INTELIGENCIA ARTIFICIAL Y MEDIDAS CAUTELARES EN EL PROCESO PENAL: TUTELA JUDICIAL EFECTIVA Y AUTODETERMINACIÓN INFORMATIVA EN POTENCIAL RIESGO

Artificial intelligence and precautionary measures in the criminal process: effective judicial protection and informative self-determination in potential risk

MARÍA VICTORIA ÁLVAREZ BUJÁN[1]
Universidad Internacional de La Rioja
mariavictoria.alvarezbujan@unir.net

Cómo citar/Citation
Álvarez Buján, M. V. (2023).
Inteligencia artificial y medidas cautelares en el proceso penal:
tutela judicial efectiva y autodeterminación informativa en potencial riesgo.
Revista Española de Derecho Constitucional, 127, 177-179.
doi: https://doi.org/10.18042/cepc/redc.127.06

Resumen

En este trabajo se realiza un examen de los riesgos y peligros que el uso presente y futuro de la inteligencia artificial puede suponer, a la hora de adoptar la medida cautelar de prisión provisional, para los derechos de la ciudadanía en general y de los justiciables en particular, haciendo especial hincapié en lo que respecta a los derechos a la autodeterminación informativa y a la tutela judicial

[1] El presente trabajo se ha realizado en el marco del Proyecto de investigación intitulado «El Tribunal Constitucional como baluarte de las garantías constitucionales en el proceso penal», de la Universidad Internacional de La Rioja (convocatoria «Financiación de Proyectos Propios UNIR 2022»). Investigador principal (IP): Pere Simón Castellano. La fecha de inicio y fin del proyecto es el 29/07/2022 y el 31/08/2024, respectivamente. La cuantía total de financiación asciende a 8.200 euros.

efectiva (entendida en sentido amplio). Asimismo, se trata de facilitar pautas que permitan hacer práctico, útil y lícito el empleo de este tipo de sistemas tecnológicos sin caer en el error de exceder los límites marcados por los principios de legalidad y proporcionalidad. Como es evidente, ante el avance que suponen los mecanismos de inteligencia artificial como método de auxilio para la mayor eficacia y agilidad del sistema judicial, el derecho debe asignarse la tarea de incardinar de forma correcta la implementación del uso de dichos recursos en este contexto, preservando las garantías constitucionales.

Palabras clave

Inteligencia artificial; proceso penal; prisión provisional; tutela judicial efectiva; autodeterminación informativa; problemática; respuestas.

Abstract

The main aim of this study is to examine the risks and dangers that the present and future use of artificial intelligence may pose, at the time of adopting the precautionary measure of provisional prison, for the rights of citizens in general and of the defendants in particular, with special emphasis on the rights to informative self-determination and effective judicial protection (understood in a broad sense). Likewise, we will try to provide guidelines that allow the use of this type of technological system to be practical, useful and lawful without falling into the error of exceeding the limits set by the principles of legality and proportionality. As is evident, given the progress that artificial intelligence mechanisms represent as a method of assistance for the greater efficiency and agility of the judicial system, the Law must assign itself the task of correctly incardinating the implementation of the use of said resources in this context, preserving constitutional guarantees.

Keywords

Artificial intelligence; criminal proceedings; precautionary imprisonment; effective judicial protection; informative self-determination; problematic; answers.

SUMARIO

I. PLANTEAMIENTO PREVIO

Es innegable el cambio de era al que asistimos, la revolución de la digitalización que, en un futuro, que ya se hace más bien presente, camina de la mano del tan célebre, en los últimos tiempos, llamado 5G. Esa quinta generación de las tecnologías y estándares de comunicación inalámbrica que nadie sabe con propiedad en qué consiste ni qué implica, pero que se concibe como un avance tecnológico, que aumentará la velocidad de conexión, permitirá que las interacciones con internet o la nube sean prácticamente instantáneas, al disminuir al mínimo la denominada «latencia» (es decir, el tiempo de respuesta de la página web o el tiempo que tarda en transferirse un conjunto de datos dentro de la red), multiplicará masivamente el número de dispositivos conectados y muy especialmente posibilitará conectar a las personas con todo lo que nos rodea (aparatos tecnológicos, electrodomésticos, vehículos…), incidiendo en la industria[2], la medicina, la salud, los hogares y hasta el sistema judicial[3]. Ese 5G que va unido al «internet de las cosas» y a la denominada inteligencia artificial (en adelante, IA) está cada día más en boga y

[2] Verbigracia, la industria de la automoción e incluso la industria de la propia telefonía, donde el *smartphone* quedará como un elemento residual, teniendo en cuenta la promoción de otro tipo de dispositivos tecnológicos (*smartwatches, smartbands* y variantes) y la *e-sim*, que paulatinamente irá reemplazando a las *sim cards* tradicionales y que consiste en un chip que está integrado en los propios dispositivos. *Vid.* información al respecto en https://bit.ly/3k7fC8c (ultima consulta: 6-12-2021).

[3] *Vid.* información en https://bit.ly/31n2XPq (última consulta: 6-12-2021).

tiene proyección en casi todos los ámbitos, incluido el jurídico (y en particular, el constitucional y procesal).

Esa IA que ya no es un ensueño de películas de ciencia ficción como *Yo, robot*, sino que se encuentra, entre otros aspectos, íntimamente ligada con la utilización de artilugios como *smartphones*, *smartwatches*[4], elementos de domótica, sistemas de asistencia a la conducción, etc., así como con el manejo masivo de datos y la utilidad que ello reviste en diversos contextos, por ejemplo, en la emisión de resoluciones por órganos jurisdiccionales (de forma «automatizada») o en 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).

Esa misma IA que desde hace años viene a poner en tela de juicio la preservación real y efectiva de determinados derechos fundamentales. Esa IA que acucia a juristas de todo el mundo, frente a la que, aun cuando pueda proponer pautas e ideas para intentar asumir y desarrollar la convivencia con tal recurso en la sociedad, tratando de evitar la materialización de graves riesgos y peligros en la esfera de los derechos fundamentales (intimidad, autodeterminación informativa, tutela judicial efectiva…), en modo alguno puede aseverar que se logren salvaguardar ni los derechos y libertades ni, por ende, las garantías inherentes a un sistema judicial instaurado en el marco de un Estado de derecho.

Esa IA ha venido para quedarse y, cuando menos, hemos de conocer sus entresijos, su cara y su cruz (dicho de otro modo, sus ventajas y sus desventajas o sus riesgos, peligros y facilidades). Pero sobre todo hemos de acometer la empresa de concienciar al sector jurídico de la importancia de no perder de vista el significado y alcance de los derechos, libertades y garantías y de no dejar en manos de la informática, la tecnología y la ciencia las respuestas que solamente el derecho (y quienes tienen encomendada la competencia o labor de valorar prueba, ponderar intereses en conflictos y argumentar de forma razonada y coherente) puede ofrecer, procurando, además (aunque ello se antoje una quimera), que no nos las ofrezca, como es costumbre, lamentablemente, demasiado tarde.

Así, en el presente trabajo analizaremos la incidencia de la IA en el marco procesal penal y, más en concreto, en lo que respecta al aseguramiento de la autodeterminación informativa, el derecho de defensa y, por extensión, el derecho a la tutela judicial efectiva en el momento de acordar una medida

[4] Que incluyen sensores biológicos para medir parámetros del cuerpo humano y sugerir pautas de conducta.

cautelar de prisión provisional, aspectos que preocupan desde una óptica tanto constitucional como procesalista y práctica.

II. EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA EN JAQUE EN EL MARCO DE UN PROCESO PENAL

1. ORIGEN, CONCEPTO Y DIMENSIONES

El derecho a la protección de datos de carácter personal o derecho a la autodeterminación informativa conforma un derecho de nueva configuración, cuyo reconocimiento se inició con la doctrina y jurisprudencia germana y se consolidó a partir de la sentencia del Tribunal Constitucional alemán, de 15 de diciembre de 1983, al entender que su protección dimanaba del contenido de los arts. 1.1 y 2.1 de la carta fundamental alemana, de forma que solamente podría ser restringido o limitado por «graves motivos de interés público» (Garriga Domínguez, 2009: 31-33).

Surgió la duda de si este derecho era una dimensión más del derecho a la intimidad o si, por el contrario, tenía contenido y finalidad diferentes e independientes. Nuestro Tribunal Constitucional se pronunció abogando por su concepción como un nuevo derecho fundamental de carácter autónomo y, justamente, considerando sus particularidades, acuñó un término específico para referirse a este, ese anteriormente mencionado y que hoy no nos resulta ya tan ajeno, derecho a la autodeterminación informativa (De Miguel Sánchez, 2004: 27-36)[5]. La autonomía de este derecho se confirma, además, a la vista del art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que adquirió fuerza vinculante con la firma del Tratado de Lisboa el 13 de diciembre de 2007. A la luz de este precepto, toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Los datos personales deben ser tratados 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. Y obviamente la propia persona sujeto de ese derecho, como una manifestación de este, debe poder tener acceso a los datos recogidos y almacenados que la conciernan y a su rectificación, gozando como garantía añadida de una autoridad independiente que controle el respeto de estas normas.

