



Universidad Miguel Hernández

Facultad de Ciencias Sociales y Jurídicas de Elche

Grado en Derecho



Trabajo Fin de Grado

EL BIG DATA, LA INTELIGENCIA ARTIFICIAL Y SUS IMPLICACIONES EN EL PROCESO

Curso académico 2022/2023

VERONICA ESTEFANIA ROMAN HONORES

Tutora:

Paloma Arrabal Platero

Índice de contenidos

ABREVIATURAS	3
INTRODUCCIÓN	4
1. Epígrafe I: El Big Data	8
1.1. Concepto, características y regulación	8
1.2. El Big Data aplicado al ámbito jurídico.	15
2. Epígrafe II: La inteligencia artificial	21
2.1. La inteligencia artificial: concepto y regulación.	22
2.2. La inteligencia artificial aplicada al ámbito jurídico.	31
2.2.1. En la fase probatoria: la IA como fuente de prueba y su uso en la valoración de la prueba en el marco del proceso penal	41
2.2.2. En las medidas cautelares	46
3. Epígrafe III: Afectación del Big Data y la IA a las garantías procesales y los derechos fundamentales	50
CONCLUSIONES	58
BIBLIOGRAFÍA	59

ABREVIATURAS

ART	Artículo
CAC	Administración del Ciberespacio de China
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CE	Constitución Española
CEPEJ	Comisión Europea para la eficiencia de la justicia o <i>European Commission for the Efficiency of Justice</i>
CGPJ	Consejo General del Poder Judicial
COMPAS	<i>Correctional Offender Management Profiling for Alternative Sanctions.</i>
ENISA	Agencia de la Unión Europea para la Ciberseguridad
FFCCSS	Fuerzas y Cuerpos de Seguridad del Estado
IA	Inteligencia Artificial
IoT	<i>Internet of Things</i>
Ley Orgánica 3/2018	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales
Ley Orgánica 7/2021	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
RAE	Real Academia de la Lengua Española
Reglamento 2019/881	Reglamento 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación
RGPD	Reglamento (UE) 2016/679 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
TC	Tribunal Constitucional
UE	Unión Europea
VioGén	Seguimiento Integral en los casos de Violencia de Género

INTRODUCCIÓN

En el presente trabajo se aborda la compleja y cambiante situación provocada por la irrupción de las tecnologías de inteligencia artificial —en adelante IA— y de Big Data dentro del panorama jurídico actual, analizando cómo se ha regulado, así como sus implicaciones en el proceso judicial, concretamente en el proceso judicial penal. Asimismo se estudia la afectación de la IA y del Big Data dentro de las garantías procesales y los derechos fundamentales de los ciudadanos y las problemáticas que han surgido en torno a dicha afectación.

Durante esta última década hemos asistido al desarrollado exponencial de la IA, pero para encontrar sus orígenes tenemos que remontarnos a finales del siglo XIX¹. En el caso del Big Data, su terminología se emplea de forma generalizada desde finales de los años 90². Se trata de tecnologías presentes en nuestro día a día, las cuales evolucionarán de forma inevitable en el futuro, y es esta imparable transformación la que genera todo un debate en torno a cómo debemos hacer frente a los retos del mañana.

En el año de elaboración de este estudio, 2023, se ha hablado intensamente sobre la IA, el Big Data y las nuevas tecnologías. Medios de comunicación, científicos, empresarios y académicos no dejan de debatir del impacto de estas³. Aplicaciones como *Dall-E*, *Midjourney* o *Stable Diffusion* —que utilizan tecnología de IA—, crean imágenes que parecen tan reales que muchas veces debemos mirarlas más de una vez para constatar que no son reales. Dada la gran calidad que estas tienen, hace que sea atractivo el subirlas a Internet y estas terminen circulando con gran difusión por el ciberespacio. Ejemplo de ello son las fotos del expresidente Donald Trump bregando con policías y siendo forcejeado o del Papa Francisco vestido con una elegante parka de la marca de ropa

¹ En 1854 el matemático George Boole argumenta por primera vez en la historia que el razonamiento lógico podría sistematizarse de la misma manera que se resuelve un sistema de ecuaciones. Para saber más sobre la historia y los orígenes de la IA visítese https://www.nationalgeographic.com.es/ciencia/breve-historia-visual-inteligencia-artificial_14419 (Última fecha de consulta: 14 de agosto de 2023).

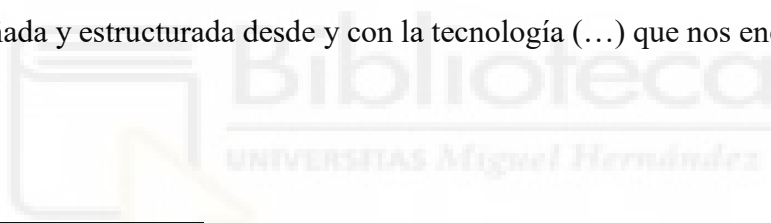
² Aunque el término "Big Data" se utiliza ampliamente desde finales de los 90, la reciente explosión de su uso no abarca los avances realizados en áreas como Internet, los dispositivos móviles y la conectividad. Algunos expertos en Big Data remontan su historia mucho más atrás, incluso a la era paleolítica. Esto puede explicarse por el deseo humano de adquirir y procesar información, que ha estado presente desde la antigüedad. Para más información, visítese en: <https://master-bigdata.com/origen-big-data/> (Última fecha de consulta: 24 de julio de 2023).

³ Dada la magnitud de estas tecnologías, el debate que ha surgido en torno a ellas ha tomado un sin fin de direcciones. Su uso —o su potencial uso— en diferentes campos (salud, agricultura, educación, justicia, etc...) ha llenado artículos periodísticos en donde se analiza y se debaten entre los pros y contras del uso de estas tecnologías. Algunos de estos son: <https://news.un.org/es/story/2023/07/1522542> <https://www.tendencias.kpmg.es/2023/06/inteligencia-artificial-generativa-apocalipticos-vs-integrados/> (Última fecha de consulta: 07 de septiembre de 2023).

Balenciaga⁴. Pero más allá de las creaciones que circulan en Internet, gracias a la IA podemos vislumbrar una realidad paralela, véase sino la maniobra publicitaria de Cruzcampo que "resucitó" a la leyenda del folclor ibérico Lola Flores para un anuncio comercial en 2021⁵.

Sin embargo, no sólo estas aplicaciones revolucionan Internet. La aparición de ChatGPT —la plataforma con mayor relevancia en la actualidad— ha impactado en el mundo de la tecnología⁶. Se trata de una herramienta de IA capaz de imitar la redacción humana con gran precisión y forma parte de una nueva oleada de aplicaciones y sitios web cada vez más sofisticados que tienen la capacidad de retroalimentarse con cada actividad y "aprender" con cada interacción⁷. En el mismo sentido, podemos encontrar también las aplicaciones *Claude 2* o *Bing*, esta última desarrollada por Microsoft.

Toda esta transformación, que viene de la mano del desarrollo tecnológico nos hace ser testigos en primera persona de la llamada “Cuarta Revolución Industrial”, autores como BARONA VILAR describen como aquella en la que una sociedad está “basada, diseñada y estructurada desde y con la tecnología (...) que nos encaminan hacia



⁴ Sobre la foto del Papa con la parka blanca, podemos observar que dicha publicación original de Twitter, lleva ya más de 27,7 millones de reproducciones. Para ver la imagen en cuestión visítese: https://twitter.com/skyferrori/status/1639647708154675200?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1639647708154675200%7Ctwgr%5Ef79bd3730eadcb2e753864e3aeb9fe563b0bd%5E%26ref_url=https%3A%2F%2Fwww.vozdeamerica.com%2Fa%2Fpeligros-ia-desinformacion-verificacion-datos%2F7037582.html (Última fecha de consulta: 24 de julio de 2023).

⁵ Este anuncio publicitario que muchos creyeron que era una entrevista de archivo de la cantante pero resultó ser uno de los mejores *deepfakes* que hemos podido ver en publicidad. Véase el comercial de Cruzcampo, “Con Mucho Acento” en <https://www.youtube.com/watch?v=Yewm6TfLZ3Q> Video publicitario de Cruzcampo, “Así se hizo #ConMuchoAcento”: <https://youtu.be/BQLTRMYHwvE>

⁶ A colación de este escrutinio sobre el uso de ChatGTP no se puede dejar de mencionar el bloqueo que impuso Italia en marzo de 2023 al uso de esta plataforma por incumplir la normativa de protección de datos. Para más información sobre ChatGTP visítese los artículos periodístico de ABC “*La UE tiene en el punto de mira a ChatGPT: ¿es posible que prohíba la inteligencia artificial?*” disponible en <https://www.abc.es/tecnologia/redes/ue-punto-mira-chatgpt-posible-prohiba-inteligencia-20230413114430-nt.html> (Última fecha de consulta 07 de agosto de 2023) y del País “*Italia bloquea el uso de ChatGPT por incumplir la normativa de protección de datos*”. Disponible en <https://elpais.com/tecnologia/2023-03-31/italia-bloquea-el-uso-de-chatgpt-por-incumplir-la-normativa-de-proteccion-de-datos.html> (última fecha de consulta 07 de agosto de 2023).

⁷ Para entender la trascendencia de ha tenido ChatGTP, solo hay que observar que en solo cinco días después de su lanzamiento, llegó a más de 1 millón de usuarios. Según las pruebas de SEO.ai, ChatGPT está disponible en casi 100 idiomas, pero el rendimiento del modelo varía según el idioma (funciona mejor en inglés). Para más información sobre ChatGTP consúltese el artículo periodístico de la BBC “*Qué es ChatGPT, el revolucionario sistema de inteligencia artificial que preocupa a algunos expertos*”, disponible en: <https://www.bbc.com/mundo/noticias-64461255#:~:text=ChatGPT%20es%20b%20C3%A1%20sicamente%20un%20robot,que%20no%20tiene%20este%20objetivo>). (Última fecha de consulta: 24 de julio de 2023).

un mundo inteligente”⁸. Esta, tal y como expresa CORVALÁN, “tiene su epicentro en el aumento exponencial de dos factores: capacidad de almacenamiento y velocidad de procesamiento de la información y de los datos”⁹.

Todos estos cambios hacen que los Estados revisen y actualicen sus legislaciones sobre esta materia, por este motivo el 14 de junio de 2023 en Estrasburgo el Parlamento Europeo aprobaba las enmiendas a la futura Ley de Inteligencia Artificial. En dicho documento se ha esbozado la senda que Europa ha marcado para el uso de esta tecnología. En esta se establece como objetivo “promover en la Unión la adopción de una inteligencia artificial fiable y centrada en el ser humano y garantizar un elevado nivel de protección de la salud, la seguridad, los derechos fundamentales, la democracia y el Estado de Derecho y del medio ambiente frente a los efectos nocivos de los sistemas de inteligencia artificial, apoyando al mismo tiempo la innovación y mejorando el funcionamiento del mercado interno”¹⁰.

Como se puede observar en el presente trabajo, uno de los mayores retos sobre el uso de estas tecnologías reside en la protección de los derechos fundamentales, la democracia y el Estado de Derecho, preocupaciones que se hacen latentes todo el tiempo y que reflejarán las legislaciones en esta materia provenientes de la Unión Europea —en adelante UE—. Los últimos avances en IA y Big Data, están teniendo un impacto significativo en varios campos, incluido el sector jurídico, en sus más variadas manifestaciones. Señala UNESCO que judicaturas, fiscalías y otros órganos judiciales de todo el mundo están explorando el uso de la IA en sus sistemas. Tal como indica este organismo, en el ámbito de la justicia penal muchos sistemas judiciales de todo el mundo ya utilizan sistemas de IA para ayudar en las investigaciones y automatizar los procesos de toma de decisiones¹¹.

⁸ 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*, vol. 3, nº. 1, 2019, pp. 1-17.

⁹ CORVALÁN, J., “Inteligencia artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia”, *Revista de Investigações Constitucionais*, nº1, vol. 5, 2018, 1, pp. 295-316.

¹⁰Extraído de https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.html (última fecha de consulta a 20 de julio de 2023).

¹¹UNESCO en “La IA y el Estado de derecho: Fortalecimiento de capacidades para los sistemas judiciales”. Disponible en <https://www.unesco.org/es/artificial-intelligence/rule-law/mooc-judges> (última fecha de consulta a 20 de julio de 2023).

Con los rápidos avances en este campo, los operadores jurídicos deben considerar los retos y oportunidades relacionados con el uso de estas tecnologías en los sistemas judiciales, así como sus implicaciones para los derechos y garantías de los ciudadanos. Sobre el impacto que tiene esta última idea, el legislativo europeo pone su mayor énfasis debido a los temores que surgen en torno a un mal manejo de estas tecnologías. Los debates en torno al uso e impacto de estas tecnologías en nuestros sistemas judiciales y el nivel de afectación que tiene o que pueden llegar a tener sobre la democracia, el Estado de Derecho, los derechos y garantías de los ciudadanos forman ya parte integrante de la agenda de la UE.

Si bien la materia es extensa y está sometida a una constante evolución, en este proyecto se proporciona información relevante sobre este tema de actualidad. En el primer epígrafe del trabajo se estudia el Big Data, se ofrece una definición y explicación de las características que lo componen, así mismo se analiza la regulación más relevante sobre esta materia. Además se profundiza sobre la aplicación del Big Data en el ámbito jurídico mostrando aplicaciones como PROMETEA, un sistema de software que “tiene como cometido principal la automatización de tareas reiterativas y la aplicación de IA para la elaboración automática de dictámenes jurídicos basándose en casos análogos para cuya solución ya existen precedentes judiciales reiterados”¹².

En el segundo epígrafe se aborda la IA, su concepto y regulación. También se estudia la aplicación de la IA en el ámbito jurídico, proporcionando ejemplos de aplicaciones que ya usan los operadores jurídicos actualmente. Ya entrado en el ámbito procesal, se analiza el uso de la IA en la fase probatoria, con especial atención a la aplicación de la IA como fuente de prueba y sus usos en la valoración de la misma, y el uso de la IA en las medidas cautelares, todo esto en el marco del proceso penal.

Por último, en el tercer epígrafe se estudia la afectación del IA y el Big Data a las garantías procesales y los derechos fundamentales y la problemática que dicha afectación genera en derechos claves en la esfera virtual de los ciudadanos como es el derecho de protección de datos personales, el derecho a la intimidad o el derecho al propio entorno virtual, entre otros.

¹² ESTÉVEZ, E., LINARES LEJARRAGA, S., FILLOTTRANI, P., “*PROMETEA. Transformando la administración de justicia con herramientas de inteligencia artificial*”, 2020.

1. Epígrafe I: El Big Data

En este primer epígrafe se centra en tratar de proporcionar un concepto del Big Data, a la par de profundizar en sus características y ver su regulación en el panorama europeo y nacional. Además se estudia la aplicación de esta tecnología dentro del ámbito jurídico.

1.1. Concepto, características y regulación

En una primera instancia resulta importante tratar de proporcionar un concepto de Big Data (o macrodatos, datos masivos...), pero esta tarea resulta cuanto menos compleja debido a que estamos frente a un concepto en evolución y del que existen numerosas definiciones.

En primer lugar, la Real Academia de la Lengua Española (RAE) define Big Data como el “conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios”¹³.

En segundo lugar, el Parlamento Europeo en su Resolución de 14 de marzo de 2017 precisa el Big Data o macrodatos como: “La recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personales, 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)”¹⁴.

En tercer lugar, a efectos prácticos tomaremos como referencia la definición más conocida, acuñada por LANEY de la consultora Gartner, que define Big Data como “*is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight,*

¹³ Véase la definición en el Diccionario panhispánico del español jurídico, 2023, disponible en <https://dpej.rae.es/lema/big-data>

¹⁴ Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)) (2018/C 263/10), p. 2. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOC_2018_263_R_0011&from=ES

*decision making, and process automation*¹⁵”, que vendría a traducirse como ‘un gran volumen, velocidad o variedad de información que demanda formas costeables e innovadoras de procesamiento de información que permitan ideas extendidas, toma de decisiones y automatización del proceso’. El Big Data es por tanto una tecnología capaz de analizar un gran volumen de datos o conjuntos de ellos a una velocidad muy elevada, obteniendo un resultado buscado¹⁶.

Adentrarse al Big Data supone hablar de los datos, su fuente y el uso de los mismos, de quien los obtiene, almacena y para qué fines se utilizan. Y es que las fuentes de datos —que generamos con cada *like*, con cada *tweet*, con cada compra en línea— se están volviendo más complejas ya que estas están impulsadas por IA, los dispositivos móviles, las redes sociales y el *Internet of Things* (IoT)¹⁷.

En lo concerniente a sus características podemos partir del concepto de GARTNER del cual extraemos lo que en un primer momento fueron las tres “uves” o las tres características clásicas asociadas Big Data: volumen, variedad y velocidad. Pero como se verá más adelante, estas características se irán ampliando a medida que el Big Data va evolucionando.

Por volumen se hace referencia a “la necesidad de procesamiento intensivo y complejo de subconjuntos de datos de gran tamaño que contienen información de valor para una organización mediante tecnologías de Big Data”¹⁸. El volumen es por tanto la cantidad de datos que son generados cada segundo en nuestro entorno. Esta característica es la que se relaciona con mayor frecuencia a la idea del Big Data, ya que hace mención a la ingente cantidad de datos que se generan día a día, los cuales se

¹⁵ Véase definición de GARTNER: <https://www.gartner.com/en/information-technology/glossary/big-data> (última fecha de consulta: 20 de abril de 2023)

¹⁶ Para ampliar información puede consultarse el blog de Profesional Review en su artículo *Tecnología Big Data: qué es y para qué sirve*, 2019. Disponible en: [Tecnología Big Data: qué es y para qué sirve \(profesionalreview.com\)](https://www.profesionalreview.com) (última fecha de consulta: 03 de mayo de 2023)

¹⁷ Según la consultora DELOITTE, podría definirse *IoT* como “la agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet, la red de redes), dónde todos ellos podrían ser visibles e interaccionar. Respecto al tipo de objetos o dispositivos podrían ser cualquiera, desde sensores y dispositivos mecánicos hasta objetos cotidianos. Cualquier cosa que se pueda imaginar podría ser conectada a Internet e interaccionar sin necesidad de la intervención humana, el objetivo por tanto es una interacción de máquina a máquina, o lo que se conoce como una interacción M2M (*machine to machine*) o dispositivos M2M”.

Para ampliar información puede consultarse la página web de DELOITTE en su artículo: “*IoT - Internet Of Things*”. Disponible en: <https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html> (última fecha de consulta: 3 de mayo de 2023).

¹⁸ PUYOL MORENO, J., “Una aproximación a Big Data”, *Revista De Derecho De La UNED (RDUNED)*, n° 14, 2018, pp. p.486

almacenan con la finalidad de procesar dicha información transformando los datos en acciones.

Por su lado, velocidad se entiende como la rapidez con la que estos datos son creados, almacenados y procesados en tiempo real. Por último, la variedad alude a las formas, tipos y fuentes en las que se registran los datos. Según señala PUJOL “la variedad tiene que ver con gestionar la complejidad de múltiples tipos de datos, incluidos los datos estructurados, semiestructurados y no estructurados”¹⁹²⁰. En los albores del Big Data los tipos de datos convencionales eran estructurados y podían organizarse claramente en una base de datos relacional. Con el auge de esta tecnología los datos se presentan en nuevos tipos no estructurados. Los tipos de datos no estructurados y semiestructurados, como el texto, audio o vídeo, requieren un pre-procesamiento adicional para poder obtener significado y habilitar los metadatos²¹.

