA que en determinadas ocasiones requieren un planteamiento centrado en el ser humano, lo cual exige velar por que las aplicaciones de IA cumplan la legislación en materia de derechos fundamentales. Para ello la propuesta del Parlamento europeo y el Consejo clasifica el riesgo asociado a los sistemas de inteligencia artificial que regula, distinguiendo en aquellos que califica como "inadmisibles", "de alto riesgo", "de riesgo limitado" y "de riesgo mínimo" en función del grado de compromiso que implica para los derechos de los ciudadanos. Igualmente, la clasificación del riesgo se fundamenta en el objetivo perseguido por el sistema de IA en consonancia con la legislación vigente de la UE en materia de seguridad de los productos, lo cual implica que depende tanto de la función desempeñada por el propio sistema de IA como de la finalidad y las modalidades específicas para las que se utilice dicho sistema[28].

En la clasificación proyectada, se consideran como "de alto riesgo" un número restringido de sistemas de IA que tienen un impacto negativo en la seguridad de las personas o en sus derechos protegidos por la Carta de los Derechos Fundamentales de la UE, y que vienen a referirse en una lista cerrada en sus anexos. Entre los sistemas considerados como de alto riesgo nos encontramos con los que están relacionados con la formación educativa o profesional; las infraestructuras críticas (como los transportes) porque puedan poner en peligro la vida o la integridad física de los ciudadanos; los componentes de seguridad de los productos; el empleo de trabajadores por cuenta ajena o el acceso al trabajo por cuenta propia

28. Por ejemplo, el alcance del uso de la aplicación de la IA y su previsible finalidad, el número de personas que eventualmente puedan verse afectadas, la dependencia respecto al resultado y la irreversibilidad de los daños, …

(por ejemplo en sistemas que clasifiquen los *curriculum vitae* de los candidatos a un determinado puesto).

Al mismo tiempo, también se incluyen otros sistemas de inteligencia artificial que son consustanciales a todo Estado de Derecho, como los relacionados con servicios públicos y privados esenciales (por ejemplo, en lo que atañe a sistemas de calificación crediticia que priven a los ciudadanos de la oportunidad de obtener un préstamo); a la aplicación de las leyes que de alguna manera puedan interferir con los derechos fundamentales de las personas (pensemos, *v. gr*. en un proceso en el que una IA evalúe la fiabilidad de las pruebas presentadas); los que afectan a la Administración de justicia y procesos democráticos; la gestión de la migración, el asilo y el control de las fronteras; y la identificación biométrica.

La eventual calificación de un sistema de IA como de alto riesgo es importante, toda vez que, con el objetivo de garantizar la confianza y un nivel elevado y coherente de protección de la seguridad y los derechos fundamentales, se les exigen una serie de requisitos de preceptivo cumplimiento relacionados con la calidad de los conjuntos de datos utilizados, la documentación técnica y la llevanza de registros, la transparencia y la divulgación de información a los usuarios, la necesaria supervisión humana, y, obviamente, requerimientos sobre la solidez, precisión y seguridad del sistema.

2. LA EXCLUSIÓN DE LOS SISTEMAS DE IA UTILIZADOS EN EL ÁMBITO TRIBUTARIO DE LA CATEGORÍA DE SISTEMAS DE ALTO RIESGO

El literal del considerando número 38 de la propuesta de Reglamento recuerda que "las actuaciones de las autoridades encargadas de la aplicación de la ley que implican determinados usos de sistemas de IA se caracterizan por un importante desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física, así como a otros efectos negativos sobre los derechos fundamentales que garantiza la Carta". Ciertamente, cualquiera de las afirmaciones recogidas con la excepción referida a la detención o la privación de la libertad salvo que nos estemos refiriendo a cuestiones relacionadas con delitos contra la Hacienda Pública, son aplicables a los sistemas de inteligencia artificial utilizados por nuestras Administraciones tributarias. También estos sistemas de IA, si no están entrenados con datos de buena calidad, no cumplen los requisitos oportunos en términos de precisión o solidez, o no se diseñan y prueba debidamente antes de introducirlos en el mercado o ponerlos en servicio, pueden "señalar a personas de manera discriminatoria,

incorrecta o injusta" y, según hemos visto podrían "impedir el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva (…) así como los derechos de la defensa y la presunción de inocencia, sobre todo cuando dichos sistemas de IA no sean lo suficientemente transparentes y explicables ni estén bien documentados" (considerando 38 de la propuesta de Reglamento).

Cuando eso ocurre, es decir, cuando pueden llegar a pervertir esos derechos fundamentales, a los sistemas de IA utilizados con fines de aplicación de la ley, se les considera de alto riesgo si "su precisión, fiabilidad y transparencia son especialmente importantes para evitar consecuencias adversas, conservar la confianza de la población y garantizar la rendición de cuentas y una compensación efectiva". Es por ello que, como hemos visto, se consideran de alto riesgo los sistemas utilizados para evaluaciones de riesgo individuales, para evaluar la fiabilidad de las pruebas o para predecir la comisión o reiteración de un delito, la elaboración de perfiles de personas físicas, … lo cual podría ser perfectamente trasladable a los sistemas de inteligencia artificial de nuestras Haciendas. Sin embargo, en ese mismo considerando 38 de la propuesta de reglamento, se indica expresamente que "no debe considerarse que los sistemas de IA destinados específicamente a que las autoridades fiscales y aduaneras los utilicen en procesos administrativos forman parte de los sistemas de IA de alto riesgo usados por las autoridades encargadas de la aplicación de la ley con el fin de prevenir, detectar, investigar y enjuiciar infracciones penales".

Esta exclusión nos plantea una serie de interrogantes que necesariamente debemos apuntar. Por un lado, más allá de las razones que hayan llevado a la configuración de los sistemas de IA de alto riesgo como aquellos que afectan únicamente a los derechos fundamentales de las personas físicas, excluyendo a aquellos que pudieran afectar al catálogo de derechos que pueden incidir también en las personas jurídicas, lo cierto es que la transgresión de estos derechos, principalmente el derecho a la igualdad, a la no discriminación y a valores como la justicia sustanciados en el derecho a la defensa, a la protección de la intimidad…, como hemos visto, verse también perfectamente afectados por la inteligencia artificial utilizada en el ámbito tributario, lo cual exige que la consideración de los sistemas de alto riesgo se extienda a la IA utilizada por nuestras Haciendas.

El anterior argumento cobra aún más importancia cuando la Administración tributaria hace uso de esa IA para recabar datos sobre conductas que pueden derivar en ilícitos penales. No tiene sentido que una misma inteligencia artificial se considere de alto riesgo cuando analiza supuestos constitutivos de delitos fiscales, pero que le sea proscrita esta consideración cuando analiza supuestos que no llegan al umbral cuantitativo que

determina cuándo una infracción tributaria se convierte en delito. Más aún, como hemos visto, cuando la Administración tributaria utiliza un software ajeno a los desarrollos propios de su organización, cuando se trata de un software comercial, puede darse la paradoja de que en su uso por la Hacienda esté exento de su consideración como sistema de alto riesgo, en tanto que si es utilizado por una empresa privada para los usos propios de su actividad empresarial tenga esa consideración, lo cual, obviamente elude el objetivo último que persigue la clasificación realizada por la propuesta de reglamento y que no es otro que el de la protección de los derechos fundamentales de los ciudadanos en cualquier ámbito.

3. LA NECESARIA RECONSIDERACIÓN DE LA PROTECCIÓN DE LOS OBLIGADOS TRIBUTARIOS DE LA INJERENCIA DE SISTEMAS DE INTELIGENCIA ARTIFICIAL DE ALTO RIESGO EN UN ÁMBITO FISCAL

De lo hasta ahora expuesto podemos colegir que el futuro de las Administraciones tributarias apunta a la utilización masiva de sistemas de inteligencia artificial en todos los procedimientos tributarios, tanto en los que atañen a la función de control del cumplimiento de las obligaciones tributarias como a aquellos que se refieren a las labores de asistencia e información. Nuestras Haciendas (tanto la estatal como las forales) han dado cuenta de las grandes utilidades que proporciona la IA en el desempeño de ambas funciones, incluso en ese "nuevo territorio" que imbrica las mismas en lo que ha venido a denominarse *compliance by design*.

Podemos decir, sin miedo a equivocarnos, que la inteligencia artificial es una realidad en el ámbito tributario, una realidad que se extiende a todas las materias en las que nuestra Administración tributaria despliega sus efectos. Este despliegue se ha realizado sin tener en cuenta el grado de afectación que el uso de esta tecnología implica en derechos fundamentales del obligado tributario como puedan ser su derecho a la intimidad, el derecho a la defensa, el derecho a recibir resoluciones motivadas, o el derecho a no ser discriminados. Se trata, como hemos visto, de una intromisión en la esfera de unos derechos fundamentales que debieran, por sí mismos, permitir la calificación de estos sistemas como de alto riesgo pese a su exclusión expresa en la propuesta de reglamento realizada en la materia por el Parlamento Europeo y el Consejo.

Por ello, debiera ofrecerse a los obligados tributarios afectados por la utilización de este tipo de metodologías las mismas garantías que ofrece la propuesta de reglamento en cuanto a la gobernanza de los datos (esto es, en cuanto a los estándares mínimos de calidad, supervisión de los

datos, sesgos…); a la reserva de humanidad en cuanto a la seguridad y supervisión del sistema, de suerte que en última instancia haya siempre una persona que controle y mitigue los posibles riesgos; deberes de transparencia que obliguen describir las características del funcionamiento del sistema y la identidad y datos del proveedor; su inscripción en una base de datos a nivel europeo; y finalmente, el sometimiento (y superación) a un test de conformidad y la obtención de la certificación correspondiente.

En definitiva, pese a que la utilización de la IA en el ámbito tributario es ya una realidad, debemos, estamos aún a tiempo, ponderar su uso con la necesaria protección de nuestros derechos como contribuyentes y personas. El uso de la inteligencia artificial no se plantea en futuros como los imaginados por Philips K. Dick, está muy presente en nuestro día a día, pero estamos aún a tiempo de que con la regulación adecuada, no se generen los abusos que la utilización de esta tecnología planteaba en sus distopías.

V. BIBLIOGRAFÍA

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

DE LA CUEVA GONZÁLEZ-COTERA, J., "Código fuente, algoritmos y fuentes del Derecho", *El Notario del Siglo XXI*, N.° 77, enero/febrero 2018, pp. 36-39.

DORADO FERRER, X. "Redes sociales, metadatos y derecho a la intimidad en los procedimientos tributarios", *Quincena Fiscal*, N.° 12, 2021, pp. 91-103.

FERNÁNDEZ LÓPEZ, R.I., "La autorización judicial para la entrada y registro en el domicilio constitucionalmente protegido del obligado tributario", en MERINO JARA, I. (Dir.) *Prevención y Fraude, nuevas medidas tributarias. Adaptado a la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal*, La Ley, Las Rozas, 2021, pp. 219-254.

GONZÁLEZ DE FRUTOS, Ubaldo "Inteligencia Artificial y Administración Tributaria" en SERRANO ANTÓN, Fernando, *Fiscalidad e inteligencia artificial: Administración Tributaria y contribuyentes en la era digital*, Thomson Reuters Aranzadi, Cizur Menor, 2020, pp. 135-166.

HALL, Claire, "Challenging Automated Decision-making by Public Bodies: Selected Case Studies from other jurisdictions", *Judicial Review*, N.° 1, 2020, pp. 8-20.

HASSAN, S. y DE FILIPPI, P. "The Expansion of Algorithmic Governance: From Code is Law to Law is Code", *Journal of Field Actions*, N.° 17, 2018, pp. 88-90, disponible en https://journals.openedition.org/factsreports/4518.

NADAL SÁNCHEZ, H., DE LA CUEVA GONZÁLEZ-COTERA, J., "Redefiniendo la isegoría: open data ciudadanos", en CERRILLO I MARTÍNEZ, A., PEGUERA, M., PEÑA-LÓPEZ, I., PIFARRÉ DE MONER, M. J., VILASAU SOLANA, M. (coords.), *Retos y oportunidades del entretenimiento en línea. Actas del VIII Congreso Internacional, Internet, Derecho y Política*, Universitat Oberta de Catalunya, Barcelona 9-10 julio, 2012, UOC-Huygens Editorial, Barcelona, pp. 283-300. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/15121/6/IDP_2012.pdf.

OCDE, *Tax Compliance by Design: Achieving Improved SME Tax Compliance by Adopting a System Perspective*, OECD Publishing, 2014. Disponible en: http://dx.doi.org/10.1787/9789264223219-en.

OLIVARES OLIVARES, B. "Transparencia y aplicaciones informáticas en la Administración Tributaria", Crónica Tributaria, N.° 174, 2020, pp. 89-112.

PÉREZ TENA, J.R. "La lucha contra el software de doble uso en la Ley General Tributaria: un ensayo de infracciones tributarias permanentes", *Estudios financieros. Revista de contabilidad y tributación: Comentarios, casos prácticos*, N.° 463, 2021, pp. 5-46.

ROMERO FLOR, Luis M.ª, "Deberes Tributarios Vs Derechos Humanos: El Derecho a No Autoinculparse en el Procedimiento Tributario", *Papeles el Tiempo de los Derechos*, n.° 5, 2014, p. 5.

SERRANO ANTÓN, F. "La Inteligencia artificial y administración tributaria. Especial referencia al procedimiento de inspección tributaria" en SERRANO ANTÓN, F. (Dir.) *Inteligencia artificial y Administración tributaria: eficiencia administrativa y defensa de los derechos de los contribuyentes*, Thomson Reuters Aranzadi, Cizur Menor, 2021, pp. 149-189.

YEUNG, K. y LODGE, M., *Algorithmic regulation*, Oxford University Press, Oxford, 2019.

Inteligencia artificial y proceso judicial

Rocío Zafra Espinosa de los Monteros

Profesora Titular de Derecho Procesal
Universidad Carlos III de Madrid
Instituto de Justicia y Litigación "Alonso Martínez"
Orcid: 0000-0001-7422-1103

I. INTRODUCCIÓN

Nuestra sociedad se caracteriza por tener un alto nivel de litigiosidad. Parece que se judicializan las relaciones sociales lo que provoca que los ciudadanos, en el momento en el que entienden que se les ha limitado de algún derecho que tienen, ya sea por parte de particulares ya por la Administración, buscan el apoyo del Estado, personalizado en los órganos judiciales, para que le den una respuesta que pueda solucionar el conflicto que surge tras el choque de pretensiones.

Así, el proceso judicial, es el instrumento que el Estado nos ofrece para poder ventilar aquellos asuntos relacionado con la tutela de nuestros derechos. En un primer momento, todos los conflictos debían ser solucionados

a través de la jurisdicción. Con el paso de los años, se fueron incorporando a los diferentes ámbitos jurisdiccionales, fórmulas que permitían la resolución de los conflictos otorgando un papel protagonista de las partes. De esta forma, desde las instituciones públicas, se fomentaron el auge de estas herramientas que favorecerían la descongestión de los juzgados y tribunales.

El espectro de estos mecanismos "alternativos o complementarios" dependiendo del ámbito en el que nos encontremos (es decir, dependiendo de la disponibilidad o no de los derechos objeto de conflicto) sigue en auge. Es más, debemos fomentar su utilización dejando a los órganos judiciales como la excepción para la solución de las controversias.

De la misma forma, las nuevas tecnologías han favorecido las relaciones, nos han aligerado las cargas diarias[1] y, por eso, debe favorecerse, el uso de las nuevas tecnologías para mejorar la buena marcha de la administración de justicia. En este sentido, debemos dar paso a la irrupción en el escenario judicial de la justicia la inteligencia artificial.

Ya son algunas las experiencias sobre el tratamiento masivo de información que pueden utilizarse para el desempeño de la función jurisdiccional por los operadores jurídicos. Es por ello, que hay que dar un paso más y ver las posibilidades que se puedan ofrecer para la buena marcha de la administración de justicia. Sin embargo, aquellas herramientas para venir a sustituir al juez personal, parece que tienen un menos encaje en el sistema.

En este sentido, no debemos perder de vista que la sociedad reclama una justicia más ágil y más humana. Este tipo de programas, puede ayudar a lo uno, le dotará de rapidez y agilidad, pero no a lo otro, al menos, tal y como debe entenderse[2].

En las siguientes páginas, me gustaría plantear el escenario en el que se desarrollará la IA y su posible engranaje con el sistema de garantías que asiste y rodea a la actividad jurisdiccional en su concepción más amplia. Para ello, comenzaremos por analizar, sucintamente, el concepto de inteligencia artificial. En segundo lugar, reflexionaré sobre su encaje en

1. En palabras de BARONA VILAR, *Todo ello enlaza a la perfección con la Cuarta Revolución Industrial, que está cambiando la forma de vivir, de trabajar y de relacionarnos los unos con los otros, y todo ello bajo el principio de la instantaneidad, de alta velocidad, masiva, transformadora social, que altera los soportes y principios esenciales que permitieron la construcción de la sociedad moderna.* En BARONA VILAR, S., "Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema?" en *Rev. Boliv. de Derecho* N. 28, julio 2019.
2. Señala SAN MIGUEL CASO: e*n términos de eficiencia, deberemos analizar la relación existente entre los recursos y los resultados, pues el término alude a una cuestión puramente economicista, encontrándonos, en este sentido, ante una justicia eficiente si se obtienen unos resultados proporcionales a los recursos que la sociedad pone a su disposición.* En "La aplicación de la Inteligencia Artificial en el proceso: un nuevo reto para las garantías procesales?", en *Ius Et Scientia*, 2021, Vol. 7, N. 1.

el proceso con todas las garantías para, finalmente, tratar algunas de las posibles aplicaciones en el ámbito de la justicia.

II. APROXIMACIÓN AL CONCEPTO DE INTELIGENCIA ARTIFICIAL

La inteligencia artificial supone el tratamiento de datos de forma masiva con la finalidad de imitar a la mente humana. Las ventajas que aporta la inteligencia artificial parten de lograr superar, las capacidades cognitivas, a partir del tratamiento masivo de datos en pocos segundos, teniendo cabida en cada vez más actividades humanas.

El Parlamento Europeo, en su página web oficial, contiene una entrada en la que se refiere a la Inteligencia Artificial como "*la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear*"[3].

Este concepto general puede llevarse a cabo de dos formas diferentes: por un lado, mediante la tramitación y búsqueda de datos; y por el otro, facilitar la actividad mental del ser humano[4]. En este sentido, hay veces que la facultad de algunos buscadores para autocompletar la idea que buscamos nos facilita, por supuesto la búsqueda, ganando tiempo en cada una de las que hacemos al día. De igual forma, nos abren las puertas a otros pensamientos que ni siquiera se nos había pasado por la cabeza y que nos hacen reflexionar sobre determinadas cuestiones. En definitiva, son muchas las posibilidades que nos ofrece la inteligencia artificial en el día a día, de lo que quizá no somos conscientes, pero que pueden ayudarnos tanto en las actividades más cotidianas como en nuestra parcela profesional, pero parece que todas cuentan con un denominador común: existe un convierte a la Inteligencia Artificial *en una combinación de tecnologías que agrupa datos, algoritmos y capacidad informática*[5].

En la era en la que vivimos y nos relacionamos, vamos dejando una serie de rastros en forma de datos. Estos datos transformados en números o algoritmos son los que enriquecen los sistemas para que una vez analizados, sean capaces de responder e imitar el comportamiento humano. En cada una de nuestras compras, conversaciones, movimientos o visitas a determinadas páginas web, vamos dejando estos rastros que engrosan los datos y, por ende, las posibilidades de actuación. Son muchos los sectores

3. Disponible en: https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa.
4. NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial,* Marcial Pons, Madrid, p. 20.
5. Libro Blanco sobre inteligencia artificial. un enfoque europeo orientado a la excelencia y la confianza. *Los avances en computación y la creciente disponibilidad de datos son, por tanto, un motor fundamental en el pronunciado crecimiento actual de la inteligencia artificial.*

donde la IA ha ayudado: salud, transporte, ciberseguridad: mejorando el uso de estos servicios mediante el análisis y comparación de los datos que recibe continuamente[6]. Nuestra vida cotidiana, está cargada de ejemplos de uso de la Big Data y la infiltración policial. Las aplicaciones que utilizamos para la búsqueda de información en Internet, las cookies que nos obligan a aceptar si queremos seguir navegando en determinadas páginas, las tarjetas de fidelización que utilizamos en algunas de nuestras compras, y como, en alguna ocasión nos bombardean u ofrecen ofertas acordes con nuestras preferencias de búsqueda o compras, son algunos de los ejemplos.

Teniendo en cuenta esta amplia y vaga concepción, cabe preguntarse qué posibilidades tiene de poder ser aplicada al proceso judicial. Lo cierto, es que la utilización de la primera de las utilidades es bastante usada por los estudiosos del derecho tanto por la academia como en la praxis judicial. Así, la búsqueda jurisprudencial, y la utilización de otras herramientas más predictivas. Igualmente, la adaptación de la actividad investigadora a la nueva realidad social y delictual.

En definitiva, la justicia debe modernizarse en mayúsculas, debe conseguir la digitalización de las tramitaciones y, sobre todo, la interconectividad entre todos los operadores y circunstancias de los hechos acaecidos, con pleno respeto del sistema de garantías, ayudaría sin duda, a evitar errores sustanciales[7].

III. COMO PUEDE AYUDAR LA INTELIGENCIA ARTIFICIAL A LA ADMINISTRACIÓN DE JUSTICIA

El Derecho siempre ha estado revestido y caracterizado por la solemnidad y lo tradicional. No obstante, hay que advertir que la aplicación de las nuevas tecnologías al mundo jurídico, ha supuesto, como en todas las facetas de las relaciones, un adelanto que supone la modernidad y agilidad de la justicia. El mundo jurídico, por tanto, no puede escapar a los beneficios aportados por la utilización de las nuevas tecnologías.

Mucho se habla de lo que la inteligencia artificial puede ayudar a la aplicación del derecho. No obstante, es necesario que analicemos cómo la aplicación de las nuevas tecnologías puede incidir en el derecho fundamental al proceso debido.

6. *Vid.* https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa.

7. Esto conllevaría, no solo rapidez en la respuesta judicial sino la evitación de errores como el que se produjo en el caso de Mari Luz, la niña que fue asesinada por Santiago del Valle. En el momento del asesinato, Del Valle debía haber entrado en prisión para el cumplimiento de una pena de 21 años por abusos infantiles.

Por el 2011, emitían en la Televisión, una serie que parecía traída del futuro, "*Person of Interest*" o vigilados, como se emitió en la parrilla televisiva. En ella, se relataba como, tras los atentados del 11-S, los EE. UU. de América, había instalado cámaras de seguridad para el seguimiento de las personas que se movían por las calles, en cumplimiento, quizá del *Patriot Act*. Al parecer, una organización sin ánimo de lucro, utilizaba las cámaras para captar imágenes de personas que, sometidas a un programa informático, era capaz de determinar si eran víctima o delincuente. Si estaba en "predisposición" de cometer un delito o de ser la víctima del mismo. Desde el instante en que se determinaba, una persona de la organización impedía que el delito se llevara a cabo. Esto que, por aquel entonces, parecía ciencia ficción, aunque en el fondo, sabiendo que podía ser verdad, es una realidad palpable en la actualidad presente.

En el seno de la inteligencia artificial, aplicada al proceso, cualquiera que sea su orden jurisdiccional, aunque fundamentalmente puede preocupar la aplicada al proceso penal por la incidencia en los derechos fundamentales, debemos distinguir dos tipos de "modalidades": por un lado, aquello que se viene utilizando, por décadas, que son los programas de búsqueda automática a través de la recopilación de datos y de la coincidencia con los parámetros utilizados, que sin duda, ayudan y agilizan la labor de los operadores jurídicos. Y por otro, la labor "predicitiva" de las decisiones judiciales que puede que asuste un poco más y que desarrollaré posteriormente.

Así, COMPAS, Correctional Offender Management Profiling for Alternative Sanctions, el software que, a través del análisis de determinados algoritmos formados por parámetros basado en el historial de la persona a la que se le somete, una encuesta contestada por la misma, así como otros ítems que poco o nada tienen que ver con la realidad delictual individualizada, calculaba el grado o probabilidad de reincidencia de una persona acusada[8]. El resultado, era considerado por determinados jueces para sostener las penas impuestas a determinadas personas. Este programa se venía utilizando en el Estado de Wisconsin y ha sido sometido a la Corte Suprema de los EE. UU. de América por entender que pueda atentar contra los derechos fundamentales. La cuestión de la utilización de este programa radica, como establece PÉREZ ESTADA, en la opacidad de las redes neuronales que, no permiten su conocimiento trasparente y la rápida evolución del mismo sistema que pueden chocar frontalmente con el derecho de defensa[9].

8. *Vid.* https://www.xataka.com/legislacion-y-derechos/este-algoritmo-sugiere-a-los-jueces-de-EE. UU.-que-condenas-imponer-pero-su-codigo-es-un-secreto.
9. PÉREZ ESTRADA, M. J., "El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías", en BARONA VILAR, S (Editora)., *Claves de la justicia penal,* Tirant lo Blanch, Valencia, 2020, p. 238.

Así, una cuestión fundamental sobre el funcionamiento de este programa, utiliza parámetros que, como se advirtió con anterioridad, pueden no identificar indicadores que revelen la responsabilidad penal individualizada, ya que, el fabricante, puede introducir un sesgo basado en la raza, sexo, edad o nivel sociocultural, entre otros aspectos, de difícil motivación de una condena privativa de libertad y que puede tener difícil encaje con el sistema de derechos fundamentales.

1. ¿POSIBLE AFECTACIÓN DEL DERECHO AL PROCESO DEBIDO DE LA INTELIGENCIA ARTIFICIAL?

El derecho al proceso debido, es un derecho fundamental recogido en el artículo 24.2 de la CE. Igualmente, el artículo 6 del Convenio Europeo de Derecho Humanos, lo regula en su artículo 6. Junto con el derecho a la tutela judicial efectiva o acceso a los tribunales referido en el párrafo 1 del mismo precepto de la CE, y el derecho de defensa constituyen el sistema de garantías fundamentales estrictamente procesales[10]. Como derecho fundamental, su desarrollo debe realizarse mediante Ley Orgánica y goza de la protección reforzada del amparo constitucional. Sin embargo, hay que tener en cuenta que, como señala ESPARZA LEÍBAR, no tiene una tutela judicial específica por sí mismo ante el Tribunal Constitucional, sino que por la limitación de algún o algunos de los derechos que conforman su contenido esencial. En este sentido, el proceso debido es aquel que permite que la tutela dispensada por los jueces y tribunales, sea efectiva[11].

En cuanto al contenido esencial se ha manifestado que se conforma por una serie de derechos de rango constitucionales que responda a una realidad dinámica desde el acceso a los tribunales hasta la consecución de una resolución firme. De este modo, se señala que conforman el derecho a un proceso debido: la prohibición a la indefensión; el derecho de defensa, el derecho a utilizar todos los medios de prueba pertinentes; el derecho al juez legal predeterminado por ley; derecho de publicidad del proceso; el principio de igualdad de armas; la presunción de inocencia; el derecho a un proceso sin dilaciones indebidas; el derecho a la tutela judicial efectiva y el derecho a un proceso con todas las garantías[12]. Igualmente, y dentro de este último, deberíamos incluir el derecho a la imparcialidad judicial[13].

10. Esto es, en palabras de GÓMEZ COLOMER, derechos fundamentales de las partes procesales. En "Prueba admisible y Prueba Prohibida: Cambios en el garantismo judicial motivados Por la lucha Contra el Crimen organizado en la realidad jurisprudencial española actual", en *Doctrina y Jurisprudencia Penal*, núm. 22, 2015.
11. ESPARZA LÉIBAR, I., *El principio del proceso debido,* JM Bosch, Barcelona, 1995, p. 166.
12. ESPARZA LÉIBAR, I., *El principio… op. cit.*, p. 243.
13. DÍEZ-PICAZO GIMÉNEZ. I., "Artículo 24. Garantías procesales", Comentarios a la Constitución Española de 1978, Tomo III, Artículos 24 a 38 de la Constitución

Teniendo en cuenta el contenido dinámico del derecho fundamental del debido proceso, se ha de advertir que la aplicación de las técnicas de inteligencia artificial puede ayudar a la consecución de alguno de ellos, pero puede chocar con la plena aplicación de otros. Es evidente que no se puede generalizar en cuanto a la afectación o no del debido proceso con el uso de la inteligencia artificial. Debemos estar a la práctica utilizada para poder determinar si su utilización puede enfrentar los derechos fundamentales.

De esta forma, si consideramos que la Inteligencia artificial es una técnica que permite el análisis de miles de datos en un tiempo mínimo y es capaz de analizar todas las posibles variantes existentes en unos pocos minutos[14], es evidente que el proceso judicial se agilizaría lo que permitiría que la tutela jurisdiccional se dispensara sin dilaciones indebidas. Otro tipo de análisis mediante algoritmos inteligentes o de aprendizaje son más cuestionados puesto que son capaces de reorganizarse y de dar una nueva respuesta, pero sin explicación, además de la posibilidad de introducir determinados sesgos relacionados con la edad, ideología, raza, religión, etc. Esta falta de transparencia podría contradecir los postulados del proceso debido e ir en contra de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

La cuestión principal que suscita el tema es el tipo de utilidad que la justicia de a la inteligencia artificial. De este modo y teniendo en cuenta que cualquier actuación por los poderes públicos debe ir precedida por el principio de igualdad, la utilización de inteligencia artificial, puede ser una herramienta óptima. Así, ante casos iguales o con pautas parecidas, la respuesta judicial será la misma. El problema es que no se tendrán en cuenta las circunstancias personales que rodean el caso salvo que se introduzca un coeficiente corrector que permita su atención. No obstante, debo plantear que tengo ciertas dudas sobre la posibilidad de que la inteligencia artificial pueda ser utilizada para la resolución de casos y que esto no suponga una

Española. Disponible en https://app.vlex.com/#WW/vid/331146: *La inclusión de la garantía de la imparcialidad judicial en el derecho a un proceso con todas las garantías se basa igualmente en el reconocimiento en el artículo 6.1 CEDH del derecho de toda persona a que su causa sea oída "por un Tribunal independiente e imparcial", lo que, a la luz del artículo 10.2 CEDH, conduce a incorporar dicho derecho a nuestra Constitución*.

14. El análisis de lo que se denomina algoritmos a través de las técnicas de la Inteligencia artificial, lo explica claramente PÉREZ ESTRADA: *El algoritmo utiliza una gran base de datos ordenados de manera comprensible (Smart data), que un modelo matemático va utilizando de manera aleatoria hasta establecer patrones de correlación entre ellos lo que permite a la herramienta realizar apreciaciones con exactitud*. "El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías" … *op. cit.*, p. 239.

posible limitación del proceso con todas las garantías teniendo en cuenta el alcance sobre la imparcialidad del juez o el derecho de defensa.