El legislador europeo ha venido persiguiendo el objetivo de garantizar que el tratamiento de los datos de carácter personal en el ámbito de la Unión

[5] Véanse las SSTC 290/2000, de 30 de noviembre, y 292/2000, de 30 de noviembre.

no devenga genérico, difuso, abstracto o masivo, sino concreto y vinculado a un fin claro, determinado y lícito. En este contexto, la obtención y tratamiento de los datos solamente se concibe bajo dos hipótesis: o el consentimiento de la persona titular de la información o, en defecto de este, la pertinente habilitación legal contemplada a tal efecto (Azaustre Ruiz, 2015: 809)[6]. Ello implica que, si se efectúa una cesión inapropiada de los datos personales (al margen de las hipótesis mencionadas), puede resultar nula (especialmente si se realiza con la pretensión de que los datos personales obtenidos sean utilizados en el ámbito de un proceso penal), y ello, con independencia de que se haya menoscabado (o no) el derecho a la intimidad de la persona titular de los datos (*op. cit.*).

Lo anterior nos conduce a afirmar que el derecho a la autodeterminación informativa no se ciñe a la facultad de negar información de carácter personal, privado o íntimo, sino a la faceta de poder controlarla. Por ello, se estima que nos hallamos ante un derecho de clara vertiente activa, por cuanto persigue que la persona pueda gozar del dominio de sus propios datos (Caruso Fontán, 2012: 137-141). Según apunta, entre otros autores, Caruso Fontán (*ibid.*: 139), haciéndose eco de Jareño Leal, se da un paso más allá de lo que sería el significado y alcance del derecho a la intimidad, pues «ya no se tratará de la libertad de exclusión que faculta al individuo a negar información relativa a las propias experiencias personales, sino de la facultad activa de dominio de la información referida a dichas experiencias o datos personales».

En efecto, el derecho fundamental a la protección de datos tiene una trascendental relevancia en el marco del proceso penal que se observa «desde el mismo momento en que la fase de investigación constituye una continuada intromisión en el ámbito de tutela que propicia toda la normativa de protección de datos personales, y tal Derecho Fundamental debería quedar incorporado también entre las garantías del debido proceso» (Ortiz Pradillo, 2022: 110).

La normativa aplicable en materia de protección de datos en el ámbito de la Unión Europea se encuentra conformada por dos instrumentos fundamentales. Por un lado, la norma esencial de aplicación en materia de protección de datos de carácter personal, que entró en vigor el 24 de mayo de 2016 y no resultó directamente aplicable hasta el 25 de mayo de 2018, esto es, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al

[6] La necesidad de incorporar habilitaciones legales que permitan el acceso a datos de carácter personal (cuando no existe consentimiento por parte de la persona afectada) viene a responder a la existencia de intereses legítimos en determinados contextos y situaciones, como puede ser, particularmente, el interés público en la investigación y persecución delictiva.

tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD), y, por otro lado, la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Este último instrumento resulta de aplicación específica al tratamiento de datos de carácter personal realizado a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, pero, a diferencia del Reglamento (directamente aplicable), necesita ser transpuesta por las legislaciones de los distintos Estados miembros. En España se llevó a cabo su transposición, con notable demora, a través de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. De hecho, como consecuencia de esta coyuntura, en el ordenamiento jurídico español, cuando las autoridades policiales y judiciales que se ocupaban de una investigación delictiva, persiguiendo un interés o fin legítimo, precisaban recurrir a la obtención de datos personales que se hallaban en poder de terceros:

> […] se venía defendiendo la suficiencia de la habilitación general a favor de los Cuerpos y Fuerzas de seguridad prevista en el artículo 22.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal —en vigor transitoriamente, también en virtud de lo dispuesto por la LO 3/2018, hasta la entrada en vigor de la reciente 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, que ha incorporado nuevas garantías y mayores salvaguardas en la obtención, tratamiento y cesión de dichos datos en el ámbito de la investigación criminal— (Ortiz Pradillo, 2022: 110).

En definitiva, nos encontramos ante un nuevo panorama, en el que el actor principal ya no es la regulación nacional, como acontecía mientras estuvo vigente la Directiva 95/46/CE, y ello, al margen de que a nivel interno los diferentes Estados miembros puedan aprobar sus propias normas de protección de

datos al objeto de incluir algunas precisiones o aspectos de desarrollo en materias en las que el RGPD así lo permita.

Si descendemos ahora al marco constitucional, dentro del ordenamiento jurídico español, podemos ver que el derecho a la autodeterminación informativa se consagra en el art. 18 de nuestra carta magna, al establecer su apartado 4 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» (Garriga Domínguez, 2009: 33-43). Este derecho se desarrolla en la ya mencionada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[7], y cuenta con dos vertientes o elementos. De un lado, engloba el elemento negativo, relativo al cumplimiento de los principios de calidad de los datos y restantes exigencias aplicables a la obtención, tratamiento y uso de los datos personales para asegurar su veracidad, así como la pertinencia, congruencia y racionalidad de su uso (Álvarez González, 2011: 56). Y, de otro lado, comprende el elemento positivo, que se materializa en un conglomerado de facultades, denominadas *habeas data*, que podrían definirse como «un conjunto de derechos que el ciudadano puede ejercitar frente a quienes sean titulares —públicos o privados— de ficheros de datos personales, con la finalidad de conocer la existencia o no de tales ficheros, su contenido, uso y destino» (Álvarez González, 2011: 56)[8].

En resumidas cuentas, las referidas facultades permiten a un sujeto averiguar «quién, qué, cuándo y con qué motivo puede conocer datos que le conciernen» (Pérez Luño, 1993: 407; Álvarez González, 2011: 56)[9]. Así las cosas, toda persona tiene derecho a que se solicite su consentimiento, que deberá ser facilitado de forma libre e informada, para proceder a la recogida, tratamiento y/o cesión de sus datos personales (Sánchez Bravo, 1998: 369). Igualmente se reconoce el derecho de información, de forma que la persona afectada por la inscripción de sus datos debe ser informada (de forma clara y comprensible) sobre la existencia de los ficheros en los que estos se encuentran y con qué finalidad (Álvarez González, 2011: 57-60; Garriga Domínguez, 2011: 29-33).

Asimismo, toda persona goza de los denominados derechos ARCO:

---

7 Con anterioridad a la aprobación del Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 arriba reseñados, en el ordenamiento jurídico español se aplicaba la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

8 *Vid*., asimismo STC 290/2000, de 30 de noviembre.

9 *Vid*. también SSTC 254/1993, de 24 de julio (FJ 7); 290/2000, de 30 de noviembre (FJ 5), y 292/2000, de 30 de noviembre (FJ 7).

— Derecho de oposición: es la facultad previa de control para intentar evitar que se efectúe el tratamiento de los datos personales o lograr que se cese este.
— Derecho de acceso: se concreta en «la facultad de control a iniciativa del interesado para comprobar qué datos sobre su persona obran en un banco de datos» (Álvarez González, 2011: 57).
— Derechos de rectificación y cancelación: «[…] constituyen un mecanismo de protección del individuo frente a la recopilación de datos inexactos o incompletos» (Álvarez González, 2011: 57-58)[10].

Amén de lo anterior, se reconoce el célebre y polémico «derecho al olvido», que procura la protección de la persona a fin de que pueda recuperar sus datos cuando haya transcurrido un largo período de tiempo o cuando haya desaparecido la finalidad legítima para la cual se recabaron, evitando que sigan utilizándose o siendo públicos (Álvarez González, 2011: 57; Garriga Domínguez, 2000: 306)[11].

En relación con este particular derecho cabe reseñar, si bien de forma tangencial, el célebre caso de Mario Costeja. En 1998, *La Vanguardia* publicó dos anuncios sobre una subasta de inmuebles ligada a un embargo por deudas con la Seguridad Social. Ulteriormente, en la edición *online* del periódico se publicó otro anuncio en el que figuraba el nombre de Mario Costeja como propietario de dichos inmuebles. En 2009, a través del buscador de Google, si se introducía «Mario Costeja», aparecía la referencia a los anuncios, aun cuando lo relativo al embargo ya se había solventado tiempo atrás. Mario Costeja contactó con la editorial del periódico para procurar el borrado de sus datos personales, pero esta se negó y conminó al afectado a contactar con Google. Tras la negativa de Google a eliminar dichos datos, el afectado interesó amparo a la Agencia Española de Protección de Datos, que conminó a Google Spain SL y a Google Inc para que retirasen los datos de Mario Costeja de su índice de búsquedas, impidiendo el acceso futuro de terceros a dicha información. Empero, Google interpuso un recurso ante la Audiencia Nacional, solicitando la nulidad de la

[10] Otro de los derechos de capital importancia en relación con el tratamiento de la inteligencia artificial es la prohibición —con carácter general, pues existen excepciones— de decisiones individuales automatizadas, incluida la elaboración de perfiles, aspecto al que aludiremos en el siguiente epígrafe de este trabajo.

[11] La protección de este singular derecho fue fortalecida en el Reglamento (UE) 2016/679, de Parlamento Europeo y del Consejo, de 27 de abril (considerandos 65 y 66).
Varios de los aspectos comentados en este subepígrafe han sido tratados en Álvarez Buján (2018: 175-190).

resolución de la AEP y este Tribunal remitió un conjunto de cuestiones prejudiciales al TJUE, que fueron resueltas en su sentencia (de la Gran Sala) de 13 de mayo de 2014, que condenó al buscador a eliminar datos que vulneren la ley de privacidad[12]. Esta fue la primera vez en que el TJUE reconoció el derecho a que se elimine de la red una información personal antigua que perjudica a un individuo (y cuya publicación ya no resulta lícita ni legítima), posibilitando, así, que otros ciudadanos pudiesen reclamar, tanto a Google como a otros buscadores de internet, la eliminación de *links* o enlaces que redirijan a páginas web donde aparezca información personal (de forma indebida)[13].