A medida que pasa el tiempo y el campo del Big Data evoluciona las tres características antes mencionadas no alcanzan a definir lo que hoy es el Big Data, por lo que este concepto se ha ido ampliado sucesivamente con nuevas «uves»: la veracidad, el valor y la variabilidad²² se incluyen actualmente como características de esta tecnología.

¹⁹ PUYOL MORENO, J., “Una aproximación...”, *Op. Cit.*

²⁰ “Los datos estructurados son el tipo de datos más sencillo de organizar y buscar. Pueden incluir datos financieros, registros de máquinas, y detalles demográficos Sus componentes están categorizados fácilmente, lo cual les permite a los diseñadores y administradores de bases de datos definir algoritmos simples para búsqueda y análisis. Los datos no estructurados pueden incluir cosas como publicaciones en redes sociales, archivos de audio, imágenes, y comentarios abiertos de clientes. Este tipo de datos no es fácil de capturar en las bases de datos relacionales de filas y columnas estándar. Los datos no estructurados se suelen almacenar en *data lakes*, almacenes de datos y bases de datos NoSQL. Los datos semiestructurados son un híbrido de datos estructurados y no estructurados. Los correos electrónicos son un buen ejemplo, ya que incluyen datos no estructurados en el cuerpo del mensaje, al igual que propiedades organizativas como emisor, destinatario, asunto y fecha. Los dispositivos que usan etiquetado geográfico, marcas de tiempo o etiquetas semánticas también pueden brindar datos estructurados junto con contenido no estructurado”.

Para ampliar información puede consultarse el blog: [¿Qué es Big Data? | Analíticas avanzadas de Big Data | SAP Insights](#) (última fecha de consulta: 3 de mayo de 2023).

²¹ El Diccionario panhispánico del español jurídico en su edición de 2023 define metadato como “la descripción estandarizada de las características de un conjunto de datos. En el contexto del documento electrónico, cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento”. Véase tal definición en: <https://dpej.rae.es/lema/metadato>

²² Desde que se acuñó la definición de Big Data hecha por Gartner, se ha tratado de llevarlo a 10 Vs, incluyendo la validez, la volatilidad, vulnerabilidad y visibilidad. Las características antes mencionadas que si bien son importantes para vislumbrar la dimensión del Big Data no se desarrollan a profundidad en el presente trabajo, ya que las mismas hacen referencia a la vertiente del Big Data más relacionada con la economía. Para ampliar información sobre estas visite la página web Datahack, *LAS 10 V 'S DEL BIG*

En cuanto a la veracidad, es el grado de confianza de la información recibida. Debido a la incertidumbre de los datos —uno de los mayores desafíos al que se enfrenta el Big Data—, la veracidad hace referencia al nivel de fiabilidad asociado a ciertos tipos de datos. PUJOL nos recuerda que “esforzarse por conseguir unos datos de alta calidad es un requisito importante y un reto fundamental de Big Data, pero incluso los mejores métodos de limpieza de datos no pueden eliminar la imprevisibilidad inherente de algunos datos, como el tiempo, la economía o las futuras decisiones de compra de un cliente”²³.

Dado que el Big Data tiene como objetivo final proporcionar información valiosa y conocimiento útil para la toma de decisiones y la resolución de problemas, el valor como menciona PUJOL, “hace referencia a los beneficios que se desprenden de su uso”²⁴: extraer valor de toda la información almacenada, a través de distintos procesos, de manera eficiente y al menor coste posible.

En cuanto a la variabilidad, esta trata sobre la forma en que se capturan los datos. Puesto que los datos puede mudar de un momento a otro, o de un lugar a otro, de manera que puede crear cierta dependencia del contexto en que se dé la recopilación de información, la variabilidad significa que los datos solo se pueden interpretar de manera significativa cuando se toma en consideración el contexto, de ahí que las tecnologías que componen una arquitectura Big Data deben ser flexibles para poder adaptarse a nuevos cambios en la forma de obtención de los datos como en su almacenamiento y procesado.

En lo concerniente a la legislación del Big Data no podemos hablar de leyes específicas para esta tecnología, sino más bien de leyes y preceptos constitucionales referentes a los datos personales y al derecho a la intimidad que se aplican por extensión a esta tecnología debido a su propia naturaleza.

Sobre la base en la que se cimenta la legislación para la tecnología del Big Data no podemos dejar de referirnos el art. 18.4 de la CE que establece 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”²⁵. Que si bien es un concepto vago y en

DATA. Disponible en: <https://www.datahack.es/10-vs-del-big-data/> (última fecha de consulta: 3 de mayo de 2023)

²³ BECERRA, J., COTINO-HUESO, L., LEÓN, I. P., SÁNCHEZ-ACEVEDO, M. E., TORRES-ÁVILA, J., & VELANDIA-VEGA, J., *Derecho y Big Data*, Ed. Editorial Universidad Católica de Colombia, Bogotá, 2018.

²⁴ Vid. BECERRA, J., COTINO-HUESO, L., LEÓN, I. P., SÁNCHEZ-ACEVEDO, M. E., TORRES-ÁVILA, J., & VELANDIA-VEGA, J., *Derecho y big...*, *Op. Cit.*

²⁵ Visto en: <https://app.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2>

palabras de RALLO LOMBARTE “se limita a mandar al legislador para que garantice los derechos fundamentales frente al uso de la informática”²⁶, nuestro Tribunal Constitucional —en adelante TC—, en su STC 254/93 ha procurado dar el reconocimiento de un derecho fundamental autónomo a la protección de datos personales. Tal y como señala el autor, de acuerdo con la citada STC: «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 las 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 CE llama “la informática”»²⁷. Del mismo modo nos indica el autor, siguiendo a VILLAVERDE, el TC ha fijado el contenido mínimo de este derecho fundamental en sus SSTC 290/2000 y 292/2000: «el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos» (STC 290/2000); «el derecho fundamental a la protección de datos persigue garantizar a la persona el 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» (STC 292/2000)²⁸. Además RALLO LOMBARTE pone de manifiesto que el contenido constitucional mínimo del derecho fundamental de protección de datos lo encontramos sustancialmente reiterado en el art. 8.2 CDFUE, el cual dice que “estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le concierne y a su rectificación”. Por lo que según el autor, puede afirmarse que “la configuración dogmática en torno a los elementos

²⁶ RALLO LOMBARTE, A., “El nuevo derecho de protección de datos”, *Revista Española de Derecho Constitucional*, nº 116, 2019.

²⁷ RALLO LOMBARTE, A., “El nuevo derecho de...”, *Op. Cit.*

²⁸ VILLAVERDE MENÉNDEZ, I., “Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993”, *Revista Española de Derecho Constitucional*, nº 41, 1994, pp.187-224.

que hacen reconocible este derecho, tanto en el plano europeo como en el constitucional, ofrece tal grado de similitud que no resulta imaginable la aparición de conflictos sustantivos”²⁹.

Una vez puesto de manifiesto la existencia del derecho fundamental de protección de datos tanto a nivel nacional como europeo, nos encontramos en nuestra normativa nacional que la regulación vinculable al Big Data se encuentra recogida principalmente en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales —en adelante Ley Orgánica 3/2018—. Esta se cimenta en el Reglamento 2016/679 y en el art. 18.4 de la CE. La Ley Orgánica 3/2018 establece las normas para la recopilación, procesamiento, almacenamiento y uso de datos personales, incluyendo aquellos que se obtienen a través de tecnologías de Big Data.

El espíritu, tanto de esta normativa como de la europea, es establecer que las empresas y organizaciones deban obtener el consentimiento explícito de los individuos para procesar sus datos personales, así como garantizar la seguridad y confidencialidad de los mismos. Una de las principales novedades que introduce la Ley Orgánica 3/2018 la encontramos en su Título X, donde se establece una serie de derechos digitales. En el mencionado Título se reconocen el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, el derecho a la desconexión digital, derecho a la intimidad frente al uso de dispositivos de video vigilancia, grabación en el lugar de trabajo y el uso de sistemas de geolocalización. Esta batería de derechos no estuvo exenta de críticas por parte de expertos en la materia, quienes no consideran del todo conveniente el incorporar los derechos digitales relativos al ámbito laboral en una ley de protección de datos³⁰.

Asimismo está 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 —en adelante Ley Orgánica 7/2021—. Esta Ley es la transposición de la Directiva 2016/680/EU de 27 de abril de 2016. Si bien en España su llegada fue tardía, tanto que fuimos, una vez más, condenados por el Tribunal de Justicia de la UE³¹, —máxime cuando su completa entrada en vigor

²⁹ RALLO LOMBARTE, A., “El nuevo derecho de...”, *Op. Cit.*

³⁰ Para ampliar información visítase el artículo en línea de PRODAT “La nueva LOPD llega con polémica incluida” (2018) <https://www.prodat.es/blog/la-nueva-lopd-llega-con-polemica-incluida/> (última consulta: 13 de junio de 2023)

³¹ STJUE de 25 de febrero de 2021, asunto Comisión Europea v. Reino de España, C658/19.

fue a finales de noviembre de 2021—. La Ley Orgánica 7/2021 viene a ser el segundo pilar normativo en materia de protección de datos en España, complementando lo ya regulado en la Ley Orgánica 3/2018. Si bien, en este caso, el ámbito de aplicación es sumamente más reducido, y es que esta Ley solo deberá ser aplicada por las autoridades públicas competentes, en concreto por las Fuerzas y Cuerpos de Seguridad, las autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal, las Administraciones Penitenciarias, la Dirección Adjunta de Vigilancia Aduanera, 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, todo ello sin perjuicio de los tratamientos llevados a cabo por órganos jurisdiccionales.

Su finalidad principal es que los datos sean tratados por las autoridades competentes de manera que se cumplan los fines deseados, así como establecer los mayores estándares de protección de los derechos fundamentales y las libertades de los ciudadanos. Igualmente se incluyen algunas previsiones específicas para el tratamiento de los datos de personas fallecidas. Resaltar también el derecho a cancelación o supresión de los datos personales en su art. 26 cuyo contenido es el siguiente: “el responsable del tratamiento, a iniciativa propia o como consecuencia del ejercicio del derecho de supresión del interesado, suprimirá los datos personales sin dilación indebida y, en todo caso, en el plazo máximo de un mes a contar desde que tenga conocimiento, cuando el tratamiento infrinja los artículos 6, 11 o 13, o cuando los datos personales deban ser suprimidos en virtud de una obligación legal a la que esté sujeto”. Tal como expone LLERENA CARRASCO, si atendemos a la literalidad de la disposición podemos observar que la Ley Orgánica 7/2021 prevé, en primer lugar y para el caso en que el interesado no ejerza su derecho, un deber u obligación por parte del responsable del tratamiento, quien actuará de oficio —a iniciativa propia, según la Ley— suprimiendo los datos personales de aquel; y en segundo lugar y para el caso en que el interesado ejerza su derecho, como un verdadero derecho que le asiste³². Por último, indicar que las autoridades públicas competentes tendrán que llevar a cabo un registro de operaciones que incluya la recogida, alteración, consulta, comunicación a terceros, transferencias

³² LLERENA CARRASCO, J., "*La Ley Orgánica 7/2021 sobre protección de datos en el ámbito policial*", Trabajo de Final de Grado, Facultad de Derecho, Universidad de Cádiz, (Tutor académico: Antonio Troncoso Reigada), 2022.

internacionales, y supresión de los datos personales, ya que tal obligación no existe en el RGPD.

En cuanto a limitaciones de la Ley Orgánica 7/2021, según YAÑEZ son dos las más importantes respecto a la normativa de protección de datos del RGPD, por un lado, la limitación del deber de transparencia u obligación de información al interesado sobre los tratamientos que se realizan, con el fin de evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales. Según este "no tiene sentido informar a una persona a la que se le está investigando si eso puede perjudicar la propia investigación u otras investigaciones asociadas". Por otro lado, tenemos la limitación en los derechos, y es que según el autor "esta ley orgánica reconoce a los interesados los derechos de derechos de acceso, rectificación, supresión (cuando sea factible) y limitación del tratamiento, pero ni rastro de los derechos de oposición y portabilidad". Además, es interesante conocer que las autoridades competentes no tienen la obligación de responder a estos ejercicios de derechos, sino que se presumirá la desestimación de la solicitud del interesado en aquellos supuestos en los que, transcurrido un mes desde su presentación, no haya recibido respuesta³³.

1.2. El Big Data aplicado al ámbito jurídico.

Habiendo abordado el concepto del Big Data, sus características y su regulación tanto nacional como a nivel europeo es hora de adentrarse en sus aplicaciones dentro ámbito jurídico. La incursión del Big Data en el ámbito jurídico está perfilando, de forma paulatina, un nuevo escenario procesal en el que diversos aspectos y garantías del proceso se ven influenciados en el marco de la "Cuarta Revolución Industrial"³⁴. Si bien los

³³ YAÑEZ, J., "Ley Orgánica 7/2021: qué es y cómo afecta a la protección de datos en causas penales", UNIR, 2021. Disponible en: <https://www.unir.net/derecho/revista/ley-organica-7-2021-proteccion-de-datos/> (última fecha de consulta: 19 de mayo de 2023).

³⁴ BARONA VILAR en "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia" de 2019, describe la "Cuarta Revolución Industrial" como aquella en la que una sociedad está "basada, diseñada y estructurada desde y con la tecnología; una sociedad en la que ocupan lugares privilegiados las redes sociales, la nube, el Internet de las cosas (IoT), la inteligencia artificial, los vehículos autónomos, la impresión 3D, la nanotecnología, la biotecnología, el Big Data, la *machine learning*, el *deep learning*, y un largo etcétera que nos encaminan hacia un mundo inteligente, un mundo que se despliega desde un Internet mucho más móvil y mundial, por sensores más pequeños y más potentes, y por inteligencia artificial y aprendizaje automático, lo que cambia con ello la forma de vivir, trabajar y relacionarnos los unos [PAP1] con los otros".

sistemas judiciales han sido enormemente criticados —y con justa razón— por su lentitud, su excesivo tradicionalismo y la compleja burocratización en sus procesos, hoy por hoy se ve en los nuevos mecanismos de procesamiento masivo de datos un camino para poder emprender las tan anheladas innovaciones en su funcionamiento y rendimiento en el marco de una sociedad cada vez más cambiante. Ahora bien, tal y como apunta CARVAJAL GEZAN “lo que resulta particularmente delicado es la sensibilidad que reviste esta función del Estado para cada entidad involucrada y para la comunidad toda. Por esta razón, la lógica de aplicación no puede tener como objetivo único la optimización de los procesos, sino también, y con igual o mayor importancia, el que dicha optimización resguarde en todo momento y maximice la protección de los derechos de los involucrados y su intimidad”³⁵.

No son pocos los posibles usos que se pueden obtener de esta tecnología. Tal como dice BUENO DE MATA el uso del Big Data enfocado a la justicia puede encontrar diversas funciones, “tanto para su propia administración en términos de aprovechamiento de información generada en el sector judicial para llegar a resultados más eficaces, cómo usar datos de los justiciables para cuestiones vinculadas a la investigación o resolución de casos”³⁶.

Asimismo el Big Data dentro del ámbito jurídico tiene interesantes aplicaciones en la predicción de resultados haciendo un aprovechamiento de la información generada en el sector judicial. Esta tecnología puede analizar grandes cantidades de datos judiciales y predecir los resultados de los casos, suponiendo un ahorro sustancial de tiempo y recursos para los operadores jurídicos. Despachos de abogados ya están experimentando importantes transformaciones como consecuencia de la incorporación de este tipo de software para la redacción de sus escritos y reforzar la petición y defensa de sus pretensiones³⁷.

Un ejemplo de esto es el software desarrollado en Silicon Valley, *LEX MACHINA*, un programa de análisis de datos legales que utiliza técnicas de Big Data para analizar patrones en la jurisprudencia y en los comportamientos de los jueces. *LEX MACHINA*

³⁵ CARVAJAL GEZAN, F., “*Big Data y su aplicación a las decisiones judiciales automatizadas*”, Tesis de Licenciatura, Universidad de Chile - Facultad de Derecho, (Tutora académica: Lorena Donoso Abarca), Santiago, Chile, 2022, pp. 20.

³⁶ BUENO DE MATA, F., “Macrodatos, inteligencia artificial y proceso: luces y sombras”, *Revista General de Derecho Procesal*, n° 5, Iustel, 2020.

³⁷ BUENO DE MATA, F., “*Macrodatos, inteligencia artificial...*”, *Op. Cit.*

ayuda a los abogados a predecir el comportamiento y los resultados de diferentes estrategias legales al extraer, etiquetar, categorizar y mejorar millones de expedientes y documentos de tribunales federales estadounidenses. Esta tecnología permite a los abogados tomar decisiones importantes basadas en datos, desarrollar estrategias de litigio, crear registros de seguimiento y decisiones clave de los “*presiding judge*”, así como revelar tendencias por resultados de casos³⁸.

Otro ejemplo del empleo del Big Data para la predicción de resultados es el canadiense Blue J Legal³⁹, un programa de análisis legal que utiliza técnicas de Big Data para analizar patrones en la jurisprudencia y en los comportamientos de los jueces. El kit de herramientas de este software consta de tres funciones: clasificadores, buscadores de casos y análisis de casos. Este utiliza un algoritmo de *machine learning*⁴⁰ para analizar grandes cantidades de datos y predecir cómo un Juez puede decidir en un caso dado, lo que permite a los abogados y clientes tomar acciones basadas en la información proporcionada por este.

Algo relevante a señalar es que la predicción de resultados no solo está penetrando en los despachos de abogados, esta tecnología empieza hacer su aparición en los juzgados, un ejemplo lo encontramos en PROMETEA un sistema de software desarrollado en 2017 por la Fiscalía de la Ciudad Autónoma de Buenos Aires que tiene como cometido principal la automatización de tareas reiterativas y la aplicación de Big Data e IA para la elaboración automática de dictámenes jurídicos basándose en casos análogos para cuya solución ya existen precedentes judiciales reiterados⁴¹. PROMETEA no solo está siendo utilizada para las predicciones de dictámenes en el Ministerio Público Fiscal de Buenos Aires, sino también este software está siendo empleado por la Corte Interamericana de

³⁸ LexisNexis Company. *LexisNexis Acquires Premier Legal Analytics Provider Lex Machina*. (2015) Disponible en <https://lexmachina.com/media/press/lexisnexis-acquires-lex-machina/>

³⁹Para más información sobre Blue J Legal, véase en su página web <https://www.bluej.com/>

⁴⁰ *Machine learning* o aprendizaje automático es una forma de IA que permite que un sistema aprenda de los datos en lugar de aprender a través de una programación explícita. Para ampliar información puede consultarse el blog de IBM en su artículo *¿Qué es Machine Learning?* Disponible en: <https://www.ibm.com/mx-es/analytics/machine-learning>

⁴¹ Según explican ESTÉVEZ, E., LINARES LEJARRAGA, S., y FILLOTTRANI, P. “el diseño y la implementación del sistema se ha encuadrado dentro del Plan Estratégico de la propia Fiscalía de Buenos Aires, como acciones proactivas para mejorar la eficiencia y la calidad del trabajo de la entidad”. Según los autores la provisión de PROMETEA se ha basado en “esfuerzos previos relacionados con: la gobernanza de datos; la identificación y cuantificación de los procesos realizados por la institución; la reingeniería de procesos específicos para eliminar tareas que no agregaban valor; la certificación de calidad de los procesos; la construcción de árboles de decisión para cada proceso; la confección de modelos estandarizados de soluciones jurídicas; y la identificación de palabras clave para cada tipo de proceso”. En ESTÉVEZ, E., LINARES LEJARRAGA, S., y FILLOTTRANI, P. en “*PROMETEA. Transformando la administración de justicia con herramientas de inteligencia artificial*”, 2020.