En mi opinión, creo que depende de la actividad judicial en la que se utilice el análisis de los algoritmos para poder entender si esta afecta al proceso debido. De este modo, si pretendemos ir a un sistema digital absoluto, en el que podemos provocar un obstáculo para determinadas personas, de acceder a la justicia, claramente, entiendo que nuestro sistema constitucional no lo soportaría. De la misma forma, aquellas aplicaciones utilizadas para el análisis de las micro-expresiones faciales con la intención de determinar si en la toma de declaración, el investigado o acusado, está mintiendo. A este respecto debemos recordad que el derecho de defensa atribuye al investigado acusado una serie de derechos instrumentales y la no obligación de no colaborar con la Administración de Justicia sin que en ningún caso esta circunstancia pueda producir un empeoramiento en su situación. Así, esta aplicación, claramente vulnera el derecho de defensa y sus derechos instrumentales como el derecho a guardar silencio o el derecho a no confesarse culpable. Es cierto que las micro-expresiones faciales, son consideradas como parte del lenguaje no verbal y que este ha sido considerado por el TS como una parte a tener en cuenta para dotar de credibilidad a las declaraciones. Pero lo cierto es que: en primer lugar, el criterio jurisprudencial debe cambiar puesto que el lenguaje no verbal, puede ser controlado por determinadas personas o nos puede revelar algo diferente al mensaje que quiere lanzar; y tenemos que considerar que el análisis de esas micro-expresiones está realizado en el contexto de la declaración, para, fundamentalmente, los testigos[15]. Además, es necesario no perder de vista que el análisis de las microexpresiones a través de aplicaciones de inteligencia artificial, supone el análisis de datos o instrucciones suministradas por un desarrollador que puede, de alguna manera, introducir sesgos relativos a la edad, nacionalidad, religión, ideología o cualquier otro que pueda afectar a la determinación de la veracidad o credibilidad sin fundamento[16].

En cambio, tengo la firme creencia de que la utilización del análisis de datos para la adopción de medidas cautelares conlleva enormes beneficios para la consecución de la finalidad del proceso y, por ende, de la tutela judicial efectiva. Igualmente, en caso de la investigación de determinadas conductas delictivas la inteligencia artificial, puede ser una

15. NIETO GARCÍA, AJ., "El principio de inmediación, el lenguaje no verbal y gestual y las microexpresiones faciales", en *Diario La Ley*, 2 de septiembre de 2019.
16. DE MIGUEL BERIAIN, I; PÉREZ ESTRADA, M. J., "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados", en *Revista de Derecho UNED*, núm. 25, 2019.

medida adecuada siempre que se la actuación policía y judicial se encuentre en la zona de equilibrio entre los derechos fundamental de la persona investigada y la finalidad de la investigación. La búsqueda y captura de personas, todas las personas dejamos rastros a través del uso de las nuevas tecnologías, algunas veces, sin saberlo o sin quererlo. El seguimiento de estos rastros digitales y el análisis de las coordenadas de localización, pueden ayudar a la persecución de la finalidad del proceso.

En lo que respecta al proceso penal es de corte garantista, pero estas deben rodear no solo la actividad dirigida a enervar la presunción de inocencia, esto es, dirigida a la actuación contra el acusado, sino que estas garantías deben rodear la salvaguarda de la víctima. En este sentido, la inteligencia artificial puede resultar de mucha ayuda en tanto que su uso podría evitar o aligerar los efectos de la revictimización. Mediante el uso de videoconferencias en las que se evitaría el encuentro entre víctima/agresor; la grabación de las declaraciones de la víctima de modo que no sea necesario repetir su declaración, son herramientas que podrían asegurar una mejora en el estado de las víctimas de los delitos.

IV. POSIBLE APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA APLICACIÓN PRÁCTICA

Qué duda cabe que son innumerables las ventajas que la IA puede reportar al mundo jurídico. Algunas de ellas, ya están siendo utilizadas por los operadores jurídicos[17]; y otras están en desarrollo y mejora[18, 19].

17. GUZMÁN FLUJA, V. C., "Sobre la aplicación de la inteligencia artificial a la solución de conflictos (Reflexiones acerca de una transformación tan apasionante como compleja)", en BARONA VILAR, S., *Justicia civil y penal en la era global,* Tirant lo Blanch, Valencia, 2017. Hace referencia al uso de las TIC's: *las notificaciones telemáticas o la presentación de escritos y documentos igualmente telemática (es decir, el sistema Lexnet), y otras están despertando ese interés, como el expediente judicial electrónico, debemos intensificar nuestra atención sobre otros temas e instituciones que integran la implantación de la administración de justicia electrónica: la sede electrónica.*

18. En este sentido, los programas informáticos que permiten la solución de determinadas controversias; la determinación de la reincidencia para la imposición de la pena; gafas de identificación de sospechosos, etc. Así programas como Jurimetría, Legal data, COMPAS, las gafas biométricas…que permiten al usuario, en este caso, a Administración de Justicia o los operadores, tener soluciones o predicciones sobre el proceso judicial en el que están inmersos. *Vid.* BARONA VILAR, S., "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", en *Revista Jurídica Digital UANDES* 3/1 (2019).

19. A este respecto, *Vid.* BUENO DE MATA, F., "Big Data judicial e inteligencia artificial: próximos desafíos del derecho procesal en la sociedad de la información", en FONTESTAD PORTALES, L (Dir.)., *La globalización del Derecho Procesal,* Tirant lo Blanch, Valencia, 2020.

En las siguientes líneas, se quiere dar un repaso a aquellas manifestaciones de Inteligencia artificial que ya encuentran su lugar dentro, fundamentalmente, del proceso penal, analizando las cuestiones más controvertidas. Igualmente, debe entenderse que el uso de estas nuevas tecnologías, así como el análisis de los datos, no es de carácter tasado y que, con la rapidez que se avanza en este campo, seguramente, estas palabras se queden obsoletas enseguida.

Partiré de la posible aplicación de la inteligencia artificial en el marco de la investigación de las conductas delictivas y seguiré con la posibilidad de aplicarla en el ámbito de la protección integral de las mujeres víctimas de violencia de género.

Ni qué decir tiene que los operadores jurídicos deben ser formados para el análisis de la cantidad ingente de datos que conlleva el buen uso de la inteligencia artificial. Como pone de manifiesto LLORENTE, la inteligencia artificial se nutre de los datos que ofrecen las nuevas tecnologías y viceversa. De modo que la combinación y análisis de los algoritmos es lo que nos dará la pauta[20]. Y somos los propios usuarios de las nuevas tecnologías, que, por poco, somos la mayoría de los humanos, los que proporcionamos los datos para engordar las pautas. Es decir, el registro de nuestros movimientos, ya sea en el ámbito privado o en lo público[21], es lo que recopilan los datos que se quedan almacenados y que, mediante las técnicas de inteligencia artificial, nos dará los resultados de la combinación. Para la realización del análisis de todas estas combinaciones y análisis de datos es necesario que el operador esté preparado puesto que, en caso contrario, saldrá un resultado en forma de galimatías de difícil aplicación práctica.

---

20. LLORENTE SÁNCHEZ-ARJONA, M., "Big Data, Inteligencia Artificial y Violencia de Género", en *Diario La Ley*, núm. 49 de 26 de marzo de 2021: *Por tanto, la Inteligencia Artificial (4) se nutre de los datos procesados y aprende de ellos, creando y reconociendo patrones, así como desarrollando soluciones sofisticadas de anal tica para todo tipo de sectores. ¡Son sistemas que se complementan por lo que, de la misma manera que el Big Data es necesario para la Inteligencia Artificial, pasa en idéntico sentido a la inversa; ingentes cantidades de datos carecerán de valor sin los modelos de Inteligencia Artificial y, a su vez, la Inteligencia Artificial necesita de datos para nutrirse de contenido y construir su inteligencia.*

21. BUENO DE MATA, F., "Big Data judicial e inteligencia artificial: próximos desafíos del derecho procesal en la sociedad de la información" … *op. cit*. Es más, el artículo 8 de la Ley orgánica en relación con el artículo 9 del Reglamento (UE) 2016/679, señala que será posible el tratamiento de los datos más íntimos, es decir, aquellos relacionados con *el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física*, cuando los tribunales actúen en el ejercicio de su función judicial.

Para finalizar, un tema que es de especial interés es la naturaleza jurídica de estos datos o del resultado de su análisis. Es decir, si el resultado del análisis podrá ser considerado una prueba científica en el proceso penal español. El concepto de prueba científica no está exento de polémica doctrinal[22]. La cuestión que se suscita a este respecto es que la prueba científica, está dando algo, por cierto, con un índice de error muy pequeño. Sin embargo, el resultado del análisis de los datos a través de inteligencia artificial, resulta algo más complicado en tanto dependerá de las combinaciones de los algoritmos. En este sentido, será necesario, ante el desconocimiento de la mayoría de los operadores jurídicos, de la visión de los expertos en la materia. Por ende, podrán ser considerados en el proceso penal, en el acto de juicio oral, siempre que el informe vaya acompañado de la declaración pericial que arroje ese conocimiento científico que se necesita para la interpretación del análisis de los datos.

1. APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA PERSECUCIÓN DE LOS DELITOS

Como se ha venido diciendo, las redes, las nuevas tecnologías y el mundo de las comunicaciones, ha supuesto la facilitación de la vida personal y de las relaciones sociales. No obstante, el uso de las nuevas tecnologías ha supuesto un grave incremento en las conductas delictivas cometidas en la red. Así, según el Observatorio Español de delitos informáticos, en 2019, se produjeron, alrededor de, 21.8302 delitos informáticos.

Es cierto que la capacidad de trasmisión de información a través de las nuevas tecnologías, así como lo avances tan rápidos que en esta esfera se suceden, hacen que el Derecho, se vea, en ocasiones, obsoleto y que las técnicas de investigación sean insuficientes para la investigación, prevención y represión de estas conductas delictivas.

Sin embargo, lo cierto es que la inteligencia artificial que se desarrolla a través de las nuevas tecnologías, puede resultar muy útil para estos fines cuando se comete un delito informático, entendido este como aquel que se comete a través de la red o mediante la utilización de las nuevas

22. Señala, acertadamente GÓMEZ COLOMER: *La mente humana se dirige inmediatamente cuando se habla de prueba científica a pensar en hechos que necesitan de conocimientos profesionales muy actualizados y exigentes basados en las ciencias más modernas, sobre todo, médicas e informáticas, utilizando en su ejecución medios tecnológicamente muy avanzados, para que puedan ser probados. Esto es indiscutible y se explica claramente.* En "La prueba científica, motor de cambios esenciales en el proceso penal moderno". Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=http%3A%2F%2Fperso.unifr.ch%2Fderechopenal%2Fassets%2Ffiles%2Farticulos%2Fa_20170408_01.pdf&clen=546639&chunk=true.

tecnologías. Debemos tener en cuenta que como pone de manifiesto ANGUITA OSUNA sobre l*a dificultad reside en el funcionamiento de los sistemas informáticos y en la estructura de Internet, ya que se trata de una estructura mundial con canales digitales que dificultan el control fronterizo, se favorece el alto nivel de opacidad de las conexiones y el anonimato de los internautas, y de momento existe una generalizada libertad normativa y lagunas legales.* Teniendo en cuenta esta circunstancia se hacía necesaria la reforma de la LECrim en aras de la adaptación de la acción investigadora a esa nueva realidad.

Y a este respecto, en el año 2015, se reforma la LECrim mediante la Ley orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. En esta ley, se recogen, entre otras cosas, una serie de diligencias de investigación, denominadas, diligencias de investigación tecnológicas. Esta reforma, pretende asumir el cambio de paradigma en las sociedades modernas y adaptar la acción investigadora a la nueva realidad social y delictual, esto es, la ciberdelincuencia.

El legislador, ha puesto en manos de los operadores jurídicos determinadas herramientas para poder hacer frente a este tipo de criminalidad. Y ante el panorama de la delincuencia actual, que, bajo el amparo del anonimato, parecen ser impunes, los poderes públicos, deben hacer uso de todas las facultades que la LECrim les proporciona para hacer frente a este tipo de criminalidad. Todas las relaciones, transacciones y gen general, todos los movimientos que se realizan a través de la Red dejan un rastro, el tratamiento y análisis de los mismos puede ser fundamental para el descubrimiento e investigación de determinadas conductas delictivas.

Ni que decir tiene que todas las actuaciones, ya se realicen en el plano físico o en el plano virtual, deben ser respetuosas con el sistema de garantías que ampara tanto nuestra Norma Suprema, como los Convenios y tratados internacionales en los que España es parte. Sobre este aspecto, la LECrim, es bastante escrupulosa con el respeto de los principios de idoneidad, especialidad, necesidad y proporcionalidad en sentido estricto debiendo ser utilizadas estas técnicas en el marco de un proceso penal en marcha, y siempre que exista una adecuación cuantitativa y cualitativa entre el fin perseguido y el derecho fundamental en juego.

Tal es el cambio de paradigma que la Jurisprudencia del Tribunal Supremo, ha acuñado un nuevo derecho fundamental que debe ser protegido en este tipo de actuaciones: el derecho al entorno virtual. Y es que las relaciones han cambiado, el modo de vivir y de exposición pública, de renuncia a la intimidad personal, ha cambiado y por tanto los ámbitos

de protección deben acomodarse ante él. En este sentido, en 2018, se promulga la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En cuanto a la adecuación entre la finalidad perseguida y la actuación que se vaya a desarrollar, es necesario partir de la insuficiencia de las tradicionales técnicas de investigación para hacer frente a esta criminalidad informática. Si pensamos en una investigación sobre pornografía infantil en la red, de poco o nada nos puede servir la entrada y registro domiciliario si ello no va seguido de un registro de los dispositivos masivos de información y, sobre todo, de los equipos desde los que se desarrollaba el delito. Es evidente que el ejemplo propuesto puede ser extremo, pero pensemos en un delito de acoso o amenazas a través de la red. En ocasiones, las víctimas de estos delitos, denuncian ante las FSCE, pero, ante la imposibilidad de encontrar al presunto autor de los hechos, no son tramitadas[23].

Así, ante este escenario, y ante el auge de las conductas delictivas a través de las nuevas tecnologías, debe reclamarse un mayor compromiso para que ninguna de estas conductas quede sin respuesta y que las nuevas tecnologías supongan un paraíso jurídico penal en el que delinquir con impunidad.

La LECrim, *permite que cualquier delito que sea cometido a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación,* pueda ser investigado por las diligencias de investigación de carácter tecnológico, claro está, respetando el principio de proporcionalidad atendiendo a las circunstancias del caso concreto.

Centrándonos en las posibilidades que ofrece la inteligencia artificial y el análisis de los datos para la investigación penal, debe comenzarse por la identificación de los presuntos responsables de los hechos delictivos. Una de las técnicas de identificación es la lofoscopia[24], más particularmente, la dactiloscopia que es la ciencia de individualizar a las personas vivas o muertas por medio del estudio de las cretas papilares existentes en las yemas de los dedos de las manos. con la finalidad de identificar a la persona que presuntamente ha cometido el hecho delictivo o identificación de cadáveres. Así, en el momento en que la Policía Judicial realiza la Inspección técnico ocular (ITO) recogerá todas aquellas huellas, vestigios o elementos que puedan esclarecer los hechos. La importancia

23. Ante estas situaciones, nos encontramos con titulares tales como: *una joven de 20 años se quita la vida tras denunciar hasta en 4 ocasiones que sufría ciberacoso*, el pasado 3 de enero de 2022. https://www.antena3.com/noticias/sociedad/joven-20-anos-suicida-despues-denunciar-cuatro-veces-que-sufria-ciberacoso_2022010361d329a220b19a00012fe3e1.html.

24. IGLESIAS GARCÍA, M. J., "La lofoscopia como medio de investigación", en *Revista Aranzadi de Derecho y Proceso Penal*, núm. 45/2017.

de esta técnica de identificación es fundamental puesto que las huellas dactilares cuentan con una serie de características tales como: la inmutabilidad; la individualidad y la perennidad. Esta ciencia, fue objeto de estudio científico por primera vez por GALTON que ideó un método para la clasificación de las huellas dactilares y, en 1891, de inició el Registro dactiloscópico. Las primeras identificaciones se realizaban a mano, comparando los pulpejos dactilares de la muestra dubitada (la recogida en la escena del crimen) con el que se tenía en el registro dactiloscópico (muestra indubitada). Actualmente, contamos con el Sistema Automatizado de Identificación Dactilar (SAID). Este sistema, en el que se encuentran las huellas dactilares de todas las personas que han sido detenidas es capaz de identificar la existencia de coincidencia entre la huella que se investiga con las almacenadas en el sistema. La automatización de este tipo de identificaciones, no hace más que aligerar la investigación criminal y agilizar el proceso judicial. El uso de la inteligencia artificial y el análisis de los datos resulta imprescindible para este análisis. En este campo, los datos son incorporados desde el registro de detenidos, es decir, desde un canal cerrado, no puede entrar ningún otro dato, pero la prontitud y fiabilidad del cotejo, son insuperables. Por supuesto, garantiza la fiabilidad del cotejo que podrá ser sometido a contradicción en el juicio oral. No obstante, existen discrepancias en cuanto a la naturaleza documental o pericial de la prueba dactiloscópica. Así la STS de 28 de enero de 1999 establece: *la contradicción jurisprudencial entre pericia y documento debe superarse, si se tiene en cuenta la equivalencia con la pericia, atiende más bien a la especialización de los funcionarios encargados de la búsqueda del correspondiente dactilograma, poniendo el acento en las características, tipos, crestas y dibujos papilares. Se trata en realidad de un documento y equivale a una certificación para acreditar que tal fotografía papilar corresponde a tal persona, ello no empece a que precise de determinados conocimientos técnicos que para llegar a tal resultado tengan que analizar las características de la huella dactiloscópica*[25].

Por otro lado, y como ya se ha comentado, nos encontramos con las novedades de las diligencias de carácter tecnológicos, incorporadas a la acción investigadora en el 2015 por el gran crecimiento de este tipo de criminalidad. Entre ellas, cabe destacar la actuación de los agentes encubiertos informáticos y el registro remoto de dispositivos electrónicos. Como se adelantó, ambas medidas comprometen el pleno ejercicio de los derechos fundamentales de las personas investigadas[26]. Es por ello, que deben de

25. SÁNCHEZ RUBIO, A., *La prueba científica en la justicia penal,* Tirant lo Blanch, Valencia, 2019.

26. LAPUERTA IRIGOYEN, C., "El cibercrimen y el agente encubierto on line", en https://ficp.es/wp-content/uploads/2017/06/Lapuerta-Irigoyen.-Comunicaci%C3%B3n.

desarrollarse bajo la estricta observancia del principio de proporcionalidad y bajo el escrupuloso control de la autoridad judicial.

En cuanto a la actuación del agente encubierto virtual, y a lo que se refiere el objeto de esta investigación, se le podrá facultar para el análisis los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos, conforme al tenor literal del apartado 6 del artículo 282 bis. Qué duda cabe que el análisis de estos datos puede arrojarnos luz a la investigación en cuanto a la localización, identificación del usuario o partes de la investigación. Además, todos los datos recabados de la investigación pueden ser incorporados a un banco de datos que permita la comparación de pautas en otras investigaciones en curso.

Al hilo de las operaciones encubiertas virtuales, y en consonancia con la inteligencia artificial, más allá del análisis de los datos, hay que traer a colación la uso que pueden darse a ordenadores robotizados que pueden ser usados por las fuerzas de represión penal para que, actuando como agentes encubiertos, puedan investigar determinadas conductas delictivas cometidas a través de la red. En este sentido, en 2014, se impone la primera condena a un pederasta que actuaba bajo el anonimato de las redes y que fue descubierto por un robot humanoide. Así, esta "niña" mantenía conversaciones con las personas investigadas a las que le enviaban o reclamaban videos de contenido sexual[27]. La cuestión principal de este concreto supuesto es la investigación en manos de particulares. La LECrim, a este respecto, habilita para que los agentes de policía judicial puedan actuar como agentes encubiertos virtuales sin abrir la puerta a la actuación de otras instituciones privadas o particulares. Por otro lado, la solicitud al órgano judicial para la adopción de estas medidas de investigación, deben recoger los elementos, indicios y delitos que deben ser perseguido con esta medida. Es una medida sometida a la reserva jurisdiccional puesto que se entiende ocasiona perjuicio en la esfera de los derechos fundamentales. El auto que resuelva la concesión de la autorización, por supuesto, deberá cuestionar la proporcionalidad de la medida al fin perseguido. En el supuesto comentado, Sweetie que así se hacía llamar la niña robot, entró en determinados canales cerrados no para investigar a alguien en concreto o una actividad delictual concreta, sino para

pdf, pone de manifiesto que la utilización irregular de las nuevas tecnologías, que puede provocar la limitación del pleno ejercicio de los derechos y libertades de la sociedad, necesita de la articulación de soluciones coordinadas y que resulten eficaces en la acción policial y judicial y, sobre todo, que respeten los principios y valores que informan el Estado de Derecho.

27. *Vid.* https://www.europapress.es/portaltic/portalgeek/noticia-nina-virtual-fue-clave-condenar-pedofilo-20141023131318.html.

investigar los movimientos en estos lugares y poder detectar a las personas que cometían estas acciones delictivas. La utilización indiscriminada de estas técnicas de investigación, en manos de particulares, pueden provocar el desuso de las mismas poniendo en jaque la actividad lícita de las Fuerzas y Cuerpos de Seguridad del Estado. No obstante, en manos de los poderes públicos, sería una herramienta de gran potencial para la investigación de delitos cometidos a través de la red y siempre que esté vigilada por los agentes de policía y cumpliendo con todas los requisitos y presupuestos previstos en la LECrim.

En cuanto al uso de registros remotos de dispositivos electrónicos, el uso de la inteligencia artificial, en modo de software resulta imprescindible. Mediante la entrada en el dispositivo de la persona investigada, previa autorización judicial, las autoridades de represión penal obtendrán información de este y sobre el dispositivo investigado. Es una de las medidas más agresiva con el sistema de garantías, lo que requiere que la duración sea breve y la estricta observancia del principio de proporcionalidad tanto en el momento de la autorización como durante el desarrollo de la medida.

Por último, me gustaría centrar mi atención en una medida de investigación que puede ayudar, sobre todo, a la prevención de determinadas conductas delictivas, sin perjuicio de arrojar datos para la investigación del delito: la utilización de drones. El Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea, establece ciertos aspectos sobre la utilización de los drones por parte de la Policía en sus labores de seguimiento y filmación. Esta regulación en conjunción con lo previsto en la LECrim, y teniendo en cuenta el carácter abierto de las medidas de investigación tecnológicas, la utilización de los drones, puede resultar imprescindible para captación de la imagen, de seguimiento y de localización en tanto que el artículo 588 quinquies a, refiere la posibilidad de llevar a cabo estas funciones por medido de cualquier dispositivo técnico. La captación de estas imágenes, deben ser considerados prueba electrónica[28].

28. A este respecto, debemos tener en cuenta el concepto de prueba electrónica dada por BUENO DE MATA: *"aquel medio electrónico que permite acreditar hechos relevantes para el proceso, ya sean hechos físicos o incluso electrónicos, y que se compone de dos elementos necesarios para su existencia, los cuales determinan la especialidad de la prueba electrónica en relación al resto de medios probatorios: un elemento técnico que hará referencia bien a*

En definitiva, no solo se deben tener en cuenta los resultados que estas técnicas de investigación pueden arrojar para el caso concreto, sino en la ingente cantidad de datos que pueden obtenerse en las investigaciones y que alimentan las bases de datos mediante la utilización de técnicas de Big Data. Así, mediante técnicas de inteligencia artificial podrán lograrse patrones que podrán responder a otras conductas criminales similares. De este modo, el punto de partida de la investigación no tendría que ser desde cero, sino que podría ser desde el modelo arrojado mediante la combinación y análisis de los algoritmos[29]. Lo que podría conllevar a predecir las posibles actividades investigadoras que puedan dar un mejor resultado para el caso concreto. Es más, en algunos supuestos en los que la investigación está estancada por falta de fuentes de prueba y no se logra el esclarecimiento de hechos, la comparación de patrones, nos podrían dar un resultado fructífero. Por supuesto, todo ello bajo la supervisión de los mandos policiales y bajo el estricto control del encargado de la investigación del delito. Ahora bien, no quiero decir que no sea necesaria la investigación, porque cada una de ellas tiene o puede tener unas características singulares, pero el poder conocer, de manera inmediata los resultados de la investigación de delitos de similares características, podría resultar de gran ayuda, sin contar con la evitación, que, en ocasiones, podría tener con respecto a la revictimización de la víctima del delito.

---

un hardware en sede judicial o bien a un canal electrónico cuando se presente mediante un sistema de gestión procesal informatizado, y un elemento lógico o software que tendrá naturaleza intangible. La prueba electrónica se presentará a través de, o bien un soporte electrónico si lo llevamos como una pieza de convicción ante el juzgador en sede judicial o bien un canal electrónico concreto articulado por un sistema técnico como LexNet o similar, que incluirá un contenido elaborado acorde a unos parámetros dados por programa informático determinado". BUENO DE MATA, F., "Propuestas y retos en torno a la prueba electrónica a tenor de las últimas reformas procesales", *Revista de Derecho y Privacidad,* n.º 4, 2016, p. 4. Sobre el tema particular de la utilización de dornas con fines de investigación. *Vid.* BUENO DE MATA, F., "La utilización de drones como diligencia de investigación tecnológica: consecuencias probatorias", en *Diario La Ley,* núm. 16, de 20 de marzo de 2018. Sobre la importancia de la utilización de los drones para garantizar la seguridad, el Plan Estratégico Nacional para el desarrollo del sector civil de los drones en España 2018-2021, estima que se estima que en 2035 se dedicarán a este tipo de servicios un total de 9.000 drones, 5.800 drones de policía y 3.200 drones de bomberos, disminuyendo esta cifra en 2050 hasta los 8.700, 5.600, 3.100 y respectivamente. Disponible en https://www.mitma.gob.es/el-ministerio/planes-estrategicos/drones-espania-2018-2021.

29. Debemos recordar que el Anteproyecto de Ley de Enjuiciamiento Criminal presentado a finales de 2020, prevé como diligencia de investigación la posibilidad de que el Juez de Garantías autorice la utilización de sistemas automatizados o inteligentes de tratamiento de datos para cruzar e interrelacionar la información disponible sobre la persona investigada con otros datos obrantes en otras bases de titularidad pública o privada, siempre que concurran.

2. APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL PARA EL TRATAMIENTO DE LOS CASOS DE VIOLENCIA DE GÉNERO

Uno de los problemas coyunturales en la sociedad actual, herencia de las culturas patriarcales, es el incesante crecimiento de la violencia de género en nuestro país. Cada vez son más las mujeres que sufren este tipo de violencia invisible para los demás, pero especialmente grave y delicada para ellas, su desarrollo y para los que la rodean, especialmente, los hijos menores de edad. Esta violencia, en cualquiera de sus modalidades, a menudo viene acompañada con la conocida como violencia vicaria. Esta es aquella que hace en la que se utilizan a los hijos para crear daño y sufrimiento a la madre y víctima de violencia de género.

Es cierto, que, en los últimos años, estamos escuchando voces que apuntan a un concepto de violencia de género más flexible, en el que se introduzcan otras mujeres víctimas, no solo a manos de las que son o han sido sus parejas sino toda aquella violencia contra las mujeres por el único fundamento de serlo y ello, conforme al Convenio de Estambul.

Sea cual sea el concepto de violencia de género que acuñemos, es necesario que el Estado dispense una protección a las mujeres víctimas de forma inmediata porque el agresor no espera plazos y en muchas ocasiones, la falta de celeridad por las Administraciones públicas, nos lleva a lamentar un desenlace fatal de estas víctimas.

Es evidente que el primer paso para salir de este tipo de situaciones, lo tiene que dar la víctima de la situación. Este tipo de violencia, normalmente, se produce en un ambiente privado, lejos de las miradas de terceras personas o familiares. La víctima, llega a normalizar la situación y vive en ella hasta que decide ponerle fin. En este sentido, nos encontramos, lamentablemente, con noticias en las que se recoge la agresión a personas que intentan protegerlas. Y es que, a pesar de que todos debemos luchar contra este tipo de violencia, son las Administraciones Públicas y sus agentes los que deben dispensar esta protección.

La protección que debe ser otorgada a la víctima debe ser integral. Esto implica que la mujer y, por ende, sus hijos, si los tuviera, se sientan protegidos en todas las facetas de su vida sin que haya obstáculo alguno al desarrollo de la personalidad.

La incorporación de la Ley orgánica 1/2004, de protección integral de las víctimas de violencia de género, diseñó el sistema de protección integral a este tipo de víctimas: sanitario, social, laboral, penal y procesal. Desde el punto de vista procesal, cuando la víctima de violencia de género, se le deben dispensar todas las medidas de protección que garanticen la plenitud de los derechos que le asisten.

Sin embargo, a pesar de las medidas adoptadas, parece que la justicia penal no es suficiente o más bien, eficiente. Está claro que la falta de recursos humanos especializados en la materia, resulta imprescindible para lograr el fin perseguido. Qué duda cabe que la dotación de más personal a las instituciones públicas, permitiría una mejor limitación o acotamiento del problema.

Se debe avanzar en la idea de la inmediatez que nos requieren las sociedades modernas, precisamente por el uso abusivo o no de las nuevas tecnologías. Esta inmediatez, puede ser lo que se necesita para dispensar la protección de que la víctima de violencia de género requiere en el momento en que quiere salir del ciclo de la violencia en el que se encuentra. Hay veces que la lentitud y solemnidad del proceso penal, asusta a las víctimas más vulnerables de la violencia de género. Ello unido a la situación de desequilibrio y baja autoestima en la que se encuentra, provoca que nos encontremos con situaciones en las que el agresor no puede ser condenado por falta de pruebas o simplemente, la víctima decide arrojarse en manos del agresor ante la sensación de abandono que siente de las autoridades públicas.

2.1. Valoración del riesgo

Cuando una víctima de violencia de género decide dar el paso y salir de la situación, puede resultar habitual que la persona del agresor intente que esto no pase. Pueden hacerlo de una forma pacífica o no. En estos supuestos, es necesario realizar una valoración del riesgo para determinar la necesidad de imponer una medida cautelar que pueda servir de protección a la víctima, más concretamente la orden de protección que prevé la LECrim para estos casos.