Pero, más allá del derecho al olvido, hemos de aludir también, como broche de oro, al denominado derecho fundamental a la protección del entorno virtual del individuo, reconocido por una corriente jurisprudencial que se ha ido abriendo paso ante las novedades de la era digital. Este derecho se vincula con la necesidad de tutelar «toda esa información digital que diariamente creamos, modificamos, almacenamos o almacenan otros respecto de nuestra vida (datos personales, económicos, sanitarios, ideológicos, de conexiones, comunicaciones, localizaciones, etc.)» (Ortiz Pradillo, 2022: 111).

Tal y como explica el Tribunal Supremo, dentro de ese denominado «derecho al propio entorno virtual» convergen aquellos otros derechos ligados al empleo de las nuevas tecnologías, y todos ellos deberán considerarse cuando haya que valorar la adopción de medidas que impliquen un sacrificio sobre estos (Ortiz Pradillo, 2022: 111), como sería, verbigracia, el acceso al contenido de las redes sociales de un sujeto (como Facebook, Twitter, TikTok o Instagram…) en el marco de una investigación delictiva[14].

En cualquier caso, llegados a este punto, debemos matizar que el asunto sobre Mario Costeja se ha comentado aquí de forma incidental por su proyección (al menos indirecta) en el uso de los sistemas de IA en el ámbito judicial, si

---

[12] El contenido de dicha resolución está disponible en https://bit.ly/2OKMoHs (última consulta: 5-1-2022).

[13] Existe información publicada en prensa sobre el icónico caso de Mario Costeja (abogado) en diversos medios; por ejemplo, https://bit.ly/2DY1KVL (última consulta: 5-1-2022). El fallo del TJUE pivota alrededor de la idea de que Google es responsable del procesamiento que hace de los datos personales que aparecen en sus páginas web, incluida la información que se publica en medios de comunicación, como *La Vanguardia*, impidiendo, así, que el gran ente usase como parapeto el derecho a la libertad de expresión a fin de justificar la publicación de información desfasada, desactualizada y, por tanto, ya no veraz que afecta a la privacidad de ciudadanos (Martínez Otero, 2017: 114-133).

[14] El autor acoge en sus reflexiones, que compartimos, la doctrina de la STS 342/2013, de 17 de abril.

bien somos conscientes de que los buscadores de internet recaban y someten a tratamiento datos personales bajo la premisa jurídica del denominado «interés legítimo», mientras que los sistemas de IA, cuyo empleo se propone para el marco del proceso penal, deben tener su sustento de tratamiento en una ley que regule el ejercicio de una función pública, como es la investigación y persecución delictiva, el ejercicio del *ius puniendi* o la impartición de justicia. Ahora bien, el hecho de que pudiéramos encontrarnos aquí ante funciones, valores o bienes jurídicos de mayor calado[15] no implica que pueda tolerarse el uso indiscriminado en cualquier caso y forma de herramientas de inteligencia artificial en el sistema judicial, pues, antes al contrario, toda restricción de derechos (en la esfera procesal penal) debe sujetarse estrictamente a los principios de legalidad y proporcionalidad. De lo contrario, las actuaciones judiciales realizadas no podrán reputarse lícitas. Así, cuando se recopile información objeto de tratamiento por los sistemas de IA en un proceso penal (y en particular para adoptar medidas de prisión provisional), deberá garantizarse que esta no se haya extraído ni cruzado mediante procesos de búsqueda indebidamente habilitados o configurados.

2. DERECHO A LA AUTODETERMINACIÓN INFORMATIVA *VS* IA EN EL MARCO DEL PROCESO PENAL

Como punto de partida en este epígrafe y teniendo en cuenta los límites previstos para el presente trabajo, que no nos permiten ahondar en la prolijidad que el examen exhaustivo del derecho a la autodeterminación informativa requeriría, a los meros efectos que nos ocupan, conviene resaltar la interrelación existente entre proceso y tecnología/informática/IA, dado que son los sistemas informáticos y ahora propios de la denominada IA los que posibilitan la recopilación, análisis, gestión, acceso y transmisión automatizada, ágil y rápida de datos a través del uso de algoritmos para su ulterior aplicación y utilización en las distintas fases y trámites procesales (desde las medidas cautelares hasta inclusive la fase de ejecución de la pena).

Tal coyuntura incrementa exponencialmente los riesgos de generar injerencias no solo en la esfera íntima de las personas titulares de la información manejada, sino también, como examinaremos, en su derecho a la defensa y a la tutela judicial efectiva (Álvarez González, 2007: 139-140; Etxeberría Guridi, 2000: 198-200). Y, en este contexto, hemos de recordar dos premisas

[15] Obviamente el interés legítimo de un buscador (e inclusive el interés que terceros puedan tener en el funcionamiento de ese buscador) es un paradigma mucho más endeble que la necesidad de garantizar, por ley, la realización de la justicia.

incuestionables a las que toda actuación jurídico-procesal ligada al uso de mecanismos o sistemas propios de IA debe supeditarse: el principio de legalidad (que solamente puede cumplirse, de forma adecuada, mediante la existencia de una previsión expresa libre de subterfugios y analogías) y el principio de proporcionalidad, entendido en sentido amplio (con los subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto).

En este orden de cosas, y colateralmente, hemos de llevar a cabo una precisión en lo tocante al principio de proporcionalidad, de consagración constitucional, a la vista de los principios, derechos y libertades que sientan las bases del Estado social y democrático de derecho y del tenor de los arts. 1.1, 9.3, 10 y 25 de la CE (Aguado Correa, 1999: 96; González-Cuéllar Serrano, 1990: 51-53). Forma parte de los denominados «límites de los límites» a los derechos fundamentales, dado que «opera como uno de los criterios empleados para controlar la actividad de los poderes públicos que incide en la órbita de tales derechos» (Lopera Mesa, 2006: 45). Además, este principio, en el ámbito del ordenamiento jurídico español, y más en particular en el marco del proceso penal, se encuentra expresamente contemplado desde la inclusión de la regulación de las medidas de investigación tecnológica en los arts. 588 a bis y siguientes de la LECrim, a través de la reforma parcial implementada sobre dicho texto legal en el año 2015[16].

El primer integrante de la proporcionalidad es el llamado subprincipio de idoneidad, que se relaciona con el «principio de finalidad» y consiste en «hacer realidad la adecuación del medio al fin, adecuación objetiva, cualitativa, derivada de la propia naturaleza de la medida y que atiende a la finalidad concreta que se trata de conseguir, y cuantitativa, que atenderá a la intensidad y repercusión, que sobre los derechos fundamentales afectados tiene la medida, de manera que la medida concretamente apetecida, resulta apta para satisfacer la finalidad a la que sirve» (Iglesias Canle, 2003: 98).

Ahora bien, la idoneidad o adecuación (de forma aislada) no es suficiente si no se une a la necesidad o subsidiariedad, lo que supone que no puede existir ninguna otra medida menos lesiva o de menor entidad para lograr el mismo fin perseguido, pues, de lo contario, habrá que decantarse por la aplicación de la medida que suponga una injerencia inferior en los derechos y libertades del sujeto al cual se aplica (Bernal Pulido, 2007: 740).

Empero, idoneidad y necesidad conforman una simbiosis con un tercer elemento, esto es, la proporcionalidad en sentido estricto, la cual «supone constatar si la medida "es ponderada o equilibrada, por derivarse de ella más

[16] Con la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

beneficios que ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto"; esto es, que la medida "aun siendo idónea y necesaria, el sacrificio que se imponga de tales derechos no resulte desmedido en comparación con la gravedad de los hechos y de las sospechas existentes" (f.j. 4.ºE)» (Etxeberría Guridi, 2000: 82). Además de lo anterior, el principio de proporcionalidad exige que una medida que limite derechos fundamentales se aplique solamente cuando recaigan indicios racionales y suficientes de criminalidad sobre una persona en concreto y exista gravedad delictiva en los hechos que se investigan (Iglesias Canle, 2003: 84-92; Álvarez Buján, 2018: 195-206).

En el marco de la adopción de la medida cautelar de prisión provisional, la exigencia de cumplir con los referidos requisitos que integran el principio de proporcionalidad se recoge en el tenor del art. 502 de la LECrim, el cual, en su apartado 2, viene a disponer que tal medida solamente se adoptará cuando sea objetivamente necesaria y siempre que no existan otras medidas menos gravosas para el derecho a la libertad a través de las cuales puedan alcanzarse los mismos fines que con la prisión provisional.

Asimismo, en su apartado 3, exige que el órgano judicial tome en cuenta la repercusión que la medida pueda tener en la persona investigada o encausada, antes de adoptarla, considerando sus circunstancias y las del hecho objeto de las actuaciones, así como la entidad de la pena que pudiera ser impuesta. Finalmente, en su apartado 4, dicho precepto prohíbe la adopción de la medida de prisión provisional cuando de las investigaciones practicadas se infiera racionalmente que los hechos no son constitutivos de delito o que fueron cometidos bajo la concurrencia de una causa de justificación.

Allende, hemos de dirigir nuestra mirada a los tan célebres denominados «algoritmos», cuyo uso va *in crescendo* en los sistemas judiciales de los distintos países, especialmente en el orden jurisdiccional civil y penal. Se están desarrollando mecanismos de IA que sirvan para apoyar e, inclusive, en determinados casos, reemplazar, las decisiones de los órganos jurisdiccionales. Y por ello no hemos de perder de vista la necesidad de que esos mecanismos de IA sean lícitos y, a tal efecto, han de atender y respetar las exigencias del principio de proporcionalidad en los términos *ut supra* indicados.