Derechos Humanos. Incluso llegó a la Corte Constitucional de Colombia, donde tiene el nombre de PretorIA y es utilizado para detectar los casos prioritarios que versan sobre temas de salud.

Según la Fiscalía de Buenos Aires, PROMETEA ha ayudado a reducir de 90 minutos a 1 minuto (99 %) la resolución de un pliego de contrataciones, de 167 días a 38 días (77 %) para procesos de requerimiento a juicio, de 190 días a 42 días (78 %) para amparos habitacionales con citación de terceros, entre otros⁴².

En la Corte Constitucional de Colombia, con intervención humana, PretorIA (PROMETEA) fue capaz de leer, analizar, detectar y sugerir casos prioritarios sobre derecho a la salud, en menos de 2 minutos frente a los 96 días hábiles de trabajo que hubiera llevado, todo a partir de la técnica “aprendizaje automático supervisado”. La herramienta fue capaz de crear de manera automatizada 14 documentos en 16 minutos, algo que a una persona le lleva 2 horas 40 minutos de trabajo. En este caso el sistema demostró un 937 % más de eficiencia.⁴³

Las ventajas que aportan estas innovaciones, tal y como señala HERNANDEZ GIMÉNEZ, “están estrechamente relacionadas con el aumento de la eficiencia y la productividad, al reducir muchísimo los tiempos que emplearía un profesional en realizar las mismas tareas. Sin embargo, se trata de aplicaciones cuya investigación, fabricación y desarrollo son muy costosos, por lo que muchos despachos de abogados no podrán asumir esos costes y acabarán desapareciendo al ser menos productivos que aquellos que sí que puedan invertir”⁴⁴. Dada el elevado coste que supone la implantación de esta tecnología en los despachos profesionales, solo podrán optar por este método aquellos que tengan los recursos económicos suficientes para hacer frente a unos gastos considerables. Tal como apunta SAN MIGUEL CASO “esta circunstancia implica, de forma indirecta, la distinción entre unos despachos y otros, suponiendo esta inversión tecnológica un criterio diferenciador y, a su vez, un nuevo método de captación de clientes

⁴² ESTÉVEZ, E., LINARES LEJARRAGA, S., y FILLOTTRANI, P. en “*PROMETEA. Transformando la administración de justicia con herramientas de inteligencia artificial*”, 2020.

⁴³ Abogados.com.ar: *PROMETEA: el primer sistema de inteligencia artificial predictivo de la justicia se presenta en el “Mundial de Inteligencia Artificial”* (2019) Última revisión 19/04/2023. Disponible en <https://abogados.com.ar/prometea-el-primer-sistema-de-inteligencia-artificial-predictivo-de-la-justicia-se-presenta-en-el-mundial-de-inteligencia-artificial/23523>

⁴⁴HERNÁNDEZ GIMÉNEZ, M., “Inteligencia artificial y Derecho Penal”, *Actualidad jurídica iberoamericana*, n° 10, 2019, pp.792-843.

con un perfil altamente definido”⁴⁵. Este criterio, trasladado a la óptica del proceso penal, equivaldría a una desigualdad manifiesta entre las partes o, dicho de otro modo, implicaría la ventaja de una parte sobre la otra al disponer de más recursos para idear una estrategia más adecuada y eficaz.

Además, HERNANDEZ GIMÉNEZ señala que este fenómeno no se limita únicamente al ámbito privado pues es extrapolable al público ya que “aquellos países que no sean capaces de estar al día en lo que a tecnología se refiere por falta de recursos, verán como su sistema judicial se debilita cada vez más, al perder la capacidad de cooperación con otros Estados, por lo que se abrirá aún más la brecha entre unos países y otros”⁴⁶. Es así que vemos como la irrupción de este tipo de herramientas tecnológicas pone en evidencia las desigualdades de aquellos países o entidades privadas (tómese como ejemplo los despachos de abogados) que puedan o no incorporarlas, suponiendo así una pérdida de competitividad o un empeoramiento en la calidad de sus sistemas judiciales.

Por consiguiente, el acceso —o no— a estas tecnologías acentúa más las desigualdades de aquellos territorios con menor capacidad adquisitiva o de aquellos territorios con problemas estructurales (ya sean sociales, económicos, de seguridad, etc...) en donde se relega la inversión a los sistemas judiciales bien por qué no sea una prioridad o porque sea imposible de llevarlo a cabo por falta de recursos. El no poder disponer de estas tecnologías deja atrás a millones de ciudadanos que merecen tener acceso a servicios públicos de calidad, acentuando más la brecha digital⁴⁷ de aquellos territorios que no puedan ver incorporada este tipo de avances en su día a día y tal como expresa CORVALÁN “cuanto más se tarde, es el ciudadano el que pierde”⁴⁸.

Otro uso del Big Data en el ámbito jurídico es en lo referente la automatización de procesos. Los datos judiciales masivos pueden ser utilizados para automatizar procesos legales, implementando sistemas de gestión y revisión de documentos y expedientes judiciales. Estos sistemas utilizan el Big Data para automatizar la clasificación y organización de los documentos judiciales, esto permite una gestión más eficiente de los

⁴⁵ SAN MIGUEL CASO, C., “La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?”, *IUS ET SCIENTIA Revista electrónica de Derecho y Ciencia*, nº 1, Vol. 7, Ed. Universidad de Sevilla, 2021.

⁴⁶ HERNÁNDEZ GIMÉNEZ, M., “Inteligencia artificial...” *Op. Cit*

⁴⁷ SERRANO, A. y MARTÍNEZ, E., entiende la “brecha digital” como la “separación que existe entre las personas (comunidades, Estados, países) que utilizan las TIC como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que aunque las tengan no saben cómo utilizarlas” en “La brecha digital: mitos y realidades” de 2003.

⁴⁸ CORVALÁN, J., “Inteligencia artificial: retos, desafíos y oportunidades...” *Op. Cit*.

expedientes y reduce el tiempo que los operadores jurídicos tienen que dedicar a la organización de los mismos lo que permite ahorrar tiempo y reducir los costes.

En España, la aplicación de tecnologías de Big Data judicial ha proliferado más en la automatización de procesos, centrándose en la gestión de expedientes y el análisis de datos en un intento de mejorar la eficiencia y la transparencia en la administración de justicia. Un ejemplo de esto es la implementación del programa Justicia Digital. Según el Ministerio de Justicia este sistema “consiste en la dotación a los órganos judiciales y fiscalías de un sistema de gestión procesal que permite realizar la tramitación electrónica de los procedimientos judiciales y garantizar la comunicación con los diferentes operadores implicados durante todo el proceso”⁴⁹.

Se trata pues de un sistema integral de gestión de expedientes para la Administración de Justicia española, el cual permite la digitalización de los documentos y la gestión electrónica de los procedimientos judiciales. El programa Justicia Digital utiliza tecnología de Big Data para analizar la carga de trabajo de los tribunales y optimizar la distribución de los casos entre los jueces. Su alcance final, en palabras del Ministerio de Justicia, es “proporcionar la gestión procesal electrónica en todos los órdenes jurisdiccionales (civil, penal, social, y contencioso-administrativo) y todas las instancias (etapas jurisdiccionales en los que se divide la presentación, estudio y resolución de todos los asuntos que se presentan ante un tribunal de justicia) del ámbito territorial del Ministerio de Justicia, incluyendo las Fiscalías”⁵⁰.

⁴⁹ Ministerio de Justicia: *Justicia Digital: la visión 360° de la Seguridad* (2019). Disponible en: https://publicadministration.un.org/unpsa/Portals/0/UNPSA_Submitted_Docs/2019/1c1229f9-0097-48ef-8ef3-c0e05a2f4e10/2020%20UNPSA_Justicia%20Digital_Document%20Memory_27112019_014713_7b5aa8fb-95b0-4d66-a0c5-0d8457d6f95f.pdf?ver=2019-11-27-134713-233#:~:text=Justicia%20Digital%20consiste%20en%20la,implicados%20durante%20todo%20el%20proceso.

⁵⁰ Vid. Ministerio de Justicia: *Justicia Digital: la visión 360° de la Seguridad* (2019).

2. Epígrafe II: La inteligencia artificial

En el imaginario colectivo cuando hablamos de IA resulta fácil pensar en un futuro lejano en el cual los robots son idóneos para realizar cualquier tipo de tareas, capaces de emular acciones y sentimientos que asociamos como puramente humanos —el amor, el odio, la tristeza, la felicidad, etc.—, o incluso máquinas e inteligencias artificiales creadas por el ser humano que se rebelan contra sus creadores y, en el más apocalíptico de los casos, acaban dominado el mundo y doblegando la voluntad humana. Esta imagen, a la que a la fuerza nos hemos hecho, en gran medida debido al cine de ciencia ficción con películas como *I, Robot* (2004), *A.I. Artificial Intelligence* (2001) o *Matrix* (1999), que mezcla y confunde la IA con la robótica⁵¹, dista mucho de la realidad en la que hoy por hoy nos encontramos inmersos.

Hace años que la IA deja ser cosa de ficción: la ruta del GPS, el reconociendo facial para desbloquear dispositivos móviles, la lista de sugerencia en nuestros carritos de la compra en Amazon son un ejemplo de cómo la IA no solo se ha colado de lleno en nuestro día, sino también en la agenda global. Hoy en día asistimos a una serie de eventos que nos muestran el gran potencial que tiene la IA en diferentes campos, véase la noticia emitida este 2023 por el ex beatle Paul McCartney donde se hacía público que la IA hará realidad el poder escuchar un tema inédito que incluye la voz de John Lennon, asesinado en 1980.⁵²

De cara a este segundo epígrafe trataremos de conceptualizar la noción de IA y como se regula la misma tanto a nivel europeo como a nivel nacional. Desde la perspectiva procesal penal, nos disponemos a examinar las aplicaciones de la IA dentro del ámbito jurídico y particularmente de su aplicación dentro del proceso penal, en fase probatoria y en la adopción de medidas cautelares.

⁵¹ Primariamente hemos de aclarar que IA y robótica son disciplinas científicas distintas, lo que no quiere decir que no se nutran de los avances que hacen la una de la otra o que no se realicen proyectos conjuntos —como pasa en otros campos científicos—. En cuanto la robótica, es definida por la RAE como la “técnica que aplica la informática al diseño y empleo de aparatos que, en sustitución de personas, realizan operaciones o trabajos, por lo general en instalaciones industriales” lo que en otras palabras viene a ser el diseño, la fabricación y la utilización de robots, definir lo que es la IA nos supondrá cuanto menos un reto debido a que no existe un único inequívoco concepto aceptado por toda la doctrina científica, dando lugar al empleo de numerosas definiciones, en gran medida por la complejidad que entraña pretender dar un significado único de lo que supone esta disciplina científica.

⁵²Noticia extraída de BBC News Mundo “*The Beatles: cómo la inteligencia artificial ayudó a producir la “última canción” de la mítica banda inglesa*” 13 junio 2023. Disponible en: <https://www.bbc.com/mundo/noticias-65891009> (Última fecha de consulta 7 de julio de 2023).

Un término genérico, tal y como expone BARONA VILAR, con el que se identifica la IA “es aquel que ofrece una noción omnicomprendiva desde la que las máquinas son capaces de llevar a cabo funciones inteligentes”⁵³. Pero como resalta la autora, tal definición no resulta la más adecuada porque no logra resolver las múltiples incógnitas de su significado. Es más, tal y como la autora señala “a medida que la tecnología ha ido avanzando y nuestra capacidad de comprensión e integración de la misma también lo ha hecho, el mismo concepto de inteligencia artificial ha ido variando”⁵⁴. A pesar de la creciente importancia que va adquiriendo la IA, no existe un término unívoco para definirla, sino muchos y provenientes de muy diversos sectores.

Desde esta premisa, intentaremos proporcionar a continuación algunas de las definiciones más destacadas.

2.1. La inteligencia artificial: concepto y regulación.

Como ya hemos hecho mención, actualmente no existe una definición legal sobre la IA, pero sí formales, en primer lugar tenemos el concepto ofrecido por la RAE que define la IA como la “disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realizan la mente humana, como el aprendizaje o el razonamiento lógico”⁵⁵.

En segundo lugar, una de las definiciones más antiguas es la acuñada por TURING quien propone que “la IA estaría presente en todos aquellos mecanismos que al interactuar con ellos desde la distancia, las personas interlocutoras no pudieran percatarse de que están interactuando con una máquina en lugar de con una persona”⁵⁶. Así, de acuerdo con este autor, se crea el conocido como “test de Turing” para determinar si estamos ante una IA, mediante el cual se evalúa la capacidad de una máquina para exhibir un comportamiento inteligente similar al del ser humano o indistinguible de este⁵⁷.

⁵³BARONA VILAR, S., *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021.

⁵⁴BARONA VILAR, S., “Algoritmización del Derecho...”, *Op. Cit.*

⁵⁵ Véase en RAE disponible en [inteligencia | Definición | Diccionario de la lengua española | RAE - ASALE](#) (última fecha de consulta: 1 de mayo de 2023)

⁵⁶ TURING, A. “Computing Machinery and Intelligence”, *Mind*, Volume LIX nº 236, 1950, pp. 433–460.

⁵⁷ Este test consiste en que un humano mantenga una conversación con una computadora y otra persona, pero sin saber quién de los dos conversadores es realmente una máquina. El objetivo de este experimento es determinar si la inteligencia artificial puede imitar las respuestas humanas. Por ello, el humano hace preguntas tanto a la otra persona como al *chatbot* y si no puede identificar si alguno de los dos sujetos es

En tercer lugar tenemos la definición proporcionada por el científico informático de la Universidad de Stanford MCCARTHY,⁵⁸ quien se refiere a esta como “la ciencia y la ingeniería de fabricar máquinas inteligentes, en especial máquinas inteligentes de computación”⁵⁹.

Pero a medida que la IA va tomando relevancia en nuestra sociedad, las instituciones públicas se ven instadas a intentar definir y delimitar lo que esta supone. Sin ánimo de ser exhaustivos⁶⁰, nos quedaremos con la definición proporcionada por el Libro Blanco sobre la inteligencia artificial, el cual ofrece una definición completa contenida en su Comunicación sobre una IA para Europa, posteriormente completada por el Grupo de Expertos de Alto Nivel y según la cual “los sistemas de inteligencia artificial (IA) son elementos de software (y en su caso, también de hardware), diseñados por seres humanos y que, dado un objetivo complejo, actúan en la dimensión física o digital, perciben su entorno mediante la adquisición e interpretación de datos estructurados o no estructurados

o no una máquina, la computadora pasa con éxito la prueba de Turing. Uno de los ejemplos de ordenadores más destacados es Kuki, anteriormente conocido como Mitsuku. Kuki ha sido capaz de superar el test de Turing y durante los últimos cuatro años, ha sido el ganador del Premio Loebner, por lo que ahora ostenta el récord mundial. Para ampliar información sobre el test de Turing visítese <https://plato.stanford.edu/entries/turing-test/> y <https://www.becas-santander.com/es/blog/test-de-turing.html> (Última fecha de consulta: 16 de agosto de 2023).

Para saber más acerca de Kuki puede visitarse su página web <https://www.kuki.ai/>, además están estos videos explicativos de cómo funciona <https://www.youtube.com/watch?v=IGfKpNVCUCQ> (Última fecha de consulta: 16 de agosto de 2023).

⁵⁸ John McCarthy fue un prominente científico informático de la Universidad de Stanford que desarrolló el tiempo compartido, inventó LISP y es considerado como uno de los padres fundadores del campo de la inteligencia artificial. De hecho, fue el responsable de introducir el término inteligencia artificial, concepto que acuñó en la Conferencia de Dartmouth en 1956. Recibió el Premio Turing en 1971 por sus importantes contribuciones en este campo. Para más información sobre John McCarthy, visítese la web: <http://jmc.stanford.edu/index.html> (Última fecha de consulta: 16 de agosto de 2023).

⁵⁹ MCCARTHY, J.: *What is Artificial Intelligence? Basic Questions* Stanford University, 2007

⁶⁰ Otras definiciones que tenemos sobre IA nos la proporcionan autores como NIEVA FENOLL, para quien la IA puede describirse como “la posibilidad de que las máquinas, en alguna medida, «piensen», o más bien imiten el pensamiento humano a base de aprender y utilizar las generalizaciones que las personas usamos para tomar nuestras decisiones habituales” en INTELIGENCIA ARTIFICIAL Y PROCESO JUDICIAL de 2018. Para NILSSON la IA “es aquella actividad dedicada a hacer que las máquinas sean inteligentes, y la inteligencia es esa cualidad que permite a una entidad funcionar de manera adecuada y con previsión en su entorno” en “*The Quest for Artificial Intelligence: A History of Ideas and Achievements*. Cambridge University Press” de 2010. Asimismo la Comisión Europea en el documento sobre “Inteligencia artificial para Europa” nos dice que “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”. Del mismo modo 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) define la IA en su art. 3.1 como “el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y 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”.

recogidos, razonan sobre el conocimiento o el procesamiento de la información derivada de estos datos e identifican y adoptan la(s) mejor(es) medida(s) a tomar para lograr el objetivo determinado”⁶¹.

Ahora bien, además de definir qué es la IA habrá que determinar el alcance potencial —tanto de las presentes, como de las futuras—. Siguiendo a MIRÓ LLINARES existen dos aspectos esenciales a tener en cuenta: por un lado su capacidad para ejecutar un mayor o menor abanico de instrucciones y, por otro lado, el grado de autonomía con el que las ejecute frente a la influencia del ser humano⁶². Respecto al primer aspecto, el autor se refiere a "la capacidad de razonamiento de la máquina en el sentido del grado de equivalencia entre la complejidad de procesamiento que realiza la máquina y el que es capaz de realizar el cerebro humano". El segundo aspecto fundamental para comprender la IA, pero íntimamente ligado con el anterior, es en palabras del autor “la cuestión del nivel real de autonomía en la toma de decisiones que puede hoy, y que podrá en el futuro, atribuirse a las máquinas”.

