EL USO JURISDICCIONAL DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL Y LA NECESIDAD DE SU ARMONIZACIÓN EN EL CONTEXTO DE LA UNIÓN EUROPEA [1]

Por

MONTSERRAT DE HOYOS SANCHO
Catedrática de Derecho Procesal
Ex - Directora del Instituto de Estudios Europeos
Universidad de Valladolid

montserrat.dehoyos@uva.es

Revista General de Derecho Procesal 55 (2021)

RESUMEN: Se exponen en este trabajo diversas utilidades de los sistemas de Inteligencia Artificial, como ayuda a la investigación y enjuiciamiento de hechos delictivos. La repercusión que el uso policial y jurisdiccional de estas herramientas puede tener sobre la efectividad de la cooperación transfronteriza en el contexto de la Unión Europea es ya hoy relevante, e irá creciendo de forma progresiva. Por tanto, es preciso contar con una normativa europea que armonice sus condiciones de uso, principalmente en relación con los sistemas denominados "de alto riesgo". Se analiza el contenido de la propuesta de Reglamento del Parlamento europeo y del Consejo para establecer reglas armonizadas en materia de Inteligencia Artificial, de abril 2021, en particular en relación con esos sistemas que pueden emplearse como apoyo a la función policial y jurisdiccional, destacando las que han de ser sus principales garantías y requisitos de uso.

PALABRAS CLAVE: Inteligencia artificial, proceso penal, uso policial y jurisdiccional sistemas IA, cooperación transfronteriza Unión Europea, armonización de garantías.

---

[1] Este trabajo se enmarca en los siguientes Proyectos y Grupos de Investigación: Ministerio de Ciencia e Innovación: "*Proceso penal y Unión Europea: análisis y propuestas*", PID2020-116848GB-100; Generalitat Valenciana: "*Claves de la justicia civil y penal en la sociedad del miedo*" -Prometeo 2018/2011-; Grupo de Investigación Reconocido, Universidad de Valladolid: "*Garantías procesales y Unión Europea*"; FEDER-Junta de Andalucía: "*El uso de las TICs en la cooperación jurídica penal internacional: construyendo la sociedad digital andaluza del futuro*" -P18-RT-1059, y "*Derechos y garantías de las personas vulnerables en el Estado del Bienestar*" -UMA18-JA175-. Además, ha sido merecedor de una de las "Ayudas Extraordinarias a la Investigación", concedida por la Fundación Privada Manuel Serra Domínguez en su edición de 2021.

THE JURISDICTIONAL USE OF ARTIFICIAL INTELLIGENCE SYSTEMS AND THE NEED FOR THEIR HARMONISATION IN THE CONTEXT OF THE EUROPEAN UNION

ABSTRACT: This paper presents various uses of Artificial Intelligence systems as an aid to the investigation and prosecution of criminal offences. The impact that the police and jurisdictional use of these tools can have on the effectiveness of cross-border cooperation in the context of the European Union is already relevant today, and will grow progressively. It is therefore necessary to adopt European legislation harmonising their conditions of use, particularly regarding the so-called "high-risk" systems. The contents of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence of April 2021 are analysed, specifically with regard to those systems that can be used to support the police and jurisdictional function, highlighting what should be their main safeguards and use requirements.

KEYWORDS: Artificial Intelligence, criminal proceedings, police and jurisdictional use of AI systems, EU cross-border cooperation, safeguards harmonisation.

I. EL USO JURISDICCIONAL DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

Partiendo de una definición general de lo que es un Sistema de Inteligencia Artificial -Sistema IA, en lo sucesivo-, esto es, *"programas informáticos -y posiblemente también equipos informáticos- diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información, fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado"*[2], podemos pasar a identificar cuáles son sus principales componentes.

En primer lugar, los datos; o mejor dicho, un gran número de datos, que por su dimensión ya se conocen como *Big data*[3]. En segundo término, los algoritmos; esto es, una secuencia finita de reglas formales -operaciones lógicas e instrucciones- que permiten obtener un resultado -*output*- a partir de un *input* inicial de información[4]. Tales resultados u objetivos pretendidos, determinados previamente por un humano, serán

[2] Esta es la definición contenida en el *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, elaborado por la Comisión Europea y publicado con fecha 19 de febrero 2020. Trae su origen en la definición previamente elaborada por el "Grupo de expertos de alto nivel" de la Comisión Europea, con base en la *Comunicación sobre la inteligencia artificial para Europa,* redactada por la propia Comisión. COM (2018) 237 final.

