PANORAMA DE LA INTELIGENCIA ARTIFICIAL EN LA JUSTICIA Y EL DERECHO ACTUALES

OVERVIEW OF ARTIFICIAL INTELLIGENCE IN JUSTICE AND LAW TODAY

Miguel L. Lacruz Mantecón
Profesor titular Derecho civil
Universidad de Zaragoza

RESUMEN

El artículo intenta hacer un resumen lo suficientemente completo del tema de la incidencia de la nueva tecnología de la Inteligencia artificial en el ámbito jurídico. Para ello se parte de la legislación española y europea en dicho ámbito, que es lo bastante amplia como para proporcionar bastantes datos acerca de los desarrollos actuales y los posibles derroteros futuros. Las realizaciones y previsiones acerca de esta tecnología se examinan en relación a las distintas especializaciones jurídicas, y se intentan completar con ejemplos que espero que sean suficientemente ilustrativos.

Palabras clave: Inteligencia artificial; IA; Jueces-robot; Justicia predictiva; Personalidad electrónica; Sistema de crédito social.

ABSTRACT

The article attempts to make a sufficiently complete summary of the issue of the impact of the new technology of Artificial Intelligence in the legal field. To do this, we start from Spanish and European legislation in this area, which is broad enough to provide enough data about current developments and possible future directions. The achievements and forecasts regarding this technology are examined in relation to the different legal

specializations, and they are attempted to be completed with examples that I hope are sufficiently illustrative.

Keywords: *Artificial intelligence; AI; Robot judges; Predictive justice; Electronic personality; Social credit system (or scoring)*

SUMARIO

I. INTRODUCCIÓN. LA IA EN ESPAÑA

El surgimiento de esta nueva técnica que es la IA va a transformar nuestra sociedad, esto es algo que se acepta sin objeciones en los círculos, económicos, políticos y militares, y universitarios o en general, entre los investigadores de cualquier rama. Aquí nos vamos a ocupar de la incidencia de la IA en el mundo jurídico, para intentar desbrozar el enmarañado y laberíntico espacio del Derecho y la Justicia, y su relación con los sistemas inteligentes y robots. La cuestión es de bastante actualidad, como anécdota leo en la sección de estrenos cinematográficos de un periódico digital[1] la siguiente noticia: «*Justicia Artificial* (13 de septiembre). Un thriller político patrio situado en un futuro cercano y protagonizado por Verónica Echegui. El gobierno español anuncia un referéndum para aprobar un sistema de Inteligencia Artificial en la Administración de Justicia que promete automatizar y despolitizar la justicia sustituyendo, en la práctica, a los jueces y juezas en todos los tribunales del país». Evidentemente se trata de ciencia ficción, pero ya existen los cimientos de una importante incidencia de la Inteligencia artificial en la Justicia y el Derecho, materia en la que entramos sin más dilación.

[1] https://www.libertaddigital.com/cultura/cine/2024-09-04/los-10-estrenos-de-cine-mas-destacados-del-mes-de-septiembre-en-espana-7160487/

Empezando por el ámbito de la legislación, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, es la que inaugura una habilitación general para la "Actuación judicial automatizada" en su artículo 42. Se inspiraba en la anterior Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, pero la incidencia de estas técnicas en ambas leyes ha sido de bajo nivel, al limitarse a la comunicación de solicitudes y documentos y su almacenamiento como archivos electrónicos, y no suple la intervención de funcionarios, letrados o jueces. Hoy esta ley ha sido derogada por la el Real Decreto-ley 6/2023, de 19 de diciembre, al que luego haré referencia.

Un dato interesante para este panorama normativo es que ya existe en España un organismo administrativo encargado de la implementación de sistemas inteligentes en la Administración de Justicia. En efecto, se trata de la Subdirección General de Nuevas Tecnologías de la Justicia, dependiente de la Secretaría General de la Administración de Justicia, y cuyas funciones son, según el art. 3.2. i) del Real Decreto 725/2017, de 21 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Justicia: *La planificación estratégica, la dirección y la ejecución de la modernización tecnológica de los juzgados y tribunales, del Ministerio Fiscal y de los registros administrativos de apoyo a la actividad judicial, así como la coordinación de las actuaciones en esta materia con otras administraciones, órganos del Estado, corporaciones profesionales e instituciones públicas.* Con anterioridad, se ocupaba de la materia el Comité técnico estatal de la Administración judicial electrónica (CTEAJE), creado por la citada Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación (TIC) en la Administración de Justicia, y que continúa con el Real Decreto-ley 6/2023, de 19 de diciembre, al que luego haré referencia.

Estas nuevas tecnologías por ahora se han restringido al campo de las TIC, tecnologías de la información y comunicación, pero recientemente extienden su actividad a la creación de herramientas de Inteligencia artificial (IA), como la ya operativa *Calculadora 988*[2], algoritmo inteligente para el cálculo de la acumulación de penas en los reos con condenas múltiples, de lo que nos da noticia Ortega Matesanz[3]. Se trata de un programa que hace el difícil cálculo de la acumulación de penas más ventajosa para el reo, pero ajustándose a reglas predefinidas (lógico, la materia no permite otras actuaciones) y sin posibilidad de autoaprendizaje, por lo que se trata de una IA débil.

---

[2] Así denominada por el artículo 988 de la Ley de Enjuiciamiento Criminal, que disciplina la materia.

[3] Ortega Matesanz, Alfonso, "Aritmética Jurídica e Inteligencia Artificial: sobre la Calculadora 988", *Revista de Estudios Jurídicos y Criminológicos*, n.º 9, Universidad de Cádiz, 2024, pp. 141-204, DOI: https://doi.org/10.25267/REJUCRIM.2024.i9.05

Por su parte, Dolz Lago[4] valora el papel que en materia de IA puede jugar, como precepto de superior rango, el art. 18.4 de nuestra Constitución, al garantizar 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.* Uso de la informática que evidentemente puede extenderse a los sistemas (informáticos) de IA.

Dejando aparte las normas procedimentales a las que luego aludiré, también inciden hoy en la materia, naturalmente, las normas referentes a protección de datos. Así, tiene ya en cuenta el tratamiento automatizado de datos personales la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Recoge la prohibición del art. 22 del Reglamento General de Protección de Datos europeo de 27 de abril de 2016, relativa a que se produzcan decisiones individuales automatizadas.

Un texto con valor puramente declarativo, en la línea de preocupación por los derechos humanos frente a esta tecnología, es la *Carta de derechos digitales*, adoptada en julio de 2021 por el Gobierno, que se inscribe en el contexto de la *Estrategia Española Nacional de Inteligencia Artificial de 2020*, pero que carece de efectos normativos. También se ha ubicado esta Carta en el peculiar Plan de Recuperación, transformación y resiliencia[5].

En fecha más reciente, el Real Decreto 729/2023, de 22 de agosto, aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial, organismo cuya creación arranca de la Ley Presupuestos Generales del Estado para el año 2022, y de la Ley 28/2022 de fomento del ecosistema de las empresas emergentes. Esta Agencia estará encargada de la asunción de las materias y competencias que deban ser asumidas por el Reino de España, como Estado miembro integrante de la Unión Europea (UE) en materia de Inteligencia Artificial, sobre todo las relacionadas con la supervisión y control administrativo de los sistemas inteligentes. Administrativamente, esta Agencia se adscribe al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, y en la Disposición adicional cuarta del Real Decreto 729/2023 se prevé su colaboración con órganos de responsabilidad en materia de inteligencia artificial del Ministerio de Defensa; pero no hay nada previsto respecto de la Subdirección General de Nuevas Tecnologías de la Justicia.

También incide tangencialmente en la materia de IA el Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia

---

[4] Dolz Lago, Manuel— Jesús, «Una aproximación jurídica a la Inteligencia Artificial», *Diario La Ley*, Nº 10096, Sección Doctrina, 23 de Junio de 2022, Wolters Kluwer, LA LEY 6033/2022.

[5] En: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

de inteligencia artificial. Se trata, como se dice en el Preámbulo, de poner en marcha un sistema de pruebas controladas para comprobar el cumplimiento de los requisitos exigidos a los sistemas de inteligencia artificial de alto riesgo del Reglamento europeo de Inteligencia artificial.

Hay que reseñar asimismo el también citado Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. Este Decreto continúa la transformación digital en el marco de la Justicia española: «el presente texto busca presentarse como una herramienta normativa completa, útil, transversal y con la capacidad suficiente para dotar a la Administración de Justicia de un marco legal, coherente y lógico en el que la relación digital se descubra como una relación ordinaria y habitual», como dice su Preámbulo (II). Se pasa a hablar de una «relación electrónica» entre los ciudadanos y la Administración, también la de Justicia.

Hay un Proyecto de Ley por la que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia, que desarrolla al RDL 6/2023 previendo la programación de actuaciones judiciales y procesales automatizadas, pero se encuentra varado en las Cámaras desde marzo de 2024.

Naturalmente, España en cuanto país europeo se ve vinculado por la legislación de la Unión, y en esta materia la norma fundamental es la Ley de la Inteligencia artificial, en concreto el Reglamento (UE) 2024/1689 Del Parlamento Europeo y del Consejo de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.

II. INCIDENCIA DE LA IA EN EL DERECHO Y EN LA JUSTICIA

En un análisis de la incidencia de la IA en el campo jurídico podemos considerar, con el profesor Petit[6], un enfoque tecnológico-legalista, consistente en ubicar en el sistema legal los diferentes problemas, campos o asuntos afectados por la IA y los robots, analizando cada uno de dichas cuestiones según la incidencia que en las mismas tenga la nueva tecnología.

Para denominar esta especialización del Derecho, Petit utiliza la expresión *Robolaw* como estudio centrado en las normas externas que gobernar el funcionamiento de la IA y los robots una vez introducidos en la sociedad. En el ámbito

[6] Petit, Nicolas, «Law and regulation of artificial intelligence and robots: Conceptual framework and normative implications», Working paper, 09 March 2017. Publicado en SSRN: https://ssrn.com/abstract=2931339 or http://dx.doi.org/10.2139/ssrn.2931339.

anglosajón predomina la expresión CiberDerecho (*CiberLaw*). Sobre si esta fuerte o decisiva influencia de la nueva tecnología de IA es suficiente para crear una nueva disciplina jurídica, existen opiniones encontradas, y su estudio hay que dejarlo para otro momento, pero en cualquier caso las realizaciones de la IA dan lugar hoy a que se haya superado el estadio meramente instrumental de la anterior Jurimetría e Informática jurídica.

Esta incidencia de la IA es bastante tímida, por ahora, pero ya ha sido puesta de relieve en estudios europeos; como señala Miguel De Asís Pulido[7], la Comisión Europea, en 2020, publicaba su *Study on the use of innovative technologies in the justice field*[8], referenciando una serie de proyectos de los países miembros conducentes a incluir las nuevas tecnologías en el campo de la justicia. Respecto a España, el documento enumeraba siete proyectos (tres impulsados por el Ministerio de Justicia y cuatro por el Centro de Documentación Judicial —CENDOJ-), fundamentalmente herramientas de transcripción de lenguaje hablado a texto, búsqueda de archivos, clasificación de documentos, seudonimización de sentencias e identificación biométrica. En mayo de 2021, el mismo Ministerio presentó el Plan Justicia 2030, con contenidos de digitalización e IA. Como advierte Dolz Lago[9], la Comisión Europea para la Eficiencia de la Justicia (CEPEJ), compuesta por expertos designados por los Estados miembros del Consejo de Europa, ya ha adoptado una «Carta ética sobre el uso de la Inteligencia Artificial en la Justicia y su entorno». Esta *Carta* proporciona un marco de principios — guía para los responsables políticos, legisladores y profesionales de la justicia ante el rápido desarrollo de la inteligencia artificial en los procesos judiciales nacionales. Concluye que la aplicación de la IA en el ámbito de la justicia puede contribuir a mejorar la eficiencia y la calidad y debe aplicarse de manera responsable, respetando los derechos fundamentales garantizados en el Convenio Europeo de Derechos Humanos y en el Convenio del Consejo de Europa para la Protección de Datos Personales.

¿Cabe la figura del Juez-robot?

Como puede deducirse de lo visto hasta ahora, esta aplicación de la IA en la materia sólo puede ser, en principio, instrumental, pues se le pide a la IA que contribuya a una Justicia más eficiente y de calidad, con respeto a los derechos humanos: en definitiva, que ayude a mejorar la Justicia, no que la dicte. En este sentido, señala Cotino Hueso[10] que tanto la Constitución como

---

[7] De Asís Pulido, Miguel, «La Justicia predictiva: tres posibles usos en la práctica jurídica», *Inteligencia Artificial y Filosofía del Derecho,* Director Fernando H. Llano Alonso, Coord. Joaquín Garrido Martín, Ramón Valdivia Jiménez, Ediciones Laborum, S.L., Murcia, 2022, pp. 285-312.

[8] European Commission: Directorate-General for Justice and Consumers, *Study on the use of innovative technologies in the justice field — Final report*, Publications Office, 2020, https://data.europa.eu/doi/10.2838/585101

[9] Dolz Lago, «Una aproximación jurídica a la Inteligencia Artificial», *Diario La Ley*, *cit.*, p. 2

[10] Cotino Hueso, Lorenzo, «El uso jurisdiccional de la inteligencia artificial: habilitación legal, garantías necesarias y la supervisión por el CGPJ», *Actualidad Jurídica Iberoamericana* Nº 21, agosto

nuestras leyes parten de la premisa de que son seres humanos quienes realizan las funciones jurisdiccionales, y en esta dirección, el Consejo General del Poder Judicial viene a afirmar en su *Informe al Anteproyecto de ley de eficiencia digital del Servicio público de justicia*[11], que por aplicación de principios constitucionales, en lo que se refiere a la labor jurisdiccional se impone lo que se ha dado en llamar una «reserva de humanidad», esto es, delimitar ciertos espacios vedados a la actuación de las IAs. Por añadidura, hay que tener en cuenta que la citada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales recoge la prohibición del art. 22 del Reglamento General de Protección de Datos europeo de 2016, de que se produzcan decisiones individuales automatizadas: «Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar».