Queda por considerar cuáles son los tipos de IA. Por una parte este autor, siguiendo el modelo de HARBERS, PEETERS y NEERINCX, propone la existencia de tres modelos de IA en la actualidad basado en el grado de interacción hombre-máquina: en primer lugar tenemos el modelo *Man in the loop*, en el cual la IA necesita aportes humanos a intervalos de tiempo regulares para poder llevar a cabo sus acciones; en segundo lugar el modelo *Man on the loop*, en el cual la máquina sí que es capaz de actuar por sí misma a partir de una programación previa, pero el humano puede intervenir interrumpiendo o modificando las acciones de la máquina en cualquier momento; y en tercer lugar el modelo *Man out of the loop*, un modelo en el que la máquina actúa de manera independiente durante ciertos intervalos de tiempo y, en estos, el ser humano no tiene influencia sobre las acciones de la máquina⁶³. Tal y como apunta el autor, “la posibilidad de interacción humana en tiempo real tan sólo es una parte de lo que podríamos denominar autonomía”, que provendría de la capacidad real de adaptar las decisiones a un contexto distinto de aquél para el que ha sido programada. En este sentido,

⁶¹ Libro Blanco de la Comisión Europea sobre Inteligencia Artificial, "*Una aproximación europea a la excelencia y a la confianza*", de 27 de febrero de 2020. Disponible en: https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_es.pdf

⁶² MIRÓ LLINARES, F. “INTELIGENCIA ARTIFICIAL Y JUSTICIA PENAL: MÁS ALLÁ DE LOS RESULTADOS LESIVOS CAUSADOS POR ROBOTS”, *Revista De Derecho Penal Y Criminología*, nº 20, 2020, pp. 87–130.

⁶³ MIRÓ LLINARES, F. “INTELIGENCIA ARTIFICIAL...”, *Op. Cit.*

una máquina autónoma pertenecería a un cuarto tipo, al cual el autor denomina «*No man on the loop*», “donde o bien el aprendizaje por el que se toma la decisión no hubiera devenido de una acción humana, sino de la propia máquina que ha aprendido por sí misma o de otra máquina «educadora» anterior, o bien el comportamiento de la máquina no dependiera de ese aprendizaje anterior y de las decisiones atribuidas previamente en la IA sino de algo ajeno a ello y propio del mismo sistema”.

Por un otra parte, BARONA VILAR siguiendo los estudios de RUSSELL y NORVIG, indica cuatro tipos de IA: sistemas en los que se emula el pensamiento humano; sistemas que permiten actuar como humanos, imitando su comportamiento; sistemas que tratan de recrear el pensamiento lógico racional del ser humano como la creación de sistemas expertos⁶⁴ y, finalmente, aquellos que pretenden copiar la forma racional del comportamiento humano⁶⁵.

Con respecto a su regulación, podemos ver como los estados nacionales empiezan a desarrollar iniciativas legislativas en torno a esta materia. En el caso de Estados Unidos, por ejemplo, se está en proceso de regular el desarrollo de las inteligencias artificiales, mientras que otros actores internacionales como China o la UE son quienes lideran esta carrera con regulaciones más avanzadas en el tema, con grandes matices en el caso chino. En lo referente a China, el 11 de abril de 2023 la Administración del Ciberespacio de China —o CAC— presentó un borrador con las “Medidas de gestión para los servicios de inteligencia artificial generativa” con los lineamientos que deberán seguir las empresas que busquen ofrecer productos con esta tecnología en el país⁶⁶. El CAC establece que estas se formularon de conformidad con la ley de seguridad de datos, la ley de protección de información personal y la ley de seguridad en Internet. Bajo este parámetro, el Gobierno chino indicó que “las IA generativas deberán reflejar los valores del socialismo, evitar la discriminación, respetar los derechos de autor y ofrecer contenido verdadero y preciso”. Así pues, las herramientas de IA desarrolladas en China estarán sometidas a una “inspección de seguridad”, en la que también se comprobará que la IA refleje “los valores

⁶⁴ La autora se refiere a sistemas expertos que “infieren una solución a través del conocimiento previo del contexto en que se aplica y hace uso de ciertas reglas o relaciones o, lo que es lo mismo, la necesidad de definir el dominio sobre el que versará el sistema, definición del o de los problemas, integración del equipo interdisciplinario, identificación de expertos cuyo conocimiento sea modelado, adquisición de conocimiento experto, representación del conocimiento experto, programación, validación del prototipo, implementación final, mantenimiento y actualización”.

⁶⁵ BARONA VILAR, S., “Cuarta revolución industrial...”, *Op. Cit.*

⁶⁶ El borrador de las “Medidas de gestión para los servicios de inteligencia artificial generativa” se encuentra disponible en: "http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm

socialistas fundamentales"⁶⁷. Entre los puntos más notables del borrador, las empresas chinas de tecnología deben responsabilizarse por la "legitimidad de las fuentes de datos" que utilicen para el entrenamiento de sus inteligencias artificiales. Además, se restringe el uso de datos personales para generar contenido con estas tecnologías y las empresas deben asegurarse que sus programas no generen "material pornográfico, o que fomente la violencia, el extremismo, el terrorismo o la discriminación". Si bien el documento es de momento un proyecto de ley, en él China deja claro los objetivos por establecer una regulación gubernamental y el camino que esta pretende tomar en el gigante asiático.

En cuanto a la UE, actualmente existen numerosos instrumentos legales que pueden considerarse directa o indirectamente vinculables con la IA. Algunas de las normas más relevantes en este ámbito, además del Tratado de Lisboa y la Carta de los Derechos Fundamentales de la UE o del art. 8 CDFUE, son por un lado el Reglamento 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y el Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial —o Ley de Inteligencia Artificial—.

En cuanto al Reglamento 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la UE para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación, —en adelante Reglamento 2019/881— debemos destacar que se trata de una norma “*ad hoc*” que se establece en el marco para la Agencia de la UE para la Ciberseguridad (ENISA). Esta agencia juega un papel crucial en la promoción y el fortalecimiento de la ciberseguridad en la UE. A continuación, se destacan algunos aspectos importantes del reglamento como son: los objetivos, las tareas de la ENISA, la cooperación y apoyo a los Estados miembros, la certificación de productos y servicios de ciberseguridad y la cooperación con el sector privado.

En el art. 4 se establecen los objetivos de ENISA, la cual tiene como objetivo mejorar el nivel de ciberseguridad en la UE y promover la cooperación entre los Estados miembros en este ámbito. En cuanto a las tareas (arts. 5 y 6) la agencia tiene una serie de

⁶⁷ Para más información sobre visítese los artículos de prensa online de: DW “China exigirá “evaluación de seguridad” a productos de inteligencia artificial”, disponible en: <https://www.dw.com/es/china-exigir%C3%A1-evaluaci%C3%B3n-de-seguridad-a-productos-de-inteligencia-artificial/a-65279421> y de Hipertextual “China revisará las IA generativas antes de aprobar su uso”, disponible en: <https://hipertextual.com/2023/04/china-regulara-ia-generativa>

tareas específicas, que incluyen el desarrollo de directrices y asesoramiento técnico en materia de ciberseguridad, la promoción de buenas prácticas, la facilitación del intercambio de información y la colaboración en la gestión de incidentes de seguridad cibernética. También se establece la cooperación y apoyo a los Estados miembros de la UE en la mejora de su capacidad de respuesta a incidentes de ciberseguridad y en la implementación de políticas y medidas relacionadas con la ciberseguridad. Además, se promueve la cooperación y el intercambio de información entre los Estados miembros.

El art. 8 del Reglamento 2019/881 implanta la certificación de productos y servicios de ciberseguridad, por lo que se establece que la ENISA debe desempeñar un papel clave en el desarrollo de un marco para la certificación de productos y servicios de ciberseguridad en la UE. Esto tiene como objetivo mejorar la confianza en los productos y servicios digitales y fomentar la adopción de estándares de seguridad. Asimismo la ENISA colabora con el sector privado, incluidas las empresas y las partes interesadas relevantes, para fomentar la adopción de buenas prácticas de ciberseguridad y promover la conciencia sobre la importancia de la ciberseguridad en la UE (art.10).

En cuanto al Reglamento 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 datos⁶⁸ —en adelante RGPD—, es una normativa clave en el ámbito de la protección de datos personales. El RGPD según RALLO LOMBARTE “constituye un desarrollo completo y exhaustivo del derecho de protección de datos reconocido en el art. 8 CDFUE”⁶⁹. Algunos puntos destacables son el ámbito de aplicación, el consentimiento, los derechos de los individuos, la responsabilidad y responsabilidad proactiva y notificación de una violación de la seguridad de los datos personales a la autoridad de control.

Sobre el ámbito de aplicación (art. 3), el RGPD se aplica a todas las organizaciones que procesan datos personales de personas dentro de la UE, independientemente de si la organización tiene su sede en la UE o no. En cuanto al consentimiento, el RGPD refuerza el requisito de obtener un consentimiento válido y explícito de los individuos para el procesamiento de sus datos personales. El consentimiento (art. 7) debe ser libremente dado, informado, específico y basado en una clara acción afirmativa por parte del

⁶⁸ Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679>

⁶⁹ RALLO LOMBARTE, A., “El nuevo derecho de protección de datos” *Revista Española de Derecho Constitucional*, nº 116, 2019, pp. 45-74.

individuo. En lo concerniente a los derechos de los individuos (Capítulo III, arts. 12-22) se otorgan a los individuos una serie de derechos en relación con sus datos personales, como el derecho de acceso, rectificación, supresión, limitación del procesamiento, portabilidad de los datos y oposición al procesamiento automatizado, entre otros.

Así mismo RGPD introduce el principio de responsabilidad, lo que significa que las organizaciones son responsables de garantizar el cumplimiento de las disposiciones de este y deben demostrar que han implementado medidas adecuadas de protección de datos. Esto implica llevar a cabo evaluaciones de impacto, implementar medidas técnicas y organizativas adecuadas y mantener registros de actividades de procesamiento de datos. También el art. 23 del RGPD establece la obligación de las organizaciones de notificar a la autoridad de protección de datos correspondiente y, en algunos casos, a los individuos afectados, en caso de violación de datos personales que pueda representar un riesgo para los derechos y libertades de los individuos.

Pero el RGPD no está exento de críticas, y como bien apunta RALLO LOMBARTE contiene un sinnúmero de remisiones al derecho de los Estados miembros “posibilitándoles su adaptación al ámbito nacional hasta el extremo de debilitar extraordinariamente su potencia armonizadora y convertirse en un *tertium genus* en el sistema de fuentes del derecho europeo”⁷⁰. Por otro extremo, si bien el RGPD está destinado a proteger la privacidad y los derechos de los individuos, algunos críticos argumentan que la regulación puede ser demasiado restrictiva y que debe haber un equilibrio adecuado entre la privacidad y otros intereses legítimos, como la seguridad pública y la investigación científica.

Por último, tenemos la que posiblemente sea la legislación más ambiciosa para regular el desarrollo de las inteligencias artificiales en la actualidad por parte de la UE. Se trata 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. —en adelante se referirá a este reglamento como el “Borrador”⁷¹—. El “Borrador” fue propuesto por la Comisión Europea en abril de 2021 como parte de su estrategia para la IA confiable y basada en los valores europeos y que ha sido sometido a enmiendas el paso 14 de junio

⁷⁰ RALLO LOMBARTE, A., “El nuevo derecho de...”, *Op. Cit.*

⁷¹ Propuesta de Reglamento disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206> (última fecha de consulta: 15 de mayo de 2023).

de 2023⁷², tiene como objetivo establecer un marco legal para el uso de la IA en la UE y abordar los riesgos asociados con su despliegue.

Uno de los mayores objetivos del Parlamento Europeo es garantizar la seguridad, la transparencia, la trazabilidad, la no discriminación y la conciencia medioambiental de los sistemas de IA utilizados en la UE⁷³. Algunos puntos clave del “Borrador” van dirigidos al ámbito de aplicación, las prohibiciones, obligaciones de los proveedores de sistemas de IA de alto riesgo, la transparencia y rendición de cuentas y la vigilancia humana. Además se hace especial hincapié en que los sistemas de IA deban ser supervisados por personas, en lugar de por la automatización, para evitar resultados perjudiciales. Asimismo el Parlamento Europeo quiere establecer una definición uniforme y tecnológicamente neutra de la IA que pueda aplicarse a futuros sistemas⁷⁴.

Uno de sus puntos fundamentales es el sistema de clasificación que determina el nivel de riesgo que una tecnología de IA podría suponer para la salud y la seguridad o los derechos fundamentales de una persona⁷⁵. El marco incluye cuatro niveles de riesgo: inaceptable, alto, limitado y mínimo. Dentro de los sistemas de IA de riesgo inaceptable, los cuales son aquellos que se consideran una amenaza para las personas y que por tanto estarán prohibidos, se incluyen: la manipulación cognitiva del comportamiento de personas o grupos vulnerables específicos, puntuación social o sistemas de identificación biométrica en tiempo real y a distancia⁷⁶.

⁷² Se tratan de las enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre 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. Dichas enmiendas se encuentran disponibles en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.html#def_1_1 (última fecha de consulta: 11 de agosto de 2023).

⁷³ Para más información diríjase a:

<https://www.europarl.europa.eu/news/es/headlines/society/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial>

⁷⁴ Para más información consulte:

<https://www.europarl.europa.eu/news/es/headlines/society/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial>

⁷⁵ Para más información diríjase a: <https://es.weforum.org/agenda/2023/04/esto-es-lo-que-dice-la-nueva-ley-de-inteligencia-artificial-de-la-union-europea/> (última fecha de consulta: 11 de agosto de 2023).

⁷⁶ Dentro de los sistemas de IA de riesgo inaceptable existen algunas excepciones. Por ejemplo, los sistemas de identificación biométrica a distancia "a posteriori", en los que la identificación se produce tras un retraso significativo, se permitirán para perseguir delitos graves y sólo cuando haya previa aprobación judicial. Esta información ha sido obtenida de la sección de noticias del Parlamento Europeo, para más información consúltese:

<https://www.europarl.europa.eu/news/es/headlines/society/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial> (última fecha de consulta: 11 de agosto de 2023).

En cuanto al ámbito de aplicación, el art. 2 del “Borrador” establece que éste se aplica a sistemas de IA desarrollados tanto en la UE como fuera de ella cuando se utilizan en la UE y están destinados a ser utilizados en áreas reguladas. Sobre las prohibiciones, el art. 5 prohíbe ciertos usos de la IA que se consideran altamente riesgosos, como la IA que manipula el comportamiento humano de manera subrepticia o la IA utilizada para puntuación social masiva en tiempo real por parte de autoridades públicas (clasificar a las personas a partir de su comportamiento o características personales), este tipo de sistemas quedarían totalmente prohibidos. Además los eurodiputados han ampliado la lista propuesta por la Comisión Europea, añadiendo prohibiciones relacionadas con usos intrusivos y discriminatorios de la IA⁷⁷.

En lo que respecta a las obligaciones de los proveedores de sistemas de IA de alto riesgo, el art. 16 establece requisitos más estrictos para los sistemas de IA considerados de alto riesgo. Estos requisitos incluyen la realización de evaluaciones de riesgos y pruebas de conformidad antes de su despliegue.

Además el “Borrador” dispone sobre la transparencia (art. 13) y la rendición de cuentas (art. 12) requiriendo que los proveedores de sistemas de IA proporcionen información clara sobre el funcionamiento, capacidades y limitaciones de sus sistemas. También se exige la creación de registros de actividades para los sistemas de alto riesgo. Por su parte el art. 14 establece la vigilancia humana, pues se establece que ciertos casos se requerirán que los sistemas de IA de alto riesgo estén sujetos a la supervisión humana para garantizar la seguridad y la supervisión adecuada⁷⁸.

Finalmente es importante remarcar el deber del legislador —tanto nacional como europeo— de establecer una normativa armonizada en este campo, en un afán de dar una respuesta conjunta a la problemática que enfrentamos como sociedad. Y aunque de momento no podamos estar seguros del rumbo que tome la IA en nuestros sistemas

⁷⁷ Algunas de las prohibiciones van dirigidas a los sistemas de identificación biométrica remota, en tiempo real, en espacios públicos; los sistemas de identificación biométrica remota, a posteriori, con la única excepción de usos policiales en investigaciones por delitos graves y con autorización judicial; los sistemas de categorización biométrica que utilicen ciertas características identitarias (por ejemplo el género, la raza, la etnia, el estatus de ciudadanía, la religión o la orientación política), los sistemas policiales predictivos (basados en la elaboración de perfiles, la ubicación o el historial delictivo); entre otras. Esta información fue extraída de la sección de noticias del Parlamento Europeo, disponible en: <https://www.europarl.europa.eu/news/es/press-room/20230609IPR96212/la-eurocamara-lista-para-negociar-la-primera-ley-sobre-inteligencia-artificial> (última fecha de consulta: 30 de agosto de 2023).

⁷⁸ Es importante remarcar que este es un resumen general del borrador del Reglamento de IA y que es posible que haya cambios o actualizaciones en la versión final adoptada por la UE, por lo que habrá que estar al tanto de las últimas novedades en materia de regulación de la IA en la UE.

judiciales y en última instancia en nuestra vida, lo cierto es que el espíritu de las normas debe estar encaminado a la salvaguarda de los derechos e intereses de los ciudadanos.

Dado que la IA no deja de innovar, a un tal punto que resulta abrumador, esto produce en cierto modo que la normativa llegue tarde y no tanto por la lentitud que impera en el ámbito jurídico, sino más bien por la velocidad con la que avanza esta tecnología. A colación de esta idea, este mismo año hemos asistido a peticiones de más regulación a la IA por parte de personajes relevantes en este sector⁷⁹, pero estas peticiones no dejan de ser cuanto menos desconcertantes por el siguiente motivo: la iniciativa de mayor regulación en este campo parte de lo que hoy por hoy es uno de los gigantes tecnológicos del sector de la IA, como es el caso de ChatGPT. Ahora bien, este tipo de empresas lograron posicionarse en el mercado en un momento en el que no había límites y podían desarrollar sus productos con una considerable libertad. Hoy por hoy las empresas o *Startups* que quieran competir en este sector se encontrarán con una mayor rigidez en comparación con las empresas que hoy piden mayor regulación.

Con esto no se quiere desvirtuar la importancia de crear una legislación homogénea para este sector, la cual brinde seguridad jurídica a los ciudadanos, sino hacer hincapié en el hecho de que estas iniciativas deben partir de nuestros órganos legislativos — nacionales o internacionales—, pues ellos son quienes tienen en última instancia el deber de velar por los intereses de la ciudadanía. Asimismo se debe incidir en que la regulación de esta materia debe hacerse con miras a que garantice los derechos fundamentales de los ciudadanos a la vez que se permita a las empresas la posibilidad de seguir innovando. Si bien muchas veces cuando se habla de la IA y su futuro en nuestras vidas se tiende a usar un tono catastrofista, desde nuestra visión esto no tiene por qué ser necesariamente así y esta no tendría por qué presentarse en términos negativos y apocalípticos todo el tiempo.

⁷⁹ Geoffrey Hinton, el “padrino de la IA”, o Sam Altman, CEO de la empresa *OpenAI*, —lo cual resulta cuanto menos insólito debido a los cargos que estos ocupan o han ocupado dentro del desarrollo de esta tecnología—. Véase por ejemplo el caso de Altman, quien este 2023 testificó ante el congreso de los Estados Unidos sobre el crecimiento exponencial de las capacidades de la IA y abogaba por la regulación a las inteligencias artificiales, así como la urgencia de crear una agencia global para licencias del funcionamiento de los sistemas de IA. Por su parte, Hinton este mismo año exponía algunos de sus temores en torno al avance de la IA sin un debido control.