Pero, además, con la recopilación masiva de datos y su análisis automatizado se realizan pruebas para tratar de identificar los patrones de decisión de los órganos jurisdiccionales (Castellanos Claramunt y Montero Caro, 2020: 75). Y aquí es, justamente, donde se pone de manifiesto la virtualidad entre la conexión del derecho a la autodeterminación informativa y el derecho a la tutela judicial efectiva. Por ello, no resulta en modo alguno baladí tratar concretamente, en el presente trabajo, ciertos pormenores del derecho a la autodeterminación informativa, puesto que, como justamente se asevera en el

considerando 26 de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril[17], a la luz de lo propugnado en el art. 47 de la Carta de Derechos Fundamentales de la Unión Europea y en el art. 6 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, «el principio de tratamiento leal en materia de protección de datos es un concepto distinto del derecho a un "juicio imparcial"». Y dicho considerando reseña acto seguido la relevancia de informar debidamente «a las personas físicas de los riesgos, reglas, salvaguardias y derechos aplicables en relación con el tratamiento de sus datos personales, así como del modo de hacer valer sus derechos en relación con dicho tratamiento».

Y más importante se revela aquí todavía el art. 11 de la mencionada Directiva (UE) 2016/680, cuyo tenor se ha trasladado a la dicción del art. 14 de la LO 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 concreto, este precepto prohíbe las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el derecho de la Unión Europea. A tal fin, exige que la norma habilitante del tratamiento establezca las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluido el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada (De Hoyos Sancho, 2022a)[18]. Además, impone que tales decisiones no se basen en las categorías especiales de datos personales contempladas en el art. 10 de la misma directiva, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado[19]. Esos datos son aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la

[17] Este instrumento regula el tratamiento de datos en las actividades de prevención, investigación y enjuiciamiento de infracciones penales, resultando, por tanto, aplicable al ámbito procesal penal.

[18] En relación con este punto, debe citarse también el art. 22 del Reglamento (UE) 2016/679 (RGPD), que, sin perjuicio de las especialidades recogidas para el ámbito de aplicación de la Directiva (UE) 2016/680, es la norma general en materia de protección de datos y reconoce el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

[19] Igualmente se prohíbe la elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales.

afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida o las orientaciones sexuales de una persona física[20]. Es decir, son precisamente esos datos que no pueden utilizarse como patrón de selección o juicio discriminatorio en la programación de los sistemas de IA.

En definitiva, aun cuando nos situemos ante dos elementos o derechos disímiles e independientes uno del otro, parece obvio que un inadecuado, incorrecto o ilícito, desviado o abusivo tratamiento o transferencia de datos de carácter personal, que infrinja las reglas de la proporcionalidad, repercutirá directa y negativamente en las garantías del debido proceso, derivando, como consecuencia, la vulneración del derecho de defensa, el derecho a la presunción de inocencia y, por extensión, el derecho a la tutela judicial efectiva (Álvarez Buján, 2018: 190). De esta idea se desprende la necesidad de utilizar con cautela y las debidas garantías los métodos de IA en el ámbito judicial, lo que, entre otros extremos, implica que se ha de asegurar que la obtención de la información y datos sometidos a tratamiento por los sistemas de IA haya sido lícita y proporcionada[21], verificando su veracidad y autenticidad y evitando que su manejo o interpretación por medio de algoritmos incurran en sesgos que puedan redundar en discriminaciones y resoluciones injustas o arbitrarias (cuestión a la que aludiremos más adelante).

III. LA (IM)POSIBILIDAD DE GARANTIZAR EL DERECHO A LA TUTELA JUDICIAL EFECTIVA

1. EL EFECTO DE LAS PREDICCIONES DERIVADAS DE LA INTELIGENCIA ARTIFICIAL SOBRE LA VIRTUALIDAD DEL DERECHO A LA TUTELA JUDICIAL EFECTIVA Y EL DERECHO A NO DECLARAR CONTRA SÍ MISMO

El paradigma de los derechos en el ámbito procesal es, sin duda, el denominado derecho a la tutela judicial efectiva, entendido en conjunto con todas

[20] Su tratamiento (art. 10 Directiva [UE] 2016/680) solamente se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando:

a) lo autorice el derecho de la Unión o del Estado miembro;
b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o
c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

[21] Esto es, sin invadir innecesaria ni injustificadamente aspectos de la privacidad de la persona.

sus manifestaciones, que se halla consagrado en el art. 24 de la CE. En síntesis, como bien apunta Vidal Fueyo (2021: 22-23), «se trata de un precepto que, con carácter general, refleja la prohibición de autotutela de los derechos e intereses propios que caracteriza el sistema de separación de poderes del Estado de Derecho, en el que un poder distinto al legislativo y al ejecutivo ostenta la facultad de impartir justicia aplicando las leyes». Se reconoce así el derecho de toda la ciudadanía 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[22]. Y esta garantía constitucional engloba diversos derechos fundamentales de configuración legal:

a) el derecho de acceso a la jurisdicción;
b) el derecho a los recursos legalmente establecidos;
c) el derecho a obtener una resolución judicial congruente, motivada y fundada en derecho;
d) el derecho a la ejecución de las resoluciones judiciales, así como a su invariabilidad o intangibilidad;
e) la garantía de indemnidad, y
f) el derecho a no sufrir indefensión.

Como comparativa, cabe recordar aquí que, a lo largo de los años, en nuestro ordenamiento jurídico, ya hemos tratado de afrontar y solventar, incluso desde la faceta legislativa, los problemas que en la praxis suponía el uso de determinadas pruebas científicas (léase los análisis de ADN o de sustancias químicas y estupefacientes) y medidas o recursos de investigación tecnológica (como la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos). Así, tuvo singular importancia la aprobación de la reforma parcial operada a través de la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales

[22] Esa tutela implica poder hacer uso efectivo de los derechos al juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia (art. 24.2 CE).

y la regulación de las medidas de investigación tecnológica[23]. Y una línea similar mantiene también el texto del Anteproyecto de LECrim de 2020, en actual tramitación y a la espera de que se dilucide si definitivamente será este texto el que implemente la reforma integral que viene demandando desde hace décadas nuestro sistema procesal penal (decimonónico), o si, al igual que sucedió con el Anteproyecto para un nuevo proceso penal de 2011 y el Borrador de Código Procesal Penal de 2012, se convertirá en un mero intento más de reforma, frustrado por problemas de índole política.

Ahora bien, el art. 24 de la CE debe ser puesto en sintonía con el art. 17 del mismo texto, el cual exige, como garantías ineludibles, que toda persona detenida sea informada con inmediatez y de forma comprensible tanto de sus derechos como de las razones de su detención, no pudiendo ser en ningún caso obligada a declarar. Además, para conseguir que el principio de presunción de inocencia se destruya es imprescindible que exista una mínima prueba de cargo, que siempre deberá ser recabada con arreglo a la ley, las garantías constitucionales y procesales. De lo contrario, dicha prueba devendrá nula *ex* art. 11.1 de la LOPJ al estimarse que se habrá obtenido mediante la vulneración de derechos y libertades fundamentales, y, por tanto, carecerá de valor y eficacia probatoria. (Álvarez de Neyra Kappler, 2008: 132-133).

Ambos preceptos constitucionales (arts. 17 y 24) sientan las bases de un complejo sistema de garantías a favor de la persona investigada, que en un Estado democrático de derecho tiene como objetivo principal el de proporcionar al justiciable una tutela judicial efectiva, asegurar en todo momento del proceso la presunción de inocencia y el derecho de defensa de forma eficaz, amén de conseguir que, en caso de que, finalmente, la persona en cuestión resulte condenada, lo sea a través de un juicio justo.

Cabe aquí que nos preguntemos hasta qué punto podría afectar el uso de la IA en relación con el derecho a no declarar, delimitado en los últimos tiempos de forma severa o restrictiva, particularmente desde que el TEDH, en su emblemática sentencia sobre el caso *John Murray contra el Reino Unido*, de

[23] Esta ley trató de incorporar una regulación expresa, aunque en cierta medida parca y mejorable, a fin de asegurar las garantías necesarias para la realización lícita de determinadas diligencias de investigación tecnológica, ya que, como reza en su propia exposición de motivos (apartado IV), tales actuaciones carecían hasta ese momento de cobertura y su subsanación no podía procurarse «acudiendo a un voluntarista expediente de integración analógica que desborda los límites de lo constitucionalmente aceptable. Solo así se podrá evitar la incidencia negativa que el actual estado de cosas está proyectando en relación con algunos de los derechos constitucionales que pueden ser objeto de limitación en el proceso penal».

8 febrero de 1996, consideró que no se infringía el art. 6 del CEDH si el tribunal nacional realizaba una inferencia probatoria contraria al silencio, es decir, si se derivaban consecuencias «negativas» del ejercicio del derecho a guardar silencio. Obviamente, esas consecuencias perjudiciales para la persona acusada no pueden aplicarse de forma generalizada, sino que es necesario que las pruebas de cargo requieran una explicación que el acusado debería/podría ser capaz de dar y, pese a ello, no la facilita, lo que permite que el órgano jurisdiccional nacional pueda concluir, por sentido común, que no existe tal explicación posible y que, por ende, el acusado es culpable[24].