No hay un procedimiento específico para la violencia de género[30]. No obstante, si se ha querido dispensar a la víctima de una protección "integral" frente a los agresores por los delitos cometidos. De este modo, podrá solicitarse, tanto a las FCSE, instituciones públicas o directamente al órgano judicial una orden de protección, circunscrita a la violencia doméstica y prevista en el art. 544 ter. LECrim que concederá el órgano judicial competente (Juez de Violencia sobre la mujer; Juez de Instrucción o Juzgado de Guardia). Esta, se podrá adoptar en cualquier momento del procedimiento siempre que se den los presupuestos establecidos para el

30. GRANDE SEARA, P., "El proceso penal por delitos de violencia de género", en VÁZQUEZ-ORTOMEÑE SEIJAS, F (Dir.)., *Violencia contra la mujer. Manual de Derecho Penal y Procesal penal. Adaptado a la Ley 1/2015, de reforma del Código Penal,* Tirant lo Blanch, Valencia, 2016.

efecto en el apartado 1 del artículo 544 ter. Esto es, cuando existan indicios fundados de la comisión de un delito o falta contra la vida, integridad física o moral, libertad sexual, libertad o seguridad. En definitiva, podrán adoptarse cualquiera de las medidas establecidas en la LECrim para otorgar beneficios sociales y jurídicos a las víctimas. En este sentido, se podrá adoptar medidas tendentes a: la prohibición de acercamiento, la obligación por parte del agresor de abandonar el domicilio familiar o prohibición de comunicación entre agresor y víctima. Igualmente, y conforme al artículo 544 bis LECrim, se podrán adoptar medidas tendentes a prohibir al agresor acudir a determinados lugares o acercarse a la persona de la víctima, así como a sus familiares teniendo en cuenta tanto la situación de peligro existente como la situación socioeconómica y sanitaria del presunto agresor.

Por las particularidades propias que presenta, estas medidas y la orden de protección no son adoptadas de forma automática, sino que debe existir un peligro real para la víctima. Así, el CGPJ, muestra que, en 2020, fueron solicitadas 35.860 órdenes de protección, inadmitidas 242; aceptadas, 35.289; y, denegadas, 10.329. Del total de las solicitadas, 6.764, lo fueron ante el Juzgado de Guardia, de las que 5182, fueron aceptadas y 1582, denegadas[31].

El órgano judicial competente podrá, en caso de que se reúnan los requisitos y presupuestos establecidos en la LECrim, adoptar la orden de protección. Para la valoración del riesgo para resolver sobre la orden de protección, utilizan el sistema VioGen[32].

En consonancia con los derechos que, el Estatuto de la víctima confiere a esta, establece el artículo 544 ter. 9) que la adopción de la orden de protección, además confiere a la víctima el derecho a estar informada, permanentemente, sobre la situación procesal del investigado o encausado,

31. https://www.poderjudicial.es/cgpj/es/Temas/Estadistica-Judicial/Estadistica-portemas/Datos-penales--civiles-y-laborales/Violencia-domestica-y-Violencia-degenero/Datos-sobre-Violencia-sobre-la-mujer-en-la-estadistica-del-CGPJ/.

32. Entre los objetivos de VioGen se encuentran: aglutinar a las diferentes instituciones públicas que tienen competencias en materia de violencia de género; integrar toda la información de interés que se estime necesaria; hacer predicción del riesgo; atendiendo al nivel de riesgo, realizar seguimiento y protección a las víctimas en todo el territorio nacional; efectuar una labor preventiva, emitiendo avisos, alertas y alarmas, a través del "Subsistema de Notificaciones Automatizadas", cuando se detecte alguna incidencia o acontecimiento que pueda poner en peligro la integridad de la víctima. http://www.interior.gob.es/web/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen. Conforme a las estadísticas presentadas por la Delegación del Gobierno contra la violencia de género, adscrita al Ministerio de Igualdad, se señalan que, en 2021, existen 62.984 casos, de los que 32.603 necesitan protección policial.

así como sobre el alcance y vigencia de las medidas cautelares adoptadas. En particular, la víctima será informada en todo momento de la situación penitenciaria del presunto agresor. A estos efectos se dará cuenta de la orden de protección a la Administración penitenciaria.

Como se ha mencionado, la concesión de la orden de protección no se hace de forma automática, ya que el riesgo que corre la víctima debe ser valorado. Sin embargo, son varios los aspectos que giran en torno a este tema: por un lado, la víctima es una persona vulnerable tanto física como emocionalmente lo que puede provocar un riesgo añadido a su persona; y por otro la peligrosidad del agresor. En este sentido, podemos encontrarnos con situaciones que lleven a consecuencias graves por la lentitud con que estas órdenes de protección son concedidas.

De este modo, sería interesante el control o valoración del riesgo de forma automatizada bajo determinados parámetros que confluyan en el supuesto concreto que violencia de género. Así, la combinación de algoritmos en la que introducimos todos los presupuestos concurrentes del caso concreto unido a las instrucciones o datos suministrados desde la casuística existente puede orientar, en poco tiempo, al órgano judicial sobre la necesidad o no de conceder esta orden de protección, cuanto menos, valorar de forma inmediata el riesgo y arrojar de forma automática dicho instrumento de protección[33]. En definitiva, como pone de manifiesto LLORENTE SÁNCHEZ-ARJONA: *la aplicación del Big Data, Inteligencia Artificial y Registros biométricos pueden contribuir en la lucha contra este tipo de violencia, si bien VioGen es susceptible de mejora*[34].

2.2. El uso de la videoconferencia

Otro de los mecanismos que pueden ser utilizados en el ámbito del proceso penal y que están íntimamente relacionados con la inteligencia artificial, es el uso de videollamadas o videoconferencias a través de las aplicaciones que nos proporcionan las nuevas tecnologías.

33. En este sentido, se pronuncia NIEVA FENOLL: *Una vez la denuncia ya consta en el sistema y por tanto esté almacenado el testimonio de que se trate, incluso con la ayuda interactiva de la propia App, se trata de localizar al sospechoso, y una vez contactado, acreditada indiciariamente su responsabilidad –para lo cual también puede ayudar la inteligencia artificial–, se formula acusación de forma automática y se procede a realizar sobre el reo una prognosis de riesgo que arrojar un perfil de personalidad que ayudar al sistema a movilizarse más rápido, lo que puede ser muy útil en supuestos de violencia de género, por ejemplo, pero también de hurtos, sin ir más lejos.* En "El tránsito de la fe a la tecnología en el proceso penal", en *Diario La Ley*, núm. 9986, de 11 de enero de 2022.
34. LLORENTE SÁNCHEZ-ARJONA, M., "Big Data, Inteligencia Artificial y Violencia de Género" … *op. cit.*

Incoado el proceso penal, se debe proceder a realizar la investigación de los hechos. El órgano judicial, deberá tomar declaración a la víctima con el fin de ratificar la denuncia, evitando la revictimización. La investigación en los casos de violencia de género, tal y como afirma el TC, deben llevar a cabo un canon reforzado que *se entenderá debidamente colmado en tanto en cuanto, subsistiendo la sospecha fundada de delito se practiquen otras diligencias de investigación que, complementando esos testimonios enfrentados de las partes unidas por una relación de afectividad, presente o pasada, permitan ahondar en los hechos descartando o confirmando aquella sospecha inicial". De ahí que, "el deber de diligencia requerirá abundar en la investigación allí donde no se hayan agotado las posibilidades razonables de indagación sobre los hechos de apariencia delictiva, vulnerándose el derecho a la tutela judicial efectiva si el órgano judicial clausura precipitada o inmotivadamente la investigación penal"*[35].

Desde que la víctima formula denuncia o querella contra el presunto agresor, se le reconoce el derecho de asistencia jurídica gratuita con independencia de sus recursos económicos[36]. La víctima podrá personarse como acusación particular en cualquier momento del proceso.

Una de las primeras actuaciones es la toma de declaración de la víctima y del agresor. En todo momento, se garantizará que víctima y victimario no coincida en el momento de prestar declaración[37]. Qué duda cabe, que, en este tipo de delitos, es imprescindible evitar la revictimización por la vulnerabilidad en la que se encuentra la víctima. Es por ello, por lo que puede resultar imprescindible para el curso del proceso, que la víctima preste declaración mediante el uso de videoconferencias. En este sentido, el Tribunal Supremo se ha pronunciado a favor de este tipo de prácticas, indicando que no es una posibilidad discrecional del juez o tribunal, *sino que medio exigible ante el Tribunal y constitucionalmente digno de protección* en tanto que da cumplimiento a los principios de inmediación, contradicción y publicidad[38]. Así, en consonancia con el artículo 230.2 LOPJ[39], *el uso de*

35. STC 87/2020, de 20 de julio.

36. En caso de que se dicte sentencia absolutoria o sobreseimiento libre, la víctima no tendrá que abonar el coste que ha supuesto ser beneficiaria del derecho a la asistencia jurídica gratuita.

37. En este sentido, el Anteproyecto de Ley de medidas de eficiencia procesal del servicio público de justicia, dispone que se añada el artículo 137 bis que establece: *Las víctimas de violencia de género, violencia sexual, trata de seres humanos, y víctimas menores de edad o con discapacidad podrán intervenir desde los lugares donde se encuentren recibiendo oficialmente asistencia, atención, asesoramiento y protección, o desde cualquier otro lugar si así lo estima oportuno el juez, siempre que dispongan de medios suficientes para asegurar su identidad y las adecuadas condiciones de la intervención conforme a lo que se determine reglamentariamente.*

38. STS 331/2019, de 27 de junio.

39. Que establece: *Los juzgados y tribunales y las fiscalías están obligados a utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para*

la videoconferencia permite la total conexión en los puntos de origen y destino como si estuvieran presentes en el mismo lugar, con lo que se da cumplimiento a la premisa de que se celebre la actuación judicial en unidad de acto. No se vulnera ningún principio procesal al poder dirigir las partes a los testigos las preguntas que sean declaradas pertinentes con contradicción y sin que pueda existir indefensión ni vulneración de la tutela judicial efectiva.

En definitiva, atendiendo a las circunstancias del caso concreto y, en el caso violencia de género, se aconseja la medida, se podrá prestar declaración utilizando los medios tecnológicos necesarios y oportunos. En el caso d la violencia de género, asegurar la protección de la víctima y evitar la revictimización, creo que son motivos suficientemente fundados para hacer uso de estos mecanismos.

2.3. Delincuencia informática en el ámbito de la violencia de género

Se ha puesto de relieve con anterioridad el incremento de determinadas conductas a través de las redes o mediante el uso de las nuevas tecnologías. En este sentido, no podemos olvidar prestar atención a las conductas delictivas, sobre todo, las que tienen que ver con amenazas o violencia psíquica, y que son perpetradas a través del as nuevas tecnologías. El agresor, se ampara en la red para atemorizar a la mujer[40]. En ocasiones, actúa bajo el anonimato por lo que podía resultar más problemática su identificación. En este sentido, las nuevas diligencias tecnológicas, han permitido la investigación de estos delitos cometidos a través de los medios tecnológicos con un mayor éxito en la persecución. Pero donde debemos poner la atención es en el crecimiento de este tipo de conductas, sobre todo, en personas jóvenes donde la violencia de género, es muy creciente.

Habitualmente, se considera que los delitos cometidos a través de la red, se protegen bajo en anonimato que les garantiza la red. En el caso de

---

el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establecen el capítulo I bis de este título y la normativa orgánica de protección de datos personales.

40. En este sentido: el acoso al que se somete a la mujer víctima de violencia de género en la red, suelen ser conductas tales como *falsas acusaciones, vigilancia, amenazas, robo de identidad, daños al equipo de la víctima o a la información que en él contiene, uso de la información robada para acosar a la víctima, mensajes acusatorios o vejatorios, etc. También podemos englobar en este terreno el sexting. Se trata del envío de material privado por parte de personas, normalmente jóvenes, a través del teléfono móvil o de Internet en el que se muestran fotografías o videos de conocidos, amigos o parejas de carácter erótico y de índole privada.* En *El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento* realizado por Delegación del Gobierno para la Violencia de Género, 2014.

la violencia de género, las conductas son cometidas a través de perfiles falsos, pero en gran parte de las ocasiones se conoce el autor de las mismas: el que es o ha sido pareja de la víctima.

En este sentido, y teniendo en cuenta la gravedad de estos delitos que pueden ser la antesala de una agresión física. Además, el padecimiento de estas conductas puede, sin duda, acarrear un peligro en la mujer de grandes magnitudes pues sienten que la amenaza sigue latente en cualquier momento, eliminando, si se puede más, su dignidad como persona y como mujer.

Así, debemos considerar que las medidas de carácter tecnológicos dispuestas en la LECrim, son perfectamente legítimas para la investigación de determinadas conductas. La utilización de dispositivos de seguimiento, así como de registro de dispositivos masivos, la interceptación de las comunicaciones, resulta imprescindible para frenar este tipo de criminalidad. Por supuesto, todos los datos que se arrojen de estas investigaciones, deben ser puesto a disposición de las bases de datos para que entren a formar parte del acervo que compone el Big Data[41] con la finalidad que pueda servir como patrón de conducta que pueda replicarse en otros casos. Sin duda, esto supondría una mejora notable de la justicia penal en el tema de la violencia de género.

V. A MODO DE CONCLUSIÓN: ALGUNAS CUESTIONES CRÍTICAS

Como refiere BUENO DE MATA, la incorporación de *las nuevas tecnologías en el proceso de una forma cautelosa y comedida, debido a la posible pérdida de derechos para los administrados y la merma de principios y garantías procesales*[42]. Hemos estudiado las posibles implicaciones que el uso de la inteligencia artificial y el *Big Data,* puede tener en el derecho a un proceso con todas las garantías. Igualmente, nos planteamos la posibilidad de que se pierda más en la humanización de la justicia. No obstante, y aunque esto supone una crítica a este nuevo sistema, no podemos perder la noción de la igualdad que debe presidir cualquier actuación de los poderes públicos y que, en mi opinión, puede asegurarse con la aplicación de las nuevas tecnologías y el uso de la inteligencia artificial en la justicia. La contrapartida a esta idea que parte de la igualdad, y, es por ello que

41. Por supuesto, todos estos datos que entren a formar parte de la Base de datos, en aras a la protección de datos de carácter personal, deberán omitir todas aquellas informaciones relacionadas con la filiación, identificación y cualquier otro dato susceptible de formar un sesgo que invalide el resultado.

42. BUENO DE MATA, F., *op. cit.*

debemos entenderlo como crítica al nuevo sistema de e-justicia, es la brecha digital existente entre las diferentes clases sociales y, sobre todo, en determinados rangos de edad que se ven perdidos ante el mundo virtual. Quizá, resulta ágil la actuación a través de los registros electrónicos y de los dispositivos virtuales, pero, en algunos sectores, puede provocar la vulneración del derecho fundamental a la tutela judicial efectiva en tanto que la nueva realidad virtual le supone un obstáculo para poder acceder a los tribunales.

Es evidente el beneficio que la inteligencia artificial reportará a la seguridad jurídica, puesto que ante determinadas circunstancias, la adopción de las actuaciones, será idéntica a través del análisis de las variables. Sin embargo, como consecuencia a estos sistemas, nos encontramos ante la despersonalización de la actuación judicial que no se atenderá a las circunstancias del caso concreto puesto que no sería posible la introducción de tantas variables como posibilidades pudieran existir. No obstante, no podemos perder de vista que, en cualquier caso, y ante la posibilidad de que las actuaciones puedan suponer la limitación de derechos fundamentales, todas las medidas adoptadas, hayan sido o no predecidlas de forma automatizada, deben obedecer al principio de proporcionalidad.

Quiero poner de manifiesto una cuestión que me resulta preocupante y problemática a la vez: esta se refiere a la seguridad de los servidores y bases de datos que nutren a los algoritmos y las aplicaciones de inteligencia artificial. Aunque es cierto que existen algunos programas de ciberseguridad que pretenden defenderse ante determinados comportamientos de ataque, no lo es menos que los más sofisticados sistemas de seguridad virtual de grandes organismos tanto públicos como privados, pueden ser sometidos. Así, cabe preguntarse si estaríamos preparados para esquivar ciertos ataques a la seguridad que podrían poner en jaque a la Administración de Justicia. Esto supondría una gran catástrofe en caso de que estos sistemas fueran hackeados. Creo que la magnitud de los datos personales, confidenciales y la posible destrucción de elementos esenciales para la toma de decisiones, supone un grave perjuicio para que la inteligencia artificial pueda apoderarse de la justicia.

Por último y me gustaría situar el acento a la importancia de la interconectividad de los sistemas. Actualmente, parece que el sistema de Ventanilla única no está muy perfeccionado y las Administraciones Públicas, no son capaces de cruzar datos que permitirían agilizar todas las tramitaciones. Ello, se debe a una falta de unificación de los programas y aplicaciones utilizadas en cada una de las instituciones públicas y de diferente rango territorial. Esto dificulta los patrones de búsqueda y por tanto la operatividad práctica. Así, se cree necesario que todas las Administraciones

deban utilizar los mismos software, que permitiera el compartir datos y la posibilidad de búsquedas menos encasilladas. De la misma forma, la aplicación de la inteligencia artificial, hace necesaria la formación de los operadores jurídicos.

VI. BIBLIOGRAFÍA

AAVV, *El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento* realizado por Delegación del Gobierno para la Violencia de Género, 2014.

BARONA VILAR, S., "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", en Revista Jurídica Digital UANDES 3/1 (2019).

– "Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema?", en *Rev. Boliv. de Derecho* N. 28, julio 2019.

BUENO DE MATA, F., "Big Data judicial e inteligencia artificial: próximos desafíos del derecho procesal en la sociedad de la información", en FONTESTAD PORTALES, L (Dir.)., *La globalización del Derecho Procesal,* Tirant lo Blanch, Valencia, 2020.

– "La utilización de drones como diligencia de investigación tecnológica: consecuencias probatorias", en *Diario La Ley,* núm. 16, de 20 de marzo de 2018.

– "Propuestas y retos en torno a la prueba electrónica a tenor de las últimas reformas procesales", *Revista de Derecho y Privacidad,* n.o 4, 2016.

DE MIGUEL BERIAIN, I; PÉREZ ESTRADA, M. J., "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados", en *Revista de Derecho UNED,* núm. 25, 2019.

DÍEZ-PICAZO GIMÉNEZ. I., "Artículo 24. Garantías procesales", Comentarios a la Constitución Española de 1978, Tomo III, Artículos 24 a 38 de la Constitución Española. Disponible en https://app.vlex.com/#WW/vid/331146.

ESPARZA LEIBAR, I., *El principio del proceso debido,* JM Bosch, Barcelona, 1995, p. 166.

GÓMEZ COLOMER, J. L., "Prueba admisible y Prueba Prohibida: Cambios en el garantismo judicial motivados Por la lucha Contra el Crimen

organizado en la realidad jurisprudencial española actual", en *Doctrina y Jurisprudencia Penal*, núm. 22, 2015.

– "La prueba científica, motor de cambios esenciales en el proceso penal moderno". Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=http%3A%2F%2Fperso.unifr.ch%2Fderechopenal%2Fassets%2Ffiles%2Farticulos%2Fa_20170408_01.pdf&clen=546639&chunk=true.

GRANDE SEARA, P., "El proceso penal por delitos de violencia de género", en VÁZQUEZ-PORTOMEÑE SEIJAS, F (Dir.)., *Violencia contra la mujer. Manual de Derecho Penal y Procesal penal. Adaptado a la Ley 1/2015, de reforma del Código Penal,* Tirant lo Blanch, Valencia, 2016.

GUZMÁN FLUJA, V. C., "Sobre la aplicación de la inteligencia artificial a la solución de conflictos (Reflexiones acerca de una transformación tan apasionante como compleja)", en BARONA VILAR, S., *Justicia civil y penal en la era global,* Tirant lo Blanch, Valencia, 2017.

IGLESIAS GARCÍA, M. J., "La lofoscopia como medio de investigación", en *Revista Aranzadi de Derecho y Proceso Penal*, núm. 45/2017.

LAPUERTA IRIGOYEN, C., "El cibercrimen y el agente encubierto on line, en https://ficp.es/wp-content/uploads/2017/06/Lapuerta-Irigoyen.-Comunicaci%C3%B3n.pdf.

LLORENTE SÁNCHEZ-ARJONA, M., "Big Data, Inteligencia Artificial y Violencia de Género", en *Diario La Ley,* núm. 49 de 26 de marzo de 2021.

NIETO GARCÍA, A. J., "El principio de inmediación, el lenguaje no verbal y gestual y las microexpresiones faciales", en *Diario La Ley,* 2 de septiembre de 2019.

NIEVA FENOLL, J., "El tránsito de la fe a la tecnología en el proceso penal", en *Diario La Ley,* núm. 9986, de 11 de enero de 2022.

– *Inteligencia artificial y proceso judicial,* Marcial Pons, Madrid.

PÉREZ ESTRADA, M. J., "El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías", en BARONA VILAR, S (Editora)., *Claves de la justicia penal,* Tirant lo Blanch, Valencia, 2020.

SAN MIGUEL CASO, C., "La aplicación de la Inteligencia Artificial en el proceso: un nuevo reto para las garantías procesales?", en *Ius Et Scientia*, 2021, Vol. 7, N. 1.

SÁNCHEZ RUBIO, A., *La prueba científica en la justicia penal,* Tirant lo Blanch, Valencia, 2019.

DEBATES PROCESALES

El problema de la falta de transparencia en la interacción de la inteligencia artificial y la justicia

Cristina Alonso Salgado

Profesora Ayudante Doctora de Derecho Procesal
Universidade de Santiago de Compostela

SUMARIO: I. CON CARÁCTER PRELIMINAR. II. INTELIGENCIA ARTIFICIAL Y JUSTICIA: APUNTES ACERCA DEL PROBLEMA DE LA OPACIDAD. III. REFERENCIAS BIBLIOGRÁFICAS.

I. CON CARÁCTER PRELIMINAR

El mundo está cambiando; ha cambiado; de hecho, siempre cambia. En lo que, ojalá, sean los estertores de la pandemia que nos ha golpeado sin avisar, el ritmo en la aceleración del cambio se ha intensificado en algo trasciende lo cuantitativo, para adentrarse en lo cualitativo. No es que el mundo cambie, o que haya cambiado; es que el golpe nos ha cogido desprevenidos y lo que hasta hace apenas unos meses era un escenario de ciencia ficción, absolutamente extravagante y, por ende, ajeno a la dogmática académica, hoy constituye una verdad casi incontestable. Sea por la urgencia de hacer la necesidad virtud, sea porque el golpe de realidad nos ha precipitado –que no empujado– a dejar de negar la evidencia de lo inevitable, lo cierto es que la inteligencia artificial ha irrumpido en el sistema de Justicia, de una manera ciertamente innegable.

Pero, ¿qué debemos entender por "inteligencia artificial"? Delimitarla conceptualmente no es empresa sencilla. No lo es, por la propia naturaleza de lo que se pretende definir –en permanente evolución–, y también porque su diferente relación con respecto a los diversos ámbitos de aplicación hace que el concepto se escore hacia los extremos en función del aspecto que pretenda destacarse, generando así, una multiplicidad de

definiciones[1]. En lo que ahora interesa, adoptaremos la definición del Dictamen del Comité Económico y Social Europeo sobre la "Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad". De conformidad con la misma, "*La IA es un concepto que engloba muchas otras (sub) áreas como la informática cognitiva (cognitive computing: algoritmos capaces de razonamiento y comprensión de nivel superior –humano–), el aprendizaje automático (machine learning: algoritmos capaces de enseñarse a sí mismos tareas), la inteligencia aumentada (augmented intelligence: colaboración entre humanos y máquinas) o la robótica con IA (IA integrada en robots)*"[2].

II. INTELIGENCIA ARTIFICIAL Y JUSTICIA: APUNTES ACERCA DEL PROBLEMA DE LA OPACIDAD

Al hilo de esto último, una vez precisados –*grosso modo*–, los umbrales más generalmente aceptados del concepto, interesa ahora abordar algunos apuntes críticos en relación a la una objeción en absoluto desdeñable: la opacidad de la inteligencia artificial en su interacción con sistema de Justicia pena. La consideración reflexiva deviene, infelizmente, imprescindible. Y ello porque, tendremos ocasión de analizar, la dificultad no es de orden menor.

Como es sabido, algunos de los sistemas más ambiciosos de inteligencia artificial presentan unos niveles de opacidad difícilmente compatibles con los parámetros de nuestro sistema de justicia. Se ha dicho en innumerables ocasiones que algunas de sus formulaciones pueden

1. Desde una perspectiva histórica, *vid.*, "*El concepto de "inteligencia artificial" fue acuñado por John McCarthy, profesor de Matemáticas en Darmouth College (New Hampshire), quien –junto con M. L. Minsky, N. Rochester y C. E. Shannon– propuso en agosto de 1955 la realización de un proyecto de investigación en el que participasen diez destacados científicos de diversas disciplinas para intentar "averiguar cómo hacer que las máquinas utilicen el lenguaje, formen abstracciones y conceptos, resuelvan tipos de problemas hasta ahora solo al alcance de los humanos y mejoren a éstos". La premisa sobre la que se asentaba tan pretensión era la asunción de que, "en principio, cualquier aspecto del aprendizaje o cualquier otro rasgo de la inteligencia puede ser descrito de una manera tan precisa que se puede conseguir que una máquina lo simule". La idea básica era, por tanto, crear máquinas capaces de realizar tareas que requieren una inteligencia humana mediante la imitación o réplica de los procesos del pensamiento*", en SOLAR CAYÓN, J. I., *La Inteligencia Artificial Jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*, Aranzadi, Cizur menor (Aranzadi), 2019, pp. 21-22.
2. Dictamen del Comité Económico y Social Europeo sobre la "Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad", disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52016IE5369&from=E S, [última consulta: 25-09-2021].

desarrollar diversos niveles de autonomía y pueden funcionar de manera independiente.

El problema radica en que estas actuaciones derivadas y sus resultados resultan imprevisibles, en tanto funcionan a modo de *black boxes*[3]. En efecto, son comunes las referencia a los algoritmos de aprendizaje automático como cajas negras. Y aun cuando las causas de la opacidad pueden ser diversas –desde por aspectos jurídicos, hasta por cuestiones de carácter organizativo–, las que mayor preocupación suscitan son aquellas que responden a causas técnicas, precisamente, por ser las que entrañan una mayor complejidad. Una monitorización a vuelapluma permite hacer inteligible lo que se viene de apuntar. Buena parte de los sistemas de inteligencia artificial se fundamentan en unos algoritmos, los de aprendizaje automático que, justamente, se desarrollan con base en el adiestramiento de los datos que le son suministrados para ajustar los logros. La complejidad inherente a este tipo de algoritmos puede acabar por imposibilitar la identificación de los datos considerados en orden a conseguir un determinado resultado[4].

Ni que decir tiene que este tipo de algoritmos cuentan con unos umbrales de eficacia difíciles de despreciar desde una lógica eficientista, toda vez que permiten anticipar comportamientos. Con todo, su "*funcionamiento resulta incomprensible lo que dificulta la legitimidad de las decisiones que adoptan. Estos algoritmos predicen, pero no explican, son capaces de reorganizar sus propias variables (se automatiza su funcionamiento) y, lo más problemático, pueden encontrar relaciones entre el resultado final que se quiere medir* (…) *y datos* (…) *Generan correlaciones entre los datos, no cadenas de causalidad*"[5].

En relación a esto que se viene de señalar, se hace preciso destacar dos consideraciones de interés: por un lado, una con respecto a la rendición de cuentas; y, por el otro, un apunte acerca del aprendizaje automático.

3. MERCHÁN MURILLO, A., "Inteligencia artificial y blockchain: retos jurídicos en paralelo", *Revista General de Derecho Administrativo*, n.° 50, 2019, p. 4.

4. CERRILLO I MARTÍNEZ, A., "El impacto de la inteligencia artificial en las Administraciones públicas: estado de la cuestión y una agenda", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Aranzadi), 2020, p. 83.

5. PÉREZ ESTRADA, M. J., "El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías", en BARONA VILAR, S. (dir.), *Claves de la Justicia penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, Tirant lo Blanch, Valencia, 2019, pp. 238-240.

   Vid. de la misma autora (en régimen de coautoría), DE MIGUEL BERIAIN, Í. y PÉREZ ESTRADA, M. J., "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados", *Revista de Derecho UNED*, n.° 25, 2019, *vid.* pp. 536-539.

En este sentido, en primer lugar, de la opacidad, esto es, de la falta de transparencia se infiere una dificultad no exenta de riesgos: la de garantizar una apropiada rendición de cuentas[6]. Aun cuando no podemos detenernos sobre este extremo, conviene notar que obran ya sobre la mesa, propuestas para tratar de arrojar luz sobre los procesos, con el horizonte de potenciar la transparencia y, por tanto, la *accountability*. Ello no obstante, a decir verdad, "*La completa transparencia, sin embargo, parece difícil de conseguir, si no imposible. La mera revelación de los datos o de los algoritmos no necesariamente logra la transparencia deseada, dada la complejidad de las interacciones que pueden dar lugar a una decisión determinada. Por otra parte, la revelación de los algoritmos puede vulnerar la propiedad intelectual y la confidencialidad de los secretos empresariales de sus titulares y puede ser de escasa utilidad para los usuarios* (…)"[7].

En segundo lugar, el aprendizaje automático tan tecnológicamente abrumador al que *supra* se hacía referencia, no hace sino potenciar y retroalimentar algunas de las objeciones que la literatura especializada[8] ha venido destacando en relación a la inteligencia artificial en su interacción con la Justicia (*lato sensu*). Debe notarse que el referido aprendizaje se articula sobre unos algoritmos que pueden identificar patrones de comportamiento con base en el examen de infinidad de datos. Pueden revelar determinados patrones en un modelo a través de una formulación y emplearlo para efectuar predicciones sobre nuevos datos[9].

Pues bien, esta posibilidad de "auto-aprender" provoca que su capacidad de reacción resulte poco previsible. Y ello porque los comportamientos pueden ser derivaciones de interacciones imprevistas entre los elementos sistémicos o con el ecosistema en el que se desarrollan, cuestiones estas que, simplemente, no son susceptibles de anticipo preventivo alguno. De este modo, estos tipos de sistemas de inteligencia artificial "*están dotados de capacidades de adaptación y de autoaprendizaje que entrañan*

6. PEGUERA POCH, M., "En búsqueda de un marco normativo para la Inteligencia Artificial", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Aranzadi), 2020, p. 46.
7. PEGUERA POCH, M., "En búsqueda de un marco normativo para la Inteligencia Artificial", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial, … op. cit.*, p. 46.
8. BARONA VILAR, S., *Algoritmización del Derecho y de la Justicia: de la inteligencia artificial a la smart justice*, Tirant lo Blanch, Valencia, 2021; ALONSO SALGADO, C., "Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad", *Ius et Scientia*, vol. 7, n.° 1, 2021; etc.
9. SOLAR CAYÓN, J. I., *La inteligencia artificial jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos, …op. cit.*, pp. 26 y ss.

un grado de imprevisibilidad en su comportamiento, ya que pueden aprender de forma autónoma de su propia experiencia variable e interactuar con su entorno de forma impredecible. Son cada vez más autodidacticas. Tienen capacidad para tomar decisiones y aplicarlas en el mundo exterior con independencia de cualquier control o influencia externa"[10].