Sobre las declaraciones realizadas por Geoffrey Hinton, véase el artículo en línea de la BBC “*AI 'godfather' Geoffrey Hinton tells the BBC of AI dangers after he quits Google*”. Disponible en: <https://www.bbc.com/news/av/world-us-canada-65453192>. Para más información sobre esta comparecencia, consúltese el artículo en línea de EuropaPress “*Sam Altman, CEO de OpenAI, pide regular herramientas como ChatGPT por su capacidad de "hacer daño"*”. Disponible en: <https://www.europapress.es/economia/noticia-sam-altman-ceo-openai-pide-regular-herramientas-chatgpt-capacidad-hacer-dano-20230522183735.html> (última fecha de consulta: 15 de mayo de 2023).

La IA ya está presente en nuestras vidas y en nuestras relaciones como sociedad y aprender a sacar el mayor provecho de ella debe ser el fin último.

2.2. La inteligencia artificial aplicada al ámbito jurídico.

En cuanto al empleo de la IA en el ámbito judicial, este presenta numerosas ventajas en términos de agilización de procesos y simplificación de tareas, especialmente cuando se aplica en procedimientos de gestión o como fuente de información jurídica (legislativa, jurisprudencial o doctrinal). El uso de IA *a priori* viene a ofrecernos una justicia más objetiva, más rápida, más eficiente y con una notable reducción de costes económicos para las arcas públicas. Ahora bien, en contraposición las dudas que suscita su aplicación, tal como expresa MONTESINOS GARCÍA, las encontramos cuando “se plantea su uso con carácter decisonal, y no meramente asistencial. Una de las mayores preocupaciones reside precisamente en la deshumanización de la Justicia”⁸⁰.

Lo cierto es que son múltiples los usos que se pueden hacer de ella, véase en lo referente al ámbito de la abogacía donde van proliferando las herramientas de investigación, la simplificación del análisis de datos y, en algunas jurisdicciones, la predicción de posibles decisiones judiciales⁸¹. Pero no solo este sector se ve alcanzado con los posibles usos previstos de esta, en el ámbito judicial las innovaciones con tecnología de IA se presentan para la mejora del acceso a la ley o a la jurisprudencia⁸².

En cuanto a la mejora del acceso a la ley, se plantea hacer uso de *chatbots*⁸³ para facilitar el acceso a las diversas fuentes de información existentes utilizando lenguaje natural o generando en línea plantillas de documentos (solicitudes judiciales, contratos de arrendamiento, etc.). Asimismo, la Comisión Europea para la Eficiencia de la Justicia

⁸⁰ MONTESINOS GARCÍA, A., “Empleo de la inteligencia artificial en algunas fases del proceso judicial civil: prueba, medidas cautelares y sentencia” en *XXXI Seminari d’estudi i pràctica jurídica. Justícia predictiva II. Àmbits civil, tributari i ADR. Sisena sessió*, 2022. Disponible en: https://eapc.gencat.cat/web/.content/home/biblioteca/fons-coleccions/docs_eapc/juridica/2022/11-XXXI-seminari-practica-juridica-sessio6/Dossier-XXXI-Seminari-estudi-i-practica-juridica-6a-sessio.pdf

⁸¹ MUÑOZ RODRIGEZ, A., “El Impacto de la Inteligencia Artificial en el proceso penal”, *Anuario de la Facultad de Derecho*, Universidad de Extremadura, n° 36, 2020, pp. 695-728.

⁸² Disponible en “*European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*” de la Comisión Europea para la eficiencia de la justicia (CEPEJ): <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (Última consulta: 09 de junio de 2023).

⁸³ Un “*chatbot*” es un agente de conversación que conversa con su usuario (por ejemplo, robots de empatía utilizados para ayudar a quienes están enfermos o servicios de conversación automatizados en las relaciones con los clientes). Esta definición fue obtenida —y traducida—, de *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment* de 2018.

(CEPEJ) proyecta el uso de la IA para la mejora de la jurisprudencia. Dado que las técnicas de *machine learning* se han implementado cada vez más en el campo del procesamiento del lenguaje natural en los últimos años, estas suponen un activo considerable para encontrar opciones de búsqueda para complementar la búsqueda de palabras clave o de texto completo. Estas herramientas podrían vincular varias fuentes (por ejemplo, constituciones y convenciones, leyes, jurisprudencia y teoría jurídica). Las técnicas de visualización de datos podrían ilustrar los resultados de búsqueda⁸⁴.

Dada la innegable capacidad de la IA para gestionar y procesar diferentes formas de datos con notable precisión y para informar de decisiones relacionadas con ellos, podemos afirmar que los beneficios potenciales de la IA son muchos en el ámbito jurídico, ahora bien en el campo procesalista nos encontramos con más de un dilema a la hora de una correcta y segura implementación. A continuación se abordan algunos de los usos de la IA que guardan una afectación directa en el proceso judicial, los cuales versan sobre: el uso de la IA en el proceso de decisión judicial⁸⁵ y la IA aplicada en la determinación judicial de la responsabilidad por la perpetración de un delito⁸⁶.

Sobre la utilización de la IA en el proceso de decisión judicial, encontramos un primer ejemplo en el proceso civil con los sistemas de apoyo a medidas alternativas de resolución de conflictos, siendo ejemplo de estos los sistemas de resolución de disputas en línea y las herramientas de “justicia predictiva”.

En cuanto a los sistemas para la resolución de disputas en línea, estos están configurados como plataformas de resolución de disputas en línea, en las cuales los litigantes que acuden a ellas —en un supuesto ideal—, deben ser informados de manera clara y comprensible si el procesamiento de su disputa se realiza de manera totalmente automatizada o con la participación de un mediador o árbitro. Además, la información proporcionada a los litigantes debe ser honesta y debe evitar darles la impresión de que un tribunal está involucrado⁸⁷. Un ejemplo de este tipo de plataformas lo tenemos en

⁸⁴ Visto en “*European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*” de la Comisión Europea para la eficiencia de la justicia (CEPEJ): <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (Última consulta: 09 de junio de 2023).

⁸⁵ BUENO DE MATA, F., “Macrodatos, inteligencia artificial...”, *Op. Cit.*

⁸⁶ MIRÓ LLINARES, F. “INTELIGENCIA ARTIFICIAL Y JUSTICIA PENAL: MÁS ALLÁ DE LOS RESULTADOS LESIVOS CAUSADOS POR ROBOTS”, *Revista De Derecho Penal Y Criminología*, nº 20, 2020, pp. 87–130.

⁸⁷ A este respecto, en “*European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*” se menciona que el término “corte en línea” se usa a menudo para este tipo de plataforma, mientras que técnicamente se trataría de una “ODR” (*Online Dispute Resolution*), lo que

*Smart Settle*⁸⁸ el cual se presenta como “un servidor neutral en Internet que actúa como mediador automatizado imparcial y confiable que comprende cómo se satisface cada parte. El servidor utiliza algoritmos inteligentes que aprenden las tácticas de licitación y las prioridades de las partes en una disputa y ayudan a avanzar hacia un arreglo para promover resultados más allá del “win-win” al recompensar el buen comportamiento de negociación”. Un caso llamativo donde se ha aplicado este tipo de mediación con éxito lo tenemos en Canadá donde la disputa subyacente se refería a honorarios impagos de aproximadamente 2.000 libras esterlinas, presuntamente adeudados por sesiones de asesoramiento personal. Luego de intentos inicialmente fallidos de mediar, se programó una audiencia en la corte. La disputa continuó durante tres meses, cuando Graham Ross, mediador y abogado, recomendó que las partes hicieran uso de *Smart Settle*. Usando el sistema, cada parte evalúa lo que desea llegar a un acuerdo, así como lo que está dispuesto a aceptar y presenta la resolución esperada, además de una oferta ciega de su *BATNA*⁸⁹. Inmediatamente después, la computadora genera un monto en dólares, basado en la entrada de cada parte del rango de liquidación, mientras favorece a la primera parte para que presente un compromiso⁹⁰. En este caso particular, el sistema permitió a las partes resolver su disputa en menos de una hora. No obstante, sobre el uso de estos sistemas, debemos mencionar que este se engloba en el grupo al que la CEPEJ cataloga para “posibles usos, pero que requieren considerables precauciones metodológicas”, por lo que resulta lógico pensar que su potencial implementación debe ser llevada respetando los derechos y garantías de las partes.

En cuanto a los sistemas de apoyo a medidas alternativas de resolución de conflictos, señala el texto europeo, *European ethical Charter on the use of Artificial Intelligence in*

vendría a ser una “plataforma de resolución de litigios en línea”, cuyo propósito es proporcionar servicios alternativos de resolución de disputas. La ORD se plantea como un espacio digital público en el que las partes pueden reunirse para resolver su disputa. Tres componentes esenciales diferencian la ODR de otras formas de resolución de disputas con soporte tecnológico y la primera es radica en que la ODR es una programa que opera exclusivamente en línea. En segundo lugar, el programa está diseñado explícitamente para ayudar a los litigantes a resolver su disputa o caso, en lugar de una plataforma tecnológica para apoyar la toma de decisiones del personal judicial o del tribunal. Y en tercer lugar, el poder judicial aloja o respalda el programa (este tercer supuesto se aplica en EUA).

⁸⁸ Para más información sobre *Smartsettle* visítase <https://www.smartsettle.com/algorithms>

⁸⁹ “*Best alternative to non-agreement*” o mejor alternativa a un trato negociado.

⁹⁰ El sistema de *Smart Settle* permite que ambas partes hagan ofertas y contraofertas de forma privada moviendo las banderas a lo largo de los controles deslizantes, mostrando al otro lado una bandera verde, que representa la cifra esperada, mientras que una bandera amarilla permanece oculta (la oferta ciega). Para ampliar información sobre este caso, visítase <https://www.lexisnexis.ca/en-ca/ihc/2019-06/from-estonian-ai-judges-to-robot-mediators-in-canada-uk.page> (última fecha de consulta: 15 de mayo de 2023).

*judicial systems and their environment*⁹¹, que ya en algunos países europeos las compañías de seguros utilizan herramientas de “justicia predictiva” para evaluar las posibilidades de éxito de un litigio y orientar al litigante hacia otro método de resolución de litigios cuando se considere que hay pocas posibilidades de éxito. Pero sobre este uso la CEPEJ nos alerta de posibles vicisitudes devenidas de un incorrecto uso de la misma. Ahora bien, en lo que respecta a las precauciones que se deberían tomar en cuanto a la resolución de disputas en línea, se hace especial énfasis en permitir a los litigantes tomar una decisión informada y que estos sistemas proporcionen información honesta. Al mismo tiempo y al tenor del documento antes citado, se deben permitir a las partes tomar una decisión informada, y en caso de no estar de acuerdo con el consejo dado por la plataforma de resolución de disputas en línea se pueda decidir ir a un tribunal real en el sentido del artículo 6 del CEDH por el cual “toda persona tiene derecho a que su causa sea oída equitativamente, públicamente y dentro de un plazo razonable, por un tribunal independiente e imparcial, establecido por la ley”. Además, en vista de los requisitos de los artículos 6 y 13 del CEDH, las formas de revisión del procedimiento de resolución de disputas en línea y su resultado por los tribunales estatales siempre deben considerarse, especialmente cuando el litigante ha dado su consentimiento para la resolución de disputas en línea totalmente automatizada.

Con todo, el uso de este tipo de herramientas, que a priori parecen ser especialmente útiles cuando se tratan de problemas cuantificables a resolver en aquellos supuestos en que las partes no buscan reparar o preservar una relación, presentan cuestiones cuanto menos interesantes a debatir. Si delegamos a estos sistemas aquellos casos que a priori parecen simples o “cuantificables” estaríamos desvirtuando el fin último de tener un sistema judicial. El ciudadano merece y tiene derecho a recibir respuesta por parte de los tribunales, porque el proceso —tanto en el ámbito privado como en el público—, no solo tiene como objeto la pretensión penal⁹² sino que va más allá, el acudir a los tribunales y tener una respuesta de los mismos es la materialización de vivir en un Estado Democrático y de Derecho. Cuando los ciudadanos dejan de acudir a los

⁹¹ Disponible en “*European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*” de Comisión Europea para la eficiencia de la justicia (CEPEJ): <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

⁹² MELLADO, J., define la pretensión penal como “la petición de una consecuencia jurídica (pena o medida de seguridad) dirigida al órgano jurisdiccional frente a una persona, fundamentada en unos hechos que se afirman coincidentes con el supuesto de hecho de una norma jurídica”, en “*Derecho Procesal Penal, Séptima Edición*” de 2015.

Tribunales por que estos no dan respuesta a sus necesidades o porque simplemente se ven abocados a recibir justicia por parte otros de órganos, entonces debemos plantearnos seriamente la salud de nuestros sistemas judiciales y por extensión la de nuestro propio Estado

En este punto no podemos dejar de mencionar los potenciales usos de la IA para su incorporación en la escena judicial penal, los cuales vengán a sustituir el pensamiento lógico racional del Juez o Magistrado, en lo que algunos llaman la implementación del “juez-robot” o la robotización de la justicia.

A este respecto debemos señalar el caso *State v. Loomis*⁹³, de 13 de julio de 2016, en donde el Tribunal Supremo del Estado de Wisconsin, en los Estados Unidos de América publicó un fallo, que tal y como enuncia DE MIGUEL BERIAIN y PÉREZ ESTRADA, llegue a considerarse histórico, pues por primera vez, un tribunal de esta importancia se ha pronunciado sobre la admisibilidad del uso de herramientas de IA, en este caso algoritmos de predicción del comportamiento, a la hora de tomar decisiones en un juicio penal, el tribunal antes mencionado avalaba el empleo del *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS), “un programa matemático desarrollado por una empresa privada completamente opaco, sobre el que el procesado no tenía información alguna, como prueba suficiente para tomar decisiones sobre una pena de privación de libertad”⁹⁴.

Aquí nos adentramos a un escenario en el que se plantea la incorporación de inteligencia computacional para impartir justicia, lo cuales emulan la forma racional del comportamiento humano haciendo uso de técnicas de *machine learning* o del *deep learning*⁹⁵. La cuestión es si la robotización de la justicia puede sustituir realmente al juez humano en los procesos penales. Debemos aclarar que esta sustitución no es posible y hacemos referencia a lo dispuesto en el art. 117. 3 CE, el cual establece que “El ejercicio

⁹³ *State v. Loomis*, 881, N.W.2d 749, 7532 (Wis, 2016).

⁹⁴ 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 De La UNED (RDUNED)*, nº 25, 2020, pp. 531–561.

⁹⁵ IBM define el *deep learning* como un subconjunto de *machine learning*, que es básicamente una red neuronal con tres o más capas. Estas redes neuronales intentan emular el comportamiento del cerebro humano —aunque lejos de igualar su capacidad— pero le permiten “aprender” a partir de grandes cantidades de datos. Aunque una red neuronal con una sola capa ya puede realizar predicciones aproximadas, las capas ocultas adicionales ayudan a optimizar y refinar la precisión. Para más información sobre este concepto consúltese la web de IBM en su artículo *¿Qué es Deep Learning?*: <https://www.ibm.com/es-es/topics/deep-learning> (Última consulta: 12 de junio de 2023).

de la potestad jurisdiccional en todo tipo de procesos, juzgando y haciendo ejecutar lo juzgado, corresponde exclusivamente a los Juzgados y Tribunales determinados por las leyes, según las normas de competencia y procedimiento que las mismas establezcan”. Por tanto, podemos ver que la función de juzgar y ejecutar lo juzgado son deberes exclusivos de jueces y magistrados, lo que significa que otros individuos o sistemas están excluidos de estas tareas.

A este respecto, encontramos apoyo en autores como BUENO DE MATA⁹⁶ quien muestra su total negativa al hecho de que una actividad tan importante como la justicia sea reducida a una mera operación matemática y que sea un algoritmo quién pueda sentenciar, pues atenta directamente contra el propio concepto de función jurisdiccional. Además el autor señala un punto muy interesante, y es con la aplicación de IA en la fase de decisión nos dirigimos ante un estadio de pensamiento único judicial, “lo que conllevaría una especie de estancamiento de la doctrina jurisprudencial y tendríamos que ver si dichos sistemas podrían percibir o no los cambios sociales y aplicarlos a las decisiones ofrecidas”. En este punto es importante recordar que la ciencia jurídica es una ciencia social, la cual logra avanzar gracias al pensamiento crítico e innovador que realizan los jueces y magistrados en el momento de dictar sentencias adecuándose a la realidad social en la que nos encontramos inmersos.

Como expresa el autor “no estamos en un terreno de blancos y negros, sino en un escenario en el que se pueden plantear una serie de escala de grises o de ‘diferentes verdades’ que se deben argumentar y defender a través de una postulación o de una serie de decisiones basadas en la aplicación material del derecho que pueden ser recurridas por entender que la aplicación del derecho puede ser otra”. La jurisprudencia se nutre de esas decisiones y gracias a ella como fuente de derecho se producen cambios significativos procedentes de sentencias en la que los jueces y magistrados ponen en valor esos cambios sociales que tiene un impacto directo en el Derecho.

Sobre este mismo punto, BARONA VILAR entiende “que extrapolar estas iniciativas de robotización judicial a la sede penal llevaría 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”⁹⁷. El uso de estas reduciría

⁹⁶ BUENO DE MATA, F., “Macrodatos, inteligencia artificial...”, *Op. Cit.*

⁹⁷ BARONA VILAR, S., “Cuarta revolución industrial...”, *Op. Cit.*

las garantías de defensa y promovería una mecanización judicial, perjudicando nuestro sistema de justicia.

En lo referente a la IA aplicada al proceso de determinación judicial de la responsabilidad por la perpetración de un delito —en adelante IAJ—, debido a las múltiples vicisitudes que su uso puede suponer para derechos y garantías fundamentales de nuestro sistema procesal penal, su implementación genera un intenso debate a nivel nacional, y también en el resto del mundo. Dentro de este grupo nos encontramos, con lo que MIRÓ LLINARES denomina, sistemas de IAJ de valoración del riesgo (IAJVR, en adelante). En lo referente a estos, tal y como el autor apunta “estos están basados en la automatización de las herramientas de valoración del riesgo, y son potencialmente aplicables a los procesos de toma de decisiones relacionados con la valoración del riesgo de aquellos individuos que se ven envueltos en el proceso judicial, tanto durante él, cómo puede ser para la aplicación de medidas cautelares, como tras la condena”⁹⁸. Estamos ante herramientas que tienen un potencial directo en torno a temas tan delicados concernientes a la concreción del régimen penitenciario, la concesión de la libertad provisional y la libertad condicional, la reubicación del reo en uno u otro régimen penitenciario, entre otras.

El ejemplo más destacado de IAJVR —aunque no el único⁹⁹— es COMPAS (del que hemos tratado con motivo del caso *State v. Loomis*). Este es un paquete de software de soporte de decisiones automatizado que integra la evaluación de riesgos y necesidades con varios otros dominios, incluidas las decisiones de sentencia, el tratamiento y la gestión de casos, y los resultados de reincidencia¹⁰⁰. Este se basa en más de cien parámetros los cuales incluyen la educación, la historia personal, el barrio o la edad del investigado y, también, utiliza toda la información jurídica disponible relativa a sentencias anteriores similares.

La implementación de sistemas como estos en EE.UU, han sido fuertemente criticados por las ONGs, las cuales cuestionan la fiabilidad de la predicción realizada por estos sistemas. Véase el reportaje periodístico realizado por ProPublica, en donde se hizo

⁹⁸ MIRÓ LLINARES, F., “INTELIGENCIA ARTIFICIAL...”, *Op. Cit.*

⁹⁹ Algunos ejemplos de sistemas de IAJ de valoración de riesgos los encontramos en *Gotham, Cloud Walk, y Rekognition*.

