



Doi: <https://doi.org/10.17398/2695-7728.38.503>

INTELIGENCIA ARTIFICIAL AL SERVICIO DEL PROCESO PENAL Y LA PROTECCIÓN DE LOS DATOS PERSONALES

ARTIFICIAL INTELLIGENCE AT THE SERVICE OF THE CRIMINAL PROCESS AND THE PROTECTION OF PERSONAL DATA

ANA ISABEL GONZÁLEZ FERNÁNDEZ¹

Universidad de Vigo

Recibido: 12/11/2022 Aceptado: 29/12/2022

RESUMEN

El objeto del trabajo ahora presentado se centra en la protección de los datos personales en un mundo globalizado dónde el auge de la tecnología está al orden del día y que donde los datos personales constituyen un elemento más a tener en cuenta a la hora de determinar la participación de un determinado sujeto en un hecho criminal. Ahora bien, debemos partir de la naturaleza sensible de estos datos recopilados y la incidencia de los mismos en nuestros derechos fundamentales. En este trabajo, nos vamos a referir especialmente al derecho a la protección de datos de carácter personal y la utilización de estos en el ámbito criminal.

Palabras clave: Derechos, protección de datos, proceso penal, big data, inteligencia artificial.

¹ Doctora en Derecho. Profesora de Derecho Procesal Penal y abogada en ejercicio en el ICA Ourense. Ha realizado estancias de investigación en Universidades nacionales (Universidad de Extremadura) e internacionales (Instituto Universitario de Maia -Portugal- y Università degli Studi del Sannio -Italia-). Las principales líneas de investigación son: métodos de resolución de controversias, violencia sexual y cooperación judicial penal.

ABSTRACT

The object of the work now presented focuses on the protection of personal data in a globalized world where the rise of technology is the order of the day and which are one more element to consider when determining the participation of a certain subject in a criminal act. However, we must start from the sensitive nature of these collected data and their impact on our fundamental rights. In this work, we will refer especially to the right to the protection of personal data and the use of these in the criminal field.

Keywords: Rights, data protection, criminal proceedings, big data, artificial intelligence.

Sumario: 1. La inteligencia artificial en el proceso. 2. La importancia de los datos y su protección. 3. La protección de datos en la UE y su incidencia en el proceso penal español. 4. Conclusiones. Referencias bibliográficas.

1. LA INTELIGENCIA ARTIFICIAL EN EL PROCESO

No cabe duda de que estamos en un mundo dinámico en constante evolución en gran medida a causa de la denominada Revolución Industrial 4.0 o tecnológica supone un cambio en la forma de vivir, de relacionarnos con los demás bajo la premisa de la instantaneidad, tener todo lo que queramos y comunicarnos a nuestro antojo con ayuda de todo tipo de sistemas inteligentes que han sido diseñados para facilitarnos la vida. La Revolución Industrial 4.0 a la que hacemos referencia, viene de la mano del desarrollo del internet de las cosas (Internet of Things), el Big Data o la Inteligencia Artificial, por ello, no se podría entender sin hablar primero, si bien de forma sucinta, de estos conceptos.

El término Internet of Things no es un concepto novedoso en la literatura especializada ya que fue objeto de un profuso análisis desde las más variadas disciplinas y objeto de tratamiento en distintos planos, tanto a nivel técnico como desde el plano legal. En concreto, este concepto se refiere a “una infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos («objetos» como tales, u objetos vinculados a otros objetos o individuos) registran, someten a tratamiento, almacenan y transfieren datos y, al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red. Dado que la Inteligencia Artificial se basa en el principio del tratamiento amplio de los datos mediante estos sensores diseñados para comunicar datos de manera inadvertida

e intercambiarlos de manera fluida, está estrechamente relacionada con las nociones de informática «generalizada» y «ubicua»². Lo que, sin duda, como veremos más adelante, supone el tratamiento masivo de los datos personales de personas identificadas e identificables.

En cuanto al Big Data también existen múltiples definiciones de este concepto, pero en este caso nos vamos a referir a la ofrecida por la Agencia Española de Protección de Datos que, tomando en consideración alguna de ellas, sintetiza que, en definitiva, el big data es un “conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo”³.

De todo ello, podemos sacar una primera conclusión, en este momento se pone en evidencia una evidente conexión entre los dos conceptos en tanto en cuanto que sin los datos que se obtienen a través del Internet of Things no podríamos hablar de la generación de los datos que forman parte del Big Data y lo que ello comporta.