Así las cosas, estamos ante una arquitectura que permite una permanente sobredimensión que, a la vista de la conocida problemática de los sesgos[11], resulta ciertamente preocupante. Porque, comoquiera que los sesgos pueden estar presentes en los algoritmos, aun cuando se trate de minimizar el impacto de los sesgos de origen en la programación originaria, de la "reproducción celular" que venimos de analizar se colige la dificultad en el propio control de daños[12].

Como es fácil entrever, esta problemática en su interacción con el sistema de Justicia resulta particularmente conflictiva. En palabras de BALCELLS, "(…) *el correcto funcionamiento justo y equitativo del sistema de justicia se ve afectado por sesgos discriminatorios que se proporcionan al algoritmo: de esta forma, un hipotético cálculo actuarial puede estar determinado por estos sesgos y lógicamente colabore en crear nuevos sesgos o perpetuar los ya establecidos*"[13].

Y por si todo ello fuera poco, nuestro análisis acerca de las objeciones, riesgos y dificultades se encuentra condicionado –que no, afortunadamente, determinado– por la complacencia automatizada y el sesgo de la

10. NÚÑEZ ZORRILLA, M. C., *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Reus, Madrid, 2019, pp. 12 y ss.
11. Sobre los sesgos: "*El análisis de LUM e ISAAC (2016) sobre el uso de PredPol para predecir el tráfico de drogas de Oakland entre los años 2009 a 2011 detectó dos problemas importantes de la herramienta de IA que afectaban a la capacidad predictiva de ésta, y que el lector ya se puede imaginar. Por un lado, que los datos iniciales ya estaban sesgados y generaban predicciones que perpetuaban dichos sesgos; por otro lado, que a medida que se generaban nuevas detenciones como consecuencia de las predicciones el algoritmo, estos arrestos eran utilizados como datos proporcionados al algoritmo, generando aun un mayor sesgo. Claramente, el riesgo del algoritmo PredPol es crear un bucle de retroalimentación de datos*", en BALCELLS, M., "Luces y sombras del uso de la inteligencia artificial en el sistema de justicia penal", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Aranzadi), 2020, pp. 154-155.
12. CERRILLO I MARTÍNEZ, A., "El impacto de la inteligencia artificial en las Administraciones públicas: estado de la cuestión y una agenda", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, *…op. cit.*, pp. 82 y ss.
13. BALCELLS, M., "Luces y sombras del uso de la inteligencia artificial en el sistema de justicia penal", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, *…op. cit.*, p. 153.

automatización[14], por la fanatización tecnológica y el poder blanqueante del "*Mathwashing*". En definitiva, de todo cuanto se viene de subrayar, la opacidad supone una objeción en absoluto desdeñable para la incorporación de sistemas fundamentados en inteligencia artificial en el ámbito jurídico: la ausencia de "explicabilidad", la perpetuación y retroalimentación de sesgos discriminatorios y, lo que es peor, su blanqueamiento, entre otros aspectos, implican no pocos riesgos en un ámbito que exige certeza y certidumbre, inteligibilidad y seguridad. Ninguna tentación "eficientista" debiera servir justificar la entrega de garantías y derechos conquistados a lo largo de siglos. Sólo así, desde el frontispicio garantista, se logrará la irrupción –y no la disrupción– tecnológica de la inteligencia artificial en el sistema de Justicia (*lato sensu*).

III. REFERENCIAS BIBLIOGRÁFICAS

ALONSO SALGADO, C., "Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad", *Ius et Scientia*, vol. 7, n.° 1, 2021.

BALCELLS, M., "Luces y sombras del uso de la inteligencia artificial en el sistema de justicia penal", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Aranzadi), 2020.

BARONA VILAR, S., *Algoritmización del Derecho y de la Justicia: de la inteligencia artificial a la smart justice*, Tirant lo Blanch, Valencia, 2021.

CERRILLO I MARTÍNEZ, A., "El impacto de la inteligencia artificial en las Administraciones públicas: estado de la cuestión y una agenda", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Aranzadi), 2020.

DE HEREDIA RUÍZ, I. B., "Automatización y obsolescencia humana", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Aranzadi), 2020.

DE MIGUEL BERIAIN, Í. y PÉREZ ESTRADA, M. J., "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre

14. DE HEREDIA RUIZ, I. B., "Automatización y obsolescencia humana", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Aranzadi), 2020, pp. 119-120.

la base de los derechos fundamentales implicados", *Revista de Derecho UNED*, n.° 25, 2019.

MERCHÁN MURILLO, A., "Inteligencia artificial y blockchain: retos jurídicos en paralelo", *Revista General de Derecho Administrativo*, n.° 50, 2019.

NÚÑEZ ZORRILLA, M. C., *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Reus, 2019.

PEGUERA POCH, M., "En búsqueda de un marco normativo para la Inteligencia Artificial", en CERRILLO I MARTÍNEZ, A. y PEGUERA POCH, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Aranzadi), 2020.

PÉREZ ESTRADA, M. J., "El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías", en BARONA VILAR, S. (dir.), *Claves de la Justicia penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, Tirant lo Blanch, Valencia, 2019.

SOLAR CAYÓN, J. I., *La Inteligencia Artificial Jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*, Aranzadi, Cizur Menor (Aranzadi), 2019.

La utilización de la videoconferencia y la Inteligencia Artificial en el proceso penal[1]

Jaime Criado Enguix

Personal Docente e Investigador FPU
Departamento de Derecho Procesal
Universidad de Granada

SUMARIO: I. ESTADO DE LA CUESTIÓN. II. HERRAMIENTAS TECNOLÓGICAS Y SU UTILIZACIÓN EN EL PROCESO PENAL: ESPECIAL ATENCIÓN AL USO DE LA VIDEOCONFERENCIA Y LA INTELIGENCIA ARTIFICIAL. 1. *Previsión legal de la videoconferencia*. 2. *Ventajas de la utilización de la videoconferencia en el proceso penal*. 3. *¿Puede afectar la digitalización de la justicia a garantías procesales penales?* 3.1. Principio procesal de publicidad. 3.2. Principio procesal de concentración. 3.3. Principio procesal de inmediación judicial. 3.4. Derecho de defensa. 4. *Inteligencia Artificial e incidencia en el panorama judicial*. 4.1. Aplicaciones de la Inteligencia Artificial en el proceso penal. 4.2. Riesgos del uso de la Inteligencia Artificial en el proceso penal. III. CONCLUSIONES. IV. BIBLIOGRAFÍA. *Referencias normativas. Referencias jurisprudenciales.*

1. Este trabajo ha sido realizado en el ámbito de los Proyectos: Acción Jean Monnet, LUDELOR, "Lucha contra la delincuencia organizada. Enfoques normativo, operativo y judicial en la recuperación y gestión de activos derivados del crimen", 2020-2022, con número de referencia 620390-EPP-1-2020-1-ES-EPPJMO-PROJECT; el proyecto con número de referencia A-SEJ-054-UGR-18 del programa operativo FEDER de la Consejería de Economía, Innovación y Ciencia de la Junta de Andalucía (Lucha contra la delincuencia organizada. Enfoques normativo, operativo y judicial en la recuperación y gestión de activos derivados del crimen); y de la Red de Cooperación internacional y de excelencia científica de estudio y análisis "Justicia, Derecho, Constitución y Proceso".

I. ESTADO DE LA CUESTIÓN

Uno de los puntos decisivos que ha provocado un impulso absoluto en la digitalización de la justicia en España ha sido la crisis sanitaria producida por el COVID-19. El incremento de litigiosidad y el colapso de la Administración de Justicia han propiciado que el legislador, bajo el marco del Plan España Digital 2025, a través del RD 16/2020, de 28 de abril, y la posterior Ley 3/2020 ley 3/2020, de 18 de septiembre, impulse medidas procesales y organizativas en el ámbito de la Administración de Justicia para garantizar el desarrollo de los procedimientos judiciales a distancia y evitar así concentraciones en las sedes judiciales. Normativa que, *ex* art. 19 del referido RD 16/2020, de 28 de abril, da cobertura a la realización de determinados actos de juicio, comparecencias, declaraciones, vistas y demás actos procesales por vía telemática. No obstante, esta tendencia hacia la digitalización de la justicia no es ninguna novedad. Por ejemplo, ya 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 apostó por un uso de la tecnología para salvar la distancia geográfica, permitir la interacción en línea, una personación sin representación legal, una reducción de los costes y de la duración del procedimiento.

Más adelante en el tiempo, **con la aparición de estructuras tecnológicas más sofisticadas, aparecen máquinas que se basan en la utilización de algoritmos y datos, que procesan la información y ejecutan una acción previamente programada, lo que se conoce como Inteligencia Artificial o "*machine learning*".** Esto último ha tenido especial incidencia en el ámbito de la administración de la justicia. La primera proyección la encontramos en el Estado de Columbia Británica, en Canadá, con la puesta en marcha en 2016 del *Civil Resolution Tribunal* (CRT). En el Reino Unido en julio de 2016 se propuso la creación de un *Online Solution Court.* En los Estados Unidos, algunos Estados están experimentando con un software denominado *Matterhorn*. El Estado de Nueva York, junto con la *Judicial Division* de la *American Bar Association*, está desarrollando un proyecto piloto de tribunal virtual o en línea también para reclamaciones dinerarias (*New York ODR debt collection pilot*). En Australia, en septiembre de 2018 se implantó, como proyecto piloto, el *Victorian Civil and Administrative Tribunal* (VCAT). En China ya se habla de los jueces robots y los "centros de litigios en línea" (el famoso asistente virtual utilizado en China "*Xiao Fa*"); en Estonia también se está apostando fuerte por la automatización de la justicia: no hay intervención humana en todo el proceso.

Desde Naciones Unidas, cabe destacar los esfuerzos que se han llevado a cabo en el Grupo de Trabajo Tercero de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (en adelante, CNUDMI)

cuyos resultados se han plasmado en las "Notas Técnicas de la CNUDMI sobre la solución de controversias en línea" de 2017[2]. La falta de un consenso suficiente, sin embargo, ha lastrado el resultado final de esta iniciativa. Y en el ámbito regional europeo en 2016 ha comenzado a funcionar la plataforma europea para la resolución de litigios de consumo[3]. Desde la Unión Europea, la *Estrategia 2019-2023 relativa a la Justicia en Red Europea* de 13 de marzo de 2019 indica que la inteligencia artificial es uno de los principales hitos logrados en los últimos años en tecnologías de la información y la comunicación, y que debe seguir desarrollándose en los próximos años, siempre y cuando se tengan en cuenta *los riesgos y desafíos que plantean los cambios futuros y el uso de estas tecnologías, en especial en lo relativo a la protección de datos y a la ética*"[4].

Por otro lado, también forma parte de este proceso de digitalización el uso de la videoconferencia, herramienta tecnológica que posibilita la comunicación de imagen y sonido en tiempo real entre dos puntos distantes, de manera que la distancia física deja de ser un impedimento para la celebración de comparecencias, como si los participantes se encontraran en la misma Sala. Aprovechando la optimización del uso de las plataformas digitales de la comunicación durante el estado de alarma por el coronavirus, y la paralización de la actividad judicial que podría haberse evitado mediante una implementación previa del uso de la videoconferencia en la justicia, conviene analizar si efectivamente esta posibilidad digital es respetuosa con los derechos y garantías procesales del justiciable.

Desde un punto de vista ético, pocos Estados de la Unión Europea han abordado hasta ahora las cuestiones éticas en la construcción de la justicia digital, a excepción de Francia, que desde 2019 cuenta con normas que han establecido restricciones con fundamento ético. El Consejo de Europa ha manifestado la importancia de identificar las exigencias éticas[5] para el desarrollo y uso de herramientas tecnológicas en la solución de litigios. En este sentido, dictó la *"Resolution 2081 (2015)1 Access to justice and the*

2. Disponible en línea: https://uncitral.un.org/es/working_groups/3/online_dispute [Fecha de consulta: 05/12/2021].
3. Disponible en línea: https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=ES [Fecha de consulta: 05/12/2021].
4. *Estrategia 2019-2023 relativa a la Justicia en Red Europea* de 13 de marzo de 2019 disponible en línea: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019XG0313(02)&from=EN [Fecha de consulta: 05/12/2021].
5. Desde un punto de vista ético, pocos Estados de la Unión Europea han abordado hasta ahora las cuestiones éticas en la construcción de la justicia digital, a excepción de Francia, que desde 2019 cuenta con normas que han establecido restricciones con fundamento ético, como la *Loi n.° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice,* Disponible en línea: https://wipolex.wipo.int/es/text/508711 [Fecha de consulta: 05/12/2021].

Internet: potential and challenges"[6] en la que planteaba la necesidad de establecer prevenciones respecto del uso de la Tecnología de la Información y la Comunicación en la solución de litigios. Asimismo, la Comisión Europea, el 4 de diciembre de 2018 adoptó la "*European Commission for the efficiency of justice (CEPEJ): European ethical Charter on the use of Artificial Intelligence in judicial systems and their environments*" en castellano, la Comisión Europea para la Eficiencia de la Justicia del Consejo de Europa la Carta Europea Ética sobre el uso de la Inteligencia Artificial en los Sistemas Judiciales, en la que, admitida la creciente importancia de la inteligencia artificial (IA) en nuestras sociedades modernas, y los beneficios esperados cuando se utilice plenamente al servicio de la eficiencia y la calidad de la justicia, el CEPEJ adopta formalmente los cinco principios fundamentales para la adopción de la Inteligencia Artificial en el panorama judicial.

A la luz de lo expuesto, resulta primordial garantizar un uso adecuado de estas tecnologías, preservar la imparcialidad e independencia de los tribunales, el respeto a los derechos, libertades y garantías de los ciudadanos, y construir así la senda hacia una nueva arquitectura de la administración de justicia en la que sea posible traducir en tutela judicial efectiva y en mejor acceso y tramitación de la justicia la potencial eficiencia que la tecnología es capaz de brindar. Ese es el reto que venimos a afrontar.

II. HERRAMIENTAS TECNOLÓGICAS Y SU UTILIZACIÓN EN EL PROCESO PENAL: ESPECIAL ATENCIÓN AL USO DE LA VIDEOCONFERENCIA Y LA INTELIGENCIA ARTIFICIAL

1. PREVISIÓN LEGAL DE LA VIDEOCONFERENCIA

El uso de la videoconferencia se encuadra en un doble marco normativo, por un lado, la Ley Orgánica del Poder Judicial (LOPJ), que establece un espacio amplio dentro del cual se debe mover la ley procesal, y, por otro lado, la Ley de Enjuiciamiento Criminal (LECrim) en la que se concretan en detalle los supuestos en que podrá admitirse la videoconferencia y los requisitos formales, en su caso, que hayan de ser observados para su válida utilización.

6. *Resolution 2081 (2015)1 Access to justice and the Internet: potential and challenges*, Disponible en línea: https://pace.coe.int/pdf/779f97588791104a196ffe8659fec7e4ce8ff9ce66e838a59eabf10835815512/resolutio n%202081.pdf [Fecha de consulta: 05/12/2021].

Respecto a la LECrim, desarrolla esta posibilidad de utilización de los recursos tecnológicos distinguiendo según su empleo se produzca durante la fase de instrucción o en el juicio oral. En este ámbito de la legislación procesal penal, la videoconferencia fue introducida de manera expresa mediante la Ley Orgánica 13/2003, de 24 de octubre que, al mismo tiempo que modificaba el art. 230 LOPJ, introdujo en el artículo 325 de la LECrim su posible utilización en la fase de instrucción para las comparecencias de los imputados, testigos o peritos, y en el artículo 731 bis LECrim para las sesiones del juicio oral, tanto para oír a los acusados como a los testigos o peritos, cuando el Juez lo acuerde de oficio o a instancia de parte, por razones de utilidad, seguridad o de orden público, así como en aquellos supuestos en que la comparecencia resulte particularmente gravosa o perjudicial.

Sin entrar a analizar, por cuestiones de extensión, todas las aportaciones introducidas por las reformas legislativas en materia de videoconferencia estos años atrás – como la nueva redacción del artículo 707 LECrim por la Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito–; o el nuevo tenor previsto para el art. 306 de la LECrim, último párrafo; o la reciente reforma del art. 230 LOPJ por la LO 4/2018, de 28 de diciembre –nos situamos en la declaración del estado de alarma por el Real Decreto 463/2020, de 14 de marzo por la crisis sanitaria originada por la pandemia del COVID–.

19. El impacto producido en la toda la actividad procesal colocó a los operadores judiciales en la necesidad de recurrir de forma masiva a los medios telemáticos para llevar a cabo determinadas actuaciones, singularmente en materia de asistencia letrada y declaración de detenidos, tanto en dependencias policiales como judiciales, y de la misma forma potenció el recurso de la videoconferencia para las declaraciones de testigos y peritos en los actos plenarios de juicio oral. La cobertura normativa para regular la situación generada se ofreció a través del Real Decreto-ley 16/2020, de 28 de abril, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia, en el que, con carácter general para todas las jurisdicciones se disponía la posibilidad de recurrir a esta técnica con carácter preferente.

Más allá de la temporal regulación expresada, la Ley 3/2020, de 18 de septiembre, prolongó estas mismas medidas procesales y organizativas hasta el 20 de junio de 2021, al contemplar en su art. 14 que *"(…) los actos de juicio, comparecencias, declaraciones y vistas y, en general, todos los actos procesales, se realizarán preferentemente mediante presencia telemática, siempre*

que los juzgados, tribunales y fiscalías tengan a su disposición los medios técnicos necesarios para ello".

Por último, disponemos del Anteproyecto de Ley de Medidas de Eficiencia Procesal del Servicio Público de Justicia, el cual fue aprobado el 15 de diciembre de 2020. El título último, sobre transformación digital, gira en torno a la innovación, al avance tecnológico, lo cual supone hacer uso de la videoconferencia para así evitar desplazamientos a las sedes judiciales, logrando una gran reducción de costes no solo económicos, sino también de carácter medioambiental y del territorio, previniendo las posibles concentraciones de personas en las oficinas judiciales.

2. VENTAJAS DE LA UTILIZACIÓN DE LA VIDEOCONFERENCIA EN EL PROCESO PENAL

El uso de la videoconferencia reporta múltiples beneficios a la justicia y a los ciudadanos. En primera instancia, refuerza el principio de economía procesal, ya que evita practicas reiteradas e innecesarias, y mantiene un justo equilibrio entre el fin y los medios. En este sentido, la actividad jurisdiccional deviene más ágil, pues evita desplazamientos innecesarios, con el correspondiente coste económico que ello supone. Por otra parte, y es interesante detenerse en ello, el uso de esta plataforma en línea favorece la seguridad del preso, al evitar, por ejemplo, la excarcelación y consiguiente traslado y custodia de reclusos y presos preventivos a los órganos judiciales, disminuyendo de esta forma, los riesgos de fuga de acusados reputados de escapistas, fuguistas o muy peligrosos[7].

El uso de la videoconferencia salvaguarda el principio de concentración, ya que, en la mayoría de casos, testigos, peritos o cualquier tercero interviniente en el proceso no podrán alegar la imposibilidad de comparecer por coincidencias con otros compromisos u obligaciones, permitiendo que se concentren todas las actuaciones en un solo acto, en la fecha del señalamiento.

Por otra parte, esta herramienta tecnológica permite la práctica de la prueba de forma inmediata en aquellos casos que devengan urgentes como, por ejemplo, cuando exista riesgo acreditado de fallecimiento del testigo por causas naturales en unas semanas. Por otro lado, y esto es importante subrayarlo, este medio de declaración opera en interés superior del menor, ya que, tras la vista, se evitaría que el acusado pudiera

7. MAGRO SERVET, V.: "Hacia el uso habitual de la videoconferencia en las vistas judiciales. 'Aprovechando las enseñanzas del Coronavirus'", en *Diario La Ley*, ISSN 1989-6913, N.° 9646, 2020.

acercarse a la víctima, evitándole, así, al menor, tener que recordar un episodio poco deseable de su vida.

El Consejo General de la Abogacía Española y la Secretaría General de Instituciones Penitenciarias han tomado cartas en el asunto, por medio de la Resolución de 15 de abril de 2021, de la Secretaría General Técnica, por la que se publica el Convenio con el Consejo General de la Abogacía Española, para la implantación del sistema de comunicación por videoconferencia entre colegios de abogados y centros penitenciarios, en el cual se permite que aquellas personas que se encuentren en los centros penitenciarios, únicamente aquellos que dependan de la Administración General del Estado van a tener la oportunidad de ponerse en contacto con sus abogados mediante videoconferencia. El objetivo de dicho convenio es poder mejorar la relación entre los internos y sus abogados, dándoles más facilidades a la hora de comunicarse. Gracias a este Convenio, se podrá progresar en el derecho a la defensa, consagrado en la Constitución Española, como derecho que tiene una protección especial, ya que constituye uno de los derechos fundamentales.

Esto, no obstante, **debe advertirse que el uso de esta herramienta también plantea algunos inconvenientes al proceso judicial**. En primer lugar, el gran damnificado podría ser el principio de inmediación judicial ya que, pese a que la presencia virtual se vaya asimilando poco a poco a la física, lo cierto es que no puede sustituirla al completo, pues la conexión telemática entraña un mínimo riesgo de pérdida de espontaneidad en la declaración del sujeto a la hora de transmitir el mensaje, lo que hace que su credibilidad se reduzca.

Por otro lado, y no es ocioso recordarlo, se debe tener en cuenta los posibles fallos del sistema o caídas de conexión que pueden irrumpir en mitad del proceso. Esta situación se puede agravar si se tiene en cuenta que la competencia en materia de tecnologías de la información y la comunicación para los Jueces y Tribunales depende en algunos lugares del Ministerios de Justicia, y en otros de la Consejería de Justicia de la Comunidad Autónoma correspondiente, lo que provoca que, al intervenir distintos órganos, los sistemas informáticos que empleen puedan resultar incompatibles entre sí.

Por otra parte, con todo este *boom* del teletrabajo y la celebración de juicios online, nuevas formas de delincuencia empiezan a emerger, como el ciberdelito, así como el robo de la información y la suplantación de identidades.

Por todo cuanto antecede, no debemos pasar por alto estos inconvenientes, pues un uso indebido de esta herramienta desvirtuaría su fin lícito, y

contagiaría desconfianza e inseguridad al ciudadano medio y al operario jurídico, lo que corrompería las bases y cimientos sobre los que descansa de nuestro Estado de Derecho. No siempre eficiencia es sinónimo de calidad. Se debe, primero, analizar y estudiar la viabilidad y respeto a las garantías de nuestro Estado de Derecho, de lo contrario, estas tecnologías, más que una oportunidad para el proceso, representarían una amenaza.

3. ¿PUEDE AFECTAR LA DIGITALIZACIÓN DE LA JUSTICIA A GARANTÍAS PROCESALES PENALES?

Según el Alto Tribunal, el empleo de la videoconferencia en el proceso penal debe resultar proporcional e idóneo en aras a conseguir el fin pretendido, debiendo el tribunal rechazar su utilización cuando afecte a los derechos de las partes, siendo el juicio más estricto cuando se trate de la intervención del acusado[8].

Debe garantizarse igualmente el respeto de los principios de oralidad, publicidad, inmediación, contradicción y defensa y que no se vulneren los derechos a la prueba y a la tutela judicial efectiva.

3.1. Principio procesal de publicidad

Respecto al principio procesal de publicidad que rige en la fase plenaria de un procedimiento penal (art. 680 LECrim), y constituye un derecho fundamental de los ciudadanos (art. 24.2 CE), se ve expuesto a posibles ciberataques, grabaciones y ulteriores difusiones del juicio, o caídas de conexión intencionados para declarar la nulidad de las actuaciones. Aun así, para el Tribunal Supremo no existe la más mínima afectación del principio de publicidad, sino todo lo contrario: *"pueden mejorar las condiciones de publicidad de las actuaciones judiciales, en cuanto las nuevas tecnologías garantizan la 'asistencia' a las actuaciones judiciales de un número mayor de personas y permite seguimiento especializado (prensa) en mejores condiciones"*[9].

3.2. Principio procesal de concentración

Por lo que se refiere al principio de concentración, no sólo no se infringe, sino que, como ya se ha señalado, la videoconferencia favorece la concentración de las actuaciones procesales, al evitar aplazamientos,

8. MONTESINOS GARCÍA, A.: *La videoconferencia como instrumento probatorio en el proceso penal*, Ed. Marcial Pons, 2009, p. 120.
9. STS 331/2019 de 27 junio.

suspensiones o demoras en los señalamientos de las diferentes actuaciones judiciales por motivos de distancia física, existiendo una equiparación jurídica entre presencia física y virtual.

3.3. Principio procesal de inmediación judicial

En cuanto a la inmediación, si bien no existe presencia física del tribunal, y no existe el contacto visual, se trata de una técnica que, gracias a la bidireccionalidad y transmisión simultánea de la imagen y sonido, al menos permite que sea el mismo tribunal que va a dictar la sentencia el que interrogue en el momento, directamente, preservándose en definitiva las ventajas que plantea la inmediación. A mayor abundamiento, y especialmente si la calidad de la imagen es buena, el tribunal puede apreciar matices, actitudes y gestos de todos los conectados.

3.4. Derecho de defensa

En relación con el derecho de defensa, es obligado referirse a la Sentencia núm. 678/2005, de 16 de mayo de la Sala Segunda del Tribunal Supremo[10] en la que, estimando los recursos de casación interpuestos por varios de los procesados, se anula no solo la sentencia dictada por la Sección 1.ª de Audiencia Provincial de Alicante en el juicio del "motín de Foncalent", sino la propia celebración del juicio oral que se había llevado a cabo mediante el sistema de videoconferencia. En esta sentencia el Alto Tribunal niega que pueda recurrirse al uso de la videoconferencia con acusados, salvo casos muy puntuales debidamente motivados por razones de excepcionalidad. El Fundamento Jurídico Tercero de la mentada Sentencia basa la nulidad en que el letrado "*podría ver seriamente limitadas sus funciones de asesoramiento y asistencia*". Continúa señalando el Tribunal Supremo que la proyección de los principios básicos del procedimiento es "*distinta según se trate de la declaración distante de un testigo o la práctica del informe del perito, que tan sólo requieren garantizar la exactitud y fiabilidad de la información recibida por el juzgador, así como el sometimiento de su generación a la contradicción de las partes, que cuando estamos ante la participación de los propios acusados, especialmente en el momento cumbre del juicio oral, a los que ha de permitírseles intervenir activamente en el ejercicio de su propio derecho de defensa*".

Por ello el Alto Tribunal considera relevante su presencia real y efectiva en el lugar de celebración de la vista oral y que pueda comunicarse

10. Disponible en línea: https://vlex.es/vid/videoconferencias-causas-justificables-18041031 [Fecha de consulta: 09/12/2021].

directamente con su Abogado para un correcto asesoramiento y asistencia, porque el inculpado puede mejorar su defensa estando en posición en que pueda intercambiar con su Letrado comentarios o información, como ocurre en el Juicio por Jurado. De lo contrario, según este planteamiento, se reduciría y mermaría el derecho de defensa, al verse limitadas las funciones de asesoramiento y asistencia del Letrado, salvo que se arbitre un sistema de comunicación permanente e independiente entre el defensor y el defendido.

4. INTELIGENCIA ARTIFICIAL E INCIDENCIA EN EL PANORAMA JUDICIAL

4.1. Aplicaciones de la Inteligencia Artificial en el proceso penal

La inteligencia artificial, como parte de un gran proceso de Revolución Digital al que hemos venido asistiendo, no ha dejado de desarrollarse adquiriendo cada vez mayor protagonismo en la sociedad, convirtiéndose en una de las grandes herramientas de trabajo en la actualidad. En el proceso penal, el uso e implementación de esta disruptiva tecnología ha supuesto un aumento de la eficiencia del sistema judicial a diferentes niveles, por un lado, por el apoyo en la persecución del delito, y, por otro, por el desarrollo y las innovaciones que presenta en el desarrollo de nuevos medios de investigación y enjuiciamiento del tipo penal.

Respecto al apoyo a la investigación judicial, nuestra LECrim, de 1882, se encontraba muy anticuada, pues no ofrecía medidas de investigación actualizadas para la persecución de las nuevas formas de criminalidad. Y es que la tecnología viene siendo utilizada para fines poco loables que ha desencadenado en nuevas formas de delincuencia.

La sociedad de la información, la inexistencia de fronteras y los empleos masivos de comunicaciones mediante dispositivos electrónicos entre cualquier punto cardinal del planeta hacen que los límites temporales y espaciales que han caracterizado al Derecho Penal sean puestos en tela de juicio. Ello ha desembocado en un nuevo tipo de criminalidad, que requiere de una investigación de características similares para una exitosa persecución. En respuesta a ello, se reformó nuestra LECrim por vía de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta reforma ha incorporado a nuestro proceso penal –a la fase de instrucción– medidas de investigación tecnológicas muy frecuentes hoy en la práctica, como son la

intervención en las comunicaciones telefónicas y telemáticas, la videovigilancia o la grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos. Estas medidas las adopta la Policía Judicial, previa autorización del Juez que conoce de la instrucción una vez quede acreditada por la unidad policial la existencia de indicios suficientes que hagan prever que mediante algunas de estas técnicas de investigación se obtendrán pruebas que incriminen a los sujetos investigados. La aplicación de alguna de estas medidas debe tener un carácter muy restrictivo y amparado en el principio de proporcionalidad, debido a que su aplicación conlleva una vulneración de derechos fundamentales de la persona investigada. En este sentido, la Agencia Europea de los Derechos Fundamentales de la Unión Europea, en informe reciente, de 14 de diciembre 2020, titulado "*Getting the future right – Artificial intelligence and fundamental rights* (Construir correctamente el futuro – La inteligencia artificial y los derechos fundamentales)"[11] manifiesta su preocupación y presenta una visión de conjunto de las tecnologías relacionadas con la IA actualmente utilizadas en la Unión Europea (UE) y analiza sus implicaciones sobre los derechos fundamentales. Concretamente, el director de esta Agencia, Michael O'Flaherty, advierte que *"Tenemos una oportunidad de diseñar la IA para que no solo respete nuestros derechos humanos y fundamentales, sino también para que los proteja y los promueva"*.