¹⁰⁰ BRENNAN, T., DIETERICH, W., y EHRET, B., “Criminal Justice and Behavior: Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System”, 2009. Disponible en https://www.researchgate.net/publication/321528262_Correctional_Offender_Management_Profiles_for_Alternative_Sanctions_COMPAS

un análisis de 10.000 causas y se reveló que "los acusados negros eran mucho más propensos de ser erróneamente juzgados por tener un mayor riesgo de reincidencia que los acusados blancos, quienes tenían más posibilidades que los acusados negros de ser tildados incorrectamente como 'de bajo riesgo'". Este suceso pone en tela de juicio la equidad del sistema que parece discriminar significativamente al grupo de población afroamericana más que al grupo de población blanca¹⁰¹.

Es por ello que la Comisión cataloga este tipo de usos como “usos a tener en cuenta con las reservas más extremas”. Sobre esto, la Resolución del Parlamento Europeo, de 20 de enero de 2021, sobre inteligencia artificial: cuestiones de interpretación y de aplicación del Derecho internacional en la medida en que la UE se ve afectada en los ámbitos de los usos civil y militar, así como de la autoridad del Estado fuera del ámbito de la justicia penal (2020/2013(INI)) nos indica que “la utilización de sistemas de IA para tomar decisiones por parte de los poderes públicos puede conducir a decisiones sesgadas que afecten negativamente a los ciudadanos y que, por tanto, debe estar sujeta a estrictos criterios de control por lo que respecta a su seguridad, transparencia, rendición de cuentas, no discriminación y responsabilidad social y ambiental, entre otros; insta a los Estados miembros a que evalúen los riesgos relativos a las decisiones basadas en IA en relación con el ejercicio de la autoridad estatal y a que establezcan salvaguardias tales como una supervisión humana apropiada, requisitos de transparencia y la posibilidad de impugnar tales decisiones”¹⁰².

El uso de los sistemas de IAJVR no debe ser tomado a la ligera¹⁰³, hechos como los descritos en ProPublicas ponen de manifiesto que la rendición de cuentas, cuando se hace uso de estos sistemas, es difícil de lograr y que estos pueden introducir sesgos en los procedimientos judiciales —con o sin intención—. Este tipo de sucesos pueden comprometer el proceso judicial penal además de lesionar los derechos y garantías

¹⁰¹ Artículo en línea de ProPublicas “*Machine Bias There's software used across the country to predict future criminals. And it's biased against blacks*”, (última fecha de consulta 25 de mayo 2023) Disponible en: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

¹⁰² Resolución disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_ES.pdf

¹⁰³ Los sucesos sacado a la luz en el reportaje de ProPublicas, no son aislados, tenemos el caso de Jacob Snow, del grupo de izquierdas Unión por las Libertades Civiles en EEUU (ACLU) quien realizó un experimento, aplicando el programa *Rekognition*, que el gigante de Internet, Amazon, está dando gratis a las policías de Florida y Oregón, con fotos de todos los miembros del Congreso de EEUU. *Rekognition* identificó como «delincuentes» a 28 congresistas. La mayoría, hispanos y negros. Sobre más ejemplos del uso de sistemas de IAJ de valoración del riesgos, véase el artículo de El Mundo “*Para qué la Inteligencia Artificial necesita clases de ética: ‘Hemos creado un Frankenstein’*” <https://www.elmundo.es/papel/futuro/2018/09/04/5b883125e5fdea97248b45d6.html> (Ultima consulta: 11 de junio de 2023)

fundamentales de las partes, asimismo se corre el riesgo de que los sesgos presentes en este tipo de herramientas refuercen los sesgos de las personas que reciben los datos procesados por sistemas de IA, creándose así sesgos por automatización¹⁰⁴.

Sobre esta cuestión, NIEVA FENOLL reflexiona lo siguiente: “que una persona entre en una serie de parámetros de riesgo no quiere decir que haya cometido un delito en concreto. Puede que la persona habite en un barrio determinado, sea de una raza concreta, tenga antecedentes o posea un determinado nivel de estudios. Nada de ello importa a la hora de juzgar, puesto que en el momento de establecer su culpabilidad o inocencia sólo se deberán tener en cuenta las pruebas que le relacionen con los hechos concretos de aquel proceso, y nada más. No factores de riesgo que hagan de él un potencial criminal, pero a quien no se pueda relacionar con los hechos. Ya es un error sentenciar así actualmente, y se observa con cierta frecuencia en los casos de insuficiencia probatoria, en los que se buscan a veces dictámenes psicológicos que hagan de la personalidad del reo el indicio fundamental de la comisión del delito. De hecho, obrar de ese modo tiene, por desgracia, gran aceptación social. Pero es completamente rechazable por las razones apuntadas”¹⁰⁵.

El uso potencial de los sistemas de IAJVR debe ser tomado con máximas reservas. Además, sobre una hipotética implementación de estas aplicaciones debemos hacer hincapié que las mismas deben tener supervisión humana.

En definitiva, si bien es cierto que los usos de la IA aplicados al ámbito jurídico pueden aportar una agilidad y eficacia a los sistemas judiciales sin precedentes, agilizando y mejorando los actuales procedimientos procesales, estos vienen también acompañados de grandes sombras. Como vemos en las tareas que despuntan en la actualidad —tanto en la IA como en el Big Data—, estas no están aisladas unos de otros, pues las múltiples aplicaciones que se implementan hoy en día son desarrolladas gracias a un trabajo conjunto de estas tecnologías, e incluso de la robótica. Estos sistemas son dinámicos y han venido para quedarse por lo que su implementación en el ámbito jurídico debe

¹⁰⁴ Se entiende sesgo por automatización «cuando las personas dan un peso excesivo a la información que aparece en sus monitores». Esto puede llevar a que alguien sea considerado sospechoso por un programa informático, que utiliza los datos disponibles para reforzar esa sospecha. Como resultado, la persona que evalúa los datos del programa puede aceptar sus conclusiones sin mayor escrutinio por descuido.

Véase más información en <https://ignasibeltran.com/2023/03/23/inteligencia-artificial-generativa-chat-gpt-y-sesgo-por-la-automatizacion-y-complacencia-automatizada/> (Última consulta: 04 de junio de 2023)

¹⁰⁵ NIEVA FENOLL, J., *La inteligencia artificial y el proceso judicial*. Ed. Marcial Pons, Madrid, 2018, p. 101.

responder al desafío que supone implementar estas tecnologías y a la vez respetar los derechos y garantías de los ciudadanos.

2.2.1. En la fase probatoria: la IA como fuente de prueba y su uso en la valoración de la prueba en el marco del proceso penal

En el proceso penal, la prueba es la actividad mediante la cual se persigue lograr la persuasión del tribunal sobre unos hechos previamente invocados por las partes, esta ha de versar principalmente sobre los hechos alegados en el proceso, controvertidos por las partes¹⁰⁶. Siguiendo a BARONA VILAR —quien a su vez sigue la diferenciación hecha por CARNELUTTI¹⁰⁷—, cuando hablamos de la prueba debemos diferenciar entre la fuente y el medio, así como valorar la manera en que se incorporan al proceso.

Dada la naturaleza de la IA se puede afirmar que esta tiene un encaje en el concepto de fuentes de prueba, pues éstas son “aquellos elementos que existen en la realidad independientemente del proceso, y son portadores de un contenido que alberga información útil para el esclarecimiento de los hechos”¹⁰⁸. Así pues, la IA como fuente de prueba puede aparecer, por ejemplo, en los datos obtenidos por medio de la utilización de dispositivos técnicos de la imagen y de seguimiento y localización durante los actos de investigación.

Pero otros ejemplos, aparecen en objetos de nuestro uso común que emplean sistemas de domótica —los cuales incorporan tecnología de IA—¹⁰⁹. Estos contienen información de nuestra esfera más íntima y que a su vez generan cientos de datos, los cuales crean patrones de comportamiento y pautas de conducta a base de información privada y sensible, la cual puede proporcionar datos valiosos para la investigación.

¹⁰⁶ MARTÍN OSTOS, J., La prueba en el proceso penal acusatorio. En Curso de Especialización en Sistema Penal Acusatorio, 2012, pp. 133-159.

¹⁰⁷ MARTINEZ GARCIA, E., BARONA VILAR, S., PLANCHADELL GARGALLO, A., ETXEBERRIA GURIDI, J. F., ESPARZA LEIBAR, I., & GÓMEZ COLOMER, J. L., *Proceso Penal Derecho Procesal III*. Ed. Tirant lo Blanch, Valencia, 2021.

¹⁰⁸ MARTINEZ GARCIA, E., BARONA VILAR, S., PLANCHADELL GARGALLO, A., ETXEBERRIA GURIDI, J. F., ESPARZA LEIBAR, I., & GÓMEZ COLOMER, J. L., *Proceso Penal... Op. Cit.*

¹⁰⁹ La RAE, en su edición de 2023 se refiere a la domótica como al “conjunto de sistemas que automatizan las diferentes instalaciones de una vivienda”.

Aun así, la utilización de la IA como fuente de prueba, tal y como apunta DE HOYOS SANCHO, plantea cuestiones problemáticas, una de las más importantes vine en relación como la paridad de armas que ha de regir el proceso penal, en donde acusación y defensa deben poder alegar y probar, conociendo previamente los elementos esenciales de la causa¹¹⁰. El problema surge en torno a la falta de transparencia¹¹¹ y claridad de los datos obtenidos por medio de la IA. Estos datos son generados y tratados automáticamente a través de algoritmos, —que pueden ser más o menos complejos—. Estos son creados por empresas (mayoritariamente privadas) las cuáles no se plantean la problemática en torno a falta de claridad y los inconvenientes que esto supone en el seno del proceso penal.

Las fuentes de pruebas empleadas en el proceso penal deben responder a los criterios de transparencia, imparcialidad y equidad, los cuales no siempre están presentes en los algoritmos que conforman la tecnología de IA. Una posible solución sería conocer el “código fuente¹¹²” del algoritmo que gobierna el sistema IA, pero como ya hemos mencionado antes, este tipo de tecnología es desarrollada principalmente por empresas privadas y todos los avances que se desarrollan en este campo —códigos de fuente incluidos— están protegidos por el derecho a la propiedad industrial y amparadas por el secreto comercial, lo cual hace que sea casi imposible que estos sean de conocimiento público. Apunta DE HOYOS SANCHO, que aunque se tuviera acceso a esa información, las partes también necesitan contar con expertos en la materia que pudieran dar fe —o no— de la fiabilidad del sistema de IA y de sus resultados en ese caso concreto¹¹³.

Asimismo, QUATROCOLO pone de manifiesto que la comprensión —en este caso— del código fuente no representa en sí mismo la solución a todos los desequilibrios generados por el uso de datos producidos automáticamente puesto que la comprensión de

¹¹⁰ 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*, nº 76, 2020, pp. 9-44.

¹¹¹ Autores como QUATROCOLO ya hacen eco de la problemática en torno a la falta de transparencia de los algoritmos presente de la IA, tal y como expresa la autora “adquiere un valor aún más marcado respecto de la justicia y, en este contexto, particularmente respecto del proceso penal, en el que están en juego bienes jurídicos supremos, como la libertad personal”.

¹¹² Se denomina código fuente al conjunto de líneas de texto que expresan, en un lenguaje de programación determinado, los pasos que debe seguir el computador para la correcta ejecución de un programa específico. Es decir, se trata de las instrucciones que el programador original del software compiló para que pudieran ser transmitidas a un sistema computacional e interpretadas de manera precisa y oportuna. para ampliar información, visítase <https://concepto.de/codigo-fuente/> (Última fecha de consulta 07 de junio de 2023).

¹¹³ DE HOYOS SANCHO, M., “EL Libro Blanco...”, *Op. Cit.*

este sigue siendo un asunto limitado únicamente a los expertos, con exclusión de los destinatarios efectivos de la 'decisión automatizada'¹¹⁴. De igual manera, CORVALÁN señala que, “aun cuando el desarrollador esté dispuesto a “abrir” el sistema (el código fuente), en los sistemas más avanzados de IA, no hay una forma técnica para determinar la trazabilidad acerca de cómo los algoritmos arriban al resultado, decisión o predicción”¹¹⁵.

Acerca de la valoración de la prueba en el marco del proceso penal, el art. 741 de la LECrim¹¹⁶ el cual consagra el principio de la libre valoración de prueba, que en palabras de FUENTES SORIANO “comporta la necesidad de dejar al Juez libertad plena —pero “responsable”— para determinar razonadamente y a la vista del conjunto de la prueba practicada, qué valor otorgará a cada una de las fuentes de prueba válidamente practicadas en el juicio”¹¹⁷. El principio se encuadra dentro de los límites de la razonabilidad que se espera de las decisiones judiciales. Esto implica que se debe cumplir las reglas de la racionalidad inductiva: el Juez, al valorar el resultado de cada prueba y de todas ellas en conjunto, debe utilizar máximas de experiencia bien fundadas que permitan, por un lado, inferir la participación del acusado en los hechos y, por otro, excluir la razonabilidad de otros hechos que le sean más favorables. Estas inferencias deben constar claramente en la sentencia para que, entre otros fines, la decisión pueda ser objeto de revisión por un tribunal superior en caso de recurso, especialmente en lo que se refiere a la base probatoria de los hechos probados¹¹⁸. Igualmente en este punto no podemos dejar de mencionar la importancia del principio de presunción de inocencia, que rige en el proceso penal y en virtud al cual “toda persona investigada o encausada en un proceso

¹¹⁴ QUATTROCOLO, S. *Intelligenza artificiale e giustizia: nella cornice della Carta ética europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, 2018. Disponible en <https://www.lalegislazionepenale.eu/wp-content/uploads/2019/02/Carta-etica-LP-impaginato.pdf> (Última fecha de consulta 07 de junio de 2023).

¹¹⁵ CORVALÁN, J., “Inteligencia artificial: retos, desafíos y oportunidades...” *Op. Cit.*

¹¹⁶ El art.741 de la LECrim establece que “el Tribunal, apreciando según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley. Siempre que el Tribunal haga uso del libre arbitrio que para la calificación del delito o para la imposición de la pena le otorga el Código Penal, deberá consignar si ha tomado en consideración los elementos de juicio que el precepto aplicable de aquél obligue a tener en cuenta”.

¹¹⁷ FUENTES SORIANO, O., “Comunicaciones telemáticas: práctica y valoración de la prueba” en *El Proceso Penal. Cuestiones Fundamentales* (Coord. FUENTES SORIANO), Ed. Tirant lo Blanch, Valencia, 2017, p. 274.

¹¹⁸ LÓPEZ YAGÜES, V., CALAZA LÓPEZ, S., ASECIO MELLADO, J. M., DEL RÍO LABARTHE, G., FUENTES SORIANO, O., RIZO GÓMEZ, M. B., RUIZ DE LA CUESTA FERNÁNDEZ, S., DOIG DÍAZ, Y., FERNÁNDEZ LÓPEZ, M., CUADRADO SALINAS, C., & OCHOA MONZÓ, V., *Derecho Procesal Penal*, Ed. Tirant lo Blanch, Valencia, 2019, p. 418.

penal debe ser tratada como inocente hasta la condena por sentencia firme. Se presumirá inocente hasta que la culpabilidad quede acreditada en juicio, con todas las garantías necesarias para una defensa”¹¹⁹.

Por lo que respecta al uso de sistemas IA en la fase de valoración de los medios de prueba, si bien consideramos que los sistemas de IA no pueden sustituir el discernimiento conjunto y razonado del Juez en la valoración de todas las pruebas legalmente aceptables que se utilicen en un caso determinado, ya que es el Juez quien, en última instancia, debe tomar su decisión basándose en la duda razonable¹²⁰, sí que pueden adoptarse para otros fines. Su uso puede venir dado en forma de herramienta de apoyo para el Juez en la tarea de valoración de la prueba.

Con la valiosa información que arrojan estos sistemas, tal como apunta BORRAS, pueden crearse “aplicaciones que faciliten al Juez información sobre los medios de prueba basándose en datos registrados o estadísticas, y que le permitirían tener un mayor conocimiento de la credibilidad de los mismos”¹²¹.

Ahora bien, es en la explicación clara de las inferencias provenientes, de la valoración hecha por el Juez, es donde actualmente la IA encuentra uno de sus principales problemas. Estas deben ser claras tanto para las partes como en caso de ser objeto de revisión por un tribunal superior en caso de recurso. En la actualidad, en los sistemas de IA es imposible “objetivar en el lenguaje de los algoritmos los criterios para una mecanizada determinación de la credibilidad de las pruebas”¹²², puesto que tal y como expone DE MIGUEL BERIAIN¹²³, los algoritmos presentes en estas tecnologías “predicen pero no explican”, por lo que de momento su implementación en este punto del proceso es todavía una teorización.

Aun así, los expertos de esta materia empiezan a señalar posibles implementaciones de la IA en este punto con miras a: valorar la credibilidad de los

¹¹⁹ Para más información sobre el principio de presunción de inocencia, visite: <https://www.conceptosjuridicos.com/gt/presuncion-de-inocencia/> (Última fecha de consulta: 5 de julio de 2023).

¹²⁰ DE HOYOS SANCHO, M., “EL Libro Blanco...”, *Op. Cit.*

¹²¹ BORRÁS ANDRÉS, N., “La verdad y la ficción de la inteligencia artificial en el proceso penal”, en *La justicia digital en España y la Unión Europea, Situación actual y perspectivas de futuro* (Coord. ARRABAL PLATERO - GARCÍA MOLINA), Ed. Atelier, 2019, pp. 31-39.

¹²² BORRÁS ANDRÉS, N., “La verdad y la ficción...”, *Op. Cit.*

¹²³ DE MIGUEL BERIAIN, I., “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*, nº 25, 2019, p. 537.

informes periciales, el contexto de las pruebas documentales o incluso las declaraciones testificales, si fuéramos capaces de objetivar los diferentes datos que aporta a este campo la ciencia de la psicología del testimonio¹²⁴; ayuda al esclarecimiento de la posible autoría o de la voluntariedad del consentimiento reflejado en la redacción de un documento, con base en el lenguaje usado o en un estilo de escritura, reconstrucción virtual de hechos delictivos complejos¹²⁵, entre otros.

Ahora bien, es relevante saber qué peso pueden tener los datos obtenidos por una IA dentro de la valoración de la prueba. Señala BORRÁS que “la información arrojada por sistemas de IA debe ser tomada en cuenta por el Juez únicamente para su propia valoración posterior, sin darles carta de verdad de forma automática”¹²⁶. Si bien está claro que las herramientas de IA actuales y futuras pueden ser muy útiles en estas tareas a menudo muy complejas, la realidad es que los datos obtenidos por una IA deben de ser vistos sólo como una herramienta que ayuda al Juez dentro de su proceso deductivo de valoración y bajo ningún concepto pueden ser aceptados automáticamente para decidir la fiabilidad —o no— de una prueba, ya que esto desvirtúa la racionalidad exigible en las decisiones judiciales, suponiendo un vicio dentro del proceso y un socavamiento de las garantías procesales de las partes¹²⁷.