[3] Debemos distinguir este concepto de *Big data* de lo que se denomina *Data mining* o "minería de datos"; esta última implica, no solo la recolección de un gran número de datos, sino que además permite extraer la información que es más relevante dentro de ese enorme conjunto de datos, mediante técnicas estadísticas y de IA, arrojando resultados específicos concretos, útiles para el usuario del sistema, ya que además permiten crear modelos predictivos o clasificar segmentando.

[4] Definición que puede leerse en la *Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno*", aprobada por la *Comisión europea para la eficacia de la justicia* -CEPEJ- con fecha de 4 de diciembre de 2018.

predicciones, recomendaciones o decisiones, que podrán influir sobre el contexto físico o digital en el que estos sistemas IA actúan. En tercer lugar, debe mencionarse también como parte esencial el *hardware*, es decir, los distintos equipos informáticos que soportan los referidos sistemas.

El uso de los sistemas IA como apoyo a la función jurisdiccional, concretamente en el ámbito de la investigación y enjuiciamiento de los hechos delictivos, al que nos referiremos en este trabajo, es ya una realidad en nuestros días.

Seguramente muchos habrán oído hablar de los "algoritmos de análisis predictivo*"* -*risk assessments tools*-[5]. Estas herramientas se basan en la utilización de un gran número de datos, de carácter personal y de otros tipos, los cuales, convenientemente procesados a través de algoritmos *ad hoc*, proporcionan unos resultados que pueden servir para predecir o vaticinar el posible comportamiento futuro de una persona en distintos contextos. Así, pueden ayudar a determinar un peligro de reincidencia delictiva o de revictimización, el grado de riesgo de incumplimiento de obligaciones procesales, de las condiciones que pudieran imponerse con carácter cautelar en una causa[6], o en la fase de ejecución de sentencias[7], entre otras utilidades[8].

La gran mayoría de los trabajos recientes sobre la materia, cuando abordan esta concreta cuestión de los algoritmos predictivos -o justicia predictiva-, hacen referencia al trascendente asunto *Eric Loomis*, y a la correlativa sentencia dictada en 2016 por la Corte de Wisconsin[9]. Este es un claro ejemplo de aplicación práctica por los tribunales

---

[5] Entre los trabajos más recientes puede destacarse: McKAY, C.: "Predicting risk in criminal procedure: actuarial tools, algorithms, AI and judicial decisión-making", *Current Issues in Criminal Justice,* 32:1, 2020, pp. 22 a 39.

[6] Véase PLANCHADELL GARGALLO, A.: "Inteligencia artificial y medidas cautelares", en la obra colectiva *Justicia algorítmica y neuroderecho,* Ed.: S. Barona Vilar, Valencia, 2021, pp. 389 y ss.

[7] También en los procesos penales que se dirigen contra menores de edad, vid. específicamente PILLADO GONZÁLEZ, E.: "Algoritmos predictivos del comportamiento y proceso penal de menores", en la obra colectiva *Justicia algorítmica y neuroderecho,* Ed.: S. Barona Vilar, Valencia, 2021, pp. 421 y ss.

[8] Que aborda BARONA VILAR en "Una Justicia 'digital' y 'algorítmica' para una sociedad en estado de mudanza", en *Justicia algorítmica y neuroderecho, op. cit.,* pp. 21 y ss., y de la misma autora, *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Valencia, 2021. Vid. también ARMENTA DEU, T.: *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambios*, Madrid, 2021.

[9] Pueden consultarse al respecto: DE MIGUEL BERIAIN, I.: "Does the use of risk assessments in sentences respect the right to due process? A critical analysis of the Wisconsin v. Loomis ruling", *Law, Probability and Risk,* Vol. 17, núm. 1, marzo 2018, pp. 45 a 53; MALDONATO, L.: "Algoritmi predittivi e discrezionalitá del giuidice: una nuova sfida per la giustizia penale", *Diritto Penale Contemporaneo*, 2/2019, pp. 391 y ss., pp. 401 y ss.; OCCHIUZZI, B.: "Algoritmi predittivi: alcune premesse metodologiche", *Diritto Penale Contemporaneo*, 2/2019, pp. 391 y ss., GIALUZ, M.: "Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei *Risk Assessment Tools* tra Stati Uniti ed Europa", *Diritto Penale Contemporaneo*, 29 mayo 2019, pp. 1 y ss., esp. pp. 6 y ss.; SIGNORATO, S.: "Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo", en *Rivista di Diritto Processuale*, 2/2020, pp. 605 y ss., esp. pp. 611 y ss.;

norteamericanos de tal tipo de herramientas IA[10] que se utilizan para predecir comportamientos futuros[11]. Además de servir para poner de manifiesto sus principales utilidades, el caso *Loomis* ha resultado también valioso para evidenciar los riesgos que conlleva una utilización de los resultados de la aplicación de tales algoritmos de pronóstico sin las garantías suficientes, en particular en el orden jurisdiccional penal.