Por otra parte, es preciso mencionar que fruto de las labores de investigación tecnológica nace el concepto de prueba electrónica, esto es, la información de valor probatorio contenida o transmitida por un medio electrónico[12]. Hablamos de cualquier clase de información, almacenada en medios electrónicos y susceptible de acreditar hechos en un proceso abierto para la investigación de todo tipo de infracciones penales. La fuente de prueba radica en la información contenida o transmitida por medios electrónicos y el medio de prueba será como se incorpora al proceso (normalmente como prueba documental o pericial, aunque cabe mediante la testifical). Y es que el uso de dispositivos basados en Inteligencia Artificial como fuente de prueba se ha incrementado de forma considerable, lo cual suscita dos problemas fundamentales, por un lado, nos encontramos con la necesidad de regular una situación de gran complejidad por el desconocimiento tecnológico-informático de estas herramientas y, por otro lado, por el desafío que implica su comprobación y utilización como

11. Disponible en el siguiente URL: https://fra.europa.eu/sites/default/files/fra_uploads/pr-2020-artificial– intelligence_es.pdf [Fecha de consulta: 07/12/2021].
12. BORGES BLÁZQUEZ, R.: "La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea" en *Rev. Boliv. de Derecho*, núm. 25, enero 2018, ISSN: 2070-8157, p. 541.

una prueba fiable dentro de un proceso judicial. Respecto a esto último, ha existido cierta controversia jurídica en torno a uno de los principales medios probatorios electrónicos[13] utilizados en la *praxis*, la aplicación *WhatsApp*. Estos datos, que han de tener entrada en el proceso a través de un concreto medio probatorio admitido por el ordenamiento, y ha de ser respetado el procedimiento que, para el concreto medio de prueba, sea contemplado por la respectiva legislación procesal para ejercitar válidamente el derecho a la prueba, son herramientas, como bien previene GASCÓN INCHAUSTI[14], susceptibles de ataques y "*hackeos*" que pueden poner en peligro, entre otros extremos, la privacidad de los sujetos implicados en un proceso, la integridad de las actuaciones o la propia fiabilidad de los elementos probatorios que tengan soporte digital.

Por las razones expuestas, la Unión Europea, por vía de la Comisión Europea, aprueba una Propuesta de Reglamento Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal[15], con la firme apuesta de abordar el problema específico derivado del carácter volátil de las pruebas electrónicas y su dimensión internacional. Intenta adaptar los mecanismos de cooperación a la era digital, ofreciendo a las autoridades judiciales y policiales herramientas para abordar la forma en que los delincuentes se comunican en la actualidad, y para luchar contra las nuevas formas de delincuencia. Estos instrumentos que se proponen estarán ligados a unos sólidos mecanismos de protección de los derechos fundamentales[16].

13. Este hecho ha provocado la articulación del concepto de prueba, originando el concepto específico de "prueba electrónica", que alude a aquella que emana de las nuevas "tecnologías de la información y comunicación". *Vid.* GARRIDO CARRILLO, F.J.: "La prueba electrónica en los procesos civiles y penales", publicado en la *Revista de la Facultad de Derecho de la Universidad de Granada*, números 16/17/18 (2013– 2014-2015), Título del número de la Revista "Crisis y Estado del Bienestar". 1o Edición, Ed. Tirant lo Blanch, Valencia 2017, p. 2.
14. GASCÓN INCHAUSTI, F.: "Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial". En *La Justicia digital en España y la Unión Europea,* dirigido por Jesús Conde Fuentes y Gregorio Serrano Hoyo. 191 206. Barcelona: Atelier, 2019, p. 192.
15. Disponible en el siguiente enlace: https://eur-lex.europa.eu/legal– content/ES/TXT/?uri=COM%3A2018%3A225%3AFIN [Fecha de consulta: 07/12/2021].
16. Y es que, una investigación que pretenda requisar soportes informáticos o interceptar comunicaciones es susceptible de incidir en la esfera de los derechos fundamentales de los ciudadanos. Afectará en todo caso a la intimidad personal (art 18.1 CE) salvo que la injerencia se haya realizado previa autorización judicial o consentimiento del afectado (STC 173/11) sin perjuicio de la posible intervención policial en casos de urgente necesidad y respetando el principio de proporcionalidad (STS 115/2913). También se puede vulnerar el derecho al secreto de las comunicaciones (Art 18.3 CE)

4.2. Riesgos del uso de la Inteligencia Artificial en el proceso penal

Esta innovadora herramienta tecnológica de la información y de la comunicación también presenta una serie de riesgos y peligros que se tornan en desafíos para el legislador. Fundamentalmente, el uso de Inteligencia Artificial y los avance de las TIC's entraña dos riesgos fundamentales: i) una restricción de los derechos fundamentales reconocidos constitucionalmente[17], ii) y nuevas oportunidades delictivas en el ciberespacio que aprovechan los delincuentes para cometer numerosos delitos.

En el primer escenario, ya se ha hecho mención en apartados anteriores de la vulneración de determinados derechos fundamentales por el empleo de Inteligencia Artificial. Los medios tecnológicos permiten investigar el delito con arreglo a mecanismos que, con frecuencia, comportan importantes restricciones de las garantías constitucionales de privacidad e intimidad contenidas en el art. 18 CE. La cuestión es que nuestro legislador ha ido a remolque de la realidad y ha tardado en dar carta de naturaleza legal a técnicas de investigación cuya posibilidad y utilidad eran claras. En cualquier caso, no se puede frenar la persecución e investigación del delito, y para ello, resulta innegable la utilidad que aportan las nuevas formas de tecnología cara a la investigación del crimen, a veces a costa de la restricción de determinados derechos fundamentales para una correcta investigación del hecho, y para la obtención de pruebas. En definitiva, el empleo de Inteligencia Artificial, o cualquier medida tecnológica invasiva para investigar o acceder a determinadas pruebas, debe respetar con carácter riguroso la esfera de los derechos de los ciudadanos. En este sentido, en fecha reciente, el Tribunal Constitucional mediante Sentencia 28/2020, de 24 de febrero, Fundamento Jurídico Quinto[18], ha recordado los límites legales que ha de primar en la adopción de medidas restrictivas de derechos fundamentales, en este sentido, necesariamente i) han de preverse en norma de rango legal; ii) orientarse a la realización de un fin constitucionalmente legítimo, iii) y perseguirlo de un modo necesario

---

y a la inviolabilidad del domicilio (Art 18.2 CE) si el dispositivo se encuentra en el interior de un lugar cerrado constitutivo de domicilio o el derecho a la autodeterminación informativa en el ámbito de protección de datos personales (Art 18.4 CE).

17. A tal fin fue aprobada la Ley Orgánica 13/2015, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, de 5 de octubre de 2015. Dice así: "*Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros*".

18. STC 28/2020, de 24 de febrero, Fundamento Jurídico Quinto, disponible en línea: https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/26245 [Fecha de consulta: 09/12/2021].

y proporcionado, esto es, que la restricción legal, además de no ser sustituible por otra menos restrictiva, no genere más perjuicios al derecho al honor que beneficios para los fines constitucionales a que sirve[19].

Si no se respetasen las pautas marcadas por el Tribunal Constitucional se incurriría en la vulneración de determinados derechos fundamentales, con consecuencias indeseables para el correcto desarrollo del proceso penal, pues podría denunciarse la vía ilícita de obtención de prueba *ex* artículo 11.1 LOPJ, o, para el caso de que alguna diligencia de investigación –como la interceptación de las comunicación telefónicas, la grabación de comunicaciones o el registro de dispositivos– se hubiere practicado sin acomodarla previamente al principio de proporcionalidad, podría alegarse de oficio o a instancia de parte la nulidad de las actuaciones y la consiguiente remisión de la causa a la fase inicial de la investigación.

Esta cuestión concierne a las instituciones y organismos europeos. Por ello, recientemente, el Informe de la Agencia de los Derechos Fundamentales de la Unión Europea sobre inteligencia artificial[20], subraya la alteración profunda que han supuesto las nuevas tecnologías en nuestro modo de organizarnos y vivir nuestras vidas. En concreto, las nuevas tecnologías basadas en los datos han impulsado el desarrollo de la IA, en particular mediante la automatización cada vez mayor de tareas que normalmente eran realizadas por humanos. La crisis sanitaria de la COVID-19 ha favorecido la adopción de la IA y el intercambio de datos, generando así nuevas oportunidades, pero también presentando retos y amenazas para los derechos humanos y los derechos fundamentales.

Este informe respalda el objetivo marcado por la Comisión Europea en el Libro Blanco sobre Inteligencia artificial: "Un enfoque europeo orientado a la excelencia y la confianza, publicado el 19 de febrero de 2020"[21], en el que resume los principios más destacados de un futuro marco normativo de la UE para la IA en Europa. En el Libro Blanco se señala que es vital que dicho marco se asiente sobre los valores fundamentales de la UE, en particular el respeto de los derechos humanos (artículo 2 del Tratado de la Unión Europea).

19. En este mismo sentido, el art. 588 bis a) LECrim establece los principios rectores que han de guiar cualquier intromisión mediante el uso de medidas de investigación tecnológica, debiendo satisfacerse los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora.
20. Disponible en línea: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence– summary_es.pdf [Fecha de consulta: 09/12/2021].
21. Disponible en línea: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial– intelligence-feb2020_es.pdf [Fecha de consulta: 09/12/2021].

Partiendo de las consideraciones anteriores, el Parlamento Europeo ha hecho pública, en fecha de 21 de abril de 2021, la propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión[22]. En vista de la velocidad a la que cambia la tecnología y las dificultades que podrían surgir, el objetivo que persigue la propuesta no es otro que buscar un enfoque equilibrado, en orden a preservar su liderazgo tecnológico y garantizar que los europeos puedan aprovechar nuevas tecnologías que se desarrollen y funcionen de acuerdo con los valores, los derechos fundamentales y los principios de la UE.

Por otra parte, el uso de Inteligencia Artificial también genera una nueva oportunidad delictiva en el ciberespacio que aprovechan los delincuentes para cometer numerosos delitos.

Y es que, el desarrollo de las tecnologías de la información y la generalización en el uso de las mismas ha tenido reflejo en la delincuencia y la criminalidad, pues la aparición de nuevos tipos delictivos y nuevas modalidades en la comisión de los delitos tradicionales determina que sean cada vez más numerosos los bienes jurídicos objeto de protección penal que pueden verse comprometidos por quienes utilizan los avances de la ciencia para llevar a efectos sus criminales propósitos. Estos cambios en la delincuencia ordinaria han convertido a la ciberdelincuencia en un reto significativo y merecedor de una respuesta legislativa adecuada. Este tipo de conductas ilícitas que se planifican y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información, presentan a los efectos de su investigación y/o enjuiciamiento, singularidades y dificultades para su descubrimiento y persecución, así como para la identificación de las personas responsables de estos comportamientos ilícitos. Nos encontramos, sencillamente, ante una nueva generación de delitos que ha supuesto la evolución en los medios y equipos de investigación, siendo necesaria la especialización de los agentes para dar respuesta a las soluciones que la sociedad demanda contra la delincuencia informática. En definitiva, con la aparición del ciberdelito, propiciado por las nuevas tecnologías, el Derecho Penal se enfrente a una criminalidad progresivamente más lesiva, que requiere a su vez los necesarios instrumentos procesales para hacerle frente.

En materia legislativa, se introdujeron, mediante reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley

22. Disponible en línea: https://eur-lex.europa.eu/legal–content/ES/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

Orgánica 10/1995, de 23 de noviembre, del Código Penal, ciertos tipos penales a fin de dar respuesta a aquellos supuestos que quedaban impunes, y resolver y solucionar así los problemas que existían de falta de tipicidad de algunas conductas. No obstante, la realidad delictiva siempre va por delante de la regulación legal. máxime en estos casos, en que la tecnología avanza a un ritmo vertiginoso.

III. CONCLUSIONES

La utilización de la videoconferencia, pese a que se ha ido utilizado desde antaño de forma ocasional en otros ámbitos de la vida de las personas, lo cierto es que su utilización masiva por cuestiones de trabajo o justicia no se ha producido hasta la llegada de la situación de pandemia. Y no contábamos, a mi juicio, con la preparación ni la concienciación suficientes para responder de manera eficaz frente a esta situación. En cualquier caso, una vez la sociedad y el panorama judicial en concreto se han ido adaptando a la nueva realidad virtual, no podemos negar que el uso de la videoconferencia ha servido de gran ayuda, ya que evitó el gran riesgo de contagio debido a la COVID-19 y permitió la celebración de todos aquellos juicios que tuvieron que haber sido celebrados durante el estado de alarma, por lo que supuso una gran herramienta para reducir la sobrecarga de los Juzgados y Tribunales. Es un medio conveniente, se considera neutral, rentable y fácil de usar, además ahorra mucho tiempo y simplifica el trabajo.

Asimismo, respecto a la incidencia de esta herramienta en las garantías procesales del justiciable, esto es, el principio de publicidad, concentración, contradicción e inmediación, debiendo preservarse por supuesto el derecho de defensa de las partes, se colige, del análisis llevado a cabo, que dichos principios no resultan afectados. El Tribunal Supremo, no obstante, mantiene un planteamiento restrictivo, considerando de aplicación subsidiaria la utilización de la videoconferencia en relación con la declaración del acusado en el proceso penal, al considerar la presencia física un valor que preservar, solo sacrificable cuando concurran razones que, debidamente ponderadas por el órgano jurisdiccional, puedan prevalecer sobre las ventajas de la proximidad física y personal entre las fuentes de prueba y el Tribunal que ha de valorarlas, debiendo justificarse en cada caso concreto, respetándose el principio de proporcionalidad.

Por otra parte, la utilización de Inteligencia Artificial ha supuesto indudablemente la eficiencia del sistema a diferentes niveles, plasmado en un reforzamiento de la persecución de la criminalidad y en nuevos medios en la investigación del delito. No obstante, un potencial riesgo que entraña el uso de este medio tecnológico es que, con frecuencia, comportan

importantes restricciones de las garantías constitucionales de privacidad e intimidad contenidas en el art. 18 CE. Lo primordial, y se debe subrayar, es que el empleo de Inteligencia Artificial, ya sea al servicio de la investigación del delito o de la actividad probatoria, resulte compatible y respetuosa con el sistema de derechos fundamentales del ciudadano.

IV. BIBLIOGRAFÍA

BORGES BLÁZQUEZ, R.: "La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea" en *Rev. Boliv. de Derecho*, núm. 25, enero 2018, ISSN: 2070-8157, p. 536-549.

GASCÓN INCHAUSTI, F.: "Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial". En AAVV, CONDE FUENTES, J. SERRANO HOYO, G. (dirs.). *La Justicia digital en España y la Unión Europea. Situación actual y perspectivas de futuro*. Ed. Atelier, España, 2019, pp. 191-206.

GARRIDO CARRILLO, F. J.: "La prueba electrónica en los procesos civiles y penales", publicado en la *Revista de la Facultad de Derecho de la Universidad de Granada*, números 16/17/18 (2013-2014-2015), Título del número de la Revista "Crisis y Estado del Bienestar". 1.ª Edición, Ed. Tirant lo Blanch, Valencia 2017.

MAGRO SERVET, V.: "Hacia el uso habitual de la videoconferencia en las vistas judiciales. 'Aprovechando las enseñanzas del Coronavirus'" en *Diario La Ley*, ISSN 1989– 6913, N.° 9646, 2020.

MONTESINOS GARCÍA, A.: *La videoconferencia como instrumento probatorio en el proceso penal*, Ed. Marcial Pons, 2009.

REFERENCIAS NORMATIVAS

– LIBRO BLANCO: sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza, de 19 de febrero de 2020.

– Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia.

– Informe de la Agencia Europea de los Derechos Fundamentales de la Unión Europea, de 14 de diciembre 2020, titulado "Getting the

future right – Artificial intelligence and fundamental rights (Construir correctamente el futuro – La inteligencia artificial y los derechos fundamentales)".

- Estrategia 2019-2023 relativa a la Justicia en Red Europea de 13 de marzo de 2019.
- Loi n.° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
- Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO.
- sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal de 17 de abril de 2018.
- Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: "Notas técnicas de la CNUDMI sobre la solución de controversias en línea", Nueva York, 2017.
- Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

REFERENCIAS JURISPRUDENCIALES

- Sentencia del Tribunal Constitucional n.° 28/2020, de 24 de febrero.
- Sentencia del Tribunal Supremo n.° 331/2019 de 27 junio.
- Sentencia del Tribunal Supremo n.° 678/2005, 16 de mayo.

La irrupción de la inteligencia artificial en la resolución alternativa de conflictos

Ana Isabel González Fernández

Doctoranda Derecho Procesal
Universidade de Vigo

SUMARIO: I. LOS MASC POR MEDIOS ELECTRÓNICOS: ODR. II. INTELIGENCIA ARTIFICIAL Y ODR. 1. *Consideraciones generales*. 2. *Negociaciones automatizadas: la implantación de la función decisora en la mediación*. III. CONCLUSIONES. IV. BIBLIOGRAFÍA.

I. LOS MASC POR MEDIOS ELECTRÓNICOS: ODR

Desde los años noventa estamos asistiendo al nacimiento de un nuevo mecanismo de resolución de conflictos de manera online, los ODR, que conjuga la eficiencia que permiten los mecanismos de resolución de conflictos con las ventajas que nos ofrecen las nuevas tecnologías[1]. Especialmente importante fue la mediación por medios electrónicos, que muchos autores la consideran como una evolución de la mediación presencial que permite una mayor interacción entre las partes y rapidez a la hora de resolver los conflictos por la simultaneidad de las comunicaciones. Incluso, como veremos en las siguientes líneas, "pudiendo aplicar programas informáticos que también por escrito transmitan la solución ideal según los algoritmos que el programa contenga"[2].

Si bien es cierto que el auge principal de los ODR se ha forjado en el ámbito de la tutela de consumidores y usuarios, dónde podemos destacar la enorme labor realizada desde las instituciones europeas en aras

1. MONTESINOS GARCÍA, A., "Inteligencia artificial y ODR", Justicia algorítmica y neuroderecho. Una mirada multidisciplinar, S. BARONA VILAR (Dir.), Valencia, 2021, p. 501.
2. BUJOSA VADELL, L., y PALOMO VÉLEZ, D., "Mediación electrónica: perspectiva europea", *Revista Ius et Praxis*, núm. 2, 2017, p. 56

de favorecer la resolución alternativa de conflictos a través de medios electrónicos. Son dos textos a los que debemos hacer referencia obligada ya que supusieron una apuesta decida de las instituciones europeas por el desarrollo y cualificación de la resolución alternativa de litigios de consumo en los EEMM. En definitiva, buscan potenciar los ODR para solventar los conflictos en el menor tiempo posible y sin que suponga un menoscabo de los derechos de los justiciables en cuanto a la satisfacción de sus intereses[3].

En primer lugar, la Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo y por la que se modifica el Reglamento (CE) n.° 2006/2004 y la Directiva 2009/22/CE (en adelante, DRAL) que persigue ofrecer al consumidor "un acceso a vías sencillas, eficaces, rápidas y asequibles para resolver los litigios nacionales y transfronterizos […] y, por consiguiente, reforzar su confianza en el mercado".

En segundo lugar, el Reglamento (UE) n.° 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) no 2006/2004 y la Directiva 2009/22/CE (en adelante, RRLL), obliga a los Estados Miembros a crear un portal interactivo en línea para la resolución extrajudicial de conflictos contractuales a través, entre otras posibilidades, de la mediación electrónica.

Ya dentro de nuestro OJ, la Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo, que en la misma línea que las normas precedentes, busca que los consumidores residentes en cualquier EEMM tengan acceso a las entidades de resolución alternativa reconocidas para la resolución de conflictos derivados del comercio, fundamentalmente, e-commerce.

Especialmente interesante esta opción en los tiempos que corren, ya que el empleo de estos mecanismos extrajudiciales, y más concretamente los celebrados por vía electrónica, suponen un factor extra para hacer

3. Entre otros, véase, MARTÍN DIZ, F., Inteligencia artificial y medios extrajudiciales de resolución de litigios online (ODR): evolución de futuro en tiempos de pandemia global (Covid-19)", *LA LEY mediación y arbitraje, N.° 2*, Sección Doctrina, 2020; Martínez Rodríguez, N. (2017), Resolución alternativa de litigios en línea y desarrollo electrónico del comercio electrónico en Europa. En F. MARTÍN DIZ (Dir.), A. CARRIZO GONZÁLEZ-CASTELL (Coord.) *Mediación en la Administración de Justicia: implantación y desarrollo*, Andavira, Santiago de Compostela, 2017.

frente a las consecuencias derivadas de la crisis sanitaria provocada por el COVID-19[4].

A mayor abundamiento, pese a los inconvenientes a nivel sanitario y personales de la pandemia que nos toca vivir, debemos verla también como una oportunidad de mejora del sistema de justicia, especialmente, en cuanto a los avances que permiten las nuevas tecnologías. En gran parte se debe a la familiaridad de la población con ellas para realizar tareas que antes se tenían que realizar de manera presencial o arcaica que favoreció a la reducción de la brecha digital, ya que esta situación condujo a un avance cultural que no se debe desaprovechar y debemos tenerlo en cuenta para potenciar el uso de las nuevas tecnologías en un ámbito tan reacio a su utilización como era la Justicia[5].

En todo caso, siguiendo las directrices marcadas por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre la solución de controversias en línea del año 2017, se establece que cualquier sistema de ODR debe sustentarse sobre los principios de equidad, transparencia, independencia, respeto de las garantías procesales y rendición de cuentas y, evidentemente, la voluntariedad de las partes, expresada como consentimiento explícito e informado. Sin duda, acreditando lo anteriormente expuesto, este organismo internacional destaca que los ODR constituyen una vía sencilla, rápida y eficiente a la hora de resolver los conflictos y que no podrá suponer un retraso importante ni cargas desproporcionadas en relación con el valor del objeto del litigio.

II. INTELIGENCIA ARTIFICIAL Y ODR

1. CONSIDERACIONES GENERALES

Estamos inmersos en la Revolución Industrial 4.0 que conlleva la transformación de nuestra forma de vivir, comunicarnos o relacionarnos con los demás bajo la idea de la instantaneidad. No hace falta recordar que hoy

4. BOZZO HAURI, S. y REMESEIRO REGUERO, R., "Resolución de conflictos en consumo: ¿una solución a través de la Inteligencia Artificial?" *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, S. BARONA VILAR (Dir.), Valencia, 2021, p. 613.

5. VÁZQUEZ DE CASTRO, E., "Técnicas de resolución de disputas en línea y mediación electrónica para superar la brecha digital y evitar el epostracismo profesional" en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 5, 2020.

   Este mismo autor, en la línea apuntada, señala que la tesitura social actual, donde la pandemia sigue vigente y, por tanto, las pautas para combatirla, supone la ocasión perfecta para potenciar definitivamente la mediación electrónica, si bien no es recomendable que sea la regla general, sobre la que volveremos a lo largo de este capítulo.

en día, a través de sistemas inteligentes, tenemos a nuestro alcance prácticamente de todo en todo momento y desde cualquier lugar. Destaca en esta Revolución el auge de la IA, que podemos definirla como una tecnología desarrollada a partir de algoritmos, alimentada a partir de nuestros datos –recabados desde una infinidad de instrumentos a nuestro alcance como los SmartWatch, sistemas de conducción inteligente, etc.–, de forma que la maquina aprenda y relacione la información que nosotros le ofrecemos, directa o indirectamente, y a partir de ella sea capaz de adquirir un comportamiento y una forma de pensar similar a los humanos[6].

La Administración de Justicia no es ajena a este fenómeno social, de hecho, de cara a obtener una justicia más rápida, moderna y certera, se ha apuntado a la digitalización de la justicia como la vía adecuada para lograr los fines apuntados y en todo caso, teniendo en cuenta el virus con el que convivimos, como pueden ser las comunicaciones telemáticas o la inclusión de instrumentos de IA para simplificar algún trámite judicial. Sobre esta cuestión, debemos señalar que no se trata de una materia exenta de riesgos en tanto en cuanto tiene incidencia directa en los derechos humanos y procesales de los justiciables –igualdad y no discriminación, protección de datos, derecho a la tutela judicial efectiva presunción de inocencia, derecho al debido proceso, etc.–[7].

En este punto debemos distinguir las distintas funciones de la IA en el campo de la Justicia. Por un lado, nos encontramos con la función asistencial que puede ser definida como un "elemento de apoyo a quienes asumen responsabilidades en el litigio, ya sean las partes –para decidir sobre el acceso a una ODR o designar a quienes asumen la posición de tercero imparcial en la resolución del litigio hasta poder preparar fundadamente y con más y

6. CATALÁN CHAMORRO, M. J. (2021), Multi-Door Justice System e Inteligencia Artificial. En Barona Vilar, S. (Dir.), Justicia algorítmica y neuroderecho. Una mirada multidisciplinar, Tirant lo Blanch, Valencia, pp. 533-534.

   La aparición de máquinas inteligentes puede hacernos pensar si realmente pensamos por nosotros mismos o estamos dirigidos de alguna manera por la IA. Pensemos que cada vez que navegamos por la red y aceptamos la política de cookies, estamos dejando rastro de nuestros gustos y, analizados por el sistema de IA, nos ofrecerán en el futuro anuncios relacionados con la búsqueda inicial.

   Lo mismo sucede con nuestro comportamiento compartido con la nube a través de los dispositivos electrónicos de nuestras viviendas o relojes inteligentes que, si bien carecen de personalidad, los datos facilitados permanecen y son tratados con diferentes fines (TAPIA HERMIDA, A. (2020), Decálogo de la Inteligencia Artificial ética y responsable en la Unión Europea, *Diario La Ley*, n.° 9749).

   Por ello, se ha elaborado desde la UE el Libro Blanco sobre la IA que establece las líneas básicas de funcionamiento de los sistemas de IA.

7. MARTÍN DIZ, F. (2020), Litigiosidad extrajudicial en sedes electrónicas. En FONTESTAD PORTALÉS, L. (Dir.) y CARO CATALÁN, J. (Coord.) La globalización del Derecho Procesal, Tirant lo Blanch, Valencia, 2020, p. 423.

mejores datos su posición en el mismo– o el tercero ajeno al mismo que ha de resolverlo (juez, árbitro o mediador), ofreciendo datos y predicciones que puedan ser de ayuda y orientación en alguna de las decisiones o actuaciones que deban desenvolver en su labor jurisdicente, arbitral o mediadora"[8].

Más arriesgada si cabe, la IA puede adoptar una función decisoria, dónde el elemento humano en la resolución del conflicto es sustituido por la IA que pasará a asumir la función de juzgar, arbitrar o mediar.

En el sentido ahora apuntado, es fundamental contar con herramientas informáticas y telemáticas de última generación que aportan un plus a la resolución de conflictos y por qué no abogando por el recurso a sistemas inteligentes. En este contexto, podemos encontrarnos con aplicaciones de inteligencia artificial que proporcionen elementos de asistencia o incluso yendo más allá y asuman funciones decisorias y, en todo caso, respetando los derechos fundamentales de las partes.

Ante el escenario que ahora se plantea, CATALÁN CHAMORRO[9] distingue dos modelos de ODR, por un lado, el analógico, existente hasta el momento y el más conocido, y el modelo de ODR digital, "fruto de la combinación que el big data ofrece a través de operaciones matemáticas, de probabilidades y de razonamientos humanos introducidos en una máquina para "enseñarla" *a pensar como los humanos*", para ello, se valdrá de las bondades que ofrece la IA para formar una estrategia, elegir entre distintas alternativas, etc.. Ahora bien, altamente controvertida es la función decisoria de la IA en el plano de la resolución de conflictos, en el caso que ahora planteamos, nos hacemos una pregunta, ¿se puede sustituir al mediador?

2. NEGOCIACIONES AUTOMATIZADAS: LA IMPLANTACIÓN DE LA FUNCIÓN DECISORA EN LA MEDIACIÓN

Hasta ahora hemos hablado de dos posibilidades de aplicar un sistema de IA en un mecanismo ODR de resolución de conflictos. Ahora nos vamos a centrar en aquellos sistemas que utilizan los sistemas inteligentes con una función decisoria, esto es, dictando la solución de forma autónoma, a su vez, podemos diferenciar dos fórmulas, una completamente autónoma dónde el factor humano no interviene en ningún momento[10].

8. MARTÍN DIZ, F. (2020), Inteligencia artificial…, *op. cit.*, p. 3.
9. CATALÁN CHAMORRO, M. J. (2021), Multi-Door Justice System e Inteligencia Artificial. En BARONA Vilar, S. (Dir.), Justicia algorítmica y neuroderecho. Una mirada multidisciplinar, Tirant lo Blanch, Valencia, pp. 259-260.
10. GUZMÁN FLUJÁ, V. (2021), Arbitraje y soluciones técnicas inteligentes: elementos para un debate. En BARONA VILAR, S. (Dir.), Justicia algorítmica y neuroderecho. Una mirada multidisciplinar, Tirant lo Blanch, Valencia, p. 556.

Hoy en día son bastantes las plataformas de comercio electrónico que integran la IA para la resolución de los conflictos de escasa cuantía entre comerciante y usuario, a modo de ejemplo, podemos citar Amazon, eBay, Paypal, Airbn. Se trata de automatizados dónde una vez que el conflicto ha surgido, ofrecen a las partes implicadas una solución para que se acepte o no. Como vemos, no se trata de una imposición de la solución, se da la oportunidad de acatar la solución ofrecida pudiendo renunciar a ella voluntariamente, realmente, en este tipo de solución del conflicto estamos ante una conciliación propiamente dicha[11].

Con carácter general, el funcionamiento de las plataformas de ODR es bastante sencillo. Entre una variedad de alternativas que resultan de aplicación al conflicto que se plantea y que previamente fue descrito y probado por las partes por medio de imágenes, vídeos, documentos, etc., se seleccionan alguna de ellas y se le da traslado a la parte en contra de quien se actúa para que ésta responda en un breve lapso de tiempo aquello que estime favorable a sus intereses. A la vista de todo lo expuesto, el sistema artificial decide cuál es la mejor solución para ese supuesto que, como dijimos, no debe vincular a las partes, esto es, propone una solución entre otras existentes pero que es más favorable a las dos partes[12].

En concreto, este sistema "a ciegas"[13], funciona de la siguiente manera "La interfaz visual de la negociación es mostrada como eje horizontal de

---

Otra opción puede ser la que, sin apenas tener algún tipo de intervención, el factor humano sí interviene, en ese caso, será necesaria la exigencia de una serie de garantías. Esta última opción creemos que puede ser de gran ayuda a cualquier procedimiento de resolución de conflictos, por ello nos adelantamos a decir que no es viable prescindir en ningún caso del elemento humano por motivos ya no sólo técnicos sino también éticos.