Añade Cotino, en base al indicado *Informe*, que la potestad jurisdiccional es una función consustancial y ontológicamente anudada a la naturaleza humana, con independencia, imparcialidad, exclusividad y con exclusivo sometimiento al imperio de la ley, lo que implica:

> «… "debidos controles, evaluaciones y las garantías adecuadas" (nº 51)… Se afirma en este sentido para los ciudadanos "el derecho a una resolución fundada en Derecho dictada por un Juez o Tribunal, esto es, el derecho a que su caso sea resuelto por un Juez-persona" (nº 164, Conclusión 68)».

Y es que, como señala Fernando Galindo[12], la inteligencia artificial solo simula algunos aspectos específicos de la inteligencia humana, no alcanza otros aspectos como los de «comprensión y reflexión según valores, significados, criterios, perspectivas vitales o puntos de vista». Por ello se hace difícil resolver conflictos estas herramientas, ya que tal resolución necesariamente involucra a personas físicas, como abogados, funcionarios e incluso ciudadanos, que como nos dice el autor, «son parte del conflicto y su solución». A tenor de la sociología del Derecho, nos recuerda el autor, la actividad de aplicación de la ley en el ámbito judicial va más allá de la idea positivista de subsunción legal, se realiza sobre la base de la comunicación entre los implicados en el proceso (Ehrlich), mediante mecanismos como la ponderación (Engisch), la empatía (Gadamer), los tópicos (Viehweg), la participación y el consenso (Habermas), modalidades de la cognición humana que la máquina difícilmente puede alcanzar. El problema, a mi juicio, hay que basarlo en la falta de conciencia de los sistemas inteligentes, que a su vez proviene de la imposibilidad de gestionar proposiciones autorreferentes

---

2024, pp. 494-527.

[11] Acuerdo adoptado por el Pleno, de 24 de febrero de 2022, https://www.poderjudicial.es

[12] Galindo Ayuda, F. (2024). «Algorithms, Sociology of Law and Justice». *Journal of Digital Technologies and Law*, 2(1), 34-45. https://doi.org/10.21202/jdtl.2024.3, p. 37.

o contradictorias consigo mismas, imposibilidad que los matemáticos refieren a los teoremas de la incompletitud de Gödel.

La muy reciente y fundamental Ley de la IA, Reglamento (UE) 2024/1689 de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, tiene algo que decir al respecto, y en concreto vemos que califica como de «alto riesgo» a los sistemas de IA destinados a la administración de justicia, y en particular los destinados a ser utilizados por una autoridad judicial para ayudar a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos: «…La utilización de herramientas de IA puede apoyar el poder de decisión de los jueces o la independencia judicial, pero no debe substituirlas: la toma de decisiones finales debe seguir siendo una actividad humana»[13]. Aquí el Considerando 61 lo deja muy claro, sólo cabe una utilización instrumental de bajo nivel no sustitutiva de la decisión humana. Se deja fuera de la calificación de alto riesgo a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia propiamente dicha, como señala este mismo Considerando.

Pero incluso una utilización accesoria de la IA como mero asesor cae dentro de la calificación de «sistema de alto riesgo» conforme al Reglamento europeo. Así, el art. 6.2 del Reglamento[14] se remite a la enumeración de sistemas de alto riesgo del Anexo III, y efectivamente entre éstos encontramos los dedicados a: *8. Administración de justicia y procesos democráticos: a) Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios.* Concreta el art. 6.3 del mismo Reglamento el motivo de este alto riesgo en plantear *un riesgo importante de causar un perjuicio a… los derechos fundamentales de las personas físicas, también …influir sustancialmente en el resultado de la toma de decisiones.* Evidentemente, tal riesgo existe en la actividad jurisdiccional.

El diseñador o proveedor del sistema va a ser quien tenga que demostrar la falta de peligrosidad del sistema mediante pruebas de evaluación del mismo y antes de su puesta en funcionamiento, en los casos en que el papel de la IA en este ámbito de la Justicia sea de perfil bajo, y tenga una finalidad realmente instrumental o accesoria. Como nos dice el artículo 6.4 del Reglamento UE: *4. El proveedor que considere que un sistema de IA contemplado en el anexo III no es de alto*

---

[13] Paralelamente, el ANEXO III recoge entre los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2 los dedicados a: «*8. Administración de justicia y procesos democráticos: a) Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios.*

[14] *6.2: Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III.*

riesgo documentará su evaluación antes de que dicho sistema sea introducido en el mercado o puesto en servicio. Dicho proveedor estará sujeto a la obligación de registro establecida en el artículo 49, apartado 2. A petición de las autoridades nacionales competentes, el proveedor facilitará la documentación de la evaluación.

Frente a este principio de protagonismo humano, Cotino Hueso valora no obstante el papel auxiliar, o incluso asesor, de los sistemas inteligentes en la Administración de Justicia, entendiendo que hay funciones jurisdiccionales que pueden realizarse mediante sistemas de IA: «La IA puede ser utilizada para la adopción o, mayormente, asistencia en la redacción de sentencias y resoluciones basadas en la jurisprudencia y normativa aplicable[15]». Cabe destacar el importante papel que este autor atribuye a la IA en cuanto permite que intervenga en la «adopción» de sentencias; bien es verdad que luego destaca su papel meramente asistencial. También puede utilizarse la IA para la valoración de las pruebas: —Redacción de informes y auditorías destinados al proceso; —evaluación de pruebas y verificación de datos; —análisis y predicción de riesgos para la toma de medidas cautelares o en la ejecución de sentencias, como las decisiones sobre peligrosidad del reo.

Otro ámbito normativo del que también se siguen normas aplicables, como destaca Cotino[16], es el de la protección de datos, y en este sentido nos indica el autor que el Reglamento General de Protección de Datos europeo de 2016 es en general aplicable a todo tratamiento automatizado de datos, al que hay que añadir la Ley Orgánica 7/2021, de 26 de mayo, que transpone la Directiva 2016/680 relativa a la protección de las personas físicas en el tratamiento de datos personales, para el ámbito penal y policial. Critica el autor las pocas garantías que existen en España cuando se realizan tratamientos masivos de datos por la AEAT, la TGSS, CNMC o inspección de trabajo, mientras que en otros países europeos se han declarado inconstitucionales normas legales que regulan tratamientos automatizados de datos por el sector público, aun incluyendo garantías que no existen en España.

Ahora bien, frente a todas estas prevenciones, y como señala el magistrado Manuel Marchena[17], la implantación de sistemas inteligentes en la Justicia ya es un hecho. Se usan como asesores legales, así en Holanda una guía legal para la separación matrimonial, en Francia el programa *Case Francia Alfa*, para predecir decisiones en materia de indemnización de daños, el programa *Coin-Contract Intelligence* para la interpretación contractual o el sistema KIRA para detectar cláusulas abusivas en los contratos. Pero también para decidir reclamaciones de

---

[15] Cotino Hueso «El uso jurisdiccional de la inteligencia artificial: habilitación legal…», *cit.*, p. 499.

[16] Cotino Hueso «El uso jurisdiccional de la inteligencia artificial: habilitación legal…», *cit.*, p. 502.

[17] Marchena Gómez, Manuel, «Inteligencia Artificial y Jurisdicción Penal», Ponencia para su ingreso en la Real Academia de Doctores de España, 26 octubre 2022, p. 7.

(relativa) poca importancia, así una aplicación británica que permite formalizar y resolver reclamaciones civiles; en Estonia, una aplicación permite la reclamación telemática para la resolución de conflictos contractuales no superiores a 7.000 euros. En España tenemos unas *Tablas orientadoras para determinar las pensiones alimenticias* de los hijos en los procesos de familia, elaboradas por el CGPJ, pensiones que se calculan con una aplicación *on line*.

China es un caso aparte, existe el Libro blanco de la Corte Suprema de China" (*Chinese Courts and Internet Judiciary*), con los «jueces-robot», que, como nos cuenta De Asís Pulido[18], ya funcionan en China, si bien todavía en funciones de apoyo y dejando la decisión final al juez humano, como el programa Xiao Zhi, en la Corte Suprema Popular de China: «… esta máquina organiza los eventos del proceso, analiza la presentación de los casos en lo relativo a su admisibilidad, resume los puntos en los que las partes están en desacuerdo, ayuda en la evaluación de las pruebas y crea propuestas de resoluciones judiciales (Chen/Li, 2020, 15)».

Aparte, como nos vienen bombardeando en noticias de la prensa digital, ya tenemos los asesores (que no abogados) inteligentes. El periódico Cinco Días (27-2-2023) hizo un reportaje a personas vinculadas a diversos despachos, como Legálitas, Reclamador, Arriaga Asociados, Unive Abogados etc., donde dieron su opinión respecto a las utilidades prácticas, ven la IA como una oportunidad, y lo utilizan para resúmenes, optimizar preguntas, orientar a los clientes con preguntas básicas, poder pasar la consulta jurídica directamente al abogado de la materia sin pasar por un intermediario, estudio de asuntos etc. Todos coinciden en que es un complemento al abogado pero que este no es reemplazable. Y ElConfidencialDigital, entrevistando al socio director de Ecija Abogados y profesor de universidad Alejandro Touriño nos dice que esta tecnología permite «automatizar y hacer más eficientes determinados procesos que son puro servicio jurídico». Eso incluye la redacción de contratos, la revisión de documentación, las herramientas de traducción y, sobre todo, la resolución de consultas legales".

III. OBSTÁCULOS A LA ACEPTACIÓN DE LA APLICACIÓN DE LA LEY POR SISTEMAS INTELIGENTES

Además de las previsiones legales del Reglamento europeo, que ya hemos visto, la utilización de la IA por la Administración de Justicia no puede llevarse a

[18] González Tapia, Mª Isabel, «Protección penal de los neuroderechos: el uso directo de las neurotecnologías sobre el ser humano», *Inteligencia Artificial y Filosofía del Derecho*, Ediciones Laborum, Murcia, 2022, p. 328.

cabo, opina Cotino[19], sin implementar además una completa regulación legal que ampare su uso, aunque sólo sea instrumental:

«En cualquier caso, hay que partir de que el RIA no vale como norma legal que legitime un tratamiento de datos o una restricción de derechos fundamentales o colme una exigencia de legalidad penal, sancionadora o procesal. Seguirá siendo necesaria una ley que habilite la existencia de un concreto sistema de alto riesgo de los regulados con carácter general en el RIA».

Aunque como apunta este mismo autor, el Real Decreto-ley 6/2023, de 19 de diciembre, de medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público, contiene una amplia referencia a sistemas automatizados o de IA que permite que actúen como cobertura legal para la utilización de sistemas inteligentes. Se habla así del uso de *algoritmos, sistemas, sistemas de información, aplicaciones, métodos electrónicos, procesos automatizados* o *realización automatizada de funciones*, términos que en opinión de Cotino permiten dotar de cierta habilitación general al uso de sistemas automatizados.

Opina por su parte De Asís Pulido[20] que la introducción de sistemas inteligentes de resolución de casos puede efectuarse cuando se trata de casos sencillos, en los que se cuente además con «procedimientos testigo» de los que habla el Proyecto de Ley de Eficiencia Procesal del Servicio Público de Justicia de 2021 que añade a la Ley de Enjuiciamiento Civil el artículo 438. ter, sentando así el concepto de procedimientos testigo en el ámbito de las condiciones generales de contratación: «debido a sencillez y estandarización, consideraremos que la aplicación de los patrones identificados por el sistema en litigios pasados pueda dar lugar a una resolución justa en el caso actual, sin que sea necesario considerar todos los matices de las circunstancias particulares de la controversia».

Los usos de la justicia predictiva en la práctica judicial podrían dividirse, según este autor, en tres conjuntos: aplicación del Derecho, fiscalización de sentencias y pronóstico de resultados para la estrategia procesal.

Ahora bien, otro obstáculo, éste más importante, para la implantación de procesos de decisiones automatizadas, está en la falta de explicabilidad de las decisiones tomadas por sistemas inteligentes, lo que se traduce en una falta o una defectuosa fundamentación.

Para concretar este obstáculo hay que hacer una breve referencia a los dos modelos de sistemas de IA más importantes, que son el modelo de sistema experto y el de red neuronal.

---

[19] Cotino Hueso «El uso jurisdiccional de la inteligencia artificial: habilitación legal…», *cit.*, p. 502.

[20] De Asís Pulido, «La Justicia predictiva: tres posibles usos en la práctica jurídica», *cit.*, p. 297.

Los sistemas expertos son los dotados de una IA que combina mediante operadores lógicos un enorme número de datos especializados sobre la materia. Proporcionan respuestas inteligentes mediante una manipulación de símbolos que sigue el sistema de reglas lógicas que guían el pensamiento formal humano. Se basan en muchos casos en sistemas de árboles decisionales que llegan a una conclusión válida tras un procedimiento de eliminación de opciones no válidas. Otras veces la respuesta inteligente tiene lugar mediante la aplicación no de reglas lógicas, sino de métodos bayesianos de probabilidad estadísticas, considerando que la solución correcta es la que tiene la mayor probabilidad del suceso, partiendo de una gran base de datos probabilísticos, llegándose a conclusiones no exactas, pero con un grado de probabilidad de acierto muy alto.