A nuestro juicio, esta tesis sostenida por el TEDH no hace sino diluir las reglas de la carga de la prueba en el proceso penal, tratando de asegurar (cuando la acusación no es capaz de recabar otro material de prueba) el ejercicio del *ius puniendi*. En efecto, si unimos esta línea argumental con lo acontecido en el caso *Wisconsin contra Loomis*, podemos encontrarnos ante un eventual peligro de que si los métodos de IA no son empleados bajo el estricto cumplimiento de los principios de legalidad y proporcionalidad, arriba mencionados, podría producirse una vulneración del derecho a no declarar, especialmente cuando se utilice (por los mecanismos de IA) una información que no haya sido facilitada, ni aclarada ni acreditada o desacreditada por la persona acusada.

En efecto, concurre:

> […] un altísimo número de procesos judiciales en los cuales se observa de forma clara e indudable la ausencia de entidad legal en el conflicto. Es decir, la exigencia de tutela «jurídica» de derechos e intereses en una destacable mayoría de asuntos carece de conflictividad legal en cuestión, o la que presenta es insuficiente y nimia, para exigir la puesta a su disposición (del conflicto) de todo el complejo entramado que implica el proceso judicial y de todos los medios personales y materiales que requiere (Martín Diz, 2014: 174).

Aquí, precisamente (aun cuando el autor citado se centra en el estudio de los ADR), es donde, entre otros ámbitos, podría tener cabida algún tipo de

[24] Correlativamente, hemos de aludir al considerando 29 de la Directiva (UE) 2016/343 del Parlamento Europeo y del Consejo, de 9 de marzo, por la que se refuerzan en el proceso penal determinados aspectos de la presunción de inocencia y el derecho a estar presente en juicio, donde se reconoce que «el ejercicio del derecho a no declarar contra sí mismo no debe impedir a las autoridades competentes recabar las pruebas que puedan obtenerse legalmente del sospechoso o acusado mediante el ejercicio legítimo de poderes coercitivos, y que tengan una existencia independiente de la voluntad del sospechoso o acusado». Véase también aquí el art. 7.3 de la citada directiva.

sistema basado en la IA, sobre todo en el marco del proceso civil. Pensemos, por ejemplo, en la resolución de un proceso monitorio, en el que, si no se formula oposición por la parte demandada, se procede a la ejecución y al embargo. Podríamos decir que la clase de resoluciones que se dictan en estos supuestos son «tipo» y que, en su consecuencia, podrían emitirse de forma ágil y rápida mediante el uso de algoritmos.

Pero, además, la IA se proyecta en el ámbito del proceso penal y, en particular, en lo que se viene denominando «justicia predictiva», especialmente a la hora de dilucidar si procede aplicar una determinada medida cautelar y, con más particularidad, la medida cautelar personal más restrictiva de derechos, es decir, la prisión provisional.

No podemos perder de vista que las medidas cautelares son un instrumento controvertido por distintas razones. La prisión provisional es la medida cautelar más grave y su adopción genera una situación excepcional (en el sentido negativo del término) para las personas internas (en virtud de tal medida) en instituciones penitenciarias, puesto que no pueden disfrutar de permisos ordinarios de salida ni acceder a programas de reinserción y tampoco tienen prioridad ni acceso a destinos, programas educativos, talleres y otras actividades ocupacionales. Y esta situación tiene repercusión en la esfera psicosocial porque, entre otros factores, se origina una suerte de discriminación entre los condenados y los internos en virtud de una medida cautelar de prisión provisional[25].

Ciertamente, en las decisiones sobre adopción de medidas cautelares, como la prisión provisional,

> […] se produce una suerte de automatismo en relación con casos parecidos o análogos que han sido resueltos con anterioridad, porque ante la falta de actividad probatoria difícilmente se pueden apoyar en algo más. Se refuerza el anclaje basado en la comodidad y la necesaria reducción de la carga de trabajo, la accesibilidad y la disponibilidad en relación con aquellos argumentos que el juzgador tiene más cerca, esto es, los de quien solicita o interesa la medida, es decir, el Ministerio Fiscal, y la representatividad (Simón Castellano, 2021: 122).

El problema que se plantea y por el cual se halla de plena actualidad el estudio para la implementación de sistemas de IA en el marco de las decisiones

[25] Esta argumentación se plasmó en la Memoria del Proyecto de Investigación INTELJURÍDICA, solicitado a finales de 2021 al Ministerio de Asuntos Económicos y Transformación Digital, por un conjunto de investigadores, incluida la propia autora de este trabajo, siendo los investigadores principales el prof. Dr. Simón Castellano y el prof. Dr. Abadías Selma.

judiciales, particularmente en lo tocante a la adopción de medidas cautelares, no es otro que el hecho de que, a fin de cuentas, los órganos judiciales se encuentran encarnados por personas que realizan sus procesos deductivos y construyen sus pensamientos y argumentaciones alrededor de ideologías, experiencias, emociones, sesgos y prejuicios, y ello, aun cuando deban ejercer las funciones jurisdiccionales bajo el paraguas de los principios de imparcialidad e independencia. Y por tal motivo, precisamente, una de las claves del tema que nos concierne reside en «determinar si tales formas de tomar decisiones pueden ser replicadas, y en su caso mejoradas, con sistema de IA que, manejando datos en mayor cantidad y de mejor calidad que los retenidos por la memoria humana, puedan servir de complemento eficaz a las decisiones judiciales, al nutrir la valoración judicial sobre los presupuestos de adopción de las medidas cautelares» (Neira Pena, 2021: 1905).

Ahora bien, hemos de preguntarnos cómo se programan y diseñan esos sistemas de IA. «Si los sistemas algorítmicos de toma de decisiones se basan en decisiones humanas previas, es probable que los mismos sesgos que potencialmente socaven la toma de decisiones humanas se repliquen y multipliquen en los sistemas algorítmicos de toma de decisiones» (Castellanos Claramunt y Montero Caro, 2020: 75). Sin duda, la realidad que nos asiste es que

> […] existe el peligro de que los sistemas de apoyo basados en inteligencia artificial sean utilizados de manera inapropiada por los jueces para «delegar» decisiones a sistemas tecnológicos que no fueron desarrollados para ese propósito y se perciben como más «objetivos» incluso cuando este no es el caso. Con ello, por ejemplo, puede ocurrir que un individuo sea sentenciado con más dureza de la que habría o debería haber sido enjuiciado (*ibid*.: 76).

2. EL ROL DE LAS PREDICCIONES A LA HORA DE DECIDIR SOBRE LA PRISIÓN PROVISIONAL

Muchos autores ponen sobre la mesa las ventajas que podría plantear el uso de sistemas de IA, adecuadamente diseñados, en tanto que suponen un método automatizado de evaluación de riesgos que se basa en evidencias y datos objetivos. Y los sugieren como mecanismos para tratar de superar justamente las deficiencias del modelo actual de adopción de medidas cautelares, originadas por los sesgos y prejuicios de los juzgadores que, además, sobrepasados en muchas ocasiones por la carga del trabajo de los juzgados y tribunales, realizan a la postre su trabajo de forma autómata, tomando (improcedentemente) por analogía las mismas decisiones que en casos similares, sin atender a las particularidades del sujeto en cuestión.

En efecto, los jueces tienden a basarse en sus procesos de pensamiento, en buena medida, en variables (consideradas muchas veces de forma desproporcionada) como la nacionalidad de la persona investigada o encausada y/o la dinámica delictiva observada. A estas variables se les otorga en ocasiones una preponderancia injustificada, simplemente porque concurrían en casos resueltos con anterioridad (y que encima pudieran ser representativos o icónicos), sin ponderar apropiadamente otras variables diferentes del caso en concreto que se enjuicia (Neira Pena, 2021: 1904).

Y aquí hemos de tomar también en consideración que, tal y como resalta Neira Pena (*ibid*.: 1902) haciéndose eco de Simón Castellano (2021: 120), «la influencia del contexto más cercano al juzgador, junto con variables emocionales, condicionadas por aspectos como la apariencia o el lenguaje empleado por el encausado, tienen todavía más peso cuando se trata de decisiones que han de adoptarse de forma rápida y con una actividad probatoria nula o muy limitada, como ocurre con las medidas cautelares».

Con certeza, contamos ya con diferentes sistemas de predicción de riesgo (*risk assessment instruments*, *Public Safety Assessment*, PSA) que se utilizan, tras la condena, en más de veinte jurisdicciones de Estados Unidos desde hace años (Castellanos Claramunt y Montero Caro, 2020: 73). En este contexto debe recordarse que en Estados Unidos ya se han introducido de forma obligatoria distintos *softwares* para predecir la probabilidad de reincidencia de delincuentes y han sido cuestionados, teniendo en cuenta, sin ir más lejos, lo sucedido con el caso *Wisconsin contra Loomis*, en el que se empleó el programa informático Compas (Castellanos Claramunt y Montero Caro, 2020: 77-78; De Hoyos Sancho, 2021: 3-4)[26].

[26] Sucinta e incidentalmente debemos explicar lo acontecido en 2013 cuando Eric Loomis fue detenido por la Policía del estado de Wisconsin (EE. UU.) cuando conducía un vehículo supuestamente involucrado en un tiroteo. Fue acusado de huir de la Policía y usar el vehículo sin autorización de su propietario. En la vista sobre su libertad condicional, el fiscal presentó un informe efectuado por el programa informático Compas (desarrollado por la empresa privada Northpointe Inc), que utiliza diversos vectores (edad, sexo, historial criminal, etc.) a fin de categorizar a los acusados en una escala de riesgo de 1 a 10. Según este programa, el riesgo de reincidencia y de cometer actos violentos era elevado y el juez impuso una pena de seis años de prisión y otros cinco años de libertad vigilada. La defensa recurrió la sentencia por haberse violado el derecho a un proceso con todas las garantías, ya que no se habían podido discutir los métodos empleados por el programa informático (el algoritmo era secreto y únicamente lo conocía la empresa creadora).