El asunto *Loomis* puso enseguida sobre el tapete una serie de problemas generales que plantea la utilización de este tipo de algoritmos: la imposibilidad de conocer de qué concretos datos se nutre el sistema, de saber cómo funciona precisamente el algoritmo aplicado, en qué medida pondera éste los diversos parámetros de referencia, dónde y porqué se ha colocado el umbral de riesgo bajo/medio/alto en un determinado punto de corte -*cut off*-, o si se respetan los principios de igualdad y no discriminación. Además, el hecho de que ese *software* esté protegido por el secreto comercial de la empresa que lo crea -y que lo vende para su uso por la Administración- hace que sea opaco para los operadores jurídicos, una *black box* que realiza un cálculo y ofrece un concreto resultado numérico, una puntuación que determina el contenido de una sentencia, la adopción de una medida cautelar, o la concesión de un permiso penitenciario, pero cuyo funcionamiento y banco de datos de los que se nutre no pueden ser conocidos, ni por el tribunal, ni por la defensa del investigado/acusado.

BURCHARD, Ch.: "L'intelligenza artificiale come fine del Diritto penale? Sulla trasformazione algorítmica della societá", *Riv.it.dir.proc.pen.,* vol. 62, núm. 4, 2019, pp. 1909 a 1942, pp. 1924 y ss.; PEREZ ESTRADA, M.J.: "El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías", en *Claves de la Justicia Penal,* S. Barona (Dir.), Valencia, 2019, pp. 235 y ss.

[10] Concretamente se utilizó el del algoritmo predictivo contenido en el *software* conocido como COMPAS -*Correctional Offender Management Profilling for Alternative Sanction*-, que fue concebido para poder determinar el grado de peligrosidad de una determinada persona, el riesgo de su reincidencia delictiva, y se utiliza en algunos Estados de EE.UU. para ayudar a los jueces en la determinación de la pena, considerando una serie de datos personales y factores sociales que, según entienden los expertos que han participado en la configuración del programa, son determinantes del grado de probabilidad de que el sujeto vuelva a delinquir. Entre otros extremos, se preguntará al detenido: cuántos de sus amigos han sido arrestados alguna vez, cuántas veces se ha mudado de casa en el último año, con qué frecuencia apenas tiene dinero, o se siente aburrido. En el siguiente enlace puede consultarse el propio cuestionario -137 preguntas- que utiliza COMPAS y que se le entrega al sospechoso en el momento de la detención: https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE

[11] Como puede suponerse, el empleo de herramientas de evaluación del riesgo no se limita al ámbito estadounidense; también pueden referirse experiencias de este tipo en Europa. Seguramente la más relevante sea la inglesa. Desde el año 2017 la policía de Durham, en colaboración con la Universidad de Cambridge, ha puesto en marcha un sistema denominado con el acrónimo *HART -Harm Assessment Risk Tool*-, una herramienta de análisis predictivo utilizada destacadamente para decidir sobre la *diversion*, esto es, acerca la posible aplicación de un programa de rehabilitación a un detenido, como alternativa al ejercicio de la acción penal. Vid. más ampliamente GIALUZ, M.: "Quando la giustizia penale…", *op. cit.* pp. 10 y ss.

A pesar de la aparente neutralidad y objetividad de este tipo de algoritmos predictivos[12], se puede concluir que la utilización de herramientas similares a las empleadas en el referido asunto *Loomis* vulnera el derecho de defensa, la igualdad de partes y la necesaria transparencia en los sistemas utilizados en la adopción de decisiones judiciales; por mucho que, como indicara la Corte Suprema de Wisconsin, no pueda ser el único elemento en que se fundamente la sentencia condenatoria[13].

Si nos colocamos ahora en el concreto ámbito de la Unión Europea, deberíamos además tener en cuenta en nuestras valoraciones que, si se pretende la utilización de *risk assessment tools* en los procesos penales, sería de aplicación la Directiva (UE) 2016/680[14], la cual, específicamente en su art. 11, apdo. 1 [15], establece que: "Los

[12] De imprescindible consulta a este respecto, en particular acerca de los conceptos de imparcialidad, exactitud, equidad y paridad estadística del algoritmo, el trabajo monográfico de KEARNS, M. / ROTH, A.: *El algoritmo ético. La ciencia del diseño de algoritmos socialmente responsables,* Madrid, 2020, esp. pp. 101 y ss.. Sobre la "aparente neutralidad" de la IA, vid. también UBERTIS, G.: "Intelligenza artificiale, giustizia penale, controllo umano significativo", en *Sistema penale*, texto presentado en Milán el 15 octubre 2020, accesible en http://www.ristretti.it/commenti/2020/novembre/pdf3/articolo_ubertis.pdf; vid. esp. pp. 2 y ss.