El sistema de redes neuronales proviene de mediados del siglo XX, se basa en el descubrimiento de las "neuronas artificiales" en 1943, por los pioneros en la IA, el neurólogo Warren McCulloch y el matemático Walter Pitts. Una neurona artificial es una función matemática que replica el funcionamiento de la neurona biológica. Como ya hemos visto, las funciones matemáticas pueden ser programadas en un ordenador, con el resultado de que podemos crear dichas neuronas en la máquina. Como señala Latorre Sentís[21]:

> «…la idea central de esta primera neurona artificial es que todo lo que hace una neurona biológica es básicamente un procesamiento de información. Unas señales entran, se procesan y el resultado se pasa a otras neuronas. Dicho de forma más contundente: información entra en neurona artificial, se procesa, se genera nueva información, información pasa a otras neuronas. Todo se reduce a manipulación de información. Eso es lo que hace nuestro cerebro constantemente».

Posteriormente, Frank Rosenblatt crea las redes neuronales al diseñar el *Perceptrón*, sistema informático que, disponiendo las neuronas en capas superpuestas, logra que la máquina aprenda por sí misma. Como la red tiene bastante profundidad, pues consta de muchísimas capas, se pasa a hablar de «aprendizaje profundo» o *Deep learning*.

Pues bien, tanto uno como otro modelo de sistema inteligente comete errores, pero en ambos es muy complicado averiguar por qué los han cometido. En el sistema experto, porque lo que nosotros creemos un conjunto de reglas bien jerarquizadas puede ser interpretado de otra manera por el sistema (recordemos que las IA no piensan, simulan el pensamiento: en realidad se limitan a realizar operaciones matemáticas, a computar). En la red neuronal, porque el resultado es el producto de una serie de funciones matemáticas que se distribuyen en paralelo y luego en redes superpuestas, pasando de capa a capa no una proposición lógica, sino una entrada de impulsos que son el resultado de cada neurona individual, impulsos que siguen capa a capa, hasta llegar a la última.

---

[21] Latorre Sentís, *Ética para máquinas*, *cit.*, pág, 105.

En definitiva, que en los sistemas inteligentes podemos ver claramente el resultado, pero es difícil averiguar cómo se ha llegado a dicho resultado. Esto se conoce como el efecto «caja negra» o *blackbox*. Veamos un par de ejemplos.

Ponen Lemley y Casey[22] un curioso ejemplo de *blackbox*: En 2014 un grupo de robotistas se hallaban adiestrando a un dron de vuelo automático; el dron debía sobrevolar un área circular y posicionarse en el centro exacto de dicho círculo. El caso es que, aunque se acercó en varios vuelos a dicho centro, al final el dron en lugar de volar hacia el objetivo, se salía fuera del área circular indicada. La razón, como se descubrió, es que los supervisadores, como parte del entrenamiento, cuando el dron se salía del área señalada, lo colocaban directamente en el centro del círculo, por lo cual la red neuronal del dron llegó por sí misma a la conclusión de que el camino más rápido para llegar al centro del círculo consistía en salirse del área delimitada, pues enseguida aparecían unos señores muy amables que le colocaban en el lugar preciso.

Tampoco los sistemas expertos se libran del problema de las instrucciones mal entendidas (por los humanos). Un ejemplo nos lo relata Luis Magdalena Layos[23], en un proceso de aprendizaje de deambulación de robots autónomos, las instrucciones que se daban al sistema —en un modelo de simulación— eran las de avanzar conservando los pies en contacto con el suelo (el robot no debe caer), que la posición final esté por delante de la inicial (avanza) y que la desviación entre los sucesivos pasos en longitud y duración sea mínima (los pasos son parecidos entre sí). Sin embargo, los resultados fueron muy malos, veamos cómo nos cuenta esto el autor:

> «Tras un fin de semana de trabajo, el ordenador completó el proceso… Los resultados eran sospechosos, demasiado buenos, no habíamos generado una, sino múltiples secuencias de marcha válidas, con diversas longitudes y duraciones de paso. Y cada secuencia era perfecta, formada por pasos idénticos. En efecto, demasiado bueno para ser cierto. ¿Qué había pasado? ¿Eran correctas las soluciones? En caso contrario, ¿dónde estaba el posible problema? No tardamos mucho en descubrirlo. El sistema de aprendizaje automático había seguido al pie de la letra nuestras instrucciones, había hecho exactamente lo que le pedíamos, pero había encontrado un atajo para alcanzar el objetivo… Todas las secuencias de marcha se reducían a un único paso. El robot daba un paso hacia delante y se detenía. Avanzaba sin caerse y con pasos idénticos, porque cuando solo das un paso, todos los pasos dados son idénticos».

Veamos ahora las incidencias de la IA en distintos campos jurídicos.

---

[22] Lemley, Mark A. y Casey, Bryan, «Remedies for Robots», *86 University of Chicago Law Review (2019), Stanford Law and Economics Olin Working Paper* No. 523, última revisió abril 2020, DOI: http://dx.doi.org/10.2139/ssrn.3223621.

[23] Magdalena Layos, Luis, «¿Por qué debería confiar en ti (máquina)?», *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0,* coord. María José Cruz Blanca, Ignacio Lledó Benito; Francisco Lledó Yagüe (dir.), Ignacio F. Benítez Ortúzar (dir.), Óscar Monje Balmaseda (dir.), Dykinson, 2021, p. 622.

IV. IA, DERECHO PROCESAL Y PROCEDIMIENTO

El carácter de ordenación sucesiva de actos reglamentados que tiene todo proceso le hace especialmente apto para su gestión mediante un algoritmo inteligente. Señala así Cotino Hueso[24] que ya el «principio de orientación al dato», que aparecen en la Exposición de Motivos y en la letra j) del artículo 35 del Real Decreto-ley 6/2023 se vincula a *la producción de actuaciones judiciales y procesales automatizadas, asistidas y proactivas, de conformidad con la ley*. Nos señala este autor que las utilizaciones a las que se refiere además este artículo son las de «c) La búsqueda y análisis de datos y documentos para fines jurisdiccionales y organizativos» e «intercambios masivos» de datos. La letra k) de este art. 35 nos habla de la IA con fines «de apoyo a la función jurisdiccional, a la tramitación, en su caso, de procedimientos judiciales», y el CGPJ alertaba que esta referencia al uso de IA en la letra k), «puede entenderse como una habilitación en blanco», más allá de las más concretas previsiones de actuaciones automatizadas. Señala Cotino que este artículo 35 vendría a habilitar legalmente el uso de sistemas inteligentes, quizá entregando a la IA un cheque en blanco, para «la producción de actuaciones judiciales y procesales automatizadas, asistidas y proactivas» (término éste que significa simplemente *decidido*, *resolutivo*, y que da idea de una decisión automatizada y sin control humano), y también para «la búsqueda y análisis de datos y documentos para fines jurisdiccionales y organizativos, los intercambios masivos de datos, el apoyo a la función jurisdiccional, y la tramitación, en su caso, de procedimientos judiciales, así como la definición y ejecución de políticas públicas relativas a la Administración de Justicia», finalidad esta última cuyo significado queda a la voluntad de la Administración.

En cualquier caso, la Ley de Enjuiciamiento civil, sobre todo tras el Real Decreto-ley 6/2023, de 19 de diciembre, ha sido modificada, y en la actualidad el art. 129 bis prevé la celebración de actos procesales mediante presencia telemática, es decir, *on line: 1. Constituido el Juzgado o Tribunal en su sede, los actos de juicio, vistas, audiencias, comparecencias, declaraciones y, en general, todos los actos procesales, se realizarán preferentemente mediante presencia telemática, siempre que las oficinas judiciales tengan a su disposición los medios técnicos necesarios para ello. La intervención mediante presencia telemática se practicará siempre a través de punto de acceso seguro…* Quedan fuera los actos de audiencia, declaración o interrogatorio de partes, testigos o peritos, la exploración de la persona menor de edad, el reconocimiento judicial personal o la entrevista a persona con discapacidad, con excepciones en algunos casos. El artículo 137 bis refiere la realización de actuaciones judiciales mediante el sistema de videoconferencia, y el 152 los actos de comunicación telemática, en la dirección electrónica habilitada al efecto, por

[24] Cotino Hueso, «El uso jurisdiccional de la inteligencia artificial: habilitación legal…», *cit.*, p. 502.

comparecencia electrónica o por los medios telemáticos o electrónicos elegidos por el destinatario.

Pero todos estos medios no son sino las antiguas TICs, tecnologías de información y comunicación, las primeras de bajo nivel de inteligencia, sólo para la recuperación de datos, las segundas sin intervención de una máquina en los resultados. Lo que se trata en la actualidad es la suplencia de la actividad intelectual del juez y letrado por un sistema inteligente, que es a lo que se refiere el artículo 35 del Real Decreto-ley 6/2023 al hablar de *la producción de actuaciones judiciales y procesales automatizadas, asistidas y proactivas*, es decir, autodecisionales.

La amplitud de la autorización legal para el uso de sistemas inteligentes en la proyectada *Ley de Eficiencia digital del Servicio público de justicia, por la que se transpone al ordenamiento jurídico español la Directiva (UE) 2019/1151* que como novedad relevante establece en los arts. 56 a 58 las denominadas *actuaciones automatizadas, proactivas y asistidas* que suponen la incorporación de herramientas de inteligencia artificial en la producción de actuaciones procesales. Esto trata de ser matizado por el Consejo General del Poder Judicial en su *Informe al Anteproyecto* de dicha Ley[25]. En este Informe se indica en su nº 124 que se distinguen dos tipos de actuaciones automatizadas, las simples y las actuaciones proactivas; las simples son actuaciones de trámite o resolutorias simples, pero en las proactivas se critica la falta de control humano y extralimitación de las Administraciones en la custodia de datos; ¿Cuáles son estas actuaciones automatizadas? Señala el mismo Informe en su nº 157 que las actuaciones automatizadas, previstas en el artículo 56 de la Ley, son las actuaciones procesales producidas por un sistema de información y comunicación (SIC) adecuadamente programado sin intervención de una persona física.

El precepto distingue dos tipos de actuaciones automatizadas, las simples y las actuaciones proactivas; las simples son actuaciones de trámite o resolutorias simples, que no requieren interpretación jurídica, como la generación de copias y certificados. Las actuaciones proactivas se definen de un modo más impreciso en el artículo 56.2 del Anteproyecto: «Se entiende por actuaciones proactivas las actuaciones automatizadas, autoiniciadas por sistemas de información sin intervención humana, que aprovecha la información incorporada en un expediente o procedimiento de una Administración pública con un fin determinado, para generar avisos o efectos directos a otros fines distintos, en el mismo o en otros expedientes, de la misma o de otra Administración pública». Aquí el CGPJ pone de relieve una falta de conexión de la regulación de estas actuaciones proactivas

---

[25] https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/Actividad-del-CGPJ/Informes/Informe-al-anteproyecto-de-Ley-de-Eficiencia-Digital-del-Servicio-Publico-de-Justicia--por-la-que-se-transpone-al-ordenamiento-juridico-espanol-la-Directiva--UE--2019-1151-del-Parlamento-Europeo-y-del-Consejo--de-20-de-junio-de-2019--por-la-que-se-modifica-la-Directiva--UE--2017-1132-en-lo-que-respecta-a-la-utilizacion-de-herramientas-y-procesos-digitales-en-el-ambito-del-Derecho-de-sociedades

con el ámbito propio de la Administración de Justicia, y señala su definición «evanescente», pues aparte de la generación de avisos, también pueden producir «"efectos directos a otros fines distintos"», lo que «constituye un arcano difícil de descifrar», nos dice el Consejo.

En definitiva, falta de control humano y extralimitación de las Administraciones en la custodia de datos; por ello insiste el CGPJ en que las actuaciones automatizadas se produzcan siempre «sin prejuicio de la dirección del proceso que corresponde a Jueces y Magistrados, que podrán establecer las instrucciones pertinentes sobre su uso o deshabilitación».

Luego tenemos las actuaciones asistidas (más bien asistenciales), que aparecen en el artículo 57 del Anteproyecto y se definen como aquellas para las que los sistemas generan un borrador total o parcial de documento complejo producido por algoritmos, que puede constituir fundamento o apoyo de una resolución judicial o procesal. Pues bien, dice el nº 161 del Informe que este borrador documental «sólo se generará a voluntad del usuario, que podrá ser libre y enteramente modificado por éste y que en ningún caso el borrador documental constituirá la resolución judicial o procesal sin la validación por parte de la autoridad competente, Juez o Magistrado, Fiscal o Letrado de la Administración de Justicia». Por tanto, control humano y por parte de los especialistas que legalmente deban decidir.

Naturalmente, el siguiente paso consistirá en pasar de la ayuda para la decisión a la decisión judicial automática, a los «jueces-robot», como nos cuenta De Asís Pulido[26] que ya funcionan en China, como hemos podido ver anteriormente.

V. DERECHO PENAL Y CRIMINOLOGÍA

1. Generalidades

El ámbito en el que más aplicaciones de la IA se detectan es el de la Justicia penal y la investigación criminal. Hay que dejar aparte la cuestión del Ciberespacio, como medio en el que puede actuar la actividad criminal o *locus delicti commissi*, como puntualizaba el recientemente fallecido Carlos Romeo Casabona[27], así como la Ciberdelincuencia como nueva tipología delictiva, que se produce en dicho medio.

---

[26] González Tapia, Mª Isabel, «Protección penal de los neuroderechos: el uso directo de las neurotecnologías sobre el ser humano», *Inteligencia Artificial y Filosofía del Derecho*, Ediciones Laborum, Murcia, 2022, p. 328.

[27] Romeo Casabona, Carlos, «El Ciberespacio como lugar virtual y legal de comisión del delito. Necesidad de nuevas respuestas jurídicas», *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial*, Vol. I: Ciberseguridad y ciberdelitos, Editorial Comares, Granada, 2023, pp. 3-21.

Apunta Cotino Hueso[28] que la regulación sobre el uso de sistemas biométricos en el ámbito policial y penal quedará bajo la cobertura especial de la Directiva 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 en el ámbito penal (testigos, víctimas o encausados)[29]. En esta Directiva, el tratamiento de los datos biométricos como datos personales aparece en el art. 10: *El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física… solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando: a) lo autorice el Derecho de la Unión o del Estado miembro…* Por su parte el Reglamento Europeo de Protección de Datos 2016/679, también de 27 de abril, considera a los datos biométricos como "datos de carácter sensible".