Ahora bien, de ello se deriva una ingente cantidad de datos personales que requieren ser tratados con eficiencia. En este contexto surge la Inteligencia Artificial. Sobre ella, podemos hacer una primera toma de contacto a través de lo que en su día dijo John McCarthy, refiriéndose a ella como “la ciencia y la ingeniería de fabricar máquinas inteligentes, en especial programas inteligentes de computación, entendiendo por inteligente la referencia a la parte de la informática orientada a obtener resultados”⁴.

2 Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, adoptado el 16 de septiembre de 2014, disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf, última consulta 01/12/2021, p. 4.

3 Agencia Española de Protección de Datos, *Código de buenas prácticas en protección de datos para proyectos de Big Data*, disponible en <https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf>, última consulta 13/11/2021, p. 3.

4 Fernando Martín Diz, “Inteligencia Artificial y Derecho Procesal: luces, sombras y cábalas en clave de derechos fundamentales”, en *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof^a. M^a Isabel González Cano*, dir. por Víctor Moreno Catena y María Isabel Romero Pradas (Valencia: Tirant lo Blanch, 2021), 970.

En el mismo sentido se ha referido la Comunicación de la Comisión al Parlamento Europeo, el Consejo Europeo, el Comité Económico y social europeo y el Comité de las Regiones sobre Inteligencia Artificial para Europa (COM (2018) 237 final), al referirse a ella de la siguiente forma: “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”.

En este sentido, podemos destacar que es imposible gestionar el gran volumen de datos que ahora se recolectan a través de los métodos tradicionales de almacenamiento, gestión, acceso y análisis, por ese motivo, se han venido implementado nuevos sistemas de Inteligencia Artificial, algoritmos y estadísticas por las que se pueden obtener patrones de comportamiento, gustos, toma de decisiones, reconocimiento de voz, la identificación de objetos, ahorro de energía, etc., además de crear perfiles personalizados en dónde aparecen reflejados nuestros gustos personales e, incluso, la elaboración de perfiles para analizar o predecir aspectos relativos al rendimiento profesional, la situación económica, la salud, los intereses, la fiabilidad, el comportamiento o la ubicación⁵. Por decirlo de algún modo, los datos que transmitimos ya no nos pertenecen en exclusiva, están disponibles para empresas, Estados e incluso para otros particulares”⁶.

Pensemos en la cantidad de datos personales que transferimos cada día a la nube a través de nuestras pulseras de actividad o Smartwatch, la información que ofrecemos a nuestra nevera inteligente, la aspiradora que analiza cada recoveco de nuestra vivienda, etc.⁷ Como vemos, la Inteligencia Artificial forma parte de nuestra vida cotidiana y hacemos uso de ella constantemente como puede ser el hecho de organizar nuestra jornada laboral, la conducción inteligente con un vehículo sin conductor, el bloqueo de ciertos correos electrónicos no deseados (spam). Como se puede intuir, la IA requiere conocer determinados datos personales para poder mejorar su rendimiento y, en consecuencia, ofrecer un mejor servicio a los usuarios⁸.

Ahora bien, del mismo modo que la Inteligencia Artificial y toda la infor-

5 Véase, Ana Garriga Domínguez, *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua*, Madrid, Dykinson, 2015.

6 Andrea Martínez Deviá, “La Inteligencia Artificial, el big data y la era digital: ¿una amenaza para los datos personales?”, *Revista la Propiedad Inmaterial* 27 (2019): 8 DOI: <https://doi.org/10.18601/16571959.n27.01>.

7 Como expone la profesora Barona Vilar. apoyándose en los postulados de Bauman, Z., con frecuencia los vigilados colaboramos con los vigilantes de manera voluntaria lo que se puede vincular con una vulneración continuada del derecho a la intimidad y dignidad de las personas con la consiguiente aceptación de este hecho por parte de la sociedad sin ni siquiera llegar a cuestionarlo. Relata Bauman que estamos en una tesitura en la que no sabemos quién, cuándo, para qué y desde donde nos controlan (Silvia Barona Vilar, “Proceso civil y penal ¿líquido? En el siglo XXI” en *Justicia Civil y penal en la era global*, dir. por Silvia Barona Vilar (Valencia: Tirant lo Blanch, 2017), p. 41).