11. Debemos tener presente la distinción entre mediación y conciliación, en tanto en cuanto la intervención del tercero en la mediación es distinta y no tiene la capacidad de ofrecer soluciones a las partes. Sensu contrario, en la conciliación, el tercero tiene la capacidad, como sucede con la aplicación de la IA en la resolución de conflicto– de ofrecer a las partes una solución adecuada su conflicto.

    La distinción entre ambas instituciones es un tema sumamente controvertido en la doctrina científica, sobre esta cuestión véase, por todos, IGLESIAS CANLE, I. C. (2011), Formas de solución de conflictos tras la Ley 13/2009, de 3 de noviembre: especial referencia a la conciliación y mediación, Dereito: Revista Xurídica da Universidade de Santiago de Compostela, vol. 20, núm. 2, pp. 65-82. http://hdl.handle.net/10347/7998.

12. AMUNÁTEGUI PERELLÓ, C. (2020), Arcana Technicae. El Derecho y la Inteligencia Artificial, Tirant lo Blanch, Valencia, pp. 105 y ss.

13. La definición de "puja a ciegas" se debe a que todas las ofertas son confidenciales, "*aunque la mayoría de negociaciones automatizadas son 'a ciegas' también existe un tipo de negociación automatizada 'visual' que se diferencia de la primera en que las ofertas sí pueden ser visualizadas por las partes*". Véase el funcionamiento de los sistemas de pujas a ciegas o *bling bidding* en MONTESINOS GARCÍA, A. "Inteligencia artificial…", *op. cit.*, pp. 517 a 518.

variables dentro de las cuales se muestra la cantidad optimista ofertada y la cantidad pesimista. Las partes al mover el ratón pueden aproximarse a la zona de acuerdo sin que se conozca la cantidad del acuerdo previamente. El algoritmo del sistema premia a la parte que se aproxima a la zona de acuerdo con un número más alto en la negociación y que demuestra mayor interés en la negociación. De manera que cuando una de las partes llega a un acuerdo dentro de la zona de acuerdo (cantidad escondida), el sistema declara un acuerdo"[14].

Ahora bien, en el recurso a este mecanismo de resolución de conflictos es de suma importancia tomar ciertas cautelas a la hora de su utilización para no comprometer a las partes. De esta forma, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta a la protección de datos personales y a la libre circulación de estos datos prevé expresamente en su art. 22 (plasmado de idéntica manera en nuestra legislación interna) que "todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar", salvo que medie consentimiento expreso por parte del usuario.

En definitiva, indirectamente se prohíbe la toma de decisiones basadas únicamente en el tratamiento automatizado de los datos que trasladamos a la correspondiente plataforma, entre otras cosas, se garantiza, si las partes así lo desean, la intervención humana. Por otro lado, las partes tendrán derecho a conocer los motivos que han llevado a la máquina a la emisión de la resolución ofrecida, con ello se busca dotar de ciertas garantías las decisiones adoptadas a través estas plataformas[15].

III. CONCLUSIONES

Sin duda, esta posibilidad de solución de conflictos supondría el ahorro de tiempo y coste a la hora de poner fin a las posibles diferencias que puedan surgir como consecuencia de la utilización de estos medios de comercio electrónico y al tratarse de materias de derecho disponible, entendemos que no existe inconveniente alguno en su puesta en funcionamiento pues las partes son libres de acatarla o no.

14. MONTESINOS GARCÍA, A., "Inteligencia artificial…", *op. cit.*, p. 517.
15. PÉREZ DAUDÍ, V. (2021), La aplicación de las nuevas tecnologías al proceso: ¿realidad o ciencia ficción? En FUENTES SORIANO, O. (Dir.), *Era digital, sociedad y derecho,* Tirant lo Blanch, Valencia, p. 378.

En definitiva, pese a las ventajas que ofrece la implementación de los ODR a la IA, deben tenerse en cuenta una serie consideraciones por la incidencia que tiene en determinados ámbitos dónde pueden surgir dudas pero, sin duda "tenemos que hacer frente, sin miedo, pero con responsabilidad y, sobre todo, exigiendo el máximo respeto a los principios y garantías del proceso (que también deben estar presentes en el propio diseño del algoritmo). El mayor de los temores lo representa la figura del árbitro robot (u otro agente inteligente) que desbanca al árbitro persona y que plantea dudas no solo éticas o de fiabilidad sino también acerca de la posible responsabilidad de la máquina. Deviene necesario, por tanto, un marco normativo y ético que garantice transparencia total e imparcialidad en la forma en la que se procesa la información"[16].

Por todo ello, también abogamos por la creación de un marco jurídico normativo y ético estable por parte del legislador que suponga que el ciudadano conozca el modo en qué se están tratando sus datos personales y la información trasmitida y que es tomada en consideración por parte de la IA. En todo caso, debe garantizarse la imparcialidad e independencia en la toma de decisiones. Sin duda, supondría generar confianza por parte del usuario afecto por ellas.

Ahora bien, pese a lo expuesto, consideramos que en determinados asuntos dónde es determinante tener en cuenta las emociones de las partes, por muy perfeccionada que esté el sistema inteligente no tendrá la misma consideración que tendría la decisión tomada por un humano, independientemente de si es un mediador, un árbitro o un Juez. Los humanos somos capaces de diferenciar las emociones de las partes, su forma de relacionarse, si tiene miedo, etc., hecho que un sistema inteligente que funciona con operaciones matemáticas y datos incorporados al sistema –al menos de momento– y pese al nivel de perfección que se alcance en el futuro a través de sistemas biométricos o de voz, no tendrán en cuenta estos elementos subjetivos tan importantes a la hora de tomar una decisión.

Sí que defendemos que sin embargo se apliquen estas formas de solución automatizada de conflicto en reclamaciones dinerarias basadas únicamente en pruebas objetivas aportadas por las partes y no suponen mayor problema de una aplicación arbitraria del derecho por parte de la máquina. Sin duda, esta posibilidad de solución de conflictos supondría el ahorro de tiempo y costes económicos en asuntos de escasa entidad. Además, al tratarse de materias de derecho disponible, entendemos que no existe inconveniente alguno en su utilización pues las partes son libres de acatarla o no.

16. MONTESINOS GARCÍA, A. Inteligencia artificial…, *op. cit.,* p. 529.

En todo caso, como ya avanzamos, el factor humano es indispensable por lo que no estamos hablando de sistemas inteligentes que opten por sustituir el elemento humano, ya sea a la hora de introducir los datos o revisando previamente la decisión que se presenta a las partes.

IV. BIBLIOGRAFÍA

AMUNÁTEGUI PERELLÓ, C. (2020), *Arcana Technicae. El Derecho y la Inteligencia Artificial*, Tirant lo Blanch, Valencia.

BARONA VILAR, S. (2017), Proceso civil y penal ¿líquido? En el siglo XXI. En BARONA VILAR, S. (Ed.), *Justicia Civil y penal en la era global*, Tirant lo Blanch, Valencia.

BOZZO HAURI, S. y REMESEIRO REGUERO, R. (2021), Resolución de conflictos en consumo: ¿una solución a través de la Inteligencia Artificial? En BARONA VILAR, S. (Dir.), *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia.

BUENO DE MATA, F. (2021), Protección de datos, investigación de infracciones penales e inteligencia artificial. Novedades y desafíos a nivel nacional y europeo en la era postcovid, *La ley penal: revista de derecho penal, procesal y penitenciario*, n.° 150, pp. 1-23.

BUJOSA VADELL, L. y PALOMO VÉLEZ, D. (2017), Mediación electrónica: perspectiva europea, *Revista Ius et Praxis*, núm. 2, pp. 51-78. http://dx.doi.org/10.4067/S0718-00122017000200051.

CATALÁN CHAMORRO, M. J. (2021), Multi-Door Justice System e Inteligencia Artificial. En BARONA VILAR, S. (Dir.), *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia.

CATALÁN CHAMORRO, M. J. (2019), *El acceso a la justicia de consumidores: los nuevos instrumentos del ADR y ODR de consumo*, Tirant lo Blanch, Valencia.

ESTEBAN DE LA ROSA, F. (2018), Desafíos de la contratación electrónica para los sistemas de resolución alternativa de litigios de consumo: radiografía de una transformación necesaria, *Revista Jurídica sobre Consumidores y Usuarios, monográfico sobre consumidores y contratación electrónica*, n.° 3, pp. 37-66. http://hdl.handle.net/10481/54055.

GIL SEATON, A. (2021), ODR de Consumo y Blockchain, *Revista Jurídica sobre consumidores*, núm. 9.

GIMENO SENDRA, V. (2010), *Introducción al Derecho Procesal*, Colex, Madrid.

GUZMÁN FLUJÁ, V. (2021), Arbitraje y soluciones técnicas inteligentes: elementos para un debate. En Barona Vilar, S. (Dir.), *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia.

IGLESIAS CANLE, I. C. (2011), Formas de solución de conflictos tras la Ley 13/2009, de 3 de noviembre: especial referencia a la conciliación y mediación, *Dereito: Revista Xurídica da Universidade de Santiago de* Compostela, vol. 20, núm. 2, pp. 65-82. http://hdl.handle.net/10347/7998.

IGLESIAS CANLE, I. C. (2021), Intercambio de información e inteligencia en el contexto europeo, con especial referencia al ordenamiento jurídico español. En BONORINO RAMÍREZ, P. R., FERNÁNDEZ ACEVEDO, R., VALCÁRCEL FERNÁNDEZ, P (Eds.) y SOBRINO GARCÍA, I. (Coord.), *Justicia, Administración y Derecho. Nuevos retos del derecho en el siglo XXI*, Thomson Reuters Aranzadi, Navarra.

MARCOS FRANCISCO, D. (2013), Las Online Dispute Resolution en materia de consumo en la Unión Europea. En Vázquez De Castro, E. (Dir.) y Fernández Canales, C. (Coords.) *Estudios sobre justicia online*, Comares, Granada.

MARTÍN DIZ, F. (2020), Inteligencia artificial y medios extrajudiciales de resolución de litigios online (ODR): evolución de futuro en tiempos de pandemia global (Covid-19), *La Ley, mediación y arbitraje*, n.° 2, Sección Doctrina.

MARTÍN DIZ, F. (2020), Litigiosidad extrajudicial en sedes electrónicas. En Fontestad Portalés, L. (Dir.) y Caro Catalán, J. (Coord.) *La globalización del Derecho Procesal*, Tirant lo Blanch, Valencia, 2020.

MARTÍNEZ RODRÍGUEZ, N. (2017), Resolución alternativa de litigios en línea y desarrollo electrónico del comercio electrónico en Europa. En F. MARTÍN DIZ (Dir.), A. CARRIZO GONZÁLEZ-CASTELL (Coord.) *Mediación en la Administración de Justicia: implantación y desarrollo*, Andavira, Santiago de Compostela, 2017.

MONTESINOS GARCÍA, A. (2021), Inteligencia artificial y ODR. En Barona Vilar, S. (Dir.), *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, Tirant lo Blanch, Valencia.

MORENO CATENA, V. y CORTÉS DOMÍNGUEZ, V. (2021), *Introducción al Derecho Procesal*, Tirant lo Blanch, Valencia.

ORTEGA HERNÁNDEZ, R. J. (2019), *Mecanismos alternativos de resolución de conflictos por medios electrónicos*, Bosch, Barcelona, 2019.

PÉREZ DAUDÍ, V. (2021), La aplicación de las nuevas tecnologías al proceso: ¿realidad o ciencia ficción?. En Fuentes Soriano, O. (Dir.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Valencia.

TAPIA HERMIDA, A. (2020), Decálogo de la Inteligencia Artificial ética y responsable en la Unión Europea, *Diario La Ley*, n.° 9749.

VÁZQUEZ DE CASTRO, E. (2020), Técnicas de resolución de disputas en línea y mediación electrónica para superar la brecha digital y evitar el epostracismo profesional, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.° 5.

Riesgos de la aplicación de la Inteligencia Artificial en la Administración de Justicia

Raúl López Martínez

Juez Sustituto adscrito al Tribunal Superior de Justicia de Aragón

Resumen: La Inteligencia Artificial ha mejorado notablemente muchos aspectos de la vida cotidiana de las personas, al simplificar numerosos procesos, con las ventajas sociales y económicas que ello implica. Por ello, se ha planteado la cuestión de su aplicación a la Administración de Justicia, ámbito tradicionalmente sustentado sobre decisiones de personas físicas en las que el Estado deposita el poder para juzgar y hacer ejecutar lo juzgado, en base a sus conocimientos y percepciones éticas. La pregunta fundamental se centra en determinar si esas técnicas artificiales cohonestarían, por lo estereotipado de su carácter, con tales principios y valores.

Abstract: *AI has notably improved many aspects of people's daily lives, by simplifying many processes, with the social and economic advantages that this implies. For this reason, the question of its application to the Administration of Justice has been raised, an area traditionally based on decisions of natural persons –Judges or Magistrates– in which the State deposits the power to judge and enforce what has been judged, based on their knowledge and ethical perceptions. The fundamental question focuses on determining whether these artificial techniques would be consistent with the principles and values of Justice.*

Palabras clave: IA; Justicia; ética; riesgo de estandarización.

Keywords: *AI; Justice; Ethic; risk of standarization.*

I. INTRODUCCIÓN

Resulta común la opinión de que la Inteligencia Artificial (en adelante, IA) es una tecnología que ha aparecido súbitamente en las últimas décadas, empero, lo cierto es que se trata de una técnica que cuenta con un importante bagaje pues, no en vano, comenzó a aplicarse a mediados de los años cincuenta del pasado siglo. En efecto, el término fue acuñado por el profesor de Matemáticas de la Universidad de Dartmouth, John McCarthy, por vez primera en 1956, en una conferencia donde se preguntaba hasta dónde podría llegar el libre albedrío de las máquinas y si llegaría el día en que una de ellas podría llegar a decidir por sí misma, como un ser humano.

El recorrido y evolución posterior de estas tecnologías de IA es de sobra conocido. Por eso, lejos de pensar que las mismas son propias de un futuro más o menos próximo, lo cierto es que la realidad demuestra que la IA está plenamente asentada en nuestras sociedades y facilita muchas tareas de la vida cotidiana, pese a que en muchas ocasiones seamos ignorantes de ello. Así, desde la sanidad hasta la educación, pasando por nichos tan cotidianos como el bancario o los seguros, son ámbitos donde la IA está totalmente integrada. Se trata de una tecnología disruptiva, por la forma en la que está influyendo y cambiando un gran número de actividades de toda índole.

Pero, ¿qué ocurre con la Administración de Justicia? ¿Resulta aplicable la IA en este ámbito? Y, en tal caso, ¿es sustituible la labor del Juez? ¿Cumple la IA los parámetros de la ética judicial? Estas son algunas de las cuestiones que trataremos de desgranar en estas páginas.

II. CONTEXTUALIZANDO LA CUESTIÓN: ¿QUÉ SE ENTIENDE POR INTELIGENCIA ARTIFICIAL (IA)?

Partiendo de una definición de corte generalista, la IA se refiere *"a todos aquellos sistemas que manifiestan un comportamiento autónomo inteligente, siendo capaces de analizar su entorno y pasar a la acción con cierto grado de autonomía, todo ello para alcanzar objetivos específicos"*[1]. En suma, esta disciplina supone el uso de tecnologías que buscan que las máquinas tengan una capacidad propia de percepción, comprensión, aprendizaje y, finalmente, actuación[2].

1. MERCHÁN MURILLO, A., "Retos Regulatorios en torno a la Inteligencia Artificial", en *Pensar, Revista de Ciencias Jurídicas*, n.° 4, 2018, p. 2.
2. SANTOS GONZÁLEZ, M. J., "Regulación legal de la robótica y la inteligencia artificial", en *Revista Jurídica de la Universidad de León*, n.° 4, 2017, pp. 22-50.

Se basa en una serie de algoritmos, entendidos como un conjunto ordenado de operaciones o procesos que permiten desarrollar una tarea determinada o hallar una solución ante un problema planteado. Desde esa perspectiva, la IA trata de elaborar sistemas capaces para poder resolver problemas y desempeñar tareas sin la intervención humana o, al menos, sin la intervención medial, ya que *ex ante* sí requiere la participación de la mano del hombre.

Esta predeterminación, que cuenta entre sus principales caracteres los de la memoria y el aprendizaje a partir de experiencias determinadas, la automatización de procesos, la capacidad para resolver problemas específicos, la reducción de errores, la adaptabilidad o la posibilidad de percepción sensorial, la mayor eficiencia en los procesos productivos o la agilización en la toma de decisiones, ha acelerado procesos y facilitado numerosas tareas relacionadas con la actividad del ser humano.

Sin embargo, la IA también presenta una cara negativa relacionada con la dificultad de acceso a los datos, por cuanto la obtención de los datos necesarios en cada momento, así como su actualización y fiabilidad, no siempre resulta una tarea sencilla; por ello, los algoritmos utilizados han de ser lo suficientemente fiables y sólidos, a fin de generar confianza y evitar errores e incoherencias. Asimismo, la IA requiere de elevados costes de implantación y mantenimiento.

La IA se diferencia de muchas otras herramientas de transformación digital y genera dificultades diferentes porque es la única tecnología que aprende y cambia sus resultados en función de dicho aprendizaje.

Pero, sin duda, uno de los mayores problemas que se revela al analizar la IA es que, debido a las características de la misma, pueda generar cierta inseguridad o desconfianza, ya que puede cometer errores más gruesos que un ser humano, por lo que todavía existen recelos para que en algunos ámbitos puedan desplegarse estas innovaciones con carácter pleno. Y la Justicia es uno de ellos.

III. ¿CABE APLICAR LA IA A LA ADMINISTRACIÓN DE JUSTICIA?

Como decimos, la IA se ha aplicado hasta la fecha con éxito en múltiples ámbitos de muy diverso signo. Y, en la trastienda de esos procesos, descansa un complejo procedimiento de cálculos y tratamiento de datos cuyo fin último es lograr un resultado objetivo, aplicable a una generalidad de casos.

Debido a ello, han surgido voces acerca de la conveniencia de la aplicación de las técnicas de IA en el ámbito de la Administración de Justicia, en concreto, en la última de sus fases, la decisoria, lo que ha generado un debate, todavía no solventado, que gira en torno a determinar si el uso indiscriminado de estas técnicas supondría hacer peligrar todo ese elenco de principios y valores que singularizan un mundo tan conservador como es el de la Justicia o si, por el contrario, su aplicación favorecería a este sector, tanto a nivel interno como externo.

Así, la aplicación de la IA en determinados procesos supondría que, mediante la aplicación de algoritmos, la consecución de una resolución se basaría en la valoración de parámetros tales como la situación económica de las partes o de circunstancias concretas, no sólo internas, sino también las del mundo circundante, además de tomar en consideración resoluciones dictadas por órganos jurisdiccionales en anteriores y similares procedimientos. Y, de esa amalgama de elementos, resultaría la Sentencia, lo que en un mundo tan tradicional como es la impartición de Justicia –muy identificada con su consideración de función eminentemente humana–, plantea dudas.

Sin ánimo de ahondar en los antecedentes históricos del término, por cuanto excedería del objeto de análisis, cabe decir que ya en el siglo IV a. C., Aristóteles consideraba al hombre como un ser social, un animal político que, al convivir con sus iguales y desarrollar sus relaciones en el seno de una sociedad, necesitaba de la implantación de un *ius*, entendido como el conjunto de normas que regulaban dichas relaciones.

Algunas centurias después, Ulpiano estableció que el término *ius* derivaba de otro concepto más genérico, el de *Iustitia*[3], esto es, Justicia, como la primera de las funciones del Estado, que los pueblos necesitaban para dar a cada uno lo suyo, como una función que se encomendaba a determinados hombres investidos de autoridad otorgada por el poder público.

Así fue, con las variaciones propias de los sistemas jurídicos y las diferentes concepciones dominantes en cada época, hasta llegar prácticamente a nuestros días. En base a ello, podría pensarse que la aplicación de la Justicia es inherente a la persona y que, precisamente por ello, no cabría establecer sistemas alejados de la voluntad humana.

No obstante, el Derecho no es una ciencia pétrea, antes al contrario, una de las principales notas características que lo definen es su capacidad de adaptación a las nuevas realidades sociales. Y es en este punto donde

3. FERNÁNDEZ DE BUJÁN, F., "Ius, Iustitia y naturaleza jurídica del advocatus en la Roma clásica", en Miguel Grande Yáñez (Coord.), *Justicia y Ética de la Abogacía*, Dykinson, Madrid, 2007, pp. 19-51.

se plantea el empleo de la IA como una técnica de enorme utilidad que podría ayudar a mejorar notablemente el funcionamiento de aquél y, más en concreto, de la Justicia.

Ahora bien, aun siendo a priori una herramienta muy útil, la IA nunca podría sustituir al Juez persona física, fundamentalmente porque ello podría lesionar muchos de los principios recogidos en nuestra vigente Constitución de 1978, en concreto en su Título VI, relativo al Poder Judicial –artículos 117 y siguientes–.

La Sentencia, como colofón del procedimiento, debe representar, en la medida de lo posible, la verdad judicial buscada y establecida tras un procedimiento judicial prefijado y recogido en la norma legal aplicable, donde confluyan todas las garantías inherentes al mismo y que resulte vinculante para las partes. En esencia, la Justicia no puede reducirse a predicciones matemáticas ni a simples aprendizajes basados en datos que perpetúen los prejuicios. Sin embargo, cabría aplicarse a determinados procedimientos, cuya tramitación resulta a priori, más sencilla, ofreciendo a las partes, sobre todo en atención al principio dispositivo que rige en el proceso civil, la posibilidad de elegir este sistema, lo que tendría en última instancia consecuencias directas en cuanto al régimen de recursos.

En suma, la aplicación de un sistema de IA en nuestra Administración de Justicia debería fijar su punto de partida en el correcto uso de los datos, cualitativa y cuantitativamente hablando. Es lo que se ha dado en llamar "Arquitectura de la Información". Para ello, resulta necesario un trabajo previo que filtre el conjunto a utilizar y procesar, dentro de unos parámetros preseleccionados. En este sentido, el ingente número de datos utilizados en el ámbito de la Justicia facilitará con mucho dicha labor, a efectos de conseguir un resultado verdaderamente objetivo, que denote la eficiencia de esta herramienta.

No debemos olvidar la necesaria observancia, en el marco de este proceso, de la normativa sobre privacidad y protección de datos, a la que cada vez se le otorga mayor importancia, como demuestra la alusión que se efectúa a la misma en las resoluciones dictadas por las autoridades judiciales españolas.

Asimismo, como se ha indicado, cabe recordar que el sistema de IA puede presentar errores puntuales en su fijación inicial, ya que, como cualquier otra técnica de estas características, se irá depurando y enriqueciendo conforme avance su puesta en funcionamiento. Es, precisamente, este punto uno de los que esgrime parte de la doctrina en sus recelos a la hora de adoptar estos sistemas en la impartición de Justicia, por cuanto una posible falibilidad –al margen del coste material que ello acarrearía–,

incidiría directamente sobre las personas intervinientes en el proceso y a las que afectan las resoluciones. Todo ello eleva el grado de responsabilidad institucional en orden a una correcta implantación de estos sistemas, basada en la ética, el principio de prudencia y las buenas prácticas, alejando así la idea de una posible aplicación experimental de los mismos. No en vano, está en juego la imagen de la Justicia y la confianza que el ciudadano deposita en ella como uno de los puntales del Estado de Derecho.

La IA implica transformación, sí, pero hemos de entender sus límites. Y estos límites deben estar definidos por una ética que no desdeñe el factor humano, mediante valores tales como la autonomía, la responsabilidad o la transparencia.

IV. UN PROBLEMA CONCRETO: LA POSIBLE INCOMPATIBILIDAD DE LA ÉTICA JUDICIAL Y LA IA

Los numerosos Códigos éticos que han proliferado en los últimos años en toda clase de profesiones, han afectado también a la Justicia. Así, al albur de lo establecido en la esfera internacional –*v. gr.* el Código de Bangalore, aprobado por las Naciones Unidas en 2002, o el Código Modelo de Ética Judicial elaborado por la Cumbre Iberoamericana de Justicia celebrada en 2006[4]– se han desarrollado estos documentos como una suerte de *vademécum* de los valores, principios y pautas éticas y de conducta que deben conformar la actuación del "buen Juez".

Esta cuestión suscita la cuestión de si los principios y valores que se plasman en esos Códigos resultarían aplicables o, cuando menos, compatibles con la implementación de la IA en el ámbito judicial. Para responder a dicha cuestión, pasaremos a enumerar someramente las principales características de la figura del "buen Juez" y, en su caso, si resultan conciliables con la IA. Y es que, como apunta Adela Cortina, *"no sólo es un buen profesional el que conoce técnicas y las aplica, sino el que se interesa por conocer técnicas y aplicarlas desde las virtudes y valores de la profesión"*[5], lo que, descendiendo al ámbito judicial, devendría en la conversión de los profesionales de la Judicatura, no sólo en buenos especialistas técnicamente hablando, sino también en creadores de un pensamiento crítico hacia sus propias decisiones, lo que conlleva que el desarrollo de sus funciones se

4. SANCHO GARGALLO, I., "Ética judicial: el paradigma del buen Juez", en *Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales ICADE*, n.° 72, 2007, pp. 117-138.
5. CORTINA ORTS, A., "La Ética de los Jueces", en *Actualidad Jurídica Uría y Menéndez*, n.° 19, 2008, pp. 7-13.

desarrolle sobre una serie de virtudes y cualidades basadas en una auténtica ética judicial, pues la Justicia no puede estar amparada solamente por el ordenamiento jurídico, sino que también deberá descansar sobre esos valores y principios que sirvan de guía para ejecutar las acciones adecuadas en cada momento.

Entre los caracteres que se recogen en el artículo 117 de la CE, hemos de mencionar, en primer lugar, la independencia. Un Poder Judicial independiente constituye una de las garantías esenciales de un Estado social y democrático de Derecho, entendida como una de las virtudes necesarias para impartir Justicia y la omisión de toda injerencia externa. En este sentido, quienes defienden su implantación esgrimen que la introducción de medios artificiales en la impartición de Justicia incluiría plenamente esta característica, pues es evidente que no se puede influir en una máquina. Sin embargo, partiendo de este mismo argumento, aunque a la inversa, cabría preguntarse por la independencia *ex ante*, esto es, valorando los posibles sesgos de las personas que programasen los algoritmos que sustentan el resultado final. En todo caso, cuestión esta difícil de solventar y que es objeto de múltiples debates ya que, a priori, estigmatizaría este tema. En segundo lugar, debemos mencionar la imparcialidad o exigencia ética que avala la confianza ciudadana en la acción de la Justicia, alejando al Juez de todo prejuicio o influencia que pudiere condicionar su actuación, como otra de las premisas necesarias para conseguir la legitimación de los actos de aquél. Otro de los pilares sobre los que debe sustentarse la ética judicial es la integridad, como entereza moral de un individuo, en este caso, del Juez.

Estos tres caracteres están interconectados, pues todos ellos responden a la necesidad de evitar injerencias de los impulsos externos. En suma, se trataría de presentar al Juez como una figura inmune a presiones y pujanzas exteriores, como un reflejo de lo que Dworkin dio en llamar el "Juez Hércules"[6], esto es, aquel que, además de ser un buen conocedor del Derecho, sustente sus decisiones en sólidos principios morales alejados de todo influjo del mundo exterior, a fin de conseguir resoluciones justas y cercanas con el conjunto social[7]. Y es lo cierto que idéntica reprobación que la apuntada respecto a la independencia en cuanto a su encaje con la IA, cabe realizar a las otras dos –imparcialidad e integridad–, esto es, que no existe una total eliminación de posibles vicios humanos, debido a que, en algún momento, la mano del hombre entra a formar parte del proceso,

6. DWORKIN, R., *Los derechos en serio*, Ariel, Barcelona, 2012.
7. DELGADO PINTO, J., *De nuevo sobre el problema del Derecho natural: discurso leído en la Solemne apertura del Curso Académico 1982-1983*, Universidad de Salamanca, 1982, p. 10.

lo que descarta la total automatización de la Justicia y la aparición del problema de los sesgos. Los algoritmos permiten estandarizar las decisiones, es decir, uniformar criterios, pero se deben evitar los sesgos propios de los seres humanos que los crean. Asimismo, desde el punto de vista completamente inverso, una absoluta automatización de la Justicia devendría en la incapacidad de captar la singularidad del ser humano, que resulta de necesaria aplicación en algunas decisiones judiciales.

A las anteriores notas, cabe unir la prudencia, característica propia de la inteligencia práctica, que sirve a las personas para decidir correctamente, con el objetivo de aplicar las leyes descendiendo a supuestos particulares. Relacionados con ella, aparecen distintos aspectos que también son propios del ser humano y, por tanto, serían difícilmente aplicables a un sistema pleno de IA, como son la equidad, la razonabilidad, la cautela y, finalmente, la motivación.

Además de las meritadas, se han señalado una serie de particularidades de corte profesional que deben destacarse en la figura del "buen Juez", como son, en primer lugar, la formación y capacitación, que, por su propia naturaleza, es evidente que se darían plenamente en la IA, puesto que cabría que una máquina, no sólo se equiparase, sino que llegara a superar el nivel de sabiduría jurídica que pudiere acumular una persona. Sin embargo, como en los casos anteriores nunca se podía suplir la inmediación, característica esta ínsita al ser humano y a su percepción. Destacar, igualmente, la responsabilidad institucional, característica necesariamente ligada al Juez persona física y que, por tanto, no podría ser reemplazada por técnicas artificiales; y lo mismo ocurre con la cortesía debida, como muestra de respeto inherente a la figura del Juez en sus relaciones con el resto de agentes jurídicos e, incluso, como referente social. Dentro de esta característica podemos mencionar la capacidad de dialogo, de comprensión y entendimiento, caracteres todos ellos que, evidentemente, no casarían bien con una total implantación de la IA. En el otro extremo, como aspectos que serían adaptables a sistemas de IA, cabe mencionar la transparencia y el secreto profesional, al garantizar el pleno respeto a la normativa sobre protección de datos. Finalmente, en lo referente a la diligencia y celeridad, entendidas en el sentido del deber que todo Juez tiene de resolver en un plazo razonable los casos de los que conozca, quizás sea este el ámbito donde un sistema de IA en la Justicia mejoraría claramente el panorama actual, con un más que evidente –y, en algunos casos, histórico– atraso en los órganos judiciales. No se trata tanto de que el Juez no resuelva dentro del plazo establecido por la Ley –que, salvo en casos puntuales, se hace, aun a costa de sacrificar horas de su vida privada–, sino a que pudiera mejorar el volumen de trabajo existente en los Juzgados.