En concreto nos señala Dolz Lago[30] que la *Resolución del Parlamento Europeo de 6 octubre 2021 sobre Inteligencia Artificial y su utilización por autoridades policiales y judiciales en asuntos penales* plantea la utilización de sistemas inteligentes por las autoridades policiales para distintas labores de vigilancia, como la identificación biométrica mediante reconocimiento facial, o el reconocimiento automático de matrículas, pero también para

> «…la identificación por voz, el reconocimiento del habla, las tecnologías de lectura de labios, la vigilancia auditiva… la investigación y el análisis autónomos de bases de datos identificadas, la predicción (actuación policial predictiva y análisis de puntos críticos de delincuencia), los instrumentos de detección del comportamiento, las herramientas avanzadas de autopsia virtual para ayudar a determinar la causa de la muerte, las herramientas autónomas para detectar fraudes financieros y la financiación del terrorismo, la vigilancia de las redes sociales (rastreo [*scraping*] y recopilación de datos para detectar conexiones) y los sistemas automatizados de vigilancia que incorporan diferentes capacidades de detección (como la detección del latido cardíaco y las cámaras térmicas)» (Considerando M).

Dentro de estas herramientas no solamente tenemos la vigilancia de personas o vehículos, sino también, como señala López Riba[31], programas de tratamiento

---

[28] Cotino Hueso, Lorenzo, «Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal», *El Cronista del Estado Social y Democrático de Derecho*, N.º 100 (Septiembre-Octubre), 2022 (Ejemplar dedicado a: Inteligencia artificial y derecho), p. 73.

[29] De la misma fecha es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos, que sustituye al anterior Reglamento General de Protección de Datos de 1995.

[30] Dolz Lago, «Una aproximación jurídica a la Inteligencia Artificial», *Diario La Ley*, *cit.*, p. 4.

[31] López Riba, José María, «Inteligencia artificial y control policial. Cuestiones para un debate frente al hype», InDret, 2.2024. DOI: 10.31009/InDret.2024.i2.10, p. 411.

de textos y del lenguaje natural, como los sistemas de rastreo de discursos de odio en redes sociales, o el proyecto europeo TENSOR para la detección de actividades terroristas en Internet. Veamos alguna de estas técnicas.

2. Sistemas predictivos del comportamiento

Las herramientas predictivas, que consisten básicamente en sistemas actuariales, como señala Urruela Mora[32], basados por tanto en la realidad estadística de datos que indican futuras conductas de reincidencia. Su utilización básica se encuentra en el estamento judicial, para la adopción de medidas de libertad provisional (o prisión preventiva) o para medir correctamente la imposición de la pena, siendo el sistema americano COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) el más conocido. Sin embargo, dado que este sistema produce bastantes falsos positivos de peligrosidad, concluye el autor que este y otros sistemas similares deben tener un papel meramente auxiliar, «pudiendo erigirse en apoyos a la decisión del experto de referencia (y ello, bajo las importantes cautelas recogidas a lo largo del presente trabajo), pero nunca sustituir el criterio de aquel». Romeo Casabona[33], sobre la importante sentencia norteamericana *Wisconsin v. Loomis*, da cuenta de la aceptación de COMPAS por la jurisprudencia americana, y de la afirmación de que no se viola el derecho del acusado aunque éste no pueda obtener información precisa sobre el mecanismo de evaluación de los riesgos: se negó a la defensa de Loomis información sobre el algoritmo de COMPAS alegando derechos de propiedad intelectual sobre el mismo. Lo esencial, se dice, es la veracidad de los datos de hecho sobre los que decide el sistema, y si éstos son ciertos, no hay posibilidad de refutar la evaluación del sistema.

Destaca Coca Payeras[34] la preocupación de la *Resolución de 6 octubre 2021 sobre Inteligencia Artificial* por la irrupción de los sistemas inteligentes, y su posible efecto negativo para la protección de los derechos de las personas, imponiendo este texto la necesidad de garantizar el respeto a los derechos y libertades

---

[32] Urruela Mora, Asier, «Instrumentos de evaluación del riesgo de violencia, justicia algorítmica y Derecho penal. Perspectiva crítica», *Estudios político-criminales, jurídico-penales y criminológicos: libro homenaje al profesor José Luis Díez Ripollés*, coord. por Noelia Corral Maraver, Deborah García Magna, Fátima Pérez Jiménez, Bertha Prado, Pablo Rando Casermeiro; Juan Muñoz Sánchez (dir.), Octavio García Pérez (dir.), Ana Isabel Cerezo Domínguez (dir.), Elisa García España (dir.), 2023, págs. 1877-1888.

[33] Romeo Casabona, Carlos, «Inteligencia artificial, predictividad y justicia penal», *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial*, Vol. II: IA y responsabilidad penal, Editorial Comares, Granada, 2023, pp. 119-139. Pp. 125-126.

[34] Coca Payeras, Miguel, (2023), «Las iniciativas de la Unión europea sobre inteligencia artificial: de la persona electrónica, al difícil equilibrio entre la necesidad de impulsarla y evitar sus riesgos», *Revista de Derecho Civil,* vol. X, núm. 2, especial (junio, 2023). En http://nreg.es/ojs/index.php/RDC, p. 24.

fundamentales consagrados en la Carta de derechos fundamentales, así como la necesidad de que la tecnología de IA se desarrolle de manera que sitúe a las personas en su centro. Además, alerta sobre la utilización de herramientas de IA por las autoridades judiciales para la toma de decisiones sobre prisión preventiva, o para dictar sentencias, calcular las probabilidades de reincidencia y determinar la libertad condicional o resolver litigios en línea (esto último referido a otro ámbito jurídico).

La Ley de la IA interviene específicamente en la declaración de estas técnicas como prácticas prohibidas, salvo que tengan un carácter meramente auxiliar o indicativo, como podemos ver en el art. 5.1.d) que prohíbe: d*) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad*; ahora bien, añade como excepción …*esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva.*

Estas técnicas son también llamadas de perfilado predictivo, en cuanto operan definiendo un perfil del sujeto y prediciendo su peligrosidad. En cuanto a su admisibilidad, ya hemos visto que se prohíben salvo que tengan carácter meramente auxiliar. Pero aun así, el Reglamento o Ley de la IA nos advierte que muchas de ellas pueden ser consideradas de alto riesgo. Así, el artículo 6.3.3 del mismo advierte que *No obstante lo dispuesto en el párrafo primero, los sistemas de IA a que se refiere el anexo III siempre se considerarán de alto riesgo cuando el sistema de IA efectúe la elaboración de perfiles de personas físicas.* Por lo tanto, todas las aplicaciones de perfilado predictivo caen bajo esta calificación. Pero además el citado Anexo III incluye como de alto riesto los sistemas dedicados a: *6. Garantía del cumplimiento del Derecho, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable: …b) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho como polígrafos o herramientas similares… d) Sistemas de IA destinados a ser utilizados por las autoridades … para evaluar el riesgo de que una persona física cometa un delito o reincida en la comisión de un delito …*

3. Sistemas de identificación biométrica

Una importante aplicación de la IA para las finalidades de investigación policial son las técnicas de identificación biométrica. La citada Resolución de 6 octubre 2021 expresa también gran preocupación por el uso por parte de las fuerzas policiales y servicios de inteligencia de bases de datos de reconocimiento facial, como la base *Clearview AI,* una base de datos de más de 3000 millones de imágenes que se han recopilado de redes sociales y otros lugares de

internet. En Italia el Garante italiano de la protección de datos considero inadmisible el 16 de abril de 2021 el «*Sistema Automatico di Riconoscimento Immagini*» *SARI*, utilizado desde 2019. Se usa también esta identificación por empresas privadas, sobre todo almacenes y tiendas, y así en España, la cadena de supermercados *Mercadona*, recibió una fuerte sanción por implantar un sistema inteligente biométrico que controlaba si quienes accedían a algunos establecimientos estaban en sus listas de «personas con una orden de alejamiento o medida judicial análoga en vigor»[35].

Ante estos sistemas de reconocimiento o biométricos, la Resolución pide a la Comisión que, por medios legislativos y no legislativos, y si es necesario a través de procedimientos de infracción, prohíba el tratamiento de datos biométricos, incluidas las imágenes faciales, mediante vigilancia masiva en espacios públicos con fines coercitivos (epígrafe 31).

Estos sistemas captación y procesamiento de los datos biométricos de las personas tienen especial interés policial y criminológico. Señala Barona Vilar[36] que las técnicas biométricas pueden ser fisiológicas, comportamentales o mixtas. Entre las técnicas que inciden en los aspectos físicos y fisiológicos caracterizadores de una persona están las huellas dactilares, el análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, geometría de las manos, otogramas de las orejas, reconocimiento facial, de la voz, análisis de ADN, análisis de poros de la piel o incluso detección de olor corporal. Las técnicas comportamentales analizan el comportamiento de la persona a través de la comprobación de la firma (figura, trazo, presión, velocidad, etc.), el análisis de la pulsación de las teclas, análisis de movimientos o forma de caminar, etc.. Las mixtas utilizan ambos tipos de datos.

Ahora bien, la incidencia de estas técnicas de identificación biométrica con la posible vulneración de muchos derechos fundamentales y libertades de las personas dan lugar a un tratamiento restrictivo en Ley de la IA de 2024. En esta se procede a definir los «Datos biométricos» en el art. 3, nº 34) como … *los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos*[37]. Además, hay que sumar a estos datos lo que el considerando 15 de la misma Ley llama «características humanas de tipo físico, fisiológico o

---

[35] Resolución de la Agencia Española de Protección de Datos, procedimiento sancionador PS 120/2022

[36] Barona Vilar, Silvia, «Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale», *Actualidad Jurídica Iberoamericana* Nº 21, agosto 2024, pp. 298-331. P. 305.

[37] Repite la definición del art. 3 de la *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo*, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales: *13) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.*

conductual», que son …*la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla…* Como vemos, todo un arsenal de datos para lograr la identificación del sujeto.

4. Identificación, verificación y categorización biométrica. Reconocimiento de emociones

Las posibles utilizaciones de estos datos biométricos se pueden deducir de lo que dicen los siguientes números de este art. 3 de la Ley de la IA de 2024: *35) «identificación biométrica»: el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos… 36) «verificación biométrica»: la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente.* Aquí la diferencia está en que la obtención del dato biométrico no tiene lugar mediante una vigilancia masiva e indiscriminada, sino sobre datos previamente recolectados y que se van presentando al sistema para que los examine, por ejemplo, el cotejo de un retrato-robot con una base de datos de fotografías de delincuentes convictos.

Destaca también la Ley de la IA cómo puede distinguirse también, en el mismo art. 3, en el nº 37 las «categorías especiales de datos personales» que son los datos personales a los que se refiere el art. 9.1 del ya citado *Reglamento (UE) 2016/679,* el también citado artículo 10 de la *Directiva (UE) 2016/680* y el artículo 10, apartado 1, del *Reglamento (UE) 2018/1725* (se trata de datos referidos al origen étnico o racial, a las opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos identificativos, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física). Se habla también en el nº 38 de *«datos operativos sensibles»: los datos operativos relacionados con actividades de prevención, detección, investigación o enjuiciamiento de delitos cuya divulgación podría poner en peligro la integridad de las causas penales.*

Aparte tenemos, también basados en datos biométricos, en el nº 39 los «sistemas de reconocimiento de emociones». Se trata de …*un sistema de IA destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos.* Este sistema sirve, fundamentalmente, para, detectando las emociones del sujeto (la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión —Considerando 16 LIA-) averiguar la verdad o falsedad de sus declaraciones, perfeccionando al polígrafo actual, o identificar otras circunstancias del sujeto. Se utilizan en el control de fronteras, como el proyecto europeo *iBorderCtrl*, un sistema inteligente de detección de mentiras que, como dice Coca Payeras (Ibid.): «elabora perfiles de los viajeros a partir de una entrevista automatizada

por ordenador realizada a través de la cámara web del viajero antes del viaje y un análisis de 38 microgestos basado en la inteligencia artificial, probado en Hungría, Letonia y Grecia». O el sistema americano para el control de fronteras en EE.UU., que permite leer emociones, detectar la verdad de las manifestaciones, y predecir futuros comportamientos, denominado Agente Virtual Automatizado para la Evaluación de la Verdad en Tiempo Real (AVATAR — *Automated Virtual Agent for Truth Assessments in Real Time*), que analiza el comportamiento no verbal y verbal de los viajeros.

El paso siguiente será la detección de pensamientos a través de la exploración neurológica del sujeto, campo en el que se dan notables avances. Así, desde las universidades de Singapur y Hong Kong, los investigadores Chen, Qing y Zhouy[38] dan cuenta de la posibilidad de decodificación directa de las señales cerebrales en imágenes y videos, utilizando la resonancia magnética. Mediante esta técnica, se capturan y codifican datos sobre la actividad cerebral del sujeto, y un sistema de reconocimiento traduce dichos datos a imágenes, en algunos casos muy fidedignas.

Y finalmente está, en el nº 40) el «sistema de categorización biométrica»: *un sistema de IA destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas*. Esta categorización se distingue de las anteriores identificación y verificación biométricas, en concreto porque utiliza los datos biométricos (*sexo, edad, el color del pelo, el color de los ojos, los tatuajes, los rasgos conductuales o de la personalidad, la lengua, la religión, la pertenencia a una minoría nacional o la orientación sexual o política* —Considerando 16-) para adscribir al sujeto a una determinada categoría racial, social o ideológica; el sistema es empleado por las autoridades chinas para identificar a las personas de la etnia uigur. Finalmente, los números 41 y 42 recogen los sistemas de identificación biométrica remota, es decir mediante cámaras de vigilancia, ya sea *en tiempo real* o *en diferido,* presupuesto para identificar al sujeto y aplicarle luego los otros sistemas de reconocimiento.