8 En definitiva, estos sistemas de IA pueden consistir en programas informáticos (como asistentes de voz –Alexa, Siri...-, motores de búsqueda, sistemas de reconocimiento facial, etc., pero también puede estar incorporada en dispositivos de *hardware*, buen ejemplo de ello son los robots avanzados, automóviles autónomos, drones o aplicaciones en nuestros dispositivos electrónicos de uso cotidiano que recolectan datos sobre nuestro comportamiento diario.

mación almacenada en el Big Data, crean oportunidades para empresas y beneficios para el conjunto de la ciudadanía no está exento de dificultades en tanto en cuanto suponen un enorme impacto en nuestros derechos y libertades fundamentales⁹.

La Administración de Justicia no es ajena a este fenómeno social, de hecho, de cara a obtener una justicia más rápida, moderna y certera, se ha apuntado a la digitalización de la Justicia como la vía adecuada para lograr los fines apuntados, como pueden ser las comunicaciones telemáticas o la inclusión de instrumentos de Inteligencia Artificial para simplificar algún trámite judicial. Sin embargo, esta posibilidad no está exenta de riesgos en tanto en cuanto tiene incidencia directa en los derechos humanos y procesales de los justiciables (igualdad y no discriminación, protección de datos, derecho a la tutela judicial efectiva presunción de inocencia, derecho al debido proceso, etc.)¹⁰.

2. LA IMPORTANCIA DE LOS DATOS Y SU PROTECCIÓN

Especialmente relevante es el respeto al derecho a la protección de datos personales que se halla implícitamente conectado con el desarrollo de los instrumentos de Inteligencia Artificial consecuencia de la enorme evolución global tecnológica que ha facilitado la magnitud de la recogida e intercambio de datos personales, planteando nuevos retos en este ámbito.

En lo que queda de trabajo nos vamos a detener fundamentalmente en el respeto a los derechos fundamentales de la ciudadanía en el marco de una investigación criminal, especialmente, al derecho a la protección de datos de carácter personal que debe ser respetado en todo momento tanto en el momento de recabarlos como en su transmisión a otros Estados Miembros en el marco de un proceso penal.

La protección de las personas físicas en relación con el tratamiento de los datos de carácter personal se recoge como un derecho fundamental, así, en el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE)

9 No hace mucho WikiLeaks revelaba las prácticas de ciberespionaje de la CIA a través de nuestros dispositivos electrónicos que utilizamos cada día, aunque quizá ya fuese algo a lo que sabíamos que nos enfrentamos con el uso de las nuevas tecnologías, en ese momento quedó patente que nuestro derecho a la intimidad y la protección de nuestros datos es el derecho fundamental más amenazado en este milenio, véase, Fernando Gudín Rodríguez-Magariños, *Nuevo reglamento europeo de protección de datos versus big data* (Valencia: Tirant lo Blanch, 2018), 22-23.

10 Martín Diz, "Inteligencia Artificial...", 973.

hace referencia a él de la forma que sigue:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Dentro de nuestro Ordenamiento Jurídico es obligada la referencia al art. 18.4 de la CE que establece que el derecho a la protección de datos es un derecho fundamental dentro del derecho a la intimidad. No obstante, la jurisprudencia se refiere a él como un derecho autónomo, en concreto, la sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre (ECLI:ES:TC:2000:292) que declara abiertamente que:

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 Constitución Española, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 Constitución Española debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 Constitución Española), bien regulando su ejercicio (art. 53.1 Constitución Española). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran¹¹.

Se puede concluir, por tanto, que con el derecho a la protección de datos de carácter personal se persigue garantizar al titular el control sobre sus datos per-

11 Puede citarse también la STC 254/199, de 20 de julio (ECLI:ES:TC:1993:254), que declaró el carácter autónomo de este derecho: “en el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama “la informática””.

sonales, su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, tal como declaró el Tribunal Constitucional en la sentencia referida. No obstante, debemos tener en cuenta que no se trata de un derecho absoluto para su titular, sino que debe ponerse en equilibrio con otros derechos fundamentales, partiendo del principio de principio de proporcionalidad y según su función en la sociedad.