Además, muchas veces el retraso no es achacable a la labor judicial o a una mayor capacidad resolutiva, sino al propio sistema, sustentado en un laberinto normativo que ralentiza en la mayoría de ocasiones la tramitación de los procedimientos, sumiéndolos en dilaciones, en muchos casos alentadas por alguna de las partes litigantes, lo que denota una ausencia de buena fe procesal.

En suma, podemos concluir que la IA supondría un eficaz complemento a la acción judicial, siempre y cuando se tuviera claro desde un primer momento que en ningún caso supondría una total exclusión de la actuación del Juez y que fuera acompañada de las necesarias reformas legales y la actualización de todos los operadores jurídicos, desde la base hasta la cúspide, contando por supuesto con el compromiso de los poderes públicos de dotar de los medios humanos y materiales –con una sustancial dotación presupuestaria– para que su aplicación resultara uniforme y exitosa, constituyendo una acción transversal a todo el sistema, pero nunca, como decimos, como sustitutivo de la figura del Juez, por cuanto el sistema debe seguir descansando sobre la percepción subjetiva y ética del mismo. La pretensión última de la IA no es sustituir al factor humano, sino apoyarlo, y que la persona siga siendo esencial en la toma de decisiones, su ejecución y el seguimiento de sus resultados. Las revoluciones tecnológicas que se han producido a lo largo de la Historia demuestran que, pese a las iniciales y lógicas suspicacias ante cualquier cambio sustancial, finalmente el ser humano termina adaptándose al mismo y eso le hace crecer y mejorar. Y nada obsta, al margen de su perfeccionamiento, para que la aplicación de la IA siga otros cauces.

El reto es mayúsculo y debería ir acompañado, como decimos, del respaldo institucional. Las aplicaciones de IA son más eficaces cuanto mayor es la cantidad y mejor la calidad de datos a procesar. Por eso, el continuo incremento de la potencia de procesamiento de los ordenadores, la generalización del uso de Internet, la creación de una gran cantidad de bases de datos y el acceso a ellas han permitido importantes avances en este campo, lo que lleva a preguntarnos si la Administración de Justicia está técnicamente preparada para su implementación.

V. CONCLUSIONES

En primer lugar, cabe destacar una realidad palpable, la cual además supone una de las principales características del Derecho y define su legitimidad, la cual es que éste es una ciencia en continuo movimiento, que se va amoldando a la realidad social conforme la misma avanza.

El aspecto judicial del Derecho no escapa de esa consideración y, por ello, relacionada con la anterior, encontramos el tema de la ética, como una cualidad que ha de permanecer ligada a dicha función, aun cuando se vaya renovando, o adaptándose a los nuevos tiempos, aquélla.

En efecto, al igual que ha ocurrido con otras profesiones, también en la judicial se han asentado los argumentos que defienden la implementación de la ética, en el sentido de hacerlos visibles por cuanto, aun cuando se presuponen en una labor con tanta trascendencia como es la de impartir Justicia, se considera que no está de más concretarlos, para evitar ideologizarlos y exponerlos a posibles influencias externas. En ese sentido, han sido varios los documentos que han recogido esos principios y valores que, necesariamente, ha de presentar la figura del denominado "buen Juez". Y lo cierto es que resulta unánime la opinión acerca de su necesidad.

Al margen de ello, y precisamente porque la función judicial, como elemento clave de la ciencia jurídica, no debe permanecer al margen de los avances y utilidades que brinden las nuevas tecnologías, comienza a plantearse desde hace unos años la posible aplicación de la llamada "Inteligencia Artificial" (IA) a determinadas decisiones judiciales que, a través de un complejo sistema de algoritmos, coadyuvaría a uniformar determinadas decisiones a las controversias planteadas.

Las ventajas que presentaría este sistema son evidentes, sobre todo en cuanto a que dotaría a la Justicia de una mayor celeridad, sencillez en la tramitación, ahorro de costes, desobstrucción de los Juzgados y seguridad en cuanto a los resultados. Para obtener los beneficios de la IA, a la vez que se mitigan los riesgos, se debería asegurarse la adopción de buenas prácticas para crear una transformación responsable usando la IA, lo que va ligado a la ética antes mencionada.

Sin embargo, no dejan de aparecer voces críticas, relacionadas con el peligro de la posible "estandarización" de la Justicia"[8], que la alejaría de los principios y valores éticos a los que hemos hecho referencia y, además, deshumanizaría un tanto la labor del impartidor de Justicia, sobre todo teniendo en cuenta si esos mismos principios y valores podrían ser subsumibles en el desempeño de esa función en el caso en que la misma fuera desarrollada por una máquina, en vez de por un ser humano, lo que plantea serias dudas en un ámbito en el que la inmediación sigue siendo

8. El propio Tribunal Supremo ha efectuado varias advertencias que podríamos relacionar con el riesgo de estandarización. Así, en cuanto al uso indiscriminado del "corta y pega", la Sala Segunda del Alto Tribunal ha alertado a los órganos jurisdiccionales del abuso de la utilización de jurisprudencia de manera indiscriminada, alejándose del deseable razonamiento, aplicado al caso concreto (por todas, STS n.° 47/2021, de 21 de enero).

un principio fundamental, sin olvidar los riesgos que podrían derivarse de una dependencia excesiva.

Como en muchas otras cuestiones, quizás la solución deseable sería llegar a un punto medio, donde confluyera una paulatina implementación de estas técnicas, sobre todo en los procedimientos más sencillos, con la garantía de la seguridad jurídica y la ética, de forma que nunca se alcanzase el riesgo de convertir a la Justicia en una indeseable máquina expendedora, con el consabido: "Su Sentencia, gracias".

VI. BIBLIOGRAFÍA

CORTINA ORTS, A., "La Ética de los Jueces", en *Actualidad Jurídica Uría y Menéndez*, n.° 19, 2008, pp. 7-13.

DELGADO PINTO, J., *De nuevo sobre el problema del Derecho natural: discurso leído en la Solemne apertura del Curso Académico 1982-1983*, Universidad de Salamanca, 1982.

DWORKIN, R., *Los derechos en serio*, Ariel, Barcelona, 2012.

FERNÁNDEZ DE BUJÁN, F., "Ius, Iustitia y naturaleza jurídica del advocatus en la Roma clásica", en Miguel Grande Yáñez (Coord.), *Justicia y Ética de la Abogacía*, Dykinson, Madrid, 2007, pp. 19-51.

MERCHÁN MURILLO, A., "Retos Regulatorios en torno a la Inteligencia Artificial", en *Pensar, Revista de Ciencias Jurídicas*, n.° 4, 2018, pp. 1-13.

SANCHO GARGALLO, I., "Ética judicial: el paradigma del buen Juez", en *Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales ICADE*, n.° 72, 2007, pp. 117-138.

SANTOS GONZÁLEZ, M. J., "Regulación legal de la robótica y la inteligencia artificial", en *Revista Jurídica de la Universidad de León*, n.° 4, 2017, pp. 22-50.

Policía predictiva (*Predictive Police*)

Tatiana López Pérez

Abogada

SUMARIO: I. RESUMEN. II. ALGORITMOS DE PREDICCIÓN POLICIAL, ORIGEN Y SU EMPLEO EN ESPAÑA. III. APLICACIÓN DE LOS DISTINTOS SISTEMAS DE INTELIGENCIA ARTIFICIAL Y SU REPERCUSIÓN PRÁCTICA. IV. RESULTADOS DEL EMPLEO DE LA POLICÍA PREDICTIVA Y SU REPERCUSIÓN EN DERECHO PENAL. V. CONCLUSIONES. VI. BIBLIOGRAFÍA. VII. ANEXO JURISPRUDENCIAL.

I. RESUMEN

Por medio del presente trabajo expongo como es la situación de la policía predictiva, las herramientas que se emplean en la prevención de delitos, ya sean patrimoniales o delitos sobre las personas y las posibles consecuencias jurídicas penales de su adecuada utilización.

II. ALGORITMOS DE PREDICCIÓN POLICIAL, ORIGEN Y SU EMPLEO EN ESPAÑA

Estados Unidos es uno de los países pioneros en aplicar esta tecnología, algo tan innovador como los algoritmos que no sólo tratan de utilizar las fuentes de información que tienen ya en sus bases de datos, las tecnologías geoespaciales y cualquier información o dato de carácter identificativo y personal de un individuo, todo ello para reducir la ciberdelincuencia, sino que se trata de mejorar la seguridad de los ciudadanos, reaccionando previamente a que se llegue a cometer el delito y desplegar cuantos recursos existan para, en consecuencia, evitarlos. La policía predictiva trabaja desde las semejanzas y analogías, unos patrones para que con ese conjunto de datos que se repiten de forma constante, puedan identificar de forma regular la manera de operan de los criminales en diferentes delitos.

En España, existen múltiples empresas del sector privado que han recibido generosas cantidades de dinero público para el diseño y realización de softwares de gestión policial con la única finalidad de venderlas a distintos estamentos públicos, de tal manera que lo publicitan como un "beneficio social" para que los Cuerpos y Fuerzas de Seguridad, puedan a través de dicha tecnología predictiva, prevenir delitos, faltas o conductas incívicas, que hoy está tan de moda a causa de la pandemia que sufrimos.

La limitación de cómo afecta a los derechos y libertades fundamentales de la personas, para preservar su intimidad, puesto que éstas no ceden, ni presta su consentimiento expresamente, para que dichos datos personalísimos, como la imagen del rostro, voz, medidas antropomórficas o cualquier otro dato de índole personal, puedan ser empleados por la Fuerzas del Estado y Seguridad, en aplicación de la policía predictiva, choca con el avance de las tecnologías y algunos de los derechos fundamentales tales como el derecho a la intimidad o privacidad y la protección de datos personales con la Agencia Española de Protección de Datos en España. A pesar de ello, en distintas corporaciones locales como en Castellón, Valencia, A Coruña o incluso la policía municipal de Rivas Vaciamadrid, se han realizado licitaciones con distintas empresas privadas en las que el modelo técnico se basa en un modelo matemático que analiza, predice y previene delitos y/o "actos incívicos" adaptando las jornadas de los agentes de policía para prevenir estas conductas con la finalidad de aumentar la eficacia y productividad de los servicios policiales.

III. APLICACIÓN DE LOS DISTINTOS SISTEMAS DE INTELIGENCIA ARTIFICIAL Y SU REPERCUSIÓN PRÁCTICA

Los algoritmos se diseñan para que se apliquen en un tipo de delito concreto, lugar concreto o en un grupo de individuos concreto. Algunos autores establecen que el agente de policía al introducir los datos en el modelo obtiene unos resultados, sin saber cómo se ha llegado a él, lo que puede llevar a dos escenarios distintos. El primero que el agente policial, puede que no tenga en cuenta las recomendaciones que establece el sistema y optará por basarse en su experiencia profesional y el segundo; que interprete que el resultado del algoritmo es óptimo para tomar una decisión sin fijarse en los resultados dados por el sistema.

La mayor alarma social se concreta en delitos o bien de agresión sexual o los cometidos en el ámbito de la pareja, realizándolos en la mayoría de las ocasiones sin premeditación y planificación, dependiendo en la mayoría de las ocasiones de la situación que no forman parte de un patrón. Según el portal estadístico de criminalidad, los delitos sexuales (excluidas las

agresiones sexuales con/sin penetración y los abusos sexuales con penetración) a nivel nacional desde el 2015 al 2019 han aumentado considerablemente, pasando de la cifra 1.306 en 2015 a 1.774 en 2019 o del delito de amenazas y coacciones pasando de la cifra 10.607 en 2015 a 12.782 en 2019.

En España se han desarrollado distintos métodos de policía predictiva, como son los procesos para prevenir y detectar la captación de los internos en Centros Penitenciarios, para prevenir el radicalismo, evaluando el riesgo utilizando herramientas que existen a nivel internacional pero adaptándolas a los centros penitenciarios españoles, empleando esta herramienta a los internos que han cometido delitos de terrorismo y poder así detectar si son vulnerables de ser captados otros internos o ya están en la fase de captación. Similar caso ocurre, con las víctimas de violencia de género que, como es conocido, por medio de la valoración de riesgo policial, desde que la denunciante, o supuesta víctima de violencia de género, a través de las preguntas que les realizan los agentes de policía y por medio de esos logaritmos que constan en el programa especial de valoración de riesgo, se obtiene un resultado que en la mayoría de las ocasiones es bastante coincidente con la realidad de la situación de peligro que ha podido tener o que tendrá la denunciante, en el supuesto de que haya reiteraciones de violencia física o psicológica respecto de la misma persona, pudiendo desde ese momento intervenir la policía para aminorar dicho peligro o prevenir el posible delito de violencia.

En la práctica en los delitos de violencia contra la mujer, cuando al realizarse de oficio este examen de valoración de riesgo en las víctimas de Violencia de Género, por ejemplo, las partes personadas en el procedimiento judicial hacen vista del resultado del informe de valoración del riesgo, les ayuda para hacerse una idea de la envergadura del delito que se haya podido cometer, puesto que dependiendo del resultado de dicha herramienta, no será lo mismo tener una nivel bajo que de riesgo que un riesgo extremo, permitiendo así a las acusaciones personadas en fase de diligencias y en base al resto de indicios, llegar incluso a pedir una medida cautelar de privación de libertad.

Cambiando de orden y en otro escenario más relajado, se ha llegado a realizar por las empresas privadas, rastreos en las redes sociales de los contenidos en inglés y en español y en italiano, de comentarios intenciones y/o comportamientos que son potencialmente peligrosos, unas semanas antes de que se jugara un partido de futbol altamente rivales y mediáticos, entre la Roma y el Real Madrid. Lo que conlleva a pensar de la importancia que de aquí a poco tiempo, tendrá que asumir el legislador puesto que actualmente nuestro Código Penal, no tiene regulado de qué manera se puede valorar esta prueba preparatoria, antes de cometer, por

ejemplo delitos de lesiones o para acreditar la pertenencia a organización criminal por su ideología política, identificada con su equipo de fútbol, llegando a instalar vigilancia de cámaras en aeropuertos, bancos, estadios, en vehículos y transporte públicos, como sucede en Dubai, que su policía, circula con patrullas, que se llaman Ghiath y que están equipadas por un sistema de inteligencia artificial y un sistema de reconocimiento facial para anticipar situaciones de peligro. Si traemos este ejemplo a España, no podemos obviar, que se estaría vulnerando varios principios, como el de libertad ambulatoria derecho a la intimidad o privacidad y la protección de datos personales y además vulneraria nuestra carta magna, puesto que todo condenado y ejecutado que haya cumplido su pena, tiene derecho a reinsertarse en la sociedad y no por ello, aparecer incluido en un fichero de "*ciudadanos altamente peligrosos*" o "*ciudadano peligroso*", porque ¿qué ocurriría, por ejemplo, con un investigado sobre el que se acordara el sobreseimiento provisional y al cabo de los años se reaperturara esa causa? Evidentemente, los algoritmos no serían del todo reales, por lo que el resultado no sería acorde a la realidad y se vería atacada su imagen y su intimidad, amparados por el Estado de Derecho.

IV. RESULTADOS DEL EMPLEO DE LA POLICÍA PREDICTIVA Y SU REPERCUSIÓN EN DERECHO PENAL

En otro orden, en España se ha desarrollado la primera herramienta con una precisión de más del 90% que estima la posibilidad de que una denuncia por robo con violencia e intimidación sea falsa, medio que emplea la policía nacional desde hace más de 4 años y que está siendo muy efectiva, se llama Veripol. Generalmente, este tipo de denuncias contra el patrimonio, se realizan por falsos denunciantes que lo que pretenden en la mayoría de las ocasiones es engañar a una compañía aseguradora y así obtener un enriquecimiento injusto e ilícito, sin que lleguen a ser delincuentes ordinarios, simplificando y facilitando mucho la investigación policial.

Existen otras herramientas como los drones que emplea la policía, por ejemplo, recientemente en Alicante, la policía local pudo localizar seis botellones localizados desde el aire llegando a disuadir a más de 130 jóvenes identificados que estaban cometiendo una conducta restringida por el coronavirus. En Madrid, la policía municipal los ha empleado para controlar los accesos de las zonas que han estado restringidas y evitar el aumento de contagios de coronavirus, durante el estado de alarma, pudiendo así detectar las infracciones cometidas por los ciudadanos y poder identificar y sancionar. Los drones se están utilizando para operaciones aéreas y

supervisar no solo espacios urbanos sino también en los espacios naturales y controlar vertidos ilegales, construcciones ilegales, proteger la flora y fauna, o incluso apoyar controles de alcohol y drogas o accidentes de tráfico, o incluso delitos aéreos como volar en aeronaves no tripuladas que vuelan en zonas no permitidas, pudiendo identificar al piloto infractor y proceder a denunciarlo. En definitiva, a través de las distintas herramientas, ya sea por algoritmos en herramientas de prevención o por medio de drones o de cualquier otro medio que desarrolle la IA, la prevención en los delitos está siendo un éxito en la actualidad.

Si trasladamos estas herramientas al derecho penal, la licitud del tratamiento de los datos, la determinará la licitud de cómo se han obtenido, así que, si se han obtenido de manera que se haya vulnerado alguna ley, por ejemplo, en el supuesto con los drones, (ya sea de aviación nacional o la normativa de sanciones de la LOPD) sería ilícita y por lo tanto no tendría ninguna validez, ni podría emplearse de ninguna manera. Para que sea consumado el delito hace falta el uso de ese instrumento electrónico para grabar sonidos y/o imágenes y además tener el ánimo de descubrir algo de alguien o vulnerar su intimidad (elemento objetivo y subjetivo). Por lo que si el fin para el que se emplea es para prever futuros delitos no afectarían ni a la intimidad ni seria constitutiva de delito.

V. CONCLUSIONES

Primera.–Por todo ello lo más destable, en mi opinión, es que para el empleo de los distintos instrumentos que dota y dotará esta policía preventiva, es que para obtener unos resultados fructíferos y se puedan plasmar satisfactoriamente en juicio oral, condenando al culpable o absolviendo al inocente, es que a pesar de que la captación de imágenes y sonidos en lugares públicos en el desarrollo de investigaciones y los seguimientos que realicen los cuerpos y fuerzas de seguridad no se considerarán vulneración de los derechos a pesar de no tener autorización judicial, para evitar posibles sorpresas en el fallo de la sentencia, y habida cuenta que en Sentencia de la Sala Segunda del Tribunal Supremo. Núm. Res. 329/2016, de 20 de abril de 2016, llegó a absolver a los supuestos culpables, porque la policía vulneró el derecho a la inviolabilidad del domicilio por utilizar los prismáticos y visualizar los actos delictivos que estaban cometiéndose en el interior de la casa los presuntos delincuentes, terminó considerando que dicha prueba era ilícita, porque no existe un fin legitimo para que se permitiera violar ese derecho y la intimidad de los acusados no podría verse vulnerando, por todo ello, y trasladándolo a los medios que emplea la policía predictiva, esa línea tan delgada que separa la vulneración a los

derechos fundamentales (intimidad, privacidad, datos de carácter personal de cada individuo…) debe estar perfectamente acreditado el fin para el que se emplean las distintas herramientas de prevención de delitos.

Segunda.–El avance imparable de las tecnologías y del Derecho, aunque a un compás distinto, pero no menos fructífero, están haciendo que los delincuentes cada vez tengan más difícil la ejecución de sus resultados punibles y uno de sus principales limites se encuentran precisamente en la inteligencia artificial y el uso de algoritmos en la lucha contra la criminalidad.

VI. BIBLIOGRAFÍA

El portal estadístico de criminalidad. Series anuales desglosadas por comunidades autónomas y provincias de los principales indicadores estadísticos de criminalidad. Web. https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico.

GONZÁLEZ-ÁLVAREZ, J. L., SANTOS-HERMOSO, J. & CAMACHO-COLLADOS (2020). *Policía predictiva en España. Aplicación y retos de futuro.* Behavior & Law Journal, 6(1), 26-41.

Periódico El Salto. Autores; Aitor JIMÉNEZ y Ekaitz CANCELA, articulo de fecha 4 febrero 2021.

Patricia RODRÍGUEZ GALVÁN, *Regulación del uso de drones y sus límites en el ámbito penal*, febrero 2019, pp. 32-54.

VII. ANEXO JURISPRUDENCIAL

– STS 329/2016, de 20 de abril (FJ Segundo, Tercero y Cuarto) (113/2015).

El impulso procesal y la inteligencia artificial

The Impulse of the Process and Artificial Intelligence

Francisco Vega Agredano

Juez Sustituto y Abogado
Máster ISDE y Máster URJC, Doctorando UMA Derecho Privado Especial

Resumen: La IA aplicada al proceso judicial puede lograr una mayor eficiencia en el funcionamiento de la administración de justicia, pero también puede generar consecuencias indeseadas sobre la tutela judicial efectiva. La IA no es infalible y puede generar grave riesgos en la transparencia del proceso, siendo el legislador quién pondere los intereses en juego para valorar la asunción del riesgo que conlleva la aplicación de esta nueva tecnología. La IA nunca deberá sustituir al juzgador en su toma de decisiones, sino que puede ser útil como herramienta de apoyo y asistencia en el impulso procesal de las fases procedimentales.

Abstract: *AI applied to the judicial process can achieve greater efficiency in the functioning of the administration of justice, but its application may generate unwanted effects and affect effective judicial protection. The AI system is not infallible and creates serious transparency risks. The legislator must weigh the interests at stake and assess whether it is worth taking the risk involved in applying this new technology. In any case, the AI should never replace the judge in their decision-making but can serve as support and assistance tool in the impulse of the different phases of the process.*

Palabras clave: Inteligencia artificial, sesgos, patrones, tutela judicial efectiva, riesgos, impulso procesal, proceso judicial, algoritmos, transparencia.

Keywords: *Artificial intelligence, biases, patterns, effective judicial protection, risks, procedural impulse, judicial process, algorithms, transparency.*

SUMARIO: I. INTRODUCCIÓN. II. EL BIG DATA Y LA INTELIGENCIA ARTIFICIAL EN SU APLICACIÓN PROCESAL. III. INTELIGENCIA ARTIFICIAL Y TUTELA JUDICIAL EFECTIVA: INCONVENIENTES. IV. CONCLUSIONES. V. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

La inteligencia artificial (en delante, IA) evoluciona a un ritmo vertiginoso y su rápida consolidación impide predecir con certeza aquellos ámbitos en los que tendrá una mayor incidencia. En efecto, una completa definición de la IA debe aglutinar aspectos considerablemente amplios, pues nos encontramos ante una tecnología omnipresente en la mayor parte de las esferas de la vida social. Sin duda, la IA abre un enorme abanico de posibilidades que lograrán revolucionar múltiples campos profesionales, científicos y sociales. En cualquier caso, todos los sistemas de IA comparten dos elementos, cuales son, el procesamiento masivo de los datos y el uso de algoritmos que establecen reglas lógicas para configurar una respuesta que emule la forma de pensar o actuar de los humanos[1].

Podemos afirmar que la IA tiene una presencia cierta pero invisible que comienza a ser ubicua, ya que en la actualidad es la tecnología que cuenta con una mayor capacidad e impacto disruptivo en la sociedad, utilizando prácticamente todos los ámbitos de la vida social a modo de laboratorio para actualizarse, evolucionar y perfeccionarse[2]. En efecto, The McKinsey Global Institute 20 afirmó rotundamente que la revolución de la IA es "diez veces más rápida y tiene una escala 300 veces mayor" que la Revolución Industrial.

En un Estado de Derecho consolidado como España, debemos evitar resignarnos ante un Justicia notablemente lenta y atrofiada. La complejidad del fenómeno de la saturación de la justicia exige una detenida reflexión que permita adoptar soluciones efectivas y que no sean cortoplacistas, así como reformas legales duraderas que afronten cambios importantes en la estructura del sistema. La IA ha llegado para quedarse y aunque pueda parecer una meta futurista e inalcanzable, debemos plantearnos de manera realista la forma en la que podrá ayudar esta tecnología al impulso y celeridad de los procesos judiciales, sin merma para los derechos de los justiciables.

1. MAYER-SCHÖNBERGER, V. & NEIL CUKIER, K., *"Big data la revolución de los datos masivos"*, Madrid, Editorial Turner, 2013, p. 13.
2. VEGA IRACELAY, J. J., "Introducción. La relevancia de la IA para la economía, la sociedad y el derecho", *Revista Iberoamericana de Derecho Informático (segunda época)*, núm. 5, 2018, pp. 16-19.

He tratado de imprimir a las próximas líneas un realismo práctico, evitando cuestiones irrealizables, sin ninguna intención de establecer dogma alguno sobre los beneficios de la IA. El fenómeno es lo suficientemente serio, desaconsejando conclusiones aventuradas y tratándose más bien, de analizar objetivamente la aplicabilidad práctica de la IA, con sus ventajas, riesgos e inconvenientes. En efecto, siendo innegable su utilidad práctica como un nuevo instrumento en el impulso de los procedimientos y trámites procesales, no podemos desconocer que existen grandes riesgos e inconvenientes en su aplicación.

La idea sobre la que se debe centrar el análisis de utilidad de la IA recae en la posible automatización de las oficinas judiciales, salvaguardando siempre la tutela judicial efectiva reconocida en el artículo 24 CE., evitando la merma de derechos y la indefensión de la partes. Lógicamente, cualquier intervención de la IA en el impulso procesal debe ser supervisada en todo momento por el personal de la oficina judicial y, en último término, por el Laj y el Juez, sin permitir que las técnicas gocen de una autonomía y un automatismo absoluto. Se trata de alcanzar el objetivo final de forma segura, es decir, lograr que la IA no solo se aplique en el ámbito teórico de las grandes bases de datos, sino que trascienda al mundo práctico del derecho procesal. En realidad, no se trata de crear una capacidades racionales iguales a las del ser humano, sino más bien combinar algoritmos, para que las máquinas sean capaces de automatizar procesos a través de generalizaciones sucesivas derivadas del aprendizaje de datos.

En cualquier caso, debe quedar claro que el presente artículo de investigación se centra en la posible aplicación de la IA, no a la toma de decisiones de derecho material por el Juez o el Laj y que todavía hoy día, como tendremos ocasión de comprobar, parece algo lejana en el tiempo. Se trataría más bien de la aplicabilidad de la IA en la toma de decisiones dentro del ámbito del derecho formal, a través del cual, los procedimientos se impulsan y avanzan a lo largo de cada una de las fases procesales, incluyendo el seguimiento de la fase ejecutiva. En efecto, se trataría de aplicar la IA en el aspecto externo de la actividad judicial, es decir, en los trámites o en la parte más mecánica de la labor de enjuiciar, formada por el proceso de búsqueda de referentes legales, doctrinales y jurisprudenciales[3].

II. EL BIG DATA Y LA INTELIGENCIA ARTIFICIAL EN SU APLICACIÓN PROCESAL

La administración de justicia se ha convertido en un complejo entramado burocrático que va mucho más allá de las Salas de Justicia y que

3. NIEVA FENOLL, J., *"Inteligencia artificial y proceso judicial"*, Madrid, Marcial Pons, 2018.

cuenta con grandes dotaciones materiales y personales. Cientos de órganos servidos por miles de personas se desenvuelven día a día dentro del ámbito de la administración de justicia, tratando de cooperar para lograr una justicia más ágil. La realidad demuestra que la administración de justicia se encuentra saturada y el trabajo incesante del personal resulta a todas luces insuficiente para acelerar los procedimientos judiciales. Los ciudadanos acuden a la justicia con frecuencia para la resolución de sus conflictos, exigiendo el moderno tráfico jurídico una mayor agilidad, celeridad y, en definitiva, una mayor seguridad jurídica.

La IA es para algunos autores una combinación de eufemismo y desiderátum[4]. Por un lado, se entiende como un término eufemístico ya que realmente se basa en un sistema de tratamiento y análisis automático de información, no obstante, esa definición es poco atractiva[5]. Por otro lado, es deseo ya que estos sistemas descansan sobre la auténtica voluntad de dotarlos de una inteligencia capaz de imitar los procesos cognitivos de los seres humanos[6]. En la doctrina científica, la IA aparece definida por primera vez en el año 1955 por John McCarthy, profesor de Standford, que en una conferencia que organizó en la Universidad de Darmouth planteó unos novedosos objetivos considerados el origen de la IA. El profesor definió la IA como *"la ciencia y la ingeniería de fabricar máquinas inteligentes, en especial máquinas inteligentes de computación"*, entendiendo por inteligente la parte informática orientada a obtener resultados.

En definitiva, se trata de buscar la mejor solución para el objetivo pretendido, basándose en el procesamiento de millones de datos y en el conocimiento. Básicamente, los algoritmos forman la compleja estructura interna de las herramientas de IA y tratan de almacenar todas las opciones y combinaciones posibles ante una eventualidad, analizando la mejor respuesta posible o la mejor toma de decisión. La IA basa su predicción en la gran cantidad de datos que analiza para formular posteriormente todas las combinaciones posibles, es decir, los algoritmos usan una base de datos que se ordenan de manera comprensible[7]. Los datos y la

4. MIRÓ LLINARES, F., *"El modelo policial que viene: mitos y realidades del impacto de la inteligencia artificial y la ciencia de datos en la prevención policial del crimen"* en: Libro Blanco de la Prevención y Seguridad Local Valenciana, Valencia, 2019, pp. 98-113.
5. BORGES BLÁZQUEZ, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal*", IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, núm. 2, 2020, pp. 54-71.
6. MIRÓ LLINARES, F., "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, núm. 20, 2018, pp. 90-91.
7. BAMBAUER, J. & ROGERS, J. E., "The Algorithm Game", *Notre Dame Law Review*, núm. 1, 2018, p. 7.

información deben recopilarse previamente para poder ser analizada por los sistemas de IA, siendo en la actualidad las herramientas de Big Data las que se encargarán de tal proceso. Se debe destacar la importancia de garantizar en todo momento, tanto la privacidad de los individuos cuyos datos se recopila, como la protección de los datos personales de estos.

La gran cantidad de información obtenida mediante los nuevos sistemas de Big Data hace posible una aplicación prácticamente indefinida de los sistemas de IA dentro de un horizonte incierto, combinando el procesamiento y almacenamiento de la información con los algoritmos, que a su vez incluyen múltiples fórmulas y combinaciones. La clave reside en la necesidad de almacenar y recuperar grandes cantidades de información conceptual en las bases de datos inteligentes, con el objetivo de lograr una fructífera sinergia entre IA y Derecho[8]. Precisamente por ello, los sistemas de IA en general y los algoritmos en particular, han visto en las herramientas de Big Data a su mejor aliado.