Pues bien, las técnicas de identificación biométrica reciben un tratamiento restrictivo con excepciones. Para empezar, el art. 5.1. h) de la Ley de Inteligencia artificial considera como práctica prohibida …*el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público*[39] *con fines de garantía del*

---

[38] Chen Zijiao, Qing Jiaxin y Zhouy Juan Helen, «CinematicMindscapes: High-quality Video Reconstruction from Brain Activity», preprint en arXiv:2305.11675, https://doi.org/10.48550/arXiv.2305.11675 [Submitted on 19 May 2023].

[39] Hace el Considerando 19 una referencia a los espacios públicos: …*cualquier espacio físico al que pueda acceder un número indeterminado de personas físicas y con independencia de si es de propiedad privada o pública y de la actividad para la que pueda utilizarse el espacio, ya sean actividades comerciales, por ejemplo, tiendas, restaurantes, cafeterías; de prestación de servicios, por ejemplo, bancos, actividades profesionales, hostelería; deportivas, por ejemplo, piscinas, gimnasios, estadios; de transporte, por ejemplo, estaciones de autobús, metro y*

cumplimiento del Derecho. Ahora bien, esta prohibición es pura fachada, porque inmediatamente a continuación se exceptúa la utilización policial para perseguir el delito, aunque con fuertes exigencias de necesidad: …*salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes: i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas, ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista, iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II*[40] *que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.* Advierte el art. 5.2.1 que 2. el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público …*para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico.* Y añade el 5.2.3 que el sistema deberá cumplir las garantías y condiciones necesarias que exija el Derecho nacional que autorice dicho uso, …*en particular en lo que respecta a las limitaciones temporales, geográficas y personales. El uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad garante del cumplimiento del Derecho ha completado una evaluación de impacto relativa a los derechos fundamentales …y ha registrado el sistema en la base de datos de la UE.* Salvo casos de urgencia debidamente justificados, en que se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida.

Además, exige el art. 5.3 que el uso policial del sistema se vea amparado por *la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente*, también salvo urgencia, pudiéndose solicitar a posteriori. Aparte, según el art. 5.4, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público …*se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales.*

---

ferrocarril, aeropuertos, medios de transporte; de entretenimiento, por ejemplo, cines, teatros, museos, salas de conciertos, salas de conferencias; de ocio o de otro tipo, por ejemplo, vías y plazas públicas, parques, bosques, parques infantiles.

[40] Se refiere a delitos de …*terrorismo, trata de seres humanos, explotación sexual de menores y pornografía infantil, tráfico ilícito de estupefacientes o sustancias psicotrópicas, tráfico ilícito de armas, municiones y explosivos, homicidio voluntario, agresión con lesiones graves, tráfico ilícito de órganos o tejidos humanos, tráfico ilícito de materiales nucleares o radiactivos, secuestro, detención ilegal o toma de rehenes, delitos que son competencia de la Corte Penal Internacional, secuestro de aeronaves o buques, violación, delitos contra el medio ambiente, robo organizado o a mano armada, sabotaje, participación en una organización delictiva…*

Aun contando con todas estas prevenciones, la Ley de la IA considera estos sistemas basados en datos biométricos como sistemas de alto riesgo. Lo señala así el art. 6.2: *Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III.* Y este Anexo III dice en su número 1: *Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA que formen parte de cualquiera de los ámbitos siguientes: 1. Biometría, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable: a) Sistemas de identificación biométrica remota. Quedan excluidos los sistemas de IA destinados a ser utilizados con fines de verificación biométrica cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser. b) Sistemas de IA destinados a ser utilizados para la categorización biométrica …. c) Sistemas de IA destinados a ser utilizados para el reconocimiento de emociones.* Aquí hay que destacar que mientras los *sistemas de identificación biométrica remota «en tiempo real»* en espacios públicos se ven sujetos a prohibición salvo las finalidades policiales autorizadas y conformes a la legalidad, los de identificación «en diferido», así como los de categorización y reconocimiento de emociones van sujetos a la calificación más benigna de «alto riesgo». Se plantean algunos problemas en cuanto al concepto de «espacio público», que intenta aclarar el considerando nº 19 de la Ley. En particular se dice que *Los espacios en línea no son lugares de acceso público, ya que no son espacios físicos. No obstante, se debe determinar caso por caso si un espacio es de acceso público o no teniendo en cuenta las particularidades de la situación concreta.* Como ejemplo de las consecuencias de una falta de cumplimiento de los requisitos legales, apunta Barona Vilar[41] el caso de una escuela secundaria de Skelleftea, en Suecia, multada por su Agencia de Protección de Datos con 18.500 euros por adoptar la tecnología de reconocimiento facial para controlar la asistencia de los alumnos al aula, entendiendo que este proyecto vulnera varios artículos del Reglamento de Protección de Datos, de obligado cumplimiento para empresas y ciudadanos.

Desde un punto de vista ceñido a los derechos fundamentales, apunta Martin Ebers[42] que el art. 5.1.d) de la LIA prohíbe los sistemas de IA de identificación biométrica remota «en tiempo real» en espacios de acceso pero que este enfoque de prohibir únicamente los sistemas de identificación biométrica utilizados para la aplicación de la ley es demasiado restrictivo, y sus excepciones demasiado amplias y permisivas. Critica además que el reconocimiento automatizado de características como el sexo, la sexualidad o el origen étnico, la categorización biométrica (*biometric categorization systems* o BCS), así como el reconocimiento automatizado de las emociones (*emotion recognition system* o ERS)[43], no están prohibidos por la LIA, sino que sean sólo de alto riesgo.

---

[41] Barona Vilar, «Tecnología biométrica y datos biométricos. Bondades y peligros…», *cit.*, p. 315.

[42] Ebers, Martin, «El futuro marco jurídico europeo de la inteligencia artificial», *Persona y derecho civil, los retos del siglo XXI: (persona, género, transgénero, inteligencia artificial y animales sensibles)* / coord. por José Luis Argudo Périz, María del Carmen Bayod López (dir.), 2023, p. 267.

[43] Un sistema inteligente de reconocimiento de emociones trata de detectar diferentes emociones del sujeto mediante la información procedente de las expresiones faciales, el movimiento

Aparte de estas restricciones, también se advierte que estas técnicas de identificación biométrica, llamadas de policía predictiva, tienen un número demasiado alto de falsos positivos y falsas alertas, por lo que están siendo abandonadas por las policías de Nueva York y Cambridge, que las habían adoptado. Da cuenta así Cotino[44] de que en Holanda la sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya declaró contrario al artículo 8 CEDH el sistema *Systeem Risicoindicatie*" ("SyRI"), para impedir fraudes a la Seguridad social y tributarios. Ratificando esto, en el ámbito policial y penal, en 2023, la sentencia del Tribunal Constitucional alemán del 16 de febrero (1 BvR 1547/19, 1 BvR 2634/20) estableció requisitos y estándares de calidad legislativa muy altos para el tratamiento automatizado de datos en la prevención del delito. López Riba[45] advierte, en cuanto a los sistemas predictivos zonales, que los algoritmos indican lugares en los que la policía vigilaba ya tradicionalmente, generalmente barrios conflictivos, por lo que se concluye que los sistemas predictivos predicen «el control policial futuro, no los delitos futuros», con el consiguiente problema de sesgo en las detenciones. El problema, como señala el autor más adelante, está en que se produce el siguiente «bucle de realimentación»: el hecho de basar las actuaciones futuras en datos sesgados de actuaciones pasadas refuerza esos mismos sesgos. Y como advierte Mark Coeckelbergh[46], el problema del sesgo en los sistemas actuariales predictivos como COMPAS radica en que para el sistema, el sesgo no es un error, sino un patrón extraído de los datos. Muchos sesgos se generan en datos sesgados. Para muchos, estos sistemas son una muestra del solucionismo tecnológico, que pone la solución de todos los problemas en la tecnología, olvidando que a veces ésta crea otros nuevos.

Es muy conocida en EE.UU. la sentencia del Tribunal de Apelaciones del Noveno Circuito de los Estados Unidos, *Patel v. Facebook*, *Inc.*[47], que condenó a *Facebook* en 2019 por la recopilación no consensuada de archivos faciales de los usuarios. El tribunal concluyó que la creación de una base de datos de rostros e identidades constituía una conducta contraria a la *Illinois Biometric Information Privacy Act (BIPA*).

En España, nos comenta Dolz Lago[48], el Cuerpo Nacional de Policía ha creado *VeriPol*, un algoritmo que, basado en el lenguaje de una denuncia presentada, indica la probabilidad de que esta no sea verdad, ayudando por tanto a los policías

---

corporal, los gestos y el lenguaje.

[44] Cotino Hueso «El uso jurisdiccional de la inteligencia artificial: habilitación legal…», *cit.*, p. 502.

[45] López Riba, «Inteligencia artificial y control policial. Cuestiones para un debate …», cit, p. 415.

[46] Coeckelbergh, Mark, *AI Ethics*, The MIT Press essential knowledge series, Cambridge, 2020, p. 127.

[47] *Patel v. Facebook, Inc.*, No. 18-15982 (9th Cir. 2019)

[48] Dolz Lago, «Una aproximación jurídica a la Inteligencia Artificial», *Diario La Ley*, *cit.*, p. 5

a enfocar la investigación de forma más eficaz, y así desincentivar las denuncias falsas. También se han desarrollado algoritmos que, en base a patrones temporales de hechos delictivos, «predicen» cuántos delitos, de qué tipo y en qué zona se van a producir en el próximo turno policial, para una mejor distribución de las patrullas y turnos policiales. Naturalmente, estamos ante herramientas informáticas útiles para el trabajo policial, que no sustituyen en modo alguno la decisión humana, sino que tienen un papel auxiliar. Lo mismo cabe decir respecto de la aplicación *VIOGEN*, para analizar el riesgo de violencia de género, unido a sistemas de control biométrico y localizadores para evitar proximidades que puedan ser peligrosas. Para la planificación de vigilancia y patrullas, el sistema *Pred-Crime* es un software para predecir el momento y lugar de ocurrencia de determinados delitos utilizado por la Policía Local de Rivas-Vaciamadrid.

Con carácter general, la Ley de la IA nos señala, en su considerando nº 42, que nunca hay que olvidar la presunción de inocencia, por lo que las personas físicas siempre deben ser juzgadas basándose en su comportamiento real: *Las personas físicas nunca deben ser juzgadas a partir de comportamientos predichos por una IA basados únicamente en la elaboración de sus perfiles, en los rasgos o características de su personalidad, como la nacionalidad, el lugar de nacimiento, el lugar de residencia, el número de hijos, el nivel de endeudamiento o el tipo de vehículo, sin una valoración humana y sin que exista una sospecha razonable, basada en hechos objetivos comprobables, de que dicha persona está implicada en una actividad delictiva. Por lo tanto, deben prohibirse las evaluaciones de riesgos realizadas con respecto a personas físicas para evaluar la probabilidad de que cometan un delito … basándose únicamente en la elaboración de perfiles de esas personas físicas o la evaluación de los rasgos y características de su personalidad.*

Sin embargo, las perspectivas a futuro son de una mayor control y creación de extensas bases de datos biométricos, pues como señala Barona Vilar[49], el Parlamento Europeo ha aprobado la creación de una base de datos biométricos de los más de 500 millones de habitantes de la UE, base de datos que incluirá la información habitual (nombre, dirección, fecha de nacimiento y número de identidad) y datos biométricos de la huella dactilar o de la cara del usuario (con foto incluida), y escaneos faciales. Esta nueva base de datos se denomina *Common Identity Repository* (CIR), que unificará los registros de 500 millones de ciudadanos de la UE, estando a disposición de las fuerzas de seguridad de los países miembros. Se establece por el art. 17(1) del Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y el Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración.

---

[49] Barona Vilar, «Tecnología biométrica y datos biométricos. Bondades y peligros…», *cit.*, p. 323.

V. DERECHO CIVIL: SUBJETIVIDAD Y RESPONSABILIDAD

1. Los robots en Derecho civil

Desde el Derecho privado, la incidencia de la IA se advierte en ámbitos como el de la subjetividad y personalidad jurídicas, en el que quieren aparecer los robots como nuevos sujetos o agentes en la vida jurídica, y relacionado con ello, el de la responsabilidad civil por daños[50]. También el ámbito de las propiedades intelectual e industrial, en el que aparecen nuevos autores e inventores no humanos, o el de los derechos al honor, intimidad personal y familiar, y otros derechos fundamentales como el de la libertad de opinión e información, en los que la IA produce alteraciones que desafían a la ciencia jurídica.

A mi juicio, la incidencia más profunda se va a producir en dos ámbitos.

Primero, el de la responsabilidad de los sistemas inteligentes, especialmente si se trata de robots androides. Ya el informe *D6.2 Guidelines on Regulating Robotics*, redactado al amparo del Proyecto europeo *Robolaw,* de mayo de 2014, señalaba que la evaluación de la responsabilidad viene dificultada por la creciente autonomía que exhiben estas máquinas y su capacidad de aprendizaje, citando el informe la opinión de varios científicos: «La suposición de que todo lo que hace un robot es el resultado de la programación, y por lo tanto la máquina puede hacer solo lo que está intencionalmente programada para hacer es una pintoresca supersimplificación (Bekey, Lin & Abney, 2011)». Además, los sistemas complejos pueden mostrar «comportamientos emergentes», es decir, modos de comportamiento que no fueron predichos por el diseñador pero que surgen como resultado de interacciones inesperadas entre los componentes del sistema o con el entorno operativo. Por tanto, se produce una imprevisibilidad del comportamiento de la máquina que hace que los criterios tradicionales de atribución de responsabilidad, basados en la negligencia o falta del cuidado adecuado, no son aplicables, pues nadie tiene suficiente control sobre la acción de la máquina.