Ahora bien, la sociedad actual y el auge de las nuevas tecnologías requieren repensar el ámbito de la tutela del contenido de los derechos fundamentales y el mayor carácter lesivo de aplicar la tecnología con fines de investigación criminal, especialmente en sede policial, en este sentido, la injerencia en el espacio “virtual” del afectado “constituye una afectación grave al Derecho fundamental a la protección de datos de carácter personal”, por ello, las autoridades competentes a los fines de represión, investigación y enjuiciamiento penal “deban acomodarse a los estándares garantistas y a los principios rectores de toda medida de investigación que afecte a derechos fundamentales, y en particular, a los principios de legalidad, especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de dichas medidas, con arreglo al art. 588 bis Ley de Enjuiciamiento Criminal”, tanto para legitimar la medida como para la obtención de la prueba de cargo lícita¹².

Por este motivo, la jurisprudencia se ha visto obligada a reconocer que el acceso a los datos contenidos en un ordenador o cualquier dispositivo móvil suponen una injerencia más allá del derecho a la intimidad del usuario, surgiendo el derecho a la protección del entorno virtual¹³. Este derecho de nuevo cuño, sin dejar de constituir una dimensión particular del derecho a la intimidad que existe en el mundo físico, es distinto en tanto en cuanto que la información volcada en las redes está enfocada a la protección de la persona y, en consecuencia, vinculado al derecho a la protección de datos de la persona física¹⁴.

12 Juan Carlos Ortiz Pradillo, “Inteligencia artificial, *Big Data*, *tecnovigilancia* y *derechos fundamentales en el proceso penal*. In *El Derecho de la Encrucijada Tecnológica*”, en *Estudios sobre Derechos Fundamentales, nuevas tecnologías e Inteligencia Artificial*, dir. por Cesar Villegas Delgado y M^a del Pilar Martín Ríos (Valencia: Tirant lo Blanch, 2022), 103-127.

En el mismo sentido, véase, María Isabel González Cano, “Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva 2016/680”, *Rev. Bras. De Direito Processual Penal* 3 (2019), 1333 y ss., DOI: <https://doi.org/10.22197/rbdpp.v5i3.279>.

13 Entre otras, STS 342/2013, de 17 de abril (ECLI:ES:TS:2013:2222)

14 Un análisis exhaustivo de la evolución jurisprudencial en este sentido puede verse en Ortiz Pradillo, “*Big Data*...”, 9 o en Sonia Calaza López, “Protección judicial del derecho a la intimidad informática en su doble dimensión de derecho a la autodeterminación informativa y derecho al entorno virtual” en *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro*

3. LA PROTECCIÓN DE DATOS EN LA UE Y SU INCIDENCIA EN EL PROCESO PENAL ESPAÑOL

De lo expuesto hasta el momento se puede concluir que en el mundo en que vivimos hoy, los datos son un verdadero tesoro para el conjunto de la ciudadanía. En este sentido, la rápida evolución tecnológica y la globalización han planteado nuevos retos en el ámbito de la protección de los datos personales, ámbito dónde se han visto incrementado de manera significativa la magnitud de la recogida e intercambio de estos datos de carácter personal que vamos dejando cada día.

De forma inconsciente vamos dejando rastro en la red de todo lo que hacemos, ubicaciones, movimientos de dinero, contacto con terceras personas, etc., ya no sólo dentro de las fronteras de un país si no de forma global. Este hecho es especialmente relevante en el tratamiento de datos personales para la realización de actividades de prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública en el seno de la Unión y la transferencia de estos datos personales a terceros países y organizaciones internacionales, al tiempo que se garantiza un alto nivel de protección de los datos personales¹⁵.

Desde el punto de vista de una investigación o proceso penal es posible que se intercambien y recopilen multitud de datos o información que pueden ser personales y sensibles para la persona física, que entonces adquiere la condición de sospechoso, investigado o encausado, rozando en algunos casos los límites que amparan al sujeto ante la vulneración de su derecho de carácter fundamental –la protección de datos de carácter personal-. Especial relevancia cobra este derecho en tanto en cuanto estos datos son susceptibles de ser transmitidos a otro Estado¹⁶. Sin embargo, esta acción está justificada en términos generales, y

homenaje a la Prof.^a M^a Isabel González Cano, dir. por Víctor Moreno Catena y María Isabel Romero Pradas (Valencia: Tirant lo Blanch, 2021), 1111-1146.

15 Véase, Inés C. Iglesias Canle, “Intercambio de información e inteligencia en el contexto europeo, con especial referencia al ordenamiento jurídico español” en *Justicia, Administración y Derecho. Nuevos retos del derecho en el siglo XXI*, dir. por Pablo R. Bonorino Ramírez, Rafael Fernández Acevedo y Patricia Valcárcel Fernández, (Navarra: Thomson Reuters Aranzadi, 2021), 91-117.