2.2.2. En las medidas cautelares

Las medidas cautelares, siguiendo a MORENO CATENA, pueden entenderse como aquellas actuaciones procesales acordadas por el Juez “encaminadas a impedir que la voluntad del sujeto pasivo logre que el proceso penal resulte ineficaz, burlando el ejercicio del ius puniendi del Estado y los derechos patrimoniales de quienes han de ser reparados de las consecuencias dañosas de los hechos”¹²⁸. En el curso de un proceso penal

¹²⁴ NIEVA FENOLL, J., *La valoración de la prueba*, Madrid, Marcial Pons, 2010, pp. 213 y ss.

¹²⁵ DE HOYOS SANCHO, M., “EL Libro Blanco...”, *Op. Cit.*

¹²⁶ BORRÁS ANDRÉS, N., “La verdad y la ficción...”, *Op. Cit.*

¹²⁷ En este sentido, encontramos apoyo en las palabras de BUENO DE MATA, quien considera 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 consistente en juzgar y hacer ejecutar lo juzgado. Así, defendemos el uso de inteligencia artificial como mecanismo de ayuda o guía al Juez en sentido amplio” en su publicación “*Macrodatos, inteligencia artificial y proceso: luces y sombras*” de 2020.

¹²⁸ MORENO CATENA, V., “Lección 19, Las medidas cautelares. La detención”, en CORTÉS DOMÍNGUEZ, V., MORENO CATENA, V., *Derecho Procesal Penal* 10a Edición, Ed. Tirant lo Blanch, Valencia, 2021, p. 320.

se pueden adoptar un amplio abanico de medidas cautelares; desde la detención preventiva, hasta el embargo de bienes para hacer frente a la responsabilidad civil. Tradicionalmente estas se dividen en dos categorías: medidas cautelares personales y medidas cautelares reales. Las primeras afectan a la persona del investigado, limitando o suspendiendo sus derechos, mientras que las segundas afectan a su patrimonio. Según el autor, estas medidas cautelares “persiguen siempre una finalidad procesal, permitiendo el normal desarrollo del proceso y el cumplimiento de la sentencia”¹²⁹.

La IA dentro de las medidas cautelares puede ser articulada, tal como plantea ÁLVAREZ BUJÁN, mediante “la implementación de sistemas de gestión de datos que permitan prever y valorar la peligrosidad de sujetos o el riesgo de reincidencia a la hora de acordar una medida cautelar de prisión provisional o una orden de protección (en materia de violencia de género)”¹³⁰.

En relación con último uso, dentro del panorama español nos encontramos con el Sistema de Seguimiento Integral en los casos de Violencia de Género —en adelante VioGén—, de la Secretaría de Estado de Seguridad del Ministerio del Interior, la cual es una aplicación web, integrada en la Red SARA española (Sistemas y Redes de Aplicaciones para Administradores). VioGén es una herramienta “diseñada para coordinar las actuaciones de los profesionales públicos españoles que se encargan del seguimiento, asistencia y protección de las mujeres denunciadas de violencia de género y de sus hijos”¹³¹. De este modo, esta aplicación pretende erigir una densa red de instituciones con competencias en el ámbito de la prevención de la violencia de género y dar respuestas rápidas, integrales, eficaces y de alto nivel a la violencia de género en todo el país¹³². VioGén tiene su origen legal en los mandatos del artículo 31 y 32 de la Ley Orgánica 1/2004 sobre las “Medidas de Protección Integral contra la Violencia de Género”¹³³.

¹²⁹ MORENO CATENA, V., “Lección 19, Las medidas cautelares. La detención”, en CORTÉS DOMÍNGUEZ, V., MORENO CATENA, V., *Derecho Procesal Penal* 10a Edición, Ed. Tirant lo Blanch, Valencia, 2021, p. 320.

¹³⁰ ÁLVAREZ BUJÁN, M. V., “Inteligencia artificial y medidas cautelares en el proceso penal: tutela judicial efectiva y autodeterminación informativa en potencial riesgo”, *Revista Española de Derecho Constitucional*, nº 127, 2023, pp. 177-179. <https://doi.org/10.18042/cepc/redc.127.06>

¹³¹ Eticas, “The External Audit of the VioGén System. Association Eticas Research and Innovation”, 2022, p. 12. Disponible en <https://eticasfoundation.org/wp-content/uploads/2022/03/ETICAS-FND-The-External-Audit-of-the-VioGen-System.pdf>

¹³² Eticas, “The External Audit of the VioGén System...” *Op. Cit* p. 12.

¹³³ Para ampliar información consúltese: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2004-21760 (Última fecha de consulta: 21 de junio de 2023).

Según el Ministerio de Interior sus objetivos son: 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 y 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 víctima¹³⁴.

VioGén pretende integrar diferentes servicios públicos, como las FFCCSS, justicia, sanidad, servicios sociales, igualdad y los sistemas penitenciarios para facilitar el intercambio de información. Cuenta con más de 30.000 usuarios con distintos niveles de permiso y acceso. Aunque todos estos usuarios pueden acceder al sistema —y algunos de ellos pueden incluso proporcionar información relevante—, sólo los agentes de la ley (agentes de la Policía y de la Guardia Civil) pueden registrar casos¹³⁵.

Este sistema parte de una serie de preguntas realizadas a la víctima sobre el incidente de agresión, como: la situación de la víctima, los hijos, el perfil del agresor y los agravantes de vulnerabilidad. Cuando la víctima presenta una denuncia oficial contra su agresor, los agentes de policía rellenan el formulario VPR5.0-H., que incluye cinco ámbitos con 35 indicadores de riesgo. Cada elemento se evalúa como "presente" o "no presente". De este modo, la recogida de información está estandarizada en todo el país. Una vez completado el formulario, el sistema asigna una puntuación de riesgo de violencia de género. Los niveles de esta puntuación de riesgo son "no apreciado", "bajo", "medio", "alto" y "extremo". En cuanto a estos niveles de puntuación, los agentes policiales sólo pueden aumentar la puntuación de riesgo a un nivel superior y no al revés; es decir, no pueden reducir la puntuación de riesgo calculada por el algoritmo de VioGén¹³⁶. En función del nivel, se ponen en marcha unas medidas de protección u otras. Por ejemplo, en riesgo extremo, la víctima cuenta con vigilancia policial las 24 horas del día. Con esta información, el sistema puede detectar el riesgo de reincidencia y/o de homicidio¹³⁷.

¹³⁴ Para más información sobre VioGén, visítese la página web del Ministerio de Interior en: <https://www.interior.gob.es/opencms/ca/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen/> (Última fecha de consulta: 21 de junio de 2023).

¹³⁵ Eticas, "The External Audit of the VioGén System..." *Op. Cit.*, p. 12.

¹³⁶ Eticas, "The External Audit of the VioGén System..." *Op. Cit.*, p. 12.

¹³⁷ Esta información fue obtenida del artículo periodístico en línea de RTVE "¿Qué es VioGén y cómo funciona?", del 20 de febrero de 2023. Para más información visite:

De acuerdo con la Auditoría Externa del Sistema VioGén realizada por ETICAS, este sistema “pretende homogeneizar la valoración policial del riesgo de violencia de género y las medidas de protección y prevención asociadas en toda España. El sistema funciona a través de dos formularios (Protocolo Dual): Valoración Policial del Riesgo (VPR) y Valoración Policial de la Evolución del Riesgo (VPER). El formulario VPR realiza la primera valoración del riesgo en el momento de la denuncia de la agresión a la policía, mientras que el formulario VPER realiza el seguimiento de la evolución del riesgo de violencia de género. Estos protocolos de valoración son revisados y corregidos por un equipo multidisciplinar de expertos”¹³⁸.

Según el Ministerio de Interior con VioGén se busca, en última instancia “establecer una tupida red que permita el seguimiento y protección de forma rápida, integral y efectiva de las mujeres maltratadas, y de sus hijos e hijas, en cualquier parte del territorio nacional”¹³⁹. El sistema VioGén se alza como uno de los mayores activos dentro de los protocolos en la lucha contra la violencia machista que tenemos en España y los cuales sirven de inspiración a otros países de nuestro entorno, como es el caso de Francia, que ve en el modelo español una inspiración a la hora de articular su propia política en materia de lucha contra la violencia machista¹⁴⁰.

Las autoridades del servicio de violencia de género¹⁴¹ explican que, aunque el sistema se basa en datos científicos para evaluar cada caso, la decisión final queda en manos de los profesionales, si estos consideran que el nivel de riesgo es superior al que ofrece el sistema pueden subirlo, nunca bajarlo. Ahora bien, como ya se ha señalado, las decisiones alcanzadas por VioGén, son impulsadas por profesionales, quienes en última instancia son quienes pueden decidir ampliar el nivel de riesgo al que está sujeto la víctima. En un sistema judicial garantista como es el nuestro, decisiones de tan importante calado solo pueden ser determinadas por los órganos judiciales competentes —y los

<https://www.rtve.es/noticias/20230220/objetivo-igualdad-funcionamiento-viogen/2424326.shtml> (Última fecha de consulta: 21 de junio de 2023).

¹³⁸ Eticas, “*The External Audit of the VioGén System...*” *Op. Cit* p. 14.

¹³⁹ Para más información sobre VioGén, visítase la página web del Ministerio de Interior en:

<https://www.interior.gob.es/opencms/ca/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen/> (última fecha de consulta: 21 de junio de 2023).

¹⁴⁰ Esta información está contenida en el Pódcast de EL PAÍS, “Así inspiró España al Ministerio de Igualdad francés”, disponible en:

<https://open.spotify.com/episode/72MNRvXwz8fZeKb8XM5TtC?si=Hoz0CeGOQoCJrYRxEXn7Eg> (Última fecha de consulta: 6 de julio de 2023).

¹⁴¹ Estas explicaciones fueron emitidas por Laura López, Jefa de servicio de violencia de género, en la entrevista hecha por RTVE “¿Qué es VioGén...?” *Op. Cit*.

agentes policiales en el caso concreto de VioGén—, pues son ellos quienes tienen el deber y la obligación de garantizar a las partes el derecho de defensa, y por extensión, la tutela judicial efectiva a la hora de acordar medidas cautelares personales (como la imposición de orden de alejamiento, el uso de pulseras telemáticas o la prisión provisional, entre otras).



3. Epígrafe III: Afectación del Big Data y la IA a las garantías procesales y los derechos fundamentales

En este contexto de profundas innovaciones que la incorporación de la tecnología de la IA y del Big Data desata en el ámbito jurídico, se reitera la necesidad de reflexionar sobre los riesgos que estas plantean: los sesgos, la falta de transparencia o la opacidad de los algoritmos son algunos de los problemas que aquejan a estas tecnologías. Analizar el impacto que estas tecnologías tienen sobre las garantías procesales y los derechos fundamentales es una cuestión primordial a la hora de abordar el uso y la regulación de las mismas dentro de nuestro panorama jurídico.

Si bien es cierto que su uso supone grandes mejoras en el ámbito judicial como la rapidez y la eficacia, es vital recordar que el proceso penal, tal y como expresa DE MIGUEL BERIAIN, “está configurado como el único sistema que permite descubrir la verdad de los hechos y determinar el sujeto responsable”¹⁴², por lo que este debe estar regido por el respeto a los derechos y garantías de las partes. En consecuencia, los derechos y garantías que lo rigen, tal como indica SIMÓN CASTELLANO, “no pueden subordinarse a criterios como la mera mejora de la eficiencia o el ahorro de costes”¹⁴³; con lo que la configuración de estas tecnologías dentro de un sistema judicial garantista como el nuestro supone todo un desafío para los operadores jurídicos.

Resulta primordial ponderar los distintos usos de la IA y del Big Data en el ámbito de la justicia frente a las garantías procesales y los derechos fundamentales en juego, pues determinadas aplicaciones generan muchos más dilemas que otras, por su grado de afectación. Por ejemplo, una aplicación destinada a la automatización de los órganos judiciales, véase la implementación de *chatbots* desarrollados a partir de IA o el uso del Big Data para la automatización de procesos en la gestión de expedientes y el análisis de datos, si bien comportan riesgos, estos no son equiparable, a los peligros que entraña la utilización de la IA para cuestiones como la determinación judicial de la responsabilidad por la prestación de un delito. En estos últimos se despliegan una serie de riesgos que, de asumirse, serían a costa de los derechos y garantías de las partes, algo totalmente inasumible.

¹⁴² DE MIGUEL BERIAIN, I., “La inteligencia artificial en...” *Op. Cit.*

¹⁴³ SIMÓN CASTELLANO, P. “Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?”, *Revista de los Estudios de Derecho y Ciencia Política UOC*, nº 33, 2021.

En relación con los problemas que aquejan al Big Data se debe hacer mención de los riesgos que generan una gran preocupación como son la falta de transparencia a la hora de la recolección de datos y por consiguiente la protección de los mismos. Sobre la primera cuestión, STUTZMAN & HARTZOG hacen referencia a la oscuridad por diseño (*obscurity by design*) que se refiere a técnicas que buscan manipular o engañar a los usuarios para que realicen acciones que favorezcan a las empresas u organizaciones que recopilan datos, sin que los usuarios estén plenamente conscientes de lo que están haciendo¹⁴⁴. Estas técnicas pueden incluir, por ejemplo, la presentación de opciones de consentimiento poco claras o confusas, la colocación de botones de aceptación en lugares difíciles de encontrar, o el uso de lenguaje técnico o legal que dificulta la comprensión por parte del usuario medio. El objetivo de estas técnicas de diseño es influir en el comportamiento del usuario y obtener su consentimiento para el uso de sus datos de una manera que beneficie a la organización que los recopila. Esto se enlaza con la preocupación generada en torno a la protección de los datos personales, tal como expone SESELOVSKY¹⁴⁵ —siguiendo a BUENADICHA—, “se espera que quienes recolectan y tratan datos masivos de la ciudadanía garanticen la privacidad de su información” algo que de hecho no se está completamente seguro con la falta de transparencia en el momento de la recolección de datos.

Las prácticas anteriormente descritas van en contra del derecho de los usuarios a controlar y proteger sus datos personales, el cual se configura como un “derecho fundamental de toda persona física que la faculta para disponer y controlar sus datos de carácter personal, pudiendo decidir cuáles proporcionar a terceros, así como conocer quién posee esos datos y para qué, y oponerse a esa posesión o tratamiento”¹⁴⁶. Es

¹⁴⁴ HARTZOG, W. & STUTZMAN, F., “Obscurity by Design”, *Washington Law Review*, University of Washington School of Law, n°88, 2013, pp. 385-418.

¹⁴⁵ SESELOVSKY GONZÁLEZ, S., “*ÉTICA Y TRANSPARENCIA ALGORÍTMICA: ¿QUÉ SE LE DEBE COMUNICAR A LA CIUDADANÍA?*”, Trabajo Final de Carrera, Universidad Adolfo Ibáñez, 2021, p. 12.

¹⁴⁶ Esta definición de derecho de protección de datos personales fue obtenida en RAE disponible en: <https://dpej.rae.es/lema/derecho-de-protecci%C3%B3n-de-datos-personales#:~:text=Const.,a%20esa%20posesi%C3%B3n%20o%20tratamiento>. (Última fecha de consulta: 26 de junio de 2023). La configuración del derecho a la protección de datos como DF nace con la STC 292/2000, de 30 de noviembre, que por primera vez reconoce la existencia del derecho de protección de datos como derecho autónomo e independiente del derecho a la intimidad, en dicha sentencia indica que «el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso».

importante tener en cuenta que la protección de los datos personales no sólo pretende salvaguardar una parte de la vida de los ciudadanos, sino que tiene una finalidad omnicomprendensiva, de protección de los derechos fundamentales en general. Tal como recoge la Agencia Española de Protección de Datos “este derecho tiene como objeto preservar la dignidad humana frente a la invasión que supone la recogida y tratamiento excesivo de datos personales. Su objetivo es el de establecer un marco de garantías que haga posible el ejercicio de los derechos fundamentales y las libertades del ser humano y con el fin de impedir que el uso de la información personal pueda utilizarse indiscriminadamente en contra de dichos derechos y libertades inherentes al ser humano”¹⁴⁷. A esta problemática se suma también lo descrito por SESELOVSKY quien apunta que “el incremento de la colección y análisis de datos puede guiar a una vigilancia estructural que puede tener efectos graves en aquellos derechos fundamentales vinculados con la libertad de expresión, reunión y manifestación o la presunción de la inocencia”¹⁴⁸.

En el terreno procesal, una recopilación de datos masivos del investigado en la fase de investigación sin los correspondientes controles, supondría una vulneración del derecho de las partes a un proceso con todas las garantías, recogido en el art. 24.2 de la CE, así como la vulneración del derecho a la intimidad, el derecho a la protección de los datos de los usuarios, e incluso implicaría una violación del derecho al propio entorno virtual, el cual tal como expone ARRABAL PLATERO “es una garantía constitucional de creación jurisprudencial que protege la información de formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntad o sin ella, genera el usuario hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos (...), y se aplica aquel conglomerado de información varias que contienen ordenador o un teléfono móvil cuya interrelación puede ofrecer un perfil muy preciso de un ciudadano”¹⁴⁹. Además la recogida y tratamiento excesivo de datos personales, sin los límites establecidos por la ley, dentro de la fase probatoria en el momento de obtención de la prueba supone su ilicitud y por tanto la invalidación de la

¹⁴⁷ Para más información consúltese el artículo en línea de la AEPD, titulado “Protección de datos y seguridad” de 20 de abril de 2020, disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/blog/proteccion-datos-seguridad> (Última fecha de consulta 19 de julio de 2023).

¹⁴⁸ SESELOVSKY GONZÁLEZ, S., “*ÉTICA Y TRANSPARENCIA ALGORÍTMICA...*”, *Op. Cit.*

¹⁴⁹ ARRABAL PATERO, P., “El derecho fundamental al propio entorno virtual y su incidencia en el proceso”, en *ERA DIGITAL, SOCIEDAD Y DERECHO*, (Coord. ARRABAL PATERO - DOIG DÍAZ - ORTEGA GIMÉNEZ - TURÉGANO MANSILLA), Tirant lo Blanch, Valencia, 2020.

misma, lo cual implicaría que en muchos caso no fuera posible acreditarse lo hechos y que el órgano judicial no “crea” la alegación de la parte que la presenta.

Es vital asegurarse de que cualquier uso de datos personales por parte de las instituciones públicas se realice de acuerdo con los principios de protección de datos personales y las leyes aplicables, además de que se cuente siempre con el oportuno consentimiento, el cual debe ser dado en una situación en donde los ciudadanos comprendan con claridad los términos en los que su información es recopilada y los usos potenciales que terceros pueden hacer de la misma.

Ligado a esto nos encontramos en la IA con el problema de la falta de transparencia de los modelos computacionales de IA y los sesgos algorítmicos. Tal como apunta ARAYA PAZ, “a pesar de que el número de aplicaciones de IA exitosas en forma transversal en muchos dominios ha crecido de forma exponencial, las decisiones en algunos casos son bastante opacas y por tanto comprensibles solamente a los científicos o diseñadores de los sistemas”¹⁵⁰. Y esto es un problema complejo: el uso de la IA en el proceso se apoya en técnicas predictivas, las cuales a su vez se basan en la obtención y análisis estadístico de diversos datos que, por medio de una programación predeterminada, pueden arrojar resultados porcentuales como consecuencia del cruce de algoritmos inteligentes.