La Corte Suprema del estado de Wisconsin desestimó estos argumentos y estimó que ese programa informático tomaba como base los factores habituales para evaluar la peligrosidad criminal y el riesgo de reincidencias, como huir de la Policía y el historial

Llegados a este extremo, y en el marco de las medidas cautelares, no podemos obviar la necesaria mención a sus dos presupuestos esenciales: el *fumus boni iuris* y el *periculum in mora*. El primero se corresponde con la célebre «apariencia de buen derecho», que se manifiesta en la imputación y consta de un elemento objetivo y otro subjetivo, que se deben inferir de las actuaciones a fin de poder decretar la prisión provisional (Moreno y Cortés, 2011: 285). En primer lugar, el elemento objetivo implica que consten en la causa uno o varios hechos que revistan caracteres de delito y que dichos delitos tengan atribuida una pena privativa de libertad de cierta gravedad[27]. En segundo lugar, el elemento subjetivo del *fumus* supone que en la causa concurran motivos suficientes para poder considerar penalmente responsable del delito a la persona investigada o encausada sobre la que se va a dictar el auto de prisión provisional (*ibid*.: 285-287).

En suma, el *fumus boni iuris* consiste en «un juicio de imputación reforzado, esto es, un juicio provisional sobre la atribución de responsabilidad al encausado por un determinado hecho. Se trata, por lo tanto, de reconstruir el pasado, valorando jurídicamente los hechos investigados, y no de predecir el futuro ni de asignar probabilidades a hechos inciertos» (Neira Pena, 2021: 1908).

Por su parte, el requisito del *periculum in mora* permite establecer los fines que ha de cumplir la prisión provisional, los cuales deben adecuarse a los postulados constitucionales. En síntesis, y según reiterada doctrina constitucional a la que alude Moreno Catena (2011: 288)[28], lo que se pretende con la adopción de esta medida es lo siguiente:

— Asegurar la presencia de la persona investigada/encausada, cuando existe peligro de fuga, evitando que se sustraiga a la acción de la justicia.

---

delictivo previo. Avaló, así, la constitucionalidad del uso de algoritmos procesados informáticamente, mediante un sistema de IA, sin comprobar si el algoritmo se utilizaba de forma acertada y si evaluaba incorrectamente, entre otros extremos, las valoraciones de género. Y aun cuando el recurrente no pudo acceder a una explicación clara sobre el tratamiento informático de los algoritmos y los datos manejados, la Corte Suprema de Estados Unidos no revisó la sentencia de la Corte Suprema de Wisconsin. No se consideró vulnerado el derecho a un proceso justo y este asunto se convirtió en el segundo caso en el que una Corte Suprema estatal aceptó la utilización de cálculos de riesgos matemáticos a la hora de dictar una resolución de condena criminal y el primero que permite y ampara que esos cálculos se efectúen transgrediendo el principio de transparencia, es decir, con un algoritmo cuyo diseño y funcionamiento es secreto (Castellanos Claramunt y Montero Caro, 2020: 77-78).

27 En relación con este punto, debe atenderse al contenido del art. 503 LECrim.

28 SSTC 40/1987, 33/1999, 14/2000, 47/2000, 169/2001, 207/2000 y 217/2001.

— Evitar que el investigado/encausado oculte, manipule o destruya fuentes de prueba.
— Impedir la reiteración delictiva.

Habida cuenta del significado y aplicación de ambos presupuestos, *fumus boni iuris* y *periculum in mora*, podemos colegir que la aplicación de la IA en lo que respecta al primero de dichos presupuestos se presenta no solo más limitada, sino también controvertida, y ello, por cuanto no resulta ni fácil ni factible sustituir al órgano judicial a la hora de valorar jurídicamente los hechos objeto de investigación, valoración que, además, no puede ser predictiva ni prospectiva y debe hacerse tomando como parámetro la preservación de la libertad de la persona investigada (ya que el carácter restrictivo de la medida implica que esta debe adoptarse con carácter subsidiario y no generalizado), el principio *in dubio pro reo* y el principio de presunción de inocencia.

Ahora bien, la IA sí podría (y puede) servirnos como herramienta para valorar ese riesgo de fuga, de destrucción de pruebas o reiteración delictiva. Así, Neira Pena (2021: 1913) explica:

> […] a la hora de valorar el riesgo de fuga es importante, por una parte, tratar de compensar los referidos sesgos —y otros de género, edad, tipología delictiva, etc.— en la construcción del algoritmo, en la selección de los datos y, especialmente, en la interpretación contextual de los resultados que el sistema arroje; y, por otra parte, que el sistema se nutra y maneje datos suficientes en cantidad y, sobre todo, de buena calidad, tanto de casos anteriores, como especialmente del caso concreto.

Y, en consonancia con tal idea, teniendo en cuenta que el arraigo familiar, social y económico son extremos que se evalúan a la hora de constatar si existe riesgo de fuga, debe valorarse no solo el hecho de que la persona investigada tenga hijos, padres u otros familiares, sino el tipo de relación que mantenga con ellos (si hay convivencia, si se mantiene el contacto y comunicación, si se cumplen los deberes como progenitor…). Del mismo modo, habrá que valorar el entorno en el que se relaciona la persona investigada (actividades que realiza, qué amistades tiene y frecuenta…). Y para evaluar el arraigo económico tampoco basta con comprobar si la persona tiene trabajo, sino que habrá que examinar el tipo de trabajo, el tipo de contrato, el salario que se percibe, la antigüedad e incluso las relaciones con el entorno laboral y las (im)posibilidades de reincorporarse a ese puesto o a uno similar tras cumplir la pena (Neira Pena, 2021: 1913).

Y se nos antoja entonces una cuestión: ¿cómo extraemos toda esa información que tiene carácter personal, privado o íntimo? Entre las posibles

fórmulas, destaca la de Simón Castellano (2021: 151), quien se decanta por un modelo en donde el sistema de IA se nutra de todos los datos que el encausado facilite voluntariamente (datos de navegación, correo electrónico, etc.). Pero ¿cómo garantizamos aquí la fiabilidad y autenticidad de los datos?, y ¿cómo la garantizamos de cualquier otro modo, es decir, aun cuando los datos se averiguasen a través de instrumentos policiales o del Punto Neutro Judicial? Aquí precisamente es donde entra en juego el derecho a la autodeterminación informativa, que camina de la mano, en este orden de cosas (y como ya hemos indicado anteriormente), del derecho a la tutela judicial efectiva.

Al hilo de esta problemática, como advierte Neira Pena (2021: 1923) haciéndose eco de Signorato, hay autores que incluso sugieren que nos encontramos frente a un derecho de nuevo cuño, dirigido a garantizar que las decisiones judiciales no se funden exclusivamente en el uso de datos de tratamiento automatizado.

Podríamos pensar que con el uso de la IA evitaríamos los sesgos en los que incurren los órganos judiciales, en tanto en cuanto se hallan encarnados por personas que también tienen prejuicios, ideas, emociones…, y así podríamos concluir (no sin errar) que, por medio de este avance tecnológico, seríamos capaces de obtener decisiones judiciales más objetivas y con un criterio más razonado, coherente o imparcial. Pero ello no haría sino introducir un nuevo sesgo en la interpretación de los resultados de los sistemas de IA, que, como señalan Castellanos Claramunt y Montero Caro (2020: 74), «consiste en aceptar, de forma acrítica, los resultados de una IA como ciertos e inamovibles, asumiendo un "principio de autoridad" derivado de las expectativas creadas por dichos sistemas».

Uno de los problemas sustanciales con los que nos encontramos es que los sistemas de IA pueden incluir sesgos y riesgos discriminatorios por razón de etnia, situación económica, zona de origen o residencia… Y la fuente de la que se obtengan los datos para evaluar o interpretar no impide que se materialicen esos sesgos o riesgos porque: ¿qué tipo de algoritmos o de proceso automatizado emplean los sistemas de IA para interpretar los datos? En el sistema de interpretación es donde se pueden incluir igualmente esos sesgos.

Empero, ¿por qué se ha planteado la posibilidad de aplicar los sistemas de IA en el marco de la adopción de medidas cautelares y peculiarmente de la prisión provisional? La respuesta es clara. Porque el modelo actual tampoco es suficientemente efectivo ni garantista. Ya hemos explicado los prejuicios y sesgos en los que, por su condición humana, incurren los jueces. Pero, a mayores, como señala Simón Castellano (2021: 121 y ss.), resulta que tanto la solicitud de Fiscalía como la decisión del órgano judicial se llevan a cabo en una especie de vacío fáctico, en el que se debe anticipar el juicio a un momento en el que aún no se posee mucha información ni se han practicado diligencias

de investigación de suma importancia, y en el que no resulta posible siquiera, por la fase procesal en la que se adopta la medida cautelar, disponer de prueba en sentido estricto.