16 Véase, Inés C. Iglesias Canle y Ana I. González Fernández, “La obtención de perfiles genéticos de ADN a través de la Orden Europea de Investigación” en *Estudios procesales sobre el espacio europeo de justicia penal*, Dir. por Mercedes Llorente Sánchez-Arjona (Pamplona: Aranzadi, 2021), 211-247, González Fernández, A. I., “La obtención de perfiles genéticos de ADN a través de la Orden Europea de Investigación” en *Nuevos Postulados de la Cooperación Judicial en la Unión Europea. Libro Homenaje a la Prof.^a M^a Isabel González Cano*, dir. por en *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof.^a M^a Isabel González Cano*,

atiende a unos fines concretos: la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Por ello, deben respetarse los derechos y garantías de los procesados en todo caso. En efecto, la Unión Europea se caracteriza por ser la vanguardia internacional y mundial en cuanto la protección del derecho a la protección de datos, que fue objeto de regulación ante el rápido desarrollo tecnológico, especialmente de internet a los efectos de “consolidar e incluso mejorar este elevado nivel de protección a través de la creación de un marco legislativo nuevo, adaptado a la realidad cambiante, al tiempo que sólido, coherente e integral. En definitiva, un entorno normativo para un mundo globalizado y digital”.

En este contexto, debemos hacer mención a la Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016¹⁷, 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, esta norma supuso la introducción de un nuevo paradigma en orden al tratamiento de los datos personales con fines penales¹⁸.

dir. por Víctor Moreno Catena y María Isabel Romero Pradas (Valencia: Tirant lo Blanch, 2021), 687-708 o Ana I. González Fernández, “La admisibilidad de la prueba obtenida mediante la orden europea de investigación en el proceso penal español”, *Revista General de Derecho Procesal*, 54.

17 Sobre el análisis de la Directiva, véase, Ignacio Colomer Hernández, “Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales” en *Justicia algorítmica y neuroderecho, una mirada multidisciplinar*, dir. por Silvia Barona Vilar, (Valencia: Tirant lo Blanch, 2021), 287 y ss.; María Isabel González Cano, “Garantías del investigado y acusado en orden a la obtención, cesión y tratamiento de datos personales en el proceso penal. A propósito de la Directiva (UE) 2016/680 y su impacto en materia de prueba penal” en *Orden Europea de Investigación y prueba transfronteriza en la Unión Europea*, dir. por María Isabel González Cano, Valencia, Tirant Lo Blanch, 2019, 98-154.

Sobre el contenido 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 véase, Marcos Ayjon, “La nueva Ley Orgánica para la protección de datos personales en la prevención, investigación, enjuiciamiento de delitos y ejecución de penas”, *La Ley Privacidad* 8, 2021, <https://dialnet.unirioja.es/servlet/articulo?codigo=8098206>.

18 En otro caso, será de aplicación el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE que trató de armonizar la protección de los derechos y libertades fundamentales de las personas físicas se aplica en los casos en los que un organismo o entidad recopila datos personales con otros fines y proceda a su tratamiento para el cumplimiento de una obligación jurídica a la que esté sujeto, lo que supone una doble vía para la protección de los datos personales de las personas físicas (Alfonso Galán Muñoz, “La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva

La Directiva Europea fue transpuesta a nuestra legislación interna, fuera del plazo establecido y la correspondiente sanción por parte de los Tribunales Europeos, 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 penales¹⁹.

De lo dispuesto en la Directiva se desprende la sujeción a una serie de principios en aras de garantizar el derecho a la protección de datos personales de las personas físicas. De esta forma, el art. 4 de la citada directiva que fueron más tarde plasmados en nuestra norma nacional, debe regirse en torno a los siguientes principios:

a) Principio de licitud y lealtad: esto requiere que los datos obtenidos deben ser tratados de manera lícita y leal;

b) Principio finalista: recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;

c) Principio de pertinencia: lo que requiere que sean adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados;

d) Principio de exactitud: los datos deben ser exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se

orientación de la política criminal de la Unión Europea”, en *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, dir por Ignacio Colomer Hernández (Pamplona: Aranzadi, 2015), 43-44).

En este sentido, por ejemplo, las instituciones financieras tienen la obligación de conservar determinados datos personales que ellas mismas tratan y únicamente facilitan dichos datos personales a las autoridades nacionales competentes en casos concretos y de conformidad con el Derecho del Estado miembro (Considerando 7 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).