[13] Interesante la consulta del documento publicado por el *Pretrial Justice Institute* de Baltimore -EE.UU-, titulado "Updated Position on Pretrial Risk Assessment Tools", con fecha de 7 de febrero de 2020, en el que la citada institución concluye que "We now see that pretrial risk assessment tools, designed to predict an individual's appearance in court without a new arrest, can no longer be a part of our solution for building equitable pretrial justice systems. Regardless of their science, brand, or age, these tools are derived from data reflecting structural racism and institutional inequity that impact our court and law enforcement policies and practices. Use of that data then deepens the inequity". (…) "We have consistently opposed the use of pretrial risk assessment tools to make *detention* decisions. We now expand that to oppose their use to determine restrictions placed on a person's pretrial liberty (reporting visits, electronic monitoring, curfews, drug testing, etc.)." Puede leerse el manifiesto completo en:

https://www.pretrial.org/wp-content/uploads/Risk-Statement-PJI-2020.pdf

[14] Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Vid. art.1, párr.1: "La presente Directiva establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública". Por cierto, con fecha de 25 de febrero 2021 el TJUE dictó sentencia imponiendo a España multas históricas -una de 15 millones de euros y otra de 89.000 euros diarios-, en aplicación del art. 260 TFUE, por la no transposición en tiempo y forma de esta Directiva 2016/680, que tenía que haber sido incorporada a nuestro ordenamiento con el límite del 6 de mayo de 2018. El 9 de febrero de 2021 el Consejo de Ministros de España aprobó el Proyecto de L.O. de Protección de Datos personales a estos fines citados en la Directiva, declarando "urgente" su tramitación. Finalmente, con fecha 26 de mayo de 2021, se publicó la L.O. 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

[15] Véase el análisis de este precepto que realiza GUZMÁN FLUJA en su trabajo "Proceso penal y justicia automatizada", *Revista General de Derecho Procesal*, núm. 53, 2021, pp. 1 y ss. esp. pp. 23 y ss. Insiste el autor en que tal "intervención humana" en la toma de las decisiones ha de ser de carácter "material", y no meramente formal; es decir, no bastaría con "validar acríticamente el resultado o la decisión que proviene del tratamiento automatizado".

Estados miembros dispondrán la *prohibición de las decisiones basadas únicamente en un tratamiento automatizado*, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, salvo que estén autorizadas por el Derecho de la Unión o del Estado miembro a la que esté sujeto el responsable del tratamiento y que establezca medidas adecuadas para salvaguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento[16]". Además, si estuviera en juego la libertad personal del sujeto imputado, debería considerarse lo previsto en los arts. 5 CEDH y 6 CDFUE: el interesado tiene en todo caso derecho a que sobre su *status* se pronuncie un juez en persona, quien deberá valorar también otros elementos probatorios, más allá del *output* resultante del *risk assessment tool.*

Por tanto, aunque excepcionalmente el derecho de la Unión y/o de los Estados miembros estableciera la posibilidad de delegar en un *software* o sistema IA la adopción de una decisión en este ámbito, siempre debería ser posible recurrir la decisión ante un juez/tribunal persona física[17].

De otro lado, los sistemas IA pueden constituir también una fuente de prueba y, eventualmente, ser aportados al proceso como medios de prueba. Estamos pensando en las posibilidades que, para formar la convicción del juzgador, ofrecen herramientas tan dispares como las que se engloban bajo los conceptos de domótica, de asistencia a la conducción, los sistemas de compra *online* vinculados a la información que recogen los *smart phones*, los relojes inteligentes con sensores biológicos que registran multitud de datos personales, prevén y sugieren pautas de conducta o, más en general, el llamado "internet de las cosas".