La IA se está consolidando en multitud de ámbitos, aunque gran parte de la población que no especialista, no es totalmente consciente de ello. Dentro del ámbito europeo, aprecian la relevancia de estas nuevas tecnologías de IA, de tal forma que el propio Parlamento Europeo ha exigido que en todo momento se garanticen los derechos fundamentales incluidos en la Carta de Derechos Fundamentales de la Unión Europea, junto a las normas de la Unión sobre privacidad y protección de datos, y de manera especial, la Directiva (UE) 2016/680. La aplicación de la IA al ámbito judicial no es ciencia ficción sino una realidad que ya está aquí, tal y como expresa el Informe del Comité de Asuntos Legales del Parlamento Europeo, de 27 de enero de 2017. En efecto, dicho informe al tratar las cuestiones jurídicas vinculadas a la robótica y la inteligencia artificial en la Unión Europea concluye que la incorporación de la tecnología en el ámbito judicial va en aumento, siendo una realidad que ha venido para quedarse[9]. Por otro lado, respecto de la IA, el Consejo Consultivo del Convenio 108 ha aprobado como herramientas de derecho dúctil o soft law dos guías, la primera en 2018, dedicada a arrojar luz sobre la forma de utilizarse las más modernas TIC para prevenir y combatir los crímenes; la segunda en enero de 2019, sobre la forma de usar la IA y sus posibles consecuencia para la protección de los datos[10].

8. LÓPEZ ONETO, M., "*Artificial Intelligence and Law*", en Fundamentos para un Derecho de la Inteligencia Artificial ¿Queremos seguir siendo humanos?, Tirant lo Blanch, Valencia, 2020, pp. 173-177.
9. MUÑOZ RODRÍGUEZ, A. B., "El impacto de la inteligencia artificial en el proceso penal", *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, núm. 36, 2020, pp. 695-728.
10. Consejo Consultivo del Convenio 108. Practical guide on the use of personal data in the police sector and new guidelines on artificial intelligence and data protection.

La mayor parte de la actividad interna de los juzgados es mecánica, ya que los funcionarios trabajan utilizando formularios de resolución en los que se modifican datos e informaciones que únicamente sirven para personalizar el proceso. También el Juez y el Laj invierten gran parte de su tiempo en la búsqueda de jurisprudencia de casos similares con independencia de la naturaleza del proceso o del orden jurisdiccional. El Big Data tiene su fundamento precisamente en la reutilización de datos que fueron obtenidos con una primera finalidad diferente a esa segunda y nueva finalidad. Ese aspecto es básicamente el que dota de beneficios y eficacia al Big Data[11]. El Big Data unido a la IA, permitirá reducir costes y mejorar la productividad en el funcionamiento de la administración de justicia, a la vez que aumentará exponencialmente el análisis predictivo.

La ventaja estratégica se basa fundamentalmente, en lograr una gran cantidad de información relevante y poder predecir el comportamiento del proceso en sus diferentes fases. Pues bien, en temas cuya resolución o avance depende básicamente de cuestiones meramente formales, o de requisitos o presupuestos procedibilidad, etc., y que hoy son multitud, la IA podrá ayudar y facilitar el conjunto de argumentos legales aplicables proponiendo ciertas decisiones[12]. También es posible que, de forma paralela, el uso de la IA pueda mejorar la transparencia del proceso y el acceso de los ciudadanos a la justicia. Precisamente la transparencia es un moderno principio de actuación básico hoy en las Administración. Por último, en la llamada resolución extrajudicial de conflictos online (Online Dispute Resolution o su abreviatura ODR) la IA puede aportar beneficios aún mayores para todas las partes. Puede servir como ejemplo, el uso de técnicas de justicia predictiva en compañías aseguradoras, que calculan y evalúan las posibilidades de éxito de acudir a los tribunales y, en función del porcentaje de éxito, acuden a los sistemas de resolución extrajudicial o a la vía judicial[13]. Sin duda, las peculiaridades de los conflictos sobre consumo, entre otros, facilitan que los programas informáticos desempeñen un interesante aporte en la resolución de conflictos, estandarizando respuestas ágiles, rápidas, económicas y predecibles[14].

Recuperado el 16 de julio de 2021 en https://rm.coe.int/practicalguide-on-the-use-of-personal-data-in-the-police-sector-couv-/16807913b4 y https://rm.coe.int/guidelineson-artificial-intelligence-and-data-protection/168091f9d8.

11. GIL GONZÁLEZ, E., "Big data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?", *Diario La Ley*, núm. 9050, 2017.
12. *Ídem.*
13. CASTELLANO PERE, S., "Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?", *Revista de los Estudios de Derecho y Ciencia Política*, núm. 33. 2021.
14. BARONA VILAR, S., "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES*, núm. 1, 2019, pp. 1-17.

III. INTELIGENCIA ARTIFICIAL Y TUTELA JUDICIAL EFECTIVA: INCONVENIENTES

La implantación y consolidación de la IA en el ámbito de la justicia debe recaer sobre el proceso y su avance, es decir, debe constituir un medio instrumental que no interfiera en la formación de la opinión, ni tampoco en la toma de decisión del juzgador[15]. En efecto, la parte procesal del procedimiento se divide a su vez entre la tramitación y búsqueda de datos, por una parte, y la actividad mental que supone el enjuiciamiento por otra[16]. La función de juzgar y hacer ejecutar lo juzgado corresponde en exclusiva a los jueces y magistrados, según el artículo 117 de nuestra Constitución. Sin embargo, fuera de este ámbito, puede resultar infinitamente más fácil conjugar el derecho a la tutela judicial efectiva con las ventajas de la IA. En la actualidad, no podemos forzar la realidad y tratar de aplicar la IA a la toma de decisiones materiales sobre el fondo del asunto. Ello es así, por la simple razón de que, la mayor parte de los asuntos exigen una ponderación adecuada de las circunstancias, necesitando una solución que no solo sea objetiva y racional, sino que sea equitativa, proporcional y, en definitiva, justa. Tampoco se puede aplicar las técnicas de IA para tratar de anticipar el sentido de las resoluciones judiciales, cuantificando y analizando detalladamente la actividad de un juzgador concreto reduciendo su margen de discrecionalidad[17].

La aplicación de una solución basada en la norma, en la equidad y en la proporcionalidad, impide acudir a la IA y exige un análisis de todos los elementos del caso más allá de una posible solución basada en los algoritmos. Sin embargo, en aquellos procedimientos en los que, por razones puramente formales se dilata la resolución durante años, la IA sí podría jugar un papel trascendental y acelerar la resolución final. En la actualidad, los esfuerzos de los investigadores especialistas en IA se centran en desarrollar aquellos algoritmos que ponen el foco en el aprendizaje automático o machine learning. El motivo de esto es que este tipo de algoritmos reúnen unas características que les otorga un mayor potencial de impacto, derivado precisamente de su capacidad de aprender a través de las experiencias previas.

El foco de atención para nosotros dentro del ámbito del proceso judicial debe centrarse en los algoritmos de predicción y no tanto en la automatización, es decir, no se debería llegar a un toma automática de la decisión. La predicción es esencial para una gestión y funcionamiento eficientes y,

15. CABRERA FLORENCIA, R., "Inteligencia artificial y su impacto en la justicia", *Revista Iberoamericana de Derecho Informático (segunda época)*, núm. 5, 2018, pp. 85-94.
16. NIEVA FENOLL, J., *"Inteligencia artificial y proceso judicial"*, *op. cit.*
17. CASTELLANO PERE, S., "Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?", *op. cit.*

por tanto, se trataría de un algoritmo de pronóstico automático, pero que no llegaría a adoptar decisiones automáticas sino meramente predictivas, es decir, el automatismo recae únicamente sobre la predicción y el aprendizaje, pero no sobre la decisión. El objetivo final para la perfección de la IA debe ser la búsqueda de la optimización de las predicciones, minimizando los errores y aumentando la fiabilidad. De manera paralela, las técnicas de IA analizarían la actividad judicial y los parámetros de eficiencia en tiempo real, permitiendo interpretar y evaluar la información del funcionamiento de la oficina judicial para implantar mejoras útiles.

En cualquier caso, no siendo posible eliminar el riesgo de error de la IA por completo, todavía no podemos dar carta de naturaleza en la administración de justicia a los algoritmos encargados de dar respuestas automáticas. La idea de un Juez o Laj mecánico y automático que toma decisiones materiales basadas en algoritmos debería ser descartada, al menos, por ahora. En efecto, debemos prescindir de lo que algún autor ha denominado la Industria Inteligente de la justicia o la Ciberindustria de la justicia del futuro, que estaría presidida por una inquietante situación de robotización judicial o juez robot en sustitución del juez persona[18].

Resultan de aplicación a la cuestión diferentes normas aisladas que incrementan la complejidad de fijación de criterios comunes para la aplicación e integración de los sistemas de IA en el ámbito de la justicia. En primer lugar, tenemos el Reglamento 2019/881, de 18 de abril de 2019, relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA). Por otro lado, contamos con la normativa europea en protección de datos, encabezada por el Reglamento 2016/679, de 27 de abril de 2016, que en su artículo 22 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, el apartado segundo del citado artículo excepciona ante los supuestos en los que se establezcan medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado[19]. Asimismo, debemos mencionar que el 21 de abril de 2021 se publicó la versión definitiva de la propuesta de Reglamento (UE) de la Comisión Europea sobre el marco jurídico aplicable a los sistemas de IA, clasificando dichos sistemas en función de cuatro niveles de riesgo. En la propuesta, se regulan los sistemas de IA de alto riesgo y de riesgo medio, estableciendo además una tercera categoría para los sistemas de IA que no se pueden ser incluidos en esas dos categorías anteriores. Se prevé además unos modelos de sistemas de IA prohibidos

18. BARONA VILAR, S., "Cuarta revolución industrial (4.0.) o ciberindustria…", *op. cit.*
19. CASTELLANO PERE, S., "Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?", *op. cit.*

y se incluyen una reglas de transparencia armonizadas para determinados sistemas. Se propone en el texto un ámbito de aplicación subjetivo y territorial amplio, en consonancia con la amplitud de definición de la que hablábamos en el primer apartado de este artículo de investigación.

Una vez más, desde el ámbito europeo se han ponen de manifiesto las grandes incertidumbres de los sistemas de IA debido a los riesgos inherentes a su funcionamiento interno. Los riesgos se han manifestado fundamentalmente en orden a la exigencia de transparencia y trazabilidad de los algoritmos. También se ha puesto de relieve la necesidad de realización de evaluaciones obligatorias del impacto sobre los derechos fundamentales antes del despliegue de cualquier sistema de IA, debiéndose ejecutar auditorías obligatorias sobre estos sistemas[20].

Uno de los principales motivos para excluir aquellos algoritmos que ponen el foco en el aprendizaje automático o machine learning, es el hecho de estos están basados en el deep learning o aprendizaje profundo[21]. El principal inconveniente de este tipo de algoritmo, sobre todo desde la óptica del derecho público, es la falta de transparencia que caracteriza a estas clases de algoritmos, al modificarse y perfeccionarse sin que el usuario sea capaz de descubrir fácilmente el motivo por el que el algoritmo ha adoptado una decisión o ha producido un determinado resultado[22]. La publicidad de la estructura interna de los algoritmos y del motivo de la toma de decisiones o predicciones, en un sentido u otro, es algo que debe solucionarse de antemano para lograr que los algoritmos puedan implantarse dentro del sistema judicial sin merma para los derechos de las partes. Los justiciables deben conocer la regla que llevaría a un algoritmo a decidir en un sentido determinado entre todas las combinaciones posibles, ya que únicamente de ese modo existiría una auténtica transparencia.

La IA no se alimenta única y exclusivamente de cifras, ya que la herramienta requiere datos que se corresponden con variables concretas que interactúan entre sí y con información social de la vida real, es decir, de un mundo que está lleno de prejuicios[23]. En efecto, el contexto y la programación se realizan por seres humanos, quienes en virtud de la información

20. MUÑOZ RODRÍGUEZ, A. B., "El impacto de la inteligencia artificial en el proceso penal", *op. cit*.
21. CASTELLANO PERE, S., "Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?", *op. cit*.
22. CERRILLO I MARTÍNEZ, A., "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", *Revista General de Derecho Administrativo*, núm. 50, 2019.
23. BORGES BLÁZQUEZ, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal", *op. cit*.

que adecúan y los algoritmos que generan para relacionar las variables, determinan el posible comportamiento predictivo[24]. La idea es evitar la parcialidad y los sesgos premeditados e interesados, pero también evitar sesgos introducidos por el mero subconsciente opaco, o por los patrones de comportamiento que se repiten en el modo de actuar humano. En los procesos simples no deben existir inconvenientes. Sin embargo, a medida que el proceso de análisis de variables y selección de soluciones aumenta en complejidad, el algoritmo comienza a apoyarse en nuevas variables basadas en el contexto[25], siendo posible que al tomar la decisión haya asignado una importancia capital a una variable, y que esta a su vez haya tenido presente los patrones del actuar humano.

Nos encontramos ante herramientas informáticas cuya configuración puede haber sido orientada en función de un interés determinado, con el objeto de propiciar variables orientadas en su mayoría en un sentido concreto. Lo anterior, ocasionaría una enorme inseguridad jurídica, así como multitud de impugnaciones y nulidades derivadas de la parcialidad y subjetividad. Por otro lado, para aumentar la complejidad del asunto, podemos afirmar con carácter general que los algoritmos deben ser igualitarios, no discriminatorios y sometidos a la ley. Pero en tal caso, si fuese así con carácter absoluto, podríamos desatender situaciones en las que el legislador ha optado por ser parcial a favor de una de las partes dada su posición de desigualdad frente a la otra[26]. En estos casos se podría solucionar el problema configurando el algoritmo de forma que tenga en cuenta determinadas circunstancias no igualitarias, pero ello supondría un grave riesgo en el proceso de toma de decisiones automáticas del algoritmo.

El derecho de defensa y la igualdad de las partes en el uso de las diversas herramientas procesales ocasiona, que las partes deban tener un total acceso a los criterios de toma de decisión o razonamiento de la herramienta de IA utilizados por el sistema judicial. En efecto, en caso de no ser así, existe un claro riesgo de que los mismos algoritmos que pueden promover la eficiencia en la administración de justicia, también pueden reforzar discriminaciones históricas u obscurecer comportamientos indeseables[27].

24. RINCÓN CARDENAS, E. & MARTÍNEZ MOLANO, V.," Un estudio sobre la posibilidad de aplicar la inteligencia artificial en las decisiones judiciales", *Revista direito GV*, núm. 1, 2021, pp. 1-29.
25. O'DONNELL, R. M., "Challenging racist predictive policing algorithms under the equal protection clause", *New York University Law Review*, núm. 3, 2019, p. 551.
26. DE ASIS PULIDO, M., "La incidencia de las nuevas tecnologías en el derecho al debido proceso", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, núm. 2, 2020, pp. 186-199.
27. PONCE SOLÉ, J., "Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", *Revista General de Derecho Administrativo*, núm. 50, 2019.

IV. CONCLUSIONES

La revolución tecnológica que ha supuesto la introducción de la IA puede ser extendida con prudencia y sosiego al Derecho Procesal. De esta forma, la IA puede jugar un papel trascendental en el ámbito practico de la actividad diaria de los Juzgados y Tribunales. Su función principal como herramienta complementaria en la ordenación e impulso de los procesos judiciales, supervisada en todo momento por personal de la oficina judicial, puede ser especialmente útil como técnica de predicción judicial.

La IA implantada dentro del funcionamiento de las oficinas judiciales, permitirá la adquisición, procesamiento e interpretación de datos a través de los sistemas informáticos, identificando y seleccionando la mejor solución para el objetivo planteado. En efecto, dentro del ámbito burocrático de la oficina judicial será donde mayor aplicación práctica puede tener la IA, y más concretamente en la tramitación de los expedientes judiciales a lo largo de las diferentes fases del proceso. Para lograr el objetivo anterior, se debe conjugar el lenguaje informático con el lenguaje jurídico, haciéndolo accesible a todos los operadores.

La lógica jurídica tradicional, es decir, el silogismo judicial, debe evolucionar hacia una lógica jurídica más amplia que incluya el desarrollo de nuevos instrumentos informático-jurídicos[28]. No se trataría en ningún caso de la sustitución del lenguaje jurídico tradicional o "natural" por el lenguaje informático, sino establecer con claridad y precisión el ámbito exacto donde llevar a cabo traducciones del lenguaje jurídico al lenguaje informático, para que los sistemas de IA logren funcionar y evolucionar correctamente de forma transparente.

Ya desde hace años existe la denominada jurimetría, basada fundamentalmente en el análisis de precedentes jurisprudenciales dentro de una óptica conductista aplicada a la informática jurídica, de manera que se traduce o convierte el lenguaje jurídico en lenguaje simbólico de las matemáticas y la lógica, con el objeto de realizar estadísticas jurídicas y estrategias de comunicación e incluso de defensa[29]. Pues bien, siguiendo el mismo esquema, podríamos trasladar esa idea central al ámbito de funcionamiento de la oficina judicial e impulsar el procedimiento a través de la IA. Respecto al ámbito de la ejecución, el sistema tradicional de comunicación entre los juzgados y los órganos administrativos ralentiza la ejecutividad de las resoluciones en general, y de las medidas adoptadas en particular, hasta el punto de hacerlas inútiles o inoperativas en algunos casos. Pues bien, frente a esa realidad, la configuración de una base sólida

28. CABRERA FLORENCIA, R., "Inteligencia artificial y su impacto en la justicia", *op. cit.*
29. BARONA VILAR, S., "Cuarta revolución industrial (4.0.) o ciberindustria…", *op. cit.*

y estructurada de datos, derivados de la IA, podría tener efectos positivos en la organización y aplicación de las medidas adoptadas en sede judicial[30].

El avance en las herramientas tecnológicas es esencial para superar lastres pretéritos, no obstante, la sociedad requiere una actualización firme, pero sin tener que renunciar a la seguridad jurídica. La implantación de un instrumento como la IA en todos los campos de la vida, exige al mismo tiempo la disminución de riesgos irreparables. La IA no es una herramienta totalmente imparcial, ya que puede llegar a interpretar y reproducir los patrones humanos y los sesgos presentes en la sociedad según lo apuntado en líneas anteriores. Tampoco podemos predicar de estos sistemas su fiabilidad absoluta, ya que cuando el algoritmo trata de interpretar contextos confusos y complejos no tienen presente factores como la equidad y la proporcionalidad.

Los sistemas de IA son el complemento perfecto del Juez o del Laj, pero nunca podrá sustituirlos en la toma decisiones, pues se vulneraría el artículo 117 de nuestra Constitución por todas las razones expuestas a lo largo del presente artículo. El derecho rituario o procesal necesita evolucionar desde sus raíces, adaptando el proceso de manera completa a unos revolucionarios avances tecnológicos, que efectivamente, pueden dotarle de la agilidad y la rapidez que exige el nuevo tráfico jurídico. En efecto, sería conveniente un mayor paralelismo ente los avances tecnológicos propios de la era digital y el hasta ahora rígido derecho procesal, velando en todo momento, eso sí, por el cumplimiento efectivo de los derechos y de los principios informadores básicos en todo proceso.

V. BIBLIOGRAFÍA

BAMBAUER, J. & ROGERS, J. E., "The Algorithm Game", *Notre Dame Law Review*, núm. 1, 2018, p. 7.

BARONA VILAR, S., "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES*, núm. 1, 2019, pp. 1-17.

BORGES BLÁZQUEZ, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, núm. 2, 2020, pp. 54-71.

30. FLORES MARTÓN, J., "Estrategias del íter procesal civil en un supuesto de Derecho de Familia: conducción artificial y humana", *Ius Et Scientia: Revista electrónica de Derecho y Ciencia*, núm. 1, 2021, pp. 85-100.

CABRERA FLORENCIA, R., "Inteligencia artificial y su impacto en la justicia", *Revista Iberoamericana de Derecho Informático (segunda época)*, núm. 5, 2018, pp. 85-94.

CASTELLANO PERE, S., "Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?", *Revista de los Estudios de Derecho y Ciencia Política*, núm. 33.2021.

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

DE ASÍS PULIDO, M., "La incidencia de las nuevas tecnologías en el derecho al debido proceso", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, núm. 2, 2020, pp. 186-199.

FLORES MARTÓN, J., "Estrategias del íter procesal civil en un supuesto de Derecho de Familia: conducción artificial y humana", *Ius Et Scientia: Revista electrónica de Derecho y Ciencia*, núm. 1, 2021, pp. 85-100.

GIL GONZÁLEZ, E., "Big data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?", *Diario La Ley*, núm. 9050, 2017.

LÓPEZ ONETO, M., *"Artificial Intelligence and Law"*, en Fundamentos para un Derecho de la Inteligencia Artificial ¿Queremos seguir siendo humanos?, Tirant lo Blanch, Valencia, 2020, pp. 173-177.

MAYER-SCHÖNBERGER, V. & NEIL CUKIER, K., *"Big data la revolución de los datos masivos"*, Madrid, Editorial Turner, 2013, p. 13.

MIRÓ LLINARES, F., *"El modelo policial que viene: mitos y realidades del impacto de la inteligencia artificial y la ciencia de datos en la prevención policial del crimen"* en: Libro Blanco de la Prevención y Seguridad Local Valenciana, Valencia, 2019, pp. 98-113.

MIRÓ LLINARES, F., "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, núm. 20, 2018, pp. 90-91.

MUÑOZ RODRÍGUEZ, A. B., "El impacto de la inteligencia artificial en el proceso penal", *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, núm. 36, 2020, pp. 695-728.

NIEVA FENOLL, J., *"Inteligencia artificial y proceso judicial"*, Madrid, Marcial Pons, 2018.

O'DONNELL, R. M., "Challenging racist predictive policing algorithms under the equal protection clause", *New York University Law Review*, núm. 3, 2019, p. 551.

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

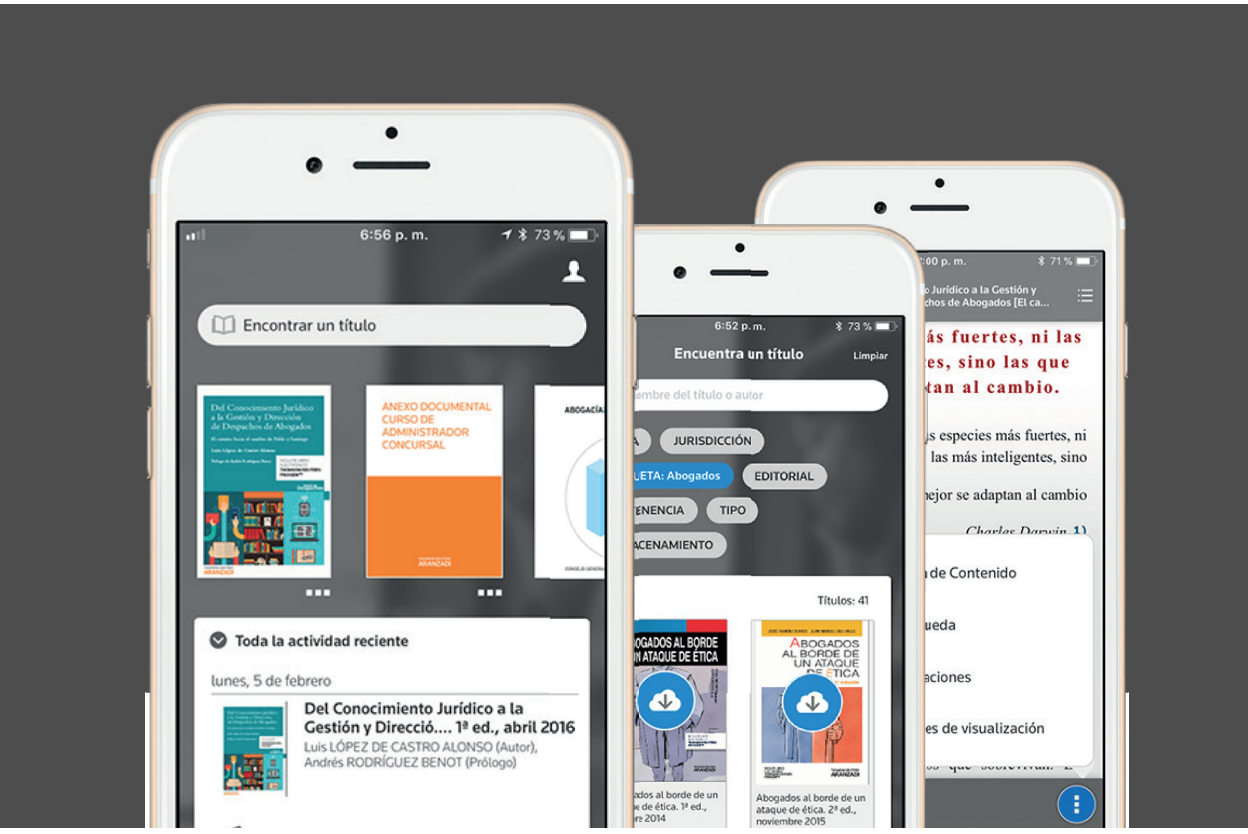
RINCÓN CÁRDENAS, E. & MARTÍNEZ MOLANO, V., "Un estudio sobre la posibilidad de aplicar la inteligencia artificial en las decisiones judiciales", *Revista direito GV*, núm. 1, 2021, pp. 1-29.

VEGA IRACELAY, J. J., "Introducción. La relevancia de la IA para la economía, la sociedad y el derecho", *Revista Iberoamericana de Derecho Informático (segunda época)*, núm. 5, 2018, pp. 16-19.

Thomson Reuters Proview
Guía de uso

¡ENHORABUENA!

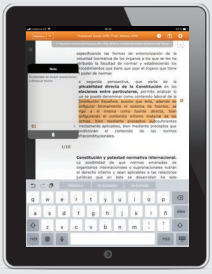
ACABAS DE ADQUIRIR UNA OBRA QUE **INCLUYE LA VERSIÓN ELECTRÓNICA.**
APROVÉCHATE DE TODAS LAS FUNCIONALIDADES.



ACCESO INTERACTIVO A LOS MEJORES LIBROS JURÍDICOS
DESDE IPHONE, IPAD, ANDROID Y
DESDE EL NAVEGADOR DE INTERNET

THOMSON REUTERS®

FUNCIONALIDADES DE UN LIBRO ELECTRÓNICO EN **PROVIEW**



SELECCIONA Y DESTACA TEXTOS
Haces anotaciones y escoges los colores para organizar tus notas y subrayados.

USA EL TESAURO PARA ENCONTRAR INFORMACIÓN
Al comenzar a escribir un término, aparecerán las distintas coincidencias del índice del Tesauro relacionadas con el término buscado.

HISTÓRICO DE NAVEGACIÓN
Vuelve a las páginas por las que ya has navegado.

ORDENAR
Ordena tu biblioteca por: Título (orden alfabético), tipo (libros y revistas), editorial, jurisdicción o área del Derecho.

CONFIGURACIÓN Y PREFERENCIAS
Escoge la apariencia de tus libros y revistas en ProView cambiando la fuente del texto, el tamaño de los caracteres, el espaciado entre líneas o la relación de colores.

MARCADORES DE PÁGINA
Crea un marcador de página en el libro tocando en el icono de Marcador de página situado en el extremo superior derecho de la página.

BÚSQUEDA EN LA BIBLIOTECA
Busca en todos tus libros y obtén resultados con los libros y revistas donde los términos fueron encontrados y las veces que aparecen en cada obra.

IMPORTACIÓN DE ANOTACIONES A UNA NUEVA EDICIÓN
Transfiere todas sus anotaciones y marcadores de manera automática a través de esta funcionalidad.

SUMARIO NAVEGABLE
Sumario con accesos directos al contenido.

THOMSON REUTERS®

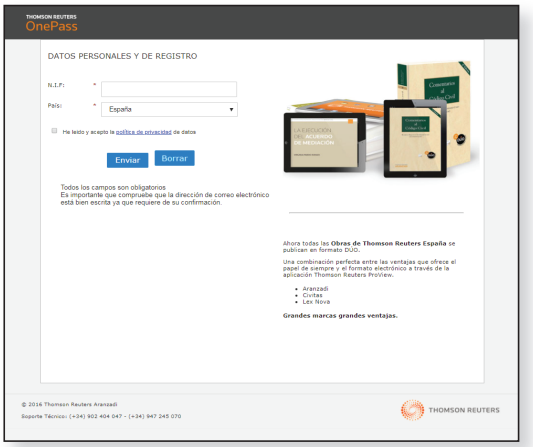
INFORMACIÓN IMPORTANTE: Si has recibido previamente un correo electrónico con el asunto **"Proview – Confirmación de Acceso",** para acceder a Thomson Reuters Proview™ deberás seguir los pasos que en él se detallan.

Estimado/a cliente/a,

Para acceder a la versión electrónica de este libro, por favor, accede a **http://onepass.aranzadi.es**

Tras acceder a la página citada, introduce tu dirección de correo electrónico (*) y el código que encontrarás en el interior de la cubierta del libro. A continuación pulsa enviar.

Si te has registrado anteriormente en **"One Pass"** (**), en la siguiente pantalla se te pedirá que introduzcas el NIF asociado al correo electrónico. Finalmente, te aparecerá un mensaje de confirmación y recibirás un correo electrónico confirmando la disponibilidad de la obra en tu biblioteca.



Si es la primera vez que te registras en **"One Pass"** (**), deberás cumplimentar los datos que aparecen en la siguiente imagen para completar el registro y poder acceder a tu libro electrónico.

- Los campos **"Nombre de usuario"** y **"Contraseña"** son los datos que utilizarás para acceder a las obras que tienes disponibles en **Thomson Reuters Proview™** una vez descargada la aplicación, explicado al final de esta hoja.

Cómo acceder a **Thomson Reuters Proview™:**

- **iPhone e iPad:** Accede a AppStore y busca la aplicación **"ProView"** y descárgatela en tu dispositivo.
- **Android:** accede a Google Play y busca la aplicación **"ProView"** y descárgatela en tu dispositivo.
- **Navegador:** accede a **www.proview.thomsonreuters.com**

Servicio de Atención al Cliente

Ante cualquier incidencia en el proceso de registro de la obra no dudes en ponerte en contacto con nuestro Servicio de Atención al Cliente. Para ello accede a nuestro Portal Corporativo en la siguiente dirección **www.thomsonreuters.es** y una vez allí en el apartado del **Centro de Atención al Cliente** selecciona la opción de **Acceso** a Soporte para no Suscriptores (compra de Publicaciones).

(*) Si ya te has registrado en **Proview™** o cualquier otro producto de Thomson Reuters (a través de One Pass), deberás introducir el mismo correo electrónico que utilizaste la primera vez.

(**) **One Pass:** Sistema de clave común para acceder a Thomson Reuters Proview™ o cualquier otro producto de Thomson Reuters.

THOMSON REUTERS®