19 De la misma forma se plasma este artículo en la Ley española en materia de protección de datos personales en su art. 14 al disponer: “1. Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada. 2. Las decisiones a las que se refiere el apartado anterior no se basarán en las categorías especiales de datos personales contempladas en el artículo 13, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. 3. Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13”.

supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados;

e) Principio de conservación: esto es, han de conservarse de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados;

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas.

En lo que se refiere al tratamiento automatizado de datos recopilados por algoritmos, el art. 11 establece que:

“los Estados miembros dispondrán la prohibición de las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, salvo que estén autorizadas por el Derecho de la Unión o del Estado miembro a la que esté sujeto el responsable del tratamiento y que establezca medidas adecuadas para salvaguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento”.

La propia norma establece una salvedad para la adopción de medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo, al menos, el derecho a obtener el derecho a obtener la intervención humana por parte del responsable del tratamiento de los datos con fines penales²⁰.

Como vemos, la legislación europea de referencia en materia de protección de datos personales en el proceso penal viene descartando ya la utilización de un sistema de Inteligencia Artificial para un tratamiento masivo de los datos de las personas encausadas y requiere participación humana a la hora de tomar alguna decisión que implique injerencia en los derechos y garantías del encausado o acusado²¹.

20 Ana E. Carrillo Del Teso, “La protección de las personas físicas en la cooperación penal europea tras la directiva (UE) 2016/680” en *Fodertics 7.0. Estudios sobre Derecho Digital*, Dir. por Federico Bueno de Mata, (Granada: Comares: 2018), 19.

21 Federico Bueno de Mata, “Protección de datos, investigación de infracciones penales e inteligencia artificial. novedades y desafíos a nivel nacional y europeo en la era postcovid”, *La ley penal: revista de derecho penal, procesal y penitenciario*, 150 (2021) <https://dialnet.unirioj.a.es/servlet/articulo?codigo=8049997>.

4. CONCLUSIONES

A pesar de las ventajas que ofrece la Inteligencia Artificial, deberá existir un control humano considerando la especial incidencia de los derechos fundamentales del justiciable. Por ello, a nuestro parecer, la Inteligencia Artificial únicamente debería ser un complemento a la vía judicial ante la imposibilidad de sustituirlo completamente, nunca ser un sustituto de la persona humana para que, de ese modo, pueda coadyuvar al proceso judicial y, especialmente, en el proceso penal.

Precisamente por este motivo es importante tener en cuenta la previsión de la Directiva y la Ley española en lo relativo al tratamiento automatizado de los datos personales en tanto en cuanto pueden tener efectos perniciosos para el investigado, encausado o condenado por un ilícito penal.

Está claro que por muy perfecta que sea la máquina, falta la capacidad de empatía y sentimientos de la persona, por lo que, en ningún caso entendemos que podamos prescindir de esa humanidad y ello creemos que será durante un largo periodo de tiempo.

REFERENCIAS BIBLIOGRÁFICAS

- Barona Vilar, Silvia. “Proceso civil y penal ¿líquido? En el siglo XXI”. En *Justicia Civil y penal en la era global*. Dir. por Silvia Barona Vilar. Valencia: Tirant lo Blanch, 2017.
- Bueno de Mata, Federico. “Protección de datos, investigación de infracciones penales e inteligencia artificial. Novedades y desafíos a nivel nacional y europeo en la era postcovid”. *La ley penal: revista de derecho penal, procesal y penitenciario* 150 (2021).
- Calaza López, Sonia, “Protección judicial del derecho a la intimidad informática en su doble dimensión de derecho a la autodeterminación informativa y derecho al entorno virtual”. En *Nuevos Postulados de la Cooperación Judicial en la Unión Europea. Libro Homenaje a la Prof.^a M^a Isabel González Cano*. Dir. por Moreno Catena, Víctor y Romero Pradas, María Isabel. Valencia: Tirant lo Blanch, 2021.
- Carrillo Del Teso, Ana E. “La protección de las personas físicas en la cooperación penal europea tras la directiva (UE) 2016/680”. En *Fodertics 7.0. Estudios sobre Derecho Digital*. Dir. por Bueno De Mata, Federico y González Pulido, Irene. Granada: Comares, 2018.
- Colomer Hernández, Ignacio. “Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales”. En *Justicia algorítmica y neuroderecho, una mirada multidisciplinar*. Dir. por Barona Vilar, Silvia. Valencia: Tirant lo Blanch, 2021.
- Galán Muñoz, Alfonso. “La protección de datos de carácter personal en los tratamientos

- destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea”. En *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*. Dir. por Colomer Hernández, Ignacio. Pamplona: Aranzadi, 2015.
- Garriga Domínguez, Ana. *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua*. Madrid: Dykinson, 2015.
- González Cano, María Isabel. “Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva 2016/680”. *Rev. Bras. De Direito Processual Penal* 3, (2019), DOI: <https://doi.org/10.22197/rbdpp.v5i3.279>.
- González Cano, María Isabel. “Garantías del investigado y acusado en orden a la obtención, cesión y tratamiento de datos personales en el proceso penal. A propósito de la Directiva (UE) 2016/680 y su impacto en materia de prueba penal”. En *Orden Europea de y prueba transfronteriza en la Unión Europea*. Dir. por González Cano, María Isabel. Valencia: Tirant Lo Blanch, 2019.
- González Fernández, Ana Isabel. “La admisibilidad de la prueba obtenida mediante la orden europea de investigación en el proceso penal español”. *Revista General de Derecho Procesal* 54 (2020).
- González Fernández, Ana Isabel. “La obtención de perfiles genéticos de ADN a través de la Orden Europea de Investigación”. En *Nuevos Postulados de la Cooperación Judicial en la Unión Europea. Libro Homenaje a la Prof.^a M^a Isabel González Cano*. Dir por: Moreno Catena, Víctor y Romero Pradas, María Isabel. Valencia: Tirant lo Blanch, 2021.
- Gudín Rodríguez-Magariños, Faustino. *Nuevo reglamento europeo de protección de datos versus big data*. Valencia: Tirant lo Blanch, 2018.
- Iglesias Canle, Inés Celia y González Fernández, Ana Isabel. “La obtención de perfiles genéticos de ADN a través de la Orden Europea de Investigación”. En *Estudios procesales sobre el espacio europeo de justicia penal*. Dir. por Llorente Sánchez-Arjona, Mercedes. Pamplona: Aranzadi, 2021.
- Iglesias Canle, Inés Celia. “Intercambio de información e inteligencia en el contexto europeo, con especial referencia al ordenamiento jurídico español”. En *Justicia, Administración y Derecho. Nuevos retos del derecho en el siglo XXI*. Dir. por Bonorino Ramírez, Pablo Raúl, Fernández Acevedo, Rafael, Valcárcel Fernández, Patricia. Navarra: Thomson Reuters Aranzadi, 2021.
- Marcos Ayjon, Marcos. “La nueva Ley Orgánica para la protección de datos personales en la prevención, investigación, enjuiciamiento de delitos y ejecución de penas”. *La Ley Privacidad* 8 (2021). <https://dialnet.unirioja.es/servlet/articulo?codigo=8098206>.
- Martín Diz, Fernando. “Inteligencia Artificial y Derecho Procesal: luces, sombras y cábalas en clave de derechos fundamentales”. En *Nuevos Postulados de la Cooperación Judicial en la Unión Europea. Libro Homenaje a la Prof.^a M^a Isabel González Cano*. Dir. por Moreno Catena, Víctor y Romero Pradas, María Isabel. Valencia: Tirant lo Blanch, 2021.
- Martínez Deviá, Andrea. “La Inteligencia Artificial, el big data y la era digital: ¿una amenaza para los datos personales?”. *Revista la Propiedad Inmaterial* 27 (2019). DOI: <https://doi.org/10.18601/16571959.n27.01>.

Ortiz Pradillo, Juan Carlos. “Inteligencia artificial, *Big Data*, *tecnovigilancia* y *derechos fundamentales en el proceso penal*. El Derecho de la Encrucijada Tecnológica”. En *Estudios sobre Derechos Fundamentales, nuevas tecnologías e Inteligencia Artificial*. Dir. por Cesar Villegas Delgado y M^a del Pilar Martín Ríos. Valencia: Tirant lo Blanch, 2022.

ANA ISABEL GONZÁLEZ FERNÁNDEZ
Área de Derecho Procesal
Departamento de Derecho Público
Facultad de Ciencias Jurídicas y del Trabajo
Universidad de Vigo
anaisagonzalezf@gmail.com
<https://orcid.org/0000-0002-4608-1411>