Todos estos y otros muchos dispositivos "inteligentes" recogen y procesan abundantísima información sobre un gran número de individuos, y también sobre el usuario concreto del sistema, lo que les permite construir perfiles, segmentando por comportamientos y finalmente por individuos, de tal manera que, después de hacer un seguimiento acerca de cómo cada uno de ellos interactúa con esos dispositivos, es capaz de determinar, y por tanto de predecir, pautas de conducta o necesidades de una persona concreta. Por ejemplo, sobre cuestiones tan diversas como las siguientes: a qué hora está en casa los días laborables -porque lo advierte el geolocalizador de sus

[16] Muy interesante en este punto el Informe publicado por *Fair Trials* en noviembre 2020, *Regulating AI for Use in Criminal Justice Systems in the EU*, en el que se llama la atención sobre la posible amplitud de las excepciones a la prohibición de decisiones automatizadas, pues basta con que lo autorice el Derecho de la Unión o de un Estado miembro. No queda claro con qué salvaguardas esto sería posible, ni qué ha de entenderse por "intervención humana". Vid. pp. 1-6 y cc. del referido Informe. https://www.fairtrials.org.

[17] En este sentido, con referencia a esta insustituible función del "*giudice in carne*" vid. GIALUZ, M.: "Quando la giustizia penale incontra…", *op. supra cit*., p. 18.

dispositivos móviles y además porque se produce un cambio en la temperatura del interior del domicilio, que detecta el sistema de domótica-; qué días tiene comensales invitados -su frigorífico "inteligente" está mucho más lleno de lo habitual-; el asistente a la conducción de su vehículo conoce los trayectos habituales para ir de casa al trabajo y también aquellos en los que el tráfico es más fluido -si por algún motivo decide desviarse de éstos, lo advertirá inmediatamente, y le sugerirá el nuevo camino de vuelta a casa-; su reloj "inteligente" conoce con precisión sus principales constantes vitales en las distintas horas del día, por lo que detectará cualquier cambio en las mismas -v.gr.: presión sanguínea y pulso extraordinariamente altos en una franja horaria que nunca se dedica a la actividad física, o nivel de ruido muy elevado en un momento que habitualmente no es de vigilia-.

En definitiva, es de suponer a la vista de estos y otros muchísimos ejemplos que ya son realidad actualmente, que estos sistemas IA pueden proporcionar información muy valiosa para una investigación y, en su caso, llegar a acceder como medio de prueba al enjuiciamiento penal, si bien no dejan de ser datos que resultan automáticamente de la aplicación de algoritmos que gobiernan el *software* de todos y cada uno de esos sistemas.

Como bien destaca la doctrina que se ha ocupado recientemente del tema[18], la captación y el tratamiento de datos personales generados automáticamente, la utilización en el proceso penal de estos elementos cognoscitivos de gran impacto, plantea problemas de envergadura equivalente a su creciente importancia práctica, como lo es, entre otros[19], el hecho de que la "eficiencia tecnológica" acabe siendo un criterio autosuficiente sobre la fiabilidad de la prueba[20], reemplazando así el juicio humano y

[18] Vid. entre otros los trabajos de S. QUATTROCOLO: "Equitá del processo penale e *automated evidence* alla luce della Convenzione europea dei diritti dell'uomo", *Revista ítalo-española de Derecho Procesal,* vol. 2, 2109, pp. 1 y ss., y *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, Springer, 2020, así como el compendio de Derecho comparado: CAIANIELLO, M. / CAMON, A. (Eds.): *Digital Forensic Evidence. Towards common European Standards in Antifraud Administrative and Criminal Investigations.),* Milano, 2021, y la abundante literatura anglosajona de referencia que allí se cita. Véase en particular el trabajo que, en relación con la prueba digital en España, firma BACHMAIER, L.: "The Handling of Digital Evidence in Spain", en *Digital Forensic Evidence. Towards common European Standards…, op. cit.,* pp. 165 y ss.

[19] QUATTROCOLO analiza toda esta problemática desde la perspectiva convencional del art. 8 CEDH, precepto inspirado en el concepto ya clásico de *privacy* -derecho a la vida familiar y privada-, que como es sabido puede ceder puntualmente y de manera proporcionada en pro de otros derechos fundamentales, como son la seguridad nacional o la prevención y represión del delito, siempre que haya previsión normativa y se considere "necesario en una sociedad democrática". Vid. más ampliamente: "Equitá del processo…", *op. cit.*, pp. 5 y ss.

[20] A pesar de que la aplicación de los algoritmos que se utilizan en los sistemas IA puede conducir a resultados erróneos, y no tanto por incompetencia o malicia humana, o por un sesgo en los datos de que se nutre, sino porque en ocasiones el "aprendizaje automático", que de alguna manera se escapa del control del creador del sistema, puede derivar en conclusiones erróneas, ni

dejando prácticamente sin efecto la presunción de inocencia. Además, también la igualdad de armas entre las partes puede verse afectada por el uso procesal de datos que han sido generados y tratados automáticamente, a través de algoritmos más