Y a lo anterior debe sumarse el propio vicio que presenta el diseño de la adopción de medidas cautelares en el sistema judicial, por cuanto se valora un riesgo de reiteración delictiva en relación con una persona que no ha sido todavía condenada por la comisión del delito investigado (pudiendo, por tanto, resultar declarada inocente)[29]. En esta línea, según precisa Neira Pena (2021: 1914), «el mismo concepto de "reiteración delictiva" parte de asumir como cierto que se ha cometido un delito, cuando en realidad, en el contexto de la adopción de la prisión provisional, o de otras medidas cautelares penales, el encausado debe de ser considerado inocente». Por eso resulta indispensable que, si se utilizan sistemas de IA en el contexto de adopción de medidas cautelares, *fumus delicti comissi* y *periculum in mora* se valoren de forma independiente y sucesiva. No cabe valorar el riesgo de reiteración delictiva antes de verificar la consistencia del denominado «juicio de imputación» que ha de tener carácter reforzado.

Y para valorar el riesgo de destrucción de pruebas, debe atenderse a lo establecido en el art. 503 de la LECrim, y, así, es necesario tener en cuenta las particularidades del caso en concreto (tipo de delito, existencia o no de estructura organizativa o de personas que guarden relación con la encausada y puedan disponer o alterar las fuentes de prueba, clase de pruebas, momento de comisión de los hechos, comportamiento de la personas investigada en la investigación, etc.), y ponerlas en relación con datos o situaciones de casos análogos que permitan detectar un nivel de riesgo. Pero, además, deben valorarse también la actitud, aptitud y capacidad del sujeto para destruir, manipular o alterar fuentes de prueba. En este contexto, precisamente no se puede caer en el error (pues el riesgo existe) de generar una inercia en el juzgador que le haga tender a confiar «a ciegas» en los resultados que arroje el sistema de IA, decantándose por justificarlos «automáticamente» y acomodar para ello sus propios razonamientos al resultado algorítmico, y no viceversa. No hemos de olvidar que las funciones jurisdiccionales, entre las que se incluye la de valoración (de indicios y elementos probatorios), suponen también una garantía del proceso justo, y lo todavía peor aquí sería que esa inercia llegase a influir en el órgano judicial a la hora de modificar o predeterminar el juicio de imputación (Završnik, 2019: 13; Neira Pena, 2021: 1908-1909).

[29] Incluso cuando se tratase de una persona investigada o encausada que ya hubiera sido condenada previamente por la comisión de algún otro ilícito habría que valorar la naturaleza del tipo delictivo que cometió anteriormente y su relación con el actual que se investiga.

Así pues, no podemos obviar que en el marco del proceso penal debe atenderse inexcusablemente al principio de presunción de inocencia, al derecho de defensa y, en caso de duda, al principio *in dubio pro reo*. Tales elementos deben ser puestos en relación con las funciones jurisdiccionales, que en ningún modo pueden ser sustituidas por métodos de IA, sin perjuicio de que dichos métodos (adecuadamente diseñados y utilizados) puedan convertirse en un mecanismo de auxilio (judicial) de interés práctico.

Consiguientemente, es necesario ser precavido a la hora de evaluar lo que los sistemas de IA pueden ofrecer y en qué condiciones se pueden utilizar, sabiendo cómo han sido diseñados y qué premisas utilizan, a fin de evitar poner en peligro el derecho a la tutela judicial efectiva en sentido amplio (incluyendo el derecho de defensa y el derecho a un juicio justo, amén del principio de presunción de inocencia).

En suma, el uso de la IA ha de concebirse como un método auxiliar, amparado bajo los principios de legalidad y proporcionalidad. Ello implica que el proceso de valoración y decisión debe quedar revestido de transparencia[30] y efectuarse de modo individualizado, teniendo en cuenta las circunstancias particulares tanto del caso en concreto como del sujeto que sufra las restricciones de derechos (libertad). En otras palabras, ningún sistema de IA puede sustituir la potestad jurisdiccional y las funciones que integran esta y que corresponden única y exclusivamente a los jueces y tribunales.

Dada la especialidad de la materia y los altos riesgos que para los derechos fundamentales supone el uso de sistema de IA, y, con particularidad, de aquellos que se califican de alto riesgo, es imperiosa la necesidad de implementar una normativa europea que armonice la regulación en el seno de la UE. Esta labor está previsto que se acometa a partir de la Propuesta de Reglamento de la Unión Europea sobre inteligencia artificial[31], cuya entrada en vigor y apli-

[30] Hemos de precisar aquí que «si no hay suficiente transparencia —acceso al código fuente, inputs y outputs del *software*— no podrá asegurarse la necesaria y suficiente paridad de armas entre acusación y defensa, el justo equilibrio procesal entre ambas posiciones. Incluso suponiendo que se tuviera acceso a tal información, sería preciso además que las partes pudieran disponer de peritos en la materia que certificaran —o no— la fiabilidad del sistema IA y de sus resultados en ese concreto supuesto» (De Hoyos Sancho, 2022a). En relación con estos extremos, la autora cita a Quattrocolo y Ferrer Beltrán.

[31] El texto de la referida 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 se encuentra disponible en: https://bit.ly/3KksvX3 (última consulta: 15-10-2022).

cación, como critica De Hoyos Sancho (2022b: 416), «llegará tarde, pues es muy poco probable que entre en vigor antes del año 2023». La realidad es que no bastará con la aprobación y entrada en vigor de dicho Reglamento, ya que será necesario elaborar normas nacionales de desarrollo e, inclusive, normativas sectoriales de complementación y de carácter más específico, tomando en cuenta la amplia amalgama de esferas (públicas y privadas) en las que se puede emplear la IA y en las que ya se están utilizando (desde hace años) sistemas de este tipo de forma efectiva, aun cuando todavía no se dispone de una regulación explícita (*op. cit.*).

En suma, para poder emplear los sistemas de IA en el ámbito del sistema judicial con las debidas garantías, sin provocar vulneraciones de los derechos a la tutela judicial efectiva y a la presunción de inocencia y, con peculiaridad, en el seno de la adopción de la medida cautelar de prisión provisional, en aras de dar cumplimiento a las exigencias del principio de legalidad, sería menester introducir una previsión normativa expresa relativa a ese concreto ámbito de aplicación y a la forma de utilización en este de los sistemas de IA (De Hoyos Sancho, 2020: 32; Ortiz Pradillo, 2022: 107-109)[32]. Pero, además, dentro de esa previsión normativa y tomando como parámetro las conclusiones apuntadas por De Hoyos Sancho (2020: 32-39), tendrían que incluirse medidas que permitan garantizar los siguientes requisitos, vinculados, a su vez, a las exigencias del principio de proporcionalidad (ya explicadas con anterioridad):

1. Llevar a cabo un control previo de la legalidad/admisibilidad del concreto algoritmo y del tratamiento de los datos que procesa el sistema IA, incluida la supervisión de su aplicación y funcionamiento.
2. Preservar la ineludible intervención humana de quien encarne el órgano judicial competente a la hora de adoptar la decisión/resolución final, posibilitando la impugnación de la decisión judicial basada en sistema de IA.
3. Garantizar la transparencia y trazabilidad de los sistemas de IA, dotando de seguridad y verificabilidad a los datos empleados, para evitar, entre otros problemas, que incurran en sesgos y discriminaciones.

De no cumplirse estos requisitos a la hora de utilizar sistemas de IA para valorar si procede o no acordar una medida de prisión provisional, estaríamos ante el uso de un instrumento inadecuado, innecesario y desproporcionado

[32] Si bien tal idea debe ser puesta, además, en relación con la necesidad de implementar una regulación armonizada sobre el uso de algoritmos por las autoridades jurisdiccionales en el ámbito del «espacio de libertad, seguridad y justicia» de la Unión Europea.

(en sentido estricto), que supondría un sacrificio excesivo e injustificado para los derechos fundamentales del sujeto afectado en cuestión (libertad, autodeterminación informativa y tutela judicial efectiva). Por tanto, su utilización sería deseablemente sustituible por el sistema actual de examen y valoración de la adopción de medidas de prisión provisional y no conseguiríamos ningún avance ni garantía procesal en la adopción de las medidas cautelares en el marco del proceso penal.

En cualquier caso, debe incidirse en que la valoración de la prueba y la concurrencia de los presupuestos fácticos y jurídicos necesarios para adoptar la prisión provisional no deja (ni puede dejar) de ser de carácter judicial. Es el órgano judicial el que debe atender a los hechos, al derecho y al caso en concreto, valorando todos los datos, indicios y pruebas existentes, razón por la cual entendemos que los sistemas de IA deben ser complementarios para contribuir a evitar decisiones sobre medidas cautelares incorrectas, desproporcionadas o generalizadas, que incurran en sesgos y no atiendan suficientemente a las particularidades del caso. La meta que alcanzar es que los sistemas de IA coadyuven a lograr mejores resoluciones y no generen errores y resoluciones injustas (como se ha verificado que puede suceder con un uso indebido de estos, a raíz del caso *Loomis*).

En consonancia con lo anterior, podría gestionarse el riesgo que implica la IA, teniendo en cuenta las herramientas que proporciona el marco constitucional y, en tal sentido, entre otras claves, resalta la de advertir «la prohibición y limitación de manifestaciones de la IA contrarias a principios y bienes de la máxima relevancia constitucional» (Sánchez Barrilao, 2016: 32). E inclusive podría plantearse la posibilidad (realizable) de que los órganos jurisdiccionales, en caso de duda, solicitasen la intervención de un asesor técnico (que explique la forma en la que el sistema de IA funciona, recoge datos y los analiza), lo que sería una figura que tendría ciertas similitudes, *mutatis mutandis*, con el *amicus curiae*, propuesto ya en su día en el Anteproyecto de Ley para un nuevo proceso penal de 2011 y referido a una persona experta que, al amparo de un interés legítimo, puede participar en la casación auxiliando al Tribunal con sus conocimientos sobre la interpretación de la norma cuestionada[33].