En un primer estadio, tal y como menciona SAN MIGUEL CASO “todo pareciera indicar que, en términos puramente probabilísticos, los resultados obtenidos serían fruto de unas complejas operaciones aritméticas que no traerían, en definitiva, mayores problemas”¹⁵¹, sin embargo esto no resulta así. Estos datos muchas veces son obtenidos por medio de algoritmos opacos, que como ya se ha resaltado son comprensibles para un reducido número de personas, a lo que ha de sumarse los posibles sesgos presentes en la información que estas tecnologías arrojan. No es de extrañar que en algunos algoritmos puedan hallarse sesgos y prejuicios, estos finalmente siguen siendo ideados y desarrollados por personas, si estas son racistas, homófobas, sexistas o clasistas etc., los algoritmos también lo serán —consciente o inconscientemente—.

¹⁵⁰ ARAYA PAZ, C., Transparencia algorítmica ¿un problema normativo o tecnológico? Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S2452-610X2021000200306 (Última fecha de consulta: 5 de julio de 2023).

¹⁵¹ SAN MIGUEL CASO, C., “La aplicación de la Inteligencia Artificial...” *Op. Cit.*

En este punto, algunos podrían rebatir alegando que al igual que los algoritmos, el juzgador puede llegar a tener sesgos. Si bien es cierto que los jueces y magistrados no dejan de ser personas con sus propias ideas y convicciones, estos cuando alcanzan dictámenes siempre deben ser respaldados por la leyes y normativas vigentes, la jurisprudencia y por los principios generales del Derecho, por tanto sus veredictos no corresponden a una voluntad arbitraria, sino que estos están sumisos a la Ley.

La opacidad no es un tema menor puesto que de llegar a estar presente en aplicaciones de IA para el ámbito judicial desembocaría en una situación de desequilibrio entre las partes, de la que ya hemos hablado anteriormente. Esta problemática pone de manifiesto la obligatoriedad de que todas las partes involucradas en el proceso puedan disponer de paridad de armas. Esta situación de desequilibrio genera una situación de indefensión entre las partes que bien puede ser corregida, dotando a estas tecnologías de una claridad para todas las partes envueltas en el proceso penal.

Sobre la opacidad algorítmica, BURELL nos ofrece una explicación de la siguiente forma: “si uno es el destinatario de la salida del algoritmo (la decisión de clasificación), rara vez tiene una idea concreta de cómo o por qué se ha llegado a una clasificación particular a partir de las entradas. Además, las entradas en sí mismas pueden ser completamente desconocidas o sólo parcialmente conocidas”¹⁵².

Este problema parece estar tan incrustado en la tecnología de IA que resulta en un quebradero de cabeza a la hora de articular que la implementación de esta tecnología pueda ser incorporada a determinados usos en el ámbito jurídico. Esta opacidad supone un menoscabo a la tutela judicial efectiva, que en virtud artículo 24.1 de la Carta Magna, se estipula que “todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión”, es por tanto un derecho que tiene toda persona a ejercitar

¹⁵² Así mismo la autora identifica tres tipos de opacidad algorítmica: opacidad como secreto corporativo o estatal intencional, opacidad derivada del analfabetismo técnico y opacidad en la forma en que los algoritmos operan a escala de aplicación. Disponible en BURRELL, J., “*How the machine ‘thinks’: Understanding opacity in machine learning algorithms*. Sage Journals, *Big Data & Society*”, 2016. Disponible en: <https://journals.sagepub.com/doi/full/10.1177/2053951715622512> (Última fecha de consulta: 5 de julio de 2023).

la defensa de sus legítimos intereses ante los órganos judiciales, con la correspondiente intervención de estos¹⁵³.

Junto a la opacidad algorítmica se suma la problemática de la incomprensibilidad en cuanto a cómo las aplicaciones de IA arrojan determinados datos. En nuestro modelo judicial, cuestiones como las que se plantean derivarían en vicios en el proceso judicial y en la consiguiente vulneración al derecho de defensa en el cual, siguiendo a SIMÓN CASTELLANO, se “exige en este campo permitir que todas las partes involucradas identifiquen el uso de la IA en el caso concreto, pudiendo verificar los datos de entrada de los que se nutre el sistema y los criterios de toma de decisión o razonamiento de la herramienta, porque solo así podrá impugnar en su caso la decisión o resultado que esta propone”¹⁵⁴.

El desconocimiento de cómo o por qué se ha llegado a una decisión por parte de los algoritmos operantes en aplicación de IA suponen situar a las parte en una manifiesta situación de indefensión pues “difícilmente podrá defenderse de algo que desconoce”¹⁵⁵. Por tanto, resulta primordial que todos los involucrados en el proceso puedan entender en todo momento cómo se llega a determinadas decisiones cuando se hace uso de estas tecnologías. Ligado a esto está la neutralidad y la objetividad que debe imperar en los instrumentos de IA utilizados por el sistema judicial, que tal como el autor apunta, estos “deben estar en cualquier caso garantizadas y ser verificables”¹⁵⁶.

Una solución a esta incomprensibilidad y opacidad de la que se ha referido es la que propone CORVALÁN, quien exhorta a instaurar lo que él llama “la transparencia algorítmica”. Según éste la IA “debe ser transparente en sus decisiones, lo que significa que se pueda inferir o deducir una explicación entendible acerca de los criterios en que se basa para arribar a una determinada conclusión, sugerencia o resultado”¹⁵⁷. Asimismo SAN MIGUEL CASO —siguiendo a CORVALÁN—, propone la conveniencia y

¹⁵³ Para más información sobre la tutela judicial efectiva, visite: <https://www.unir.net/derecho/revista/tutela-judicial-efectiva/> (Última fecha de consulta: 26 de junio de 2023).

¹⁵⁴ SIMÓN CASTELLANO, P. “Inteligencia artificial y...” *Op. Cit.*

¹⁵⁵ SAN MIGUEL CASO, C., “La aplicación de la Inteligencia Artificial...” *Op. Cit.*

¹⁵⁶ SIMÓN CASTELLANO, P. “Inteligencia artificial y...” *Op. Cit.*

¹⁵⁷ CORVALÁN, J., “Inteligencia artificial: retos, desafíos y oportunidades...” *Op. Cit.*

necesidad de que “la Inteligencia Artificial se explique en un lenguaje accesible para todos y que, como consecuencia, rige el principio de transparencia algorítmica”¹⁵⁸.

La repercusión de los sesgos resulta trascendental, pues esta representa uno de los principales obstáculos para la salvaguarda de las garantías procedimentales¹⁵⁹. Tal y como expone ARAYA PAZ, “en determinadas situaciones los sistemas de IA se “alimentan” con la experiencia o los conocimientos humanos, para posteriormente tomar decisiones autónomamente. Sin embargo, esto puede acarrear importantes sesgos relacionados con el sexo, la raza, la edad, etc., que pueden ser perjudiciales para las personas”¹⁶⁰.

Ahora bien lo cierto es que en la construcción de tecnologías inteligentes tales como la IA o el Big Data —como en cualquier otro sistema inteligente—, el diseño e implementación de los algoritmos necesarios, que no están exentos de la parcialidad del validador, pues tal como expone MARTÍNEZ GARAY, “los algoritmos son un mero reflejo de los datos con los que se los alimenta, de modo que si esos datos incorporan sesgos el algoritmo los reproducirá, o peor aún, los exacerbará”¹⁶¹.

Es particularmente importante mencionar los sesgos que pueden filtrarse en el momento del diseño. Dado que esta tecnología está desarrollada por personas, no es descabellado pensar que los sesgos propios de estos puedan verse reflejados en la misma, queriéndose o no queriéndose. La predictibilidad que nos ofrecen estos programas, tal y como lo refleja BARONA VILLAR “se eleva a la cúspide de los resultados, pero a costa de las personas o, mejor si cabe, de determinadas personas”¹⁶². Un ejemplo que nos plantea la autora es el de algunos estados americanos que a través de la elaboración de programas informáticos que determinan los altos índices de probabilidad de que el acusado (negro o latino, hombre, de clase social muy baja) vuelva a delinquir, estimula a una condena con una pena más grave¹⁶³. Resulta cuanto menos inquietante que por una mala configuración de esos sistemas se emitan dictámenes o consejos que a la hora de

¹⁵⁸ SAN MIGUEL CASO, C., “Las técnicas de predicción judicial y su repercusión en el proceso”, *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro*, Atelier, 2019, pp. 41-49.

¹⁵⁹ SAN MIGUEL CASO, C., “La aplicación de la Inteligencia Artificial...” *Op. Cit.*

¹⁶⁰ ARAYA PAZ, C., Transparencia algorítmica ¿un problema normativo o tecnológico? Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S2452-610X2021000200306 (Última fecha de consulta: 5 de julio de 2023).

¹⁶¹ MARTÍNEZ GARAY, L., “PELIGROSIDAD, ALGORITMOS Y DUE PROCESS: EL CASO STATE vs. LOOMIS”, *Revista De Derecho Penal Y Criminología*, n°20, 2020, pp. 485-502.

¹⁶² BARONA VILAR, S., “Cuarta revolución industrial...”, *Op. Cit.*

¹⁶³ BARONA VILAR, S., “Cuarta revolución industrial...”, *Op. Cit.*

fijar la sentencia y fijar la calidad y cantidad de la pena resulten discriminatorios para determinados colectivos en base a una fe ciega a la tecnología que en muchas ocasiones se muestra como infalible pero que evidentemente puede tener fallos. Sin lugar a dudas la presencia de sesgos es una de las mayores amenazas cuando se plantea la entrada de estas tecnologías dentro del ámbito judicial y muy especialmente cuando se trata del proceso penal.

En este punto traemos a colación la propuesta de CORVALÁN sobre la aplicación del principio de imparcialidad del validador. De acuerdo con este principio quienes diseñan, entrenan o desarrollan los algoritmos inteligentes, no puedan participar en el proceso de validación. El autor enfatiza la indispensabilidad en cuanto a que las autoridades públicas intervengan en el proceso y exijan legalmente que esto ocurra. Esto no implica que todos los sistemas de IA deban someterse a este proceso de verificación y validación, pero es crucial cuando se desarrollan algoritmos que afectan a la vida, la seguridad, la libertad y la salud de las personas¹⁶⁴.

Llegados a este punto es importante que este desarrollo tecnológico —tanto del Big Data judicial, como la IA empleada en el ámbito jurídico—, sea desarrollado conjuntamente con especialistas jurídicos y humanistas que puedan ayudar a proporcionar un enfoque más amplio, al meramente tecnológico, a la hora de como poder innovar el ámbito judicial y al mismo tiempo respetar los derechos y garantías de los ciudadanos, que se ven amenazados cuando el diseño de los mismo no es claro y transparente.

Para finalizar, los ejemplos expuestos en este epígrafe (que si bien no es una lista cerrada dada la naturaleza y mutabilidad de estas tecnologías), ponen de relieve la complejidad y dificultad de abordar esta innovación. Tal como expresa CORVALÁN “es clave poner el tema en agenda, pensar en un esquema de cooperación internacional y, al mismo tiempo, crear entornos normativos propicios”¹⁶⁵. Esto supone también establecer principios rectores aplicables a los sistemas de IA y Big Data, que sean compatibles con nuestro modelo procesal penal, por lo que se aboga por un desarrollo de estas tecnologías que sea compatible con el Estado constitucional y en particular con nuestro derecho procesal.

¹⁶⁴ CORVALÁN, J., “Inteligencia artificial: retos, desafíos y oportunidades...” *Op. Cit.*

¹⁶⁵ CORVALÁN, J., “Inteligencia artificial: retos, desafíos y oportunidades...” *Op. Cit.*

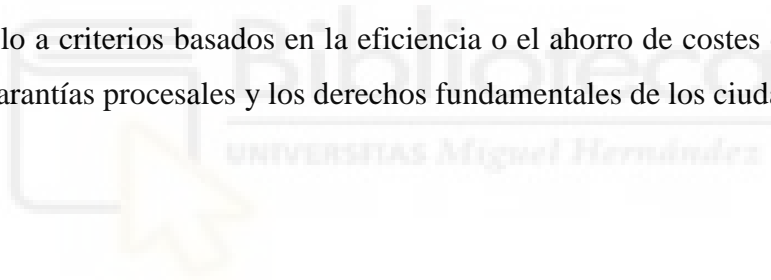
CONCLUSIONES

Primera. La aplicación del Big Data en el ámbito judicial amplía las brechas entre países desarrollados que pueden adquirir e implementar dichas aplicaciones en el ámbito judicial frente a los menos desarrollados que no puedan adquirirlas. Estos últimos se enfrentan a situaciones que ponen de manifiesto las desigualdades existentes y el empeoramiento en la calidad de los sistemas judiciales.

Segunda. El uso de la IA en lo referente a la toma de decisiones judiciales sólo debe plantearse como una ayuda a los jueces y magistrados y no como una sustitución de los mismos.

Tercera. Las aplicaciones que se desarrollen mediante tecnología de IA y Big Data dentro del ámbito jurídico deben pasar todos los filtros que garanticen una transparencia en ellas, asimismo estas deben ser impulsadas no solo por ingenieros o desarrolladores de software, sino también por expertos jurídicos y humanistas que puedan proporcionar una visión amplia del panorama judicial y social.

Cuarta. La incorporación de la IA y del Big Data en el ámbito de la justicia no puede supeditarse solo a criterios basados en la eficiencia o el ahorro de costes cuando entran en juego las garantías procesales y los derechos fundamentales de los ciudadanos.



BIBLIOGRAFÍA

ÁLVAREZ BUJÁN, M. V., “Inteligencia artificial y medidas cautelares en el proceso penal: tutela judicial efectiva y autodeterminación informativa en potencial riesgo”, *Revista Española de Derecho Constitucional*, nº 127, 2023.

ARRABAL PATERO, P., “El derecho fundamental al propio entorno virtual y su incidencia en el proceso”, en *ERA DIGITAL, SOCIEDAD Y DERECHO*, (Coord. ARRABAL PATERO - DOIG DÍAZ - ORTEGA GIMÉNEZ - TURÉGANO MANSILLA), Tirant lo Blanch, Valencia, 2020.

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*, vol. 3, nº 1, 2019, pp. 1-17.

BARONA VILAR, S., *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021.

BECERRA, J., COTINO-HUESO, L., LEÓN, I. P., SÁNCHEZ-ACEVEDO, M. E., TORRES-ÁVILA, J., VELANDIA-VEGA, J., *Derecho y big data*, Ed. Editorial Universidad Católica de Colombia, Bogotá, 2018.

BORRÁS ANDRÉS, N., “La verdad y la ficción de la inteligencia artificial en el proceso penal”, en *La justicia digital en España y la Unión Europea, Situación actual y perspectivas de futuro* (Coord. ARRABAL PLATERO - GARCÍA MOLINA), Ed. Atelier, 2019, pp. 31-39.

BUENO DE MATA, F., “Macrodatos, inteligencia artificial y proceso: luces y sombras”, *Revista General de Derecho Procesal*, nº 5, Iustel, 2020.

BUJOSA VADELL, L., BUENO DE MATA, F., *La Prueba en el Proceso Penal. Perspectivas Nacionales*, Ed. Tirant lo Blanch, Valencia, 2018.

CORTÉS DOMÍNGUEZ, V., MORENO CATENA, V., *Derecho Procesal Penal 10a Edición*, Ed. Tirant lo Blanch, Valencia, 2021.

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*, nº 76, 2020, pp. 9-44.

DE LA OLIVA SANTOS, A., FERNÁNDEZ, M. A., *Derecho Procesal Civil, vol. II*, Centro de Estudios Areces, Madrid, 1996, p. 305.

DE MIGUEL BERIAIN, I., “La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados”, *Revista De Derecho De La UNED (RDUNED)*, nº 25, 2019, pp. 531-561.

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 De La UNED (RDUNED)*, nº 25, 2020, pp. 531–561.

FUENTES SORIANO, O., “Comunicaciones telemáticas: práctica y valoración de la prueba”, en *El Proceso Penal. Cuestiones Fundamentales* (Coord. FUENTES SORIANO), Ed. Tirant lo Blanch, Valencia, 2017, pp. 254-278.

HARTZOG, W. & STUTZMAN, F., “Obscurity by Design”, *Washington Law Review*, University of Washington School of Law, nº88, 2013, pp. 385-418.

HERNÁNDEZ GIMÉNEZ, M., “Inteligencia artificial y Derecho Penal”, *Actualidad Jurídica Iberoamericana*, nº 10, 2019, pp.792-843.

MARTÍN OSTOS, J., “La prueba en el proceso penal acusatorio”, en *Curso de Especialización en Sistema Penal Acusatorio*, 2012, pp. 133-159.

MARTÍNEZ GARAY, L., “PELIGROSIDAD, ALGORITMOS Y DUE PROCESS: EL CASO STATE vs. LOOMIS”, *Revista De Derecho Penal Y Criminología*, nº 20, 2020, pp. 485-502

MARTINEZ GARCIA, E., BARONA VILAR, S., PLANCHADELL GARGALLO, A., ETXEBERRIA GURIDI, J. F., ESPARZA LEIBAR, I., GÓMEZ COLOMER, J. L., *Proceso Penal Derecho Procesal III*, Tirant lo Blanch, Valencia, 2021.

MIRÓ LLINARES, F., “Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots”, *Revista De Derecho Penal Y Criminología*, nº 20, 2020, pp. 87–130.

MUÑOZ RODRIGEZ, A., “EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL”, *Anuario de la Facultad de Derecho*, Universidad de Extremadura, nº 36, 2020, pp. 695-728.

NIEVA FENOLL, J., *La inteligencia artificial y el proceso judicial*. Ed. Marcial Pons, Madrid, 2018.

NIEVA FENOLL, J., *La valoración de la prueba*, Marcial Pons, Madrid, 2010, pp. 213 y ss.

PUYOL MORENO, J., “Una aproximación a Big Data”, *Revista De Derecho De La UNED (RDUNED)*, nº 14, 2018, pp. 471–506.

RALLO LOMBARTE, A., “El nuevo derecho de protección de datos” *Revista Española de Derecho Constitucional*, nº 116, 2019, pp. 45-74.

SAN MIGUEL CASO, C., “La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?”, *IUS ET SCIENTIA Revista electrónica de Derecho y Ciencia*, nº 1, Vol. 7, Ed. Universidad de Sevilla, 2021.

SAN MIGUEL CASO, C., “Las técnicas de predicción judicial y su repercusión en el proceso”, *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro*, Atelier, 2019, pp. 41-49.

SESELOVSKY GONZÁLEZ, S., “ÉTICA Y TRANSPARENCIA ALGORÍTMICA: ¿QUÉ SE LE DEBE COMUNICAR A LA CIUDADANÍA?”. Trabajo Final de Carrera, Universidad Adolfo Ibáñez, 2021.

SIMÓN CASTELLANO, P., “Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?”, *Revista de los Estudios de Derecho y Ciencia Política UOC*, nº 33, 2021.

VILLAVERDE MENÉNDEZ, I., “PROTECCIÓN DE DATOS PERSONALES, DERECHO A SER INFORMADO Y AUTODETERMINACIÓN INFORMATIVA DEL INDIVIDUO. A PROPÓSITO DE LA STC 254/1993” *Revista Española de Derecho Constitucional*, nº 41, 1994, pp.187-224.

VVAA, *Derecho Procesal Penal* (Dir. ASECIO MELLADO; Coord. FUENTES SORIANO), Ed. Tirant lo Blanch, Valencia, 2019.