El Informe también incide en las posibles vías de solución de esta especial responsabilidad, una de las cuales era la creación de personalidad jurídica para

---

[50] El penalista Romeo Casabona se ha ocupado de un tema estrechamente relacionado con éste, como es el de la responsabilidad penal de robots. Su aceptación exigiría el cambio hacia un concepto funcional de culpabilidad, similar al de las personas jurídicas, que reconociendo cierta personalidad en los robots dotados de libertad de elección, permitiera el concepto de «robot culpable». Apunta también el autor que en tales casos la pena por el delito no cumpliría ningún fin de prevención, ni siquiera especial, pues lo que podría prevenir la reincidencia del robot no es la pena, sino la reprogramación. Este es además el principal argumento de quienes niegan la responsabilidad penal a los robots: aunque tengan una plena autonomía decisoria, fruto de la autoprogramación que les permite el Deep learning, carecen de conciencia y por lo tanto no pueden sentir culpa. Romeo Casabona, Carlos María, «La discusión sobre la atribución de responsabilidad penal a sistemas de inteligencia artificial, en particular a sistemas autónomos», *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial*, Vol. II: IA y responsabilidad penal, Editorial Comares, Granada, 2023, pp. 57-81. Pp. 71-74.

los robots con el fin de responsabilizar al propio robot de los daños causados. Aunque podría defenderse la responsabilidad del propietario del robot, de la misma manera que la tiene el poseedor de un animal por las lesiones causadas por éste, o la responsabilidad de los padres por daños producidos por sus hijos menores, se propugna esta personalidad responsable del robot porque, en última instancia, el propietario tampoco podrá controlar perfectamente el comportamiento de la máquina debido a estos comportamientos emergentes. Esta idea comporta la necesidad de crear un patrimonio del robot para las indemnizaciones. También de esta opinión, Wagner[51] estima que si los robots son tratados como personas, esto se hace a los solos efectos de gestionar su responsabilidad. Añade que esto es para el cumplimiento de los dos fines que debe conseguir un buen sistema de responsabilidad, pues se trata no solamente de indemnizar, de reparar el daño, sino también de disuadir de la causación de daños futuros, es decir, de prevenir, para lo cual se trata de imputar la reparación al que realmente los ha causado porque así adoptará en el futuro las correspondientes medidas para evitarlos. Ahora bien, esto es un argumento en contra de la personalidad del robot, pues éste no aprende obligándole a indemnizar, sino mejorando su programación, y por ello el autor también alerta sobre el hecho de que esta responsabilidad robótica puede ser utilizada como medio de externalizar costes y evitar responsabilidades, del mismo modo que la creación de personas jurídicas mercantiles, las sociedades, obedece en gran parte a la finalidad de limitar la responsabilidad de los socios.

En segundo lugar, y relacionado con la responsabilidad, está la subjetividad robótica. Pese a lo que se dijo desde la archiconocida Resolución UE de 16 de febrero de 2017, y su tan repetida personalidad electrónica para robots, no creo que esta subjetividad venga por la concesión de una personalidad a estos entes, siquiera sea para gestionar su responsabilidad. Son máquinas, y aunque realizan tareas inteligentes, su inteligencia no es humana, y cometeremos un grave error si nos confundimos en este punto. Señala Lasalle que hoy la IA es «"algo" o, si se prefiere, una cosa, que aspira a ser "alguien" o no-cosa consciente de su identidad y de sí misma, entonces, el ser humano ha de ser su conciencia crítica y decisoria[52]». Evidentemente, es el ser humano el que tiene que aplicar su conciencia a la utilización del robot, porque desde luego el robot no tiene

---

[51] Aplicando criterios del análisis económico estima este autor que además con esta atribución de responsabilidad se logra una mejor distribución de los recursos: «El objetivo es maximizar el excedente neto para la sociedad, es decir, la diferencia entre las ganancias de actividades que involucran robots y los costes de producirlos y controlarlos, incluidos los costes de las precauciones y de la indemnización de los accidentes que, a pesar de las precauciones adoptadas, ocurran. El coste de la internalización se logra solo si el importe de los daños causados por las actividades del agente que participa en tales actividades se atribuyen al mismo, de modo que el precio de la actividad en cuestión refleja sus costes totales», es decir el coste auténtico, real. Wagner, Gerhard, «Robot, Inc.: Personhood for Autonomous Systems?», Fordham Law Review, *cit.*, pág. 600.

[52] Lassalle Ruiz, José María, «Inteligencia artificial, sabiduría humana y justicia», *El notario del siglo XXI*, enero/febrero 2024 nº 113, p. 16.

conciencia alguna, por lo que ni es consciente de su identidad ni puede aspirar a nada parecido.

Somos los seres humanos quienes sufrimos un fenómeno de empatía con los robots, especialmente los androides, cegados como estamos por su comportamiento inteligente. Esta inteligencia artificial crea en los humanos que interactúan con los robots un espejismo de humanidad que les impide tratarlos como máquinas. El reconocimiento de una cierta subjetividad de los robots vendrá impuesta por razones de conveniencia, como sucedió con las personas jurídicas, y por nuestra propia ética, no por la inexistente humanidad de las máquinas

2. La responsabilidad por daños de la IA.

Volviendo a la responsabilidad por daños causados por un sistema de IA o un robot, Francisca Ramón Fernández[53] opina que son tres las posiciones que se pueden adoptar frente a este problema:

a) La teoría de la inmunidad selectiva a los fabricantes. Se trata de no frenar los desarrollos en IA fijando la falta de responsabilidad de los desarrolladores por los daños imprevisibles, que entrarían en el ámbito de lo fortuito como riesgo de desarrollo.

b) Teoría de la personalidad jurídica que hace al sistema inteligente responsable directo de los daños a terceros. Requiere de la denominada personalidad electrónica, y la creación de un registro para la identificación de los robots, junto con un fondo de responsabilidad para hacer frente a las indemnizaciones. Una derivación es conceder a robots y sistemas inteligentes una subjetividad propia, pero delegando la responsabilidad en el usuario o propietario del robot, de forma análoga al caso de los daños de personas por quienes se debe responder (menores o empleados), o a los daños causados por los animales, derivando la responsabilidad al propietario.

c) Teoría del incremento de la responsabilidad del propietario del robot. Se parte de la idea de la dificultad de la prueba de la negligencia del propietario, o del defecto del producto y el nexo de causalidad, por la complejidad de estas máquinas. Sería una responsabilidad objetiva del propietario, con un límite máximo de resarcimiento. Otra posibilidad es continuar con el esquema de responsabilidad cuasiobjetiva pero permitiendo la prueba del caso fortuito o de la causación del daño por el propio perjudicado.

La personalidad electrónica, que como hemos visto era un modelo para solucionar la cuestión de los daños causados por sistemas inteligentes y robots,

---

[53] Ramón Fernández, Francisca, «Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?», Diario La Ley, Nº 9365, Sección Doctrina, 25 de Febrero de 2019, Editorial Wolters Kluwer, p. 3/13.

aparecía en la citada Resolución de 2017. Pero posteriores textos europeo han propuesto otras soluciones, como el Informe *Liability for Artificial Intelligence and other Emerging Digital Technologies*[54], que rechaza atribuir personalidad jurídica a los sistemas de IA:

> «Aun así, los expertos creen que actualmente no hay necesidad de dar una personalidad jurídica a las tecnologías digitales emergentes. El daño causado por tecnologías totalmente autónomas es generalmente reducible a los riesgos atribuibles a las personas físicas o categorías existentes de personas jurídicas, y cuando esto no sea el caso, una nueva regulación dirigiendo la responsabilidad hacia los individuos es una mejor respuesta que crear una nueva categoría de persona jurídica».

En mi opinión, la responsabilidad será del utilizador del sistema, porque esta inteligencia por un lado produce beneficios (robots asistenciales, sistemas de contratación *on line*, robots en cadenas de montaje…) y por otro puede causar daños. Parece extraño que el utilizador o propietario del robot obtenga los beneficios de su uso, y no responda de los eventuales daños. La solución debe ser la misma, aplicando el principio *ubi emolumentum, ibi onus*, debe ser el utilizador de la máquina quien responda también de los daños causados por ésta.

Esta idea de trasladar la responsabilidad de la máquina a la persona física o jurídica que está utilizando la máquina es mucho más productiva. La intervención del ser humano (o de la persona jurídica) y su consiguiente responsabilidad se aprecia muy bien en el ámbito de las intervenciones quirúrgicas robotizadas, en las que estima Monterroso Casado[55] que, si es el cirujano el que tiene el control del robot y puede supervisar y corregir su tarea si es necesario, la imputación de la responsabilidad en el caso de daños debe hacerse al mismo, si se aprecia culpa en su actuación; si el fallo es de gestión o diagnóstico, al Hospital o a la Compañía de servicios médicos, en el caso de que dicha actuación humana sea impecable pero el fallo provenga de una gestión defectuosa de la intervención (aquí por considerar que hay una responsabilidad por hecho ajeno similar a la del empresario del art. 1903 Cc.). Si la monitorización de los mecanismos y actualización del software del robot lo lleva a cabo la compañía fabricante o la de programación, o una de servicios, serán los ingenieros y la empresa los responsables si el daño proviene de la mala puesta a punto del robot. Nos dice la autora:

> «El criterio del control como criterio de imputación de la responsabilidad tiene sentido cuando los humanos tienen el control sobre los sistemas automatizados, pueden actualizar, modificar e introducir mejoras en esta tecnología o, por lo

---

[54] *Liability for Artificial Intelligence and other Emerging Digital Technologies*, pág. 38. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.group

[55] Monterroso Casado, Esther, «Responsabilidad civil por daños causados por robots en el ámbito sanitario», en *Inteligencia Artificial y Riesgos Cibernéticos. Responsabilidades y Aseguramiento*, Directora Esther Monterrosso Casado, Coordinador Alberto Muñoz Vilarreal, Tirant lo Blanch, Valencia, 2019, pág. 133.

> menos, pueden desactivarlos si lo consideran preciso conforme a nuestro juicio humano».

Pero añade que esto no es aplicable cuando el ser humano pierde el control sobre la máquina, y en especial el poder de detenerla.

Para solucionar la difícil cuestión de la atribución o el reparto de responsabilidad cuando existan varias personas susceptibles de responder del daño, la autora recurre al habitual sistema de exigir un aseguramiento obligatorio. También Ramón Fernández[56] insiste en este punto, pidiendo un régimen de seguro obligatorio «similar a los vehículos, pero cubriendo todas las responsabilidades potenciales y no sólo las actuaciones humanas y los fallos mecánicos. Complemento con un fondo para garantizar la reparación de los daños en los casos de ausencia de cobertura del seguro».

La relevancia del sujeto utilizador de la máquina, y la falta de protagonismo de ésta, que llega a perder incluso cualquier indicio de subjetividad, se pone de relieve desde el punto de vista penal, en relación al ciberdelito. De hecho, en el ámbito penal, Romeo Casabona[57] considera que los robots son meros instrumentos, y que el delito le es imputable al humano que utiliza el robot para cometerlo o, si el robot es autónomo, no actúa para evitarlo.

Establecida por tanto la imputación de responsabilidad a la persona que maneja o utiliza el sistema inteligente, hay que pasar a determinar qué tipo de responsabilidad sea ésta. Al respecto es fundamental la *Resolución 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*, propone el establecimiento de un régimen de responsabilidad civil, objetiva y subjetiva según los casos, para que pueda ser reclamado cualquier daño causado por la IA. También se ha ocupado de la responsabilidad civil el nuevo Reglamento de IA de 2024 (o Ley de la IA), como normativa horizontal, la *Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial*, COM(2022) 496 final 2022/0303 (COD), de 28 de septiembre 2022, y la también de 28 de septiembre de 2022 *Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos*, COM(2022) 495 final, 2022/0302 (COD).

La primera de estas Propuestas, frente a la opacidad y dificultades de prueba derivadas de los sistemas inteligentes, propugna que la IA es fiable cuando las normas garanticen …*que las víctimas de daños causados por la IA obtengan una protección equivalente a la de las víctimas de daños causados por los*

---

[56] Ramón Fernández, Francisca, «Robótica, inteligencia artificial y seguridad…», *cit.*, p. 5/13.

[57] Romeo Casabona, «La discusión sobre la atribución de responsabilidad penal a sistemas de inteligencia artificial…», *cit., p*p. 67-69.

demás productos. Rubí Puig[58] estima que esta Directiva no se inclina por un concreto sistema de responsabilidad, ya guiado por la culpa, ya objetivo, sino que deja libertad a los Estados miembros para optar por uno o por otro. Ortiz Fernández[59] insiste en esta idea y añade que la Directiva es un mero complemento a las legislaciones nacionales, aligerando la carga probatoria para el demandante mediante el establecimiento de una serie de presunciones, pero, como se ha dicho, sin establecer un tipo de responsabilidad concreta. En concreto, nos señala Pacheco Cañete[60], esta Directiva persigue establecer reglas europeas uniformes para facilitar el acceso a la información necesaria, que facilite al perjudicado la prueba de los presupuestos de la responsabilidad, en particular la culpa y el nexo causal: «De este modo prevé en su articulado la exhibición de pruebas y presunción refutable de incumplimiento (art. 3) y contempla presunciones *iuris tantum* con vistas a facilitar la prueba del nexo causal y también una presunción refutable de relación de causalidad en el caso de culpa (art. 4[61])». Destaca Ortiz Fernández[62] que estas facilidades para reclamar se introducen para paliar los problemas de prueba que plantea el funcionamiento de la IA como caso de «caja negra» o *blackbox*, que puede, como dice el texto europeo, *dificultar o hacer excesivamente costoso para las víctimas determinar cuál es la persona responsable y probar que se cumplen los requisitos para una demanda de responsabilidad civil.*

La Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos pretende dejar

---

[58] Rubí Puig, Antoni, «Capítulo 6. Responsabildiad civil e Inteligencia Artificial. Un examen crítico de la Propuesta de Directiva de 28 de septiembre de 2022», *Perspectivas regulatorias de la Inteligencia Artificial en la Unión Europea*, Reus Editorial, Madrid, 2023, pp. 245 y ss.

[59] Ortiz Fernández, Manuel, «La "adaptación" del Derecho de daños a la inteligencia artificial: La propuesta de Directiva sobre responsabilidad», *Revista de Internet, Derecho y Política*, nº 40 (marzo 2024), págs. 1-12. P. 5.

[60] Pacheco Cañete, Matilde. «Reflexiones sobre la responsabilidad civil del empresario por los daños causados por sistemas de IA», *Revista General de Legislación y Jurisprudencia*, 2023, número 2: páginas 283-319, p. 298.

[61] Artículo 4. Presunción refutable de relación de causalidad en caso de culpa. *1.Sin perjuicio de los requisitos establecidos en el presente artículo, los órganos jurisdiccionales nacionales presumirán, a efectos de la aplicación de las normas de responsabilidad a demandas por daños y perjuicios, el nexo causal entre la culpa del demandado y los resultados producidos por el sistema de IA o la no producción de resultados por parte del sistema de IA, siempre y cuando se cumplan todas las condiciones siguientes: a) que el demandante haya demostrado o el órgano jurisdiccional haya supuesto, de conformidad con el artículo 3, apartado 5, la culpa del demandado o de una persona de cuyo comportamiento sea responsable el demandado, consistente en el incumplimiento de un deber de diligencia establecido por el Derecho de la Unión o nacional destinado directamente a proteger frente a los daños que se hayan producido; b) que pueda considerarse razonablemente probable, basándose en las circunstancias del caso, que la culpa ha influido en los resultados producidos por el sistema de IA o en la no producción de resultados por parte del sistema de IA; c)que el demandante haya demostrado que la información de salida producida por el sistema de IA o la no producción de una información de salida por parte del sistema de IA causó los daños…*

[62] Ortiz Fernández, «La "adaptación" del derecho de daños a la inteligencia artificial: la propuesta de Directiva sobre responsabilidad», *cit.*, p. 7.

sentado, nos dice Coca Payeras[63], que los sistemas de IA y los bienes basados en la IA son «productos», y que por lo tanto entran en el ámbito de aplicación de la Directiva; asimismo, que tanto los fabricantes de equipos informáticos como los proveedores de programas informáticos y de servicios digitales que influyan en el funcionamiento del producto (como un servicio de navegación en un vehículo autónomo) pueden ser considerados responsables. Su aplicación, nos dice Ortiz Fernández[64], es preferente cuando estemos ante un consumidor, dejando la aplicación de la Propuesta sobre responsabilidad extracontractual para los casos en los que el dañado no tenga la condición de consumidor o usuario o no estemos ante daños encuadrables en la noción de producto defectuoso o derivados de éste.

Señala Pacheco Cañete[65] que aunque en la actualidad no sea necesario probar la culpa, sí que hay que probar la existencia del defecto, lo que, dado el carácter eminentemente técnico y la poca transparencia que presenta a veces el comportamiento automático de los sistemas, esto puede ser mucho más complejo que la prueba de la falta de diligencia del productor. Pero, por otra parte, tenemos los daños causados no por el mal funcionamiento del sistema, sino los que se derivan de un correcto funcionamiento, pero que no fueron tenidos en cuenta. Los daños más importantes que puede causar la IA no se producirán porque funcione mal, sino al contrario, porque funciona demasiado bien.

Como ejemplo de esto tenemos la diferenciación recogida en el art. 5 de la llamada Ley de Inteligencia Artificial (LIA, en realidad la Propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas en materia de IA, de 2021) entre las técnicas de inteligencia artificial prohibidos y las que «solamente» son de alto riesgo. Entre los prohibidos se cuentan las técnicas de persuasión y alteración subliminal de comportamientos (como los *nudges*), las de perfilado de sujetos y su calificación social (como el sistema de crédito social chino, o los sistemas de control de fronteras iBorder ctrl[66] o AVATAR, que ya se han visto). También los sistemas de identificación biométrica remota «en tiempo real», como el también mencionado sistema

---

[63] Coca Payeras, Miguel, «Las iniciativas de la Unión europea sobre inteligencia artificial: de la persona electrónica, al difícil equilibrio entre la necesidad de impulsarla y evitar sus riesgos», *Revista de Derecho Civil*, vol. X, núm. 2, especial (junio, 2023), p. 24. En http://nreg.es/ojs/index.php/RDC, p. 37.

[64] Ortiz Fernández, «La "adaptación" del derecho de daños a la inteligencia artificial: la propuesta de Directiva sobre responsabilidad», *cit.*, p. 6.

[65] Pacheco Cañete, «Reflexiones sobre la responsabilidad civil del empresario por los daños …», *cit.*, p. 299.

[66] De hecho, reacciona en contra de este sistema el Informe de 13 de julio de 2021 de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (A9-0232/2021), que insta a la Comisión para que deje de financiar investigaciones, aplicaciones o programas biométricos que puedan concluir probablemente en una vigilancia masiva e indiscriminada en espacios públicos.

policial SARI (italiano) o el sistema inglés AFR (*Automated Facial Recognition*). Tras éstos la Ley de la IA refiere una serie de sistemas que son calificados como de alto riesgo: sistemas para la gestión de la sanidad, funcionamiento del tráfico rodado y el suministro de agua, gas, calefacción y electricidad, sistemas de selección para el acceso a instituciones educativas y acceso al empleo, etc.

Comparando estos dos tipos de sistemas, vemos que los prohibidos lo son porque su mismo funcionamiento causa daños en derechos fundamentales de las personas, derechos a la intimidad, a la libertad de información y a la libre formación y manifestación de opinión, etc. Y este daño a los derechos se produce, precisamente, porque la perfección del sistema va más allá de la falibilidad e imperfección humanas. En cambio, los sistemas de alto riesgo causan daños cuando su funcionamiento no es todo lo perfecto que debe ser, sobre todo en ámbitos especialmente sensibles como el de la sanidad y medicina, la justicia, el tráfico y las comunicaciones, o los suministros básicos para la vida humana.

VI. INCIDENCIA DE LA IA EN EL ÁMBITO LABORAL Y MERCANTIL

En Derecho laboral, se ha planteado la utilización de datos biométricos para finalidades tan justificadas como "fichar" en el puesto de trabajo. Sin embargo no hay que olvidar que estamos ante datos personales muy sensibles que requieren consentimiento expreso, y así aporta Barona Vilar[67], el caso decidido por la Sentencia del Juzgado de lo Social n 2 de Alicante 190/2023, de 15 de septiembre (REC 489/2023), que declaró la vulneración del derecho a la intimidad personal y familiar y a la propia imagen del trabajador por la utilización de su información biométrica sin su consentimiento para el fichaje de entrada y salida, condenando a la empresa a una indemnización moral de más de seis mil euros. El trabajador solo había autorizado a la empresa el uso de sus derechos de imagen para publicaciones en páginas web y redes sociales, propiedad de la empresa, campañas, revistas, publicaciones, folletos, publicidad corporativa y demás materiales de apoyo, pertinentes para la difusión y promoción de la actividad de la empresa, pero no había autorizado que la empresa realizara una fotografía de la cara de los empleados desde un dispositivo de "entrada" y que esa imagen fuera usada para fichar la entrada y la salida en el puesto de trabajo; de hecho, el trabajador manifiesta que ni siquiera fue informado del uso de los datos biométricos.

Sin embargo, la cuestión candente es la cotización o no de los robots industriales como trabajadores, al objeto de subvenir la crisis de empleo que puedan causar estas máquinas inteligentes. Dado que gran parte de las cotizaciones

---

[67] Barona Vilar, «Tecnología biométrica y datos biométricos. Bondades y peligros…», *cit.*, p. 326.

sociales se aportan directamente por vía de Presupuestos, otra solución es la creación de impuestos especiales que recauden finalistamente cantidades para subvenir las necesidades de nuestro esquema Ponzi de Seguridad social. En tal caso, el interesado será el Derecho financiero y tributario, como señala la doctrina en este punto.

En Derecho mercantil: En la vida mercantil tenemos el campo de los nuevos «contratos inteligentes», que combinan la IA con una tecnología de cifrado denominada Tecnología de Registros Distribuídos (DLT —*Distributed Ledger Technology,* su modalidad más conocida es la de *Blockchain*). Esta tecnología permite la detección de la realización del intercambio y la comprobación de los sujetos intervinientes, de manera que se puede comprobar tanto el cumplimiento como el incumplimiento, llevando éste último a la automática resolución del contrato.

Además, la tecnología DLT puede utilizarse para la creación de archivos digitales que incorporen bienes valiosos y den fe de su titularidad, archivos que se denominan tokens. Nos dice Robert Guillén[68] que un *token* se define como «una unidad de valor interno» que se maneja con un determinado sistema de tecnología *blockchain*, consistiendo en un conjunto de datos encriptados en un archivo que se gestiona con un sistema de Tecnología de Registros Distribuidos mediante el cual los datos están almacenados en distintos servidores y además interconectados. Este archivo contiene una representación digital «…de un activo (es decir, de cualquier información, bien o derecho, de la que se admita su representación digital y vinculación a un *token*) con una identificación única». Para Ruiz-Gallardón[69], el token es «un activo o derecho representado digitalmente, que existe en la medida en que forma parte de una base de datos de la que resulta su titularidad y que se diferencia de un activo digital "tradicional" en el hecho de que base de datos donde desarrolla su existencia es gestionada utilizando tecnología *blockchain*».

Señala Pacheco Jiménez[70] que en España la Comisión Nacional del Mercado de Valores (CNMV) lleva desde 2018 analizando este tipo de emisiones, con especial atención hacia aspectos tan importantes como la prevención del blanqueo de capitales, la protección de datos o la fiscalidad aplicable. Por esto la CNMV considera tanto a las criptomonedas como a los tokens emitidos al lanzar una ICO (*Initial Coin Offerings*) como «valores negociables incardinables en el meritado artículo 2.1 del TRLMV (Texto Refundido de la Ley de Mercado de

---

[68] Robert guillén, Santiago, "Cesión de facultades de explotación en el entorno *blockchain* y su automatización mediante contratos inteligentes", en *Nuevos desafíos para el Derecho de autor. Robótica, Inteligencia artificial, Tecnología*, Susana Navas Navarro, Dir, Editorial Reus, Madrid, 2019, pág. 155.

[69] Ruiz-Gallardón y García de la Rasilla, Miguel, "Tokenización de activos y *blockchain*aspectos jurídicos", *Anales de la Academia Matritense del Notariado*, Tomo 60, 2020, pág. 272.

[70] Pacheco Jiménez, María Nieves, "De la tecnología *blockchain* a la economía del token", *Revista de la Facultad de Derecho de la Universidad de Castilla-La Mancha,* N° 83, 2019, diciembre-mayo, pág. 79. DOI: https://doi.org/10.18800/derechopucp.201902.003.

Valores), debiendo someterse a requisitos tales como la elaboración de un folleto informativo, el mantenimiento de un registro contable y la consecuente asunción de responsabilidades». Mientras que Palá Laguna[71] precisa que los tokens son «representaciones digitales de valor o derechos que pueden transferirse y almacenarse electrónicamente mediante la tecnología de registro descentralizado u otra tecnología similar», definición que toma del art. 3 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos (MiCA), de 19 de noviembre del 2021 [2020/0265 (COD)].

VII. INCIDENCIA DE LA IA EN LA VULNERACIÓN DE DERECHOS FUNDAMENTALES

Señala Barona Vilar[72] que en algunos países asiáticos se ha acometido un desarrollo tecnológico para favorecer este control a través del reconocimiento facial masivo. Es China es el principal banco de pruebas de esta tecnología, no solo para controlar criminales, sino para llevar a cabo una monitorización (laboral, en las escuelas, universidades, etc), para vigilar a minorías étnicas o para efectuar seguimiento de disidentes políticos:

> «En suma, se muestra como un cauce para implementar un sistema de vigilancia policial predictiva, una monitorización de los ciudadanos, de dónde van, con quién van, qué compran, con quién hablan, si hacen deporte, si viajan mucho, y un largo etcétera. Así, con la tecnología biométrica de identificación facial se permite realizar, como ha sucedido en China, una clasificación ciudadana que, allende la funcionalidad de seguridad ciudadana, convierte a las personas en un número, un color, se le cosifica, y todo ello con ineludibles consecuencias jurídicas».

Uno de los proyectos de clasificación fue el desplegado en la región china de Xinjang, en la ciudad de Tumxuk, donde los funcionarios han recogido sin consentimiento muestras de sangre de cientos de uigures como parte de una campaña de recolección masiva de ADN, siendo el objetivo de ello crear imágenes faciales exactas con la información de las muestras de ADN, una tecnología que podría emplearse contra la minoría uigur —son cerca de 11 millones de uigures los que viven en la citada región china y son una minoría predominantemente musulmana— así como respecto de opositores disidentes políticos. El desarrollo tecnológico se realiza en laboratorios dependientes del Ministerio de Sanidad chino con la intervención de dos científicos chinos del Ministerio financiados por la

---

[71] Palá Laguna, Reyes, «Los tokens del metaverso», Análisis GA_P (Gómez-Acebo & Pombo), marzo 2022, en https://www.ga-p.com/publicaciones/que-es-el-metaverso.

[72] Barona Vilar, «Tecnología biométrica y datos biométricos. Bondades y peligros…», *cit.*, pp. 315 y 323.

Max-Planck Society y la Erasmus University Medical Center de Holanda. Ha provocado campañas de represión gubernamental contra esta y otras minorías de la provincia, con detenciones masivas, con argumentos de lucha preventiva terrorista y del extremismo islámico. Con el sistema tecnológico chino se aúnan las bases de datos de ADN (la más grande del mundo, con más de 80 perfiles, según medios chinos), que podrían alimentar los sistemas de vigilancia masiva y reconocimiento facial simultáneamente, de manera que se mantendría un férreo control sobre la sociedad civil al permitir no solo rastrear a delincuentes, sino también a manifestantes o a disidentes, con el fin de garantizar las políticas de segregación.

Señala Barona Vilar varios ejemplos de tecnologías biométricas en China, como que se permite el uso de gafas con reconocimiento facial y ADN, piel, comportamiento de movilidad, etc., para identificar sospechosos de delitos, pero también para disidentes, descontentos o personas contrarias al régimen. Pero sobre todo está el sistema de crédito social o *scoring*, que es un instrumento que utiliza el *big data* para calificar el comportamiento de los usuarios o para detectar en las escuelas el absentismo escolar[73]. Según nos cuenta Lizzy Rettinger[74], la idea del «crédito social» se adecúa perfectamente al carácter chino, por reproducir la idea de la confianza social predicada por Confucio.

Como señalan Roberts, Cowls, Morley y otros[75], esta tecnología del *scoring* viene a ser sancionada por el *Plan de Desarrollo de la Inteligencia Artificial de la Nueva Generación,* aprobado por el supremo órgano del gobierno chino, el Consejo estatal. Este plan tiene tres ámbitos de proyección: Desafío internacional, Desarrollo económico y Gobernabilidad o «Construcción» social, siendo este último el que más nos interesa. El Sistema de Crédito Social todavía no se ha implantado a nivel nacional, pero como nos dicen los citados autores, los ambiciosos objetivos del mismo «…ofrecen un convincente ejemplo de la intención del gobierno de confiar en la tecnología digital, no sólo para gobernanza social, sino también para una regulación más detallada del comportamiento»[76]. Añade Rettinger[77] que en 2018, cuarenta gobiernos municipales y provinciales establecieron planes piloto de

---

[73] Añade la autora otros ejemplos como los siguientes: «en Shangai se habla de incorporar en los autobuses un sistema de reconocimiento facial que detecte la fatiga de los conductores (en algunos automóviles de tecnología avanzada ya existe en Europa). O,en los baños públicos del Cielo de Pekín, se usa una máquina que escanea el rostro del usuario, le dispensa de un trozo de papel higiénico de 60 centímetros de longitud y no le permite volver a usar más hasta que han pasado nueve minutos». Barona Vilar, «Tecnología biométrica y datos biométricos. Bondades y peligros…», *cit.,* p. 323.

[74] Rettinger, Lizzy, «The Human Rights Implications of China's Social Credit System», *Journal of High Technology Law*, vol. XXI, nº 1, (2021), pp. 1-33, p. 3.

[75] Roberts, Huw, Cowls, Josh, Morley, Jessica et al., «The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation». *AI & Society* 36, 59-77 (2021). https://doi.org/10.1007/s00146-020-00992-2.

[76] Roberts, Cowls, Morley et al., «The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation», *cit.* p. 66.

[77] Rettinger, «The Human Rights Implications of China's Social Credit System», *cit.*, p. 6.

sistemas de crédito social, y que la situación actual muestra un sistema fragmentado en tres ámbitos: «sistema de listas negras» a nivel nacional, sistemas de crédito social en determinados municipios, y sistemas de crédito social a efectos financieros pilotados por instituciones financieras. Consecuencias de estar en una lista negra pueden ser: —no se puede viajar en avión, o en buenos trenes, —no se pueden contratar algunos destinos turísticos, o ciertos hoteles, o —no se puede inscribir a los hijos en los mejores colegios, dificultades para arrendar un piso o conseguir un crédito, y —su identidad se publica en mupis y plataformas de crédito social. Pero, sobre todo, se produce un aislamiento social del individuo puesto que el contacto con individuos de baja puntuación repercute en la puntuación de quien interactúa con ellos.

En definitiva, se trata del control de los comportamientos sociales, cuya implantación es un proyecto perfectamente establecido, como se deduce del documento «Esquema para el establecimiento de un sistema de crédito social» del Consejo estatal para la implantación del sistema, publicado en 2014. Este documento subrayó que el Sistema de Crédito Social no solo tenía como objetivo regular las finanzas y acciones corporativas de empresas y ciudadanos, sino el comportamiento social de los individuos, persiguiendo conductas como evasión fiscal, alarmas sobre la seguridad alimentaria y deshonestidad académica, mediante el sistema de «listas negras». Pero a ello hay que añadir otros datos, como que la ciudad de Fuzhou enriquece el currículo social de sus ciudadanos con una cifra que expresa su empleabilidad, según datos de desempeño y constancia en el trabajo; a lo que hay que sumar el desarrollo de ciudades inteligentes, con tecnologías de vigilancia basadas en el reconocimiento facial y seguimiento de teléfonos móviles para rastrear a quienes el gobierno presenta como potenciales disidentes o terroristas, sobre todo de la etnia uigur.

VIII. BIBLIOGRAFÍA

Barona Vilar, Silvia, «Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale», Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, pp. 298-331. p. 305.

Chen Zijiao, Qing Jiaxin y Zhouy Juan Helen, «CinematicMindscapes: High-quality Video Reconstruction from Brain Activity», preprint en arXiv:2305.11675, https://doi.org/10.48550/arXiv.2305.11675 [Submitted on 19 May 2023].

Coca Payeras, Miguel, (2023), «Las iniciativas de la Unión europea sobre inteligencia artificial: de la persona electrónica, al difícil equilibrio entre la necesidad de impulsarla y evitar sus riesgos», *Revista de Derecho Civil*, vol. X, núm. 2, especial (junio, 2023). En http://nreg.es/ojs/index.php/RDC.

Coeckelbergh, Mark, AI Ethics, The MIT Press essential knowledge series, Cambridge, 2020, p. 127.

Cotino Hueso, Lorenzo, «El uso jurisdiccional de la inteligencia artificial: habilitación legal, garantías necesarias y la supervisión por el CGPJ», Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, pp. 494-527.

Cotino Hueso, Lorenzo, «Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal», El Cronista del Estado Social y Democrático de Derecho, N.º 100 (Septiembre-Octubre), 2022 (Ejemplar dedicado a: Inteligencia artificial y derecho).

De Asís Pulido, Miguel, «La Justicia predictiva: tres posibles usos en la práctica jurídica», Inteligencia Artificial y Filosofía del Derecho, Director Fernando H. Llano Alonso, Coord. Joaquín Garrido Martín, Ramón Valdivia Jiménez, Ediciones Laborum, S.L., Murcia, 2022, pp. 285-312.

Dolz Lago, Manuel— Jesús, «Una aproximación jurídica a la Inteligencia Artificial», Diario La Ley, Nº 10096, Sección Doctrina, 23 de Junio de 2022, Wolters Kluwer, LA LEY 6033/2022.

Ebers, Martin, «El futuro marco jurídico europeo de la inteligencia artificial», *Persona y derecho civil, los retos del siglo XXI: (persona, género, transgénero, inteligencia artificial y animales sensibles)* / coord. por José Luis Argudo Périz, María del Carmen Bayod López (dir.), 2023, págs. 185-216.

European Commission: Directorate-General for Justice and Consumers, Study on the use of innovative technologies in the justice field — Final report, Publications Office, 2020, https://data.europa.eu/doi/10.2838/585101

Galindo Ayuda, F. (2024). «Algorithms, Sociology of Law and Justice». *Journal of Digital Technologies and Law,* 2(1), 34-45. https://doi.org/10.21202/jdtl.2024.3.

González Tapia, Mª Isabel, «Protección penal de los neuroderechos: el uso directo de las neurotecnologías sobre el ser humano», *Inteligencia Artificial y Filosofía del Derecho*, Ediciones Laborum, Murcia, 2022, p. 328.

Lassalle Ruiz, José María, «Inteligencia artificial, sabiduría humana y justicia», El notario del siglo XXI, enero/febrero 2024 nº 113.

Lemley, Mark A. y Casey, Bryan, «Remedies for Robots», 86 *University of Chicago Law Review* (2019), Stanford Law and Economics Olin Working Paper No. 523, última revisió abril 2020, DOI: http://dx.doi.org/10.2139/ssrn.3223621.

López Riba, José María, «Inteligencia artificial y control policial. Cuestiones para un debate frente al hype», *InDret*, 2.2024, pp. 407-436. DOI: 10.31009/InDret.2024.i2.10.

Magdalena Layos, Luis, «¿Por qué debería confiar en ti (máquina)?», *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0,* coord. María José Cruz Blanca, Ignacio Lledó Benito; Francisco Lledó Yagüe (dir.), Ignacio F. Benítez Ortúzar (dir.), Óscar Monje Balmaseda (dir.), Dykinson, 2021.

Marchena Gómez, Manuel, «Inteligencia Artificial y Jurisdicción Penal», Ponencia para su ingreso en la Real Academia de Doctores de España, 26 octubre 2022, https://confilegal.com/wp-content/uploads/2023/03/INTELIGENCIA-ARTIFICIAL-INGRESO-MARCHENA-REAL-ACADEMIA-DE-DOCTORES—.pdf

Monterroso Casado, Esther, «Responsabilidad civil por daños causados por robots en el ámbito sanitario», en Inteligencia Artificial y Riesgos Cibernéticos. Responsabilidades y Aseguramiento, Directora Esther Monterrosso Casado, Coordinador Alberto Muñoz Vilarreal, Tirant lo Blanch, Valencia, 2019.

Ortega Matesanz, Alfonso, "Aritmética Jurídica e Inteligencia Artificial: sobre la Calculadora 988", *Revista de Estudios Jurídicos y Criminológicos*, n.º 9, Universidad de Cádiz, 2024, pp. 141-204, DOI: https://doi.org/10.25267/REJUCRIM.2024.i9.05

Ortiz Fernández, Manuel, «La "adaptación" del Derecho de daños a la inteligencia artificial: La propuesta de Directiva sobre responsabilidad», *Revista de Internet, Derecho y Política*, nº 40 (marzo 2024), págs. 1-12.

Pacheco Cañete, Matilde. «Reflexiones sobre la responsabilidad civil del empresario por los daños causados por sistemas de IA», *Revista General de Legislación y Jurisprudencia*, 2023, número 2: páginas 283-319.

Pacheco Jiménez, María Nieves, "De la tecnología blockchain a la economía del token", *Revista de la Facultad de Derecho de la Universidad de Castilla-La Mancha*, N° 83, 2019, diciembre-mayo. DOI: https://doi.org/10.18800/derechopucp.201902.003.

Palá Laguna, Reyes, «Los tokens del metaverso», *Análisis GA_P (Gómez-Acebo & Pombo)*, marzo 2022, en https://www.ga-p.com/publicaciones/que-es-el-metaverso.

Ramón Fernández, Francisca, «Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?», *Diario La Ley*, Nº 9365, Sección Doctrina, 25 de Febrero de 2019, Editorial Wolters Kluwer.

Rettinger, Lizzy, «The Human Rights Implications of China's Social Credit System», *Journal of High Technology Law*, vol. XXI, nº 1, (2021), pp. 1-33.

Robert Guillén, Santiago, "Cesión de facultades de explotación en el entorno blockchain y su automatización mediante contratos inteligentes", en *Nuevos desafíos para el Derecho de autor. Robótica, Inteligencia artificial, Tecnología*, Susana Navas Navarro, Dir, Editorial Reus, Madrid, 2019.

Roberts, Huw, Cowls, Josh, Morley, Jessica et al., «The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation». *AI & Society* 36, 59-77 (2021). https://doi.org/10.1007/s00146-020-00992-2.

Romeo Casabona, Carlos María, «La discusión sobre la atribución de responsabilidad penal a sistemas de inteligencia artificial, en particular a sistemas autónomos», *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial*, Vol. II: IA y responsabilidad penal, Editorial Comares, Granada, 2023, pp. 57-81.

Romeo Casabona, Carlos, «El Ciberespacio como lugar virtual y legal de comisión del delito. Necesidad de nuevas respuestas jurídicas», *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial*, Vol. I: Ciberseguridad y ciberdelitos, Editorial Comares, Granada, 2023, pp. 3-21.

Romeo Casabona, Carlos, «Inteligencia artificial, predictividad y justicia penal», *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial*, Vol. II: IA y responsabilidad penal, Editorial Comares, Granada, 2023, pp. 119-139.

Rubí Puig, Antoni, «Capítulo 6. Responsabildiad civil e Inteligencia Artificial. Un examen crítico de la Propuesta de Directiva de 28 de septiembre de 2022», *Perspectivas regulatorias de la Inteligencia Artificial en la Unión Europea*, Reus Editorial, Madrid, 2023.

Ruiz-Gallardón y García de la Rasilla, Miguel, "Tokenización de activos y blockchainaspectos jurídicos", *Anales de la Academia Matritense del Notariado*, Tomo 60, 2020.

Urruela Mora, Asier, «Instrumentos de evaluación del riesgo de violencia, justicia algorítmica y Derecho penal. Perspectiva crítica», *Estudios político-criminales, jurídico-penales y criminológicos: libro homenaje al profesor José Luis Díez Ripollés*, coord. por Noelia Corral Maraver, Deborah García Magna, Fátima Pérez Jiménez, Bertha Prado, Pablo Rando Casermeiro; Juan Muñoz Sánchez (dir.), Octavio García Pérez (dir.), Ana Isabel Cerezo Domínguez (dir.), Elisa García España (dir.), 2023, págs. 1877-1888.

Wagner, Gerhard, «Robot, Inc.: Personhood for Autonomous Systems?», *88 Fordham L. Rev. 591 (2019)*. Available at: https://ir.lawnet.fordham.edu/flr/vol88/iss2/8.