IV. REFLEXIONES FINALES

Es obvio que no podemos prescindir de las ventajas y avances que la ciencia y la tecnología ponen a disposición de la sociedad, porque ello sería

[33] https://bit.ly/3Zpo9lV (última consulta: 12-12-2021).

negar el progreso, pero ese progreso no debe dejar de ser garantista con el principio de presunción de inocencia y con los derechos y libertades fundamentales. No podemos cometer el riesgo ni el error de caer en falacias a la hora de aplicar y emplear los sistemas de IA.

Pero esto no es una tarea que pueda desarrollarse de forma sencilla. Resultan necesarios conocimientos técnicos, informáticos y experiencia. No sirve ser «analfabeto informático» y aplicar automáticamente los resultados sin cuestionar nada. Es necesario que se proporcione (y quiera recibirse) formación sobre los sistemas de IA, su diseño y funcionamiento. Asimismo, deben garantizarse la transparencia, publicidad, auditabilidad, trazabilidad y derecho a recurso (y protesta) frente al algoritmo (Simón Castellano, 2021: 164). No puede tolerarse que la justicia llegue a quedar en manos de potentes multinacionales privadas, en la línea de lo que parece haber acontecido en el caso *Loomis*.

La IA no puede ser vinculante para el órgano judicial ni sus resultados, de aplicación automática, sino que ha de configurarse simplemente como un método auxiliar. Los sistemas de IA deben conformar instrumentos que usar con conocimiento y cautela de sus ventajas, pero también de sus riesgos y perjuicios. Y en este contexto, desde luego, no ayuda en modo alguno que, en la práctica, se perciba una cierta tendencia a ejercer determinadas profesiones jurídicas (judicatura, fiscalía…) de forma autómata.

Resulta así imprescindible que los operadores jurídicos tomen conciencia de su función y la asuman con responsabilidad, rigor y profesionalidad. De igual modo, es necesario que se continúe investigando y profundizando en los pormenores de la aplicación de la IA en el marco del sistema judicial para conocer y comprender sus pros y contras y llegar a realizar una utilización lícita y positiva de las posibilidades que brinda la era de la digitalización. Hemos de procurar, por todos los medios posibles, no caer en el error de que el avance tecnológico se convierta (como lastimosamente en ocasiones parece estar sucediendo) en un retroceso en la salvaguarda de los derechos y libertades.

Bibliografía

Aguado Correa, T. (1999). *El principio de proporcionalidad en Derecho Penal*. Madrid: Edersa.

Álvarez Buján, M. V. (2018). *La prueba de ADN como prueba científica: su virtualidad jurídico-procesal*. Valencia: Tirant lo Blanch.

Álvarez de Neyra Kappler, S. (2008). *La prueba de ADN en el proceso penal*. Granada: Comares.

Álvarez González, S. (2007). *Derechos fundamentales y protección de datos genéticos*. Madrid: Dykinson.

—— (2011). El habeas data biosanitario: especiales situaciones de conflicto en relación con los datos genéticos. En A. Garriga Domínguez. y S. Álvarez González (dirs.). *Historia clínica y protección de datos personales. Especial referencia al registro obligatorio de los portadores de VIH* (pp. 51-70). Madrid: Dykinson.

Azaustre Ruiz, P. (2015). La nulidad del proceso penal por la indebida transmisión de datos personales en la cooperación judicial en el seno de la Unión Europea. En I. Colomer Hernández y S. Oubiña Barbolla (dirs.). *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea* (pp. 801-827). Cizur Menor (Navarra): Aranzadi.

Bernal Pulido, C. (2007). *El principio de proporcionalidad y los derechos fundamentales: el principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculante para el legislador*. Madrid: Centro de Estudios Políticos y Constitucionales.

Caruso Fontán, M. V. (2012). Base de datos policiales sobre identificadores obtenidos a partir del ADN y derecho a la intimidad genética. *Foro, Nueva época*, 15 (1), 135-167. Disponible en: https://doi.org/10.5209/rev_FORO.2012.v15.n1.39585.

Castellanos Claramunt, J. y Montero Caro, M. D. (2020). Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales. *Ius et Scientia*, 6 (2), 72-82. Disponible en: https://doi.org/10.12795/IETSCIENTIA.2020.i02.06.

De Hoyos Sancho, M. (2020). El Libro Blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como 'sector del riesgo'. *Revista Española de Derecho Europeo*, 76, 9-44. Disponible en: https://doi.org/10.37417/REDE/num76_2020_534.

—— (2021). El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea. *Revista General de Derecho Procesal*, 55 (3).

—— (2022a). Delincuencia organizada e inteligencia artificial. Estrategias y propuestas normativas en el contexto de la Unión Europea desde la perspectiva procesal. En F. J. Garrido Carrillo (dir.) y V. Faggiani (coord.). *Respuesta institucional y normativa al crimen organizado. Perfiles estratégicos para una lucha eficaz* (pp. 283-314). Cizur Menor (Navarra): Aranzadi.

—— (2022b). El Proyecto de Reglamento de la Unión Europea sobre inteligencia artificial, los sistemas de alto riesgo y la creación de un ecosistema de confianza. En S. Barona Vilar (dir.). *Justicia poliédrica en periodo de mudanza: Nuevo conceptos, nuevo sujetos, nuevos instrumentos y nueva intensidad* (pp. 403-422). Valencia: Tirant lo Blanch.

De Miguel Sánchez, N. (2004). *Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público (especial referencia al sida, técnicas de reproducción asistida e información genética)*. Valencia: Tirant lo Blanch.

Etxeberría Guridi, J. F. (2000). *Los análisis de ADN y su aplicación al proceso penal*. Granada: Comares.

Garriga Domínguez, A. (2000). La nueva Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales, ¿un cambio de filosofía? *Anales de la Cátedra Francisco Suárez*, 34, 299-322.

—— (2009). *Tratamiento de datos personales y derechos fundamentales* (2.ª ed.). Madrid: Dykinson.

—— (2011). La protección de los datos de carácter personal en el ámbito sanitario. Usos de la historia clínica. En A. Garriga Domínguez y S. Álvarez González (dirs.). *Historia clínica y protección de datos personales. Especial referencia al registro obligatorio de los portadores de VIH* (pp. 11-50). Madrid: Dykinson.

González-Cuéllar Serrano, N. (1990). *Proporcionalidad y derechos fundamentales en el proceso penal*. Madrid: Colex.

Iglesias Canle, I. C. (2003). *Investigación penal sobre el cuerpo humano y prueba científica*. Madrid: Colex.

Lopera Mesa, G. P. (2006). *Principio de proporcionalidad y ley penal: bases para un modelo de control de constitucionalidad de las leyes penales*. Madrid: Centro de Estudios Políticos y Constitucionales.

Martín Diz, F. (2014). Del derecho a la tutela judicial efectiva hacia el derecho a una tutela efectiva de la justicia. *Revista europea de derechos fundamentales* (Ejemplar dedicado a: Tutela judicial efectiva en el siglo xxi: un análisis interdisciplinar), 23, 161-176.

Martínez Otero, J. M. (2017). La aplicación del derecho al olvido en España tras la STJUE Google contra AEPD y Mario Costeja. *Revista Boliviana de Derecho*, 23, 112-133.

Moreno Catena, V. y Cortés Domínguez, V. (2011). *Derecho Procesal Penal*. Valencia: Tirant lo Blanch.

Neira Pena, A. M. (2021). Inteligencia artificial y tutela cautelar. Especial referencia a la prisión provisional. *Rev. Bras. de Direito Processual Penal*, 7, 3, 1897-1933. Disponible en: https://doi.org/10.22197/rbdpp.v7i3.618.

Ortiz Pradillo, J. C. (2022). Inteligencia artificial, Big data, tecnovigilancia y derechos fundamentales en el proceso penal. En C. Villegas Delgado y P. Martín-Riós (eds.). *El derecho en la Encrucijada tecnológica: Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial* (pp. 103-127). Valencia: Tirant lo Blanch.

Pérez Luño, A. E. (1993). Comentario legislativo: La LORTAD y los derechos fundamentales. *Derechos y Libertades, Revista del Instituto Bartolomé de las Casas*, 1, 405-424.

Sánchez Barrilao, J. F. (2016). El derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional. *Estudios de Deusto*, 64 (2), 225-258. Disponible en: https://doi.org/10.18543/ed-64(2)-2016pp225-258.

Sánchez Bravo, A. A. (1988). *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla: Universidad de Sevilla.

Simón Castellano, P. (2021). *Justicia cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos judiciales*. Barcelona: Bosch. Disponible en: https://doi.org/10.2307/j.ctv1tqcxbh.

Vidal Fueyo, M. C. (2021). El derecho a la tutela judicial efectiva en tiempos de pandemia. En M. P. Biglino Campos y J. F. Durán Alba (dirs.). *Los efectos horizontales de la Covid-19 sobre el sistema constitucional: estudios sobre la primera oleada* (pp. 113-139). Zaragoza: Fundación Manuel Giménez Abad. Disponible en: https://doi.org/10.47919/FMGA.OC20.0007.

Završnik, A. (2019). Algorithmic justice: Algorithms and big data in criminal justice setting. *European Journal of criminology*, 18 (5), 623-642. Disponible en: https://doi.org/10.1177/1477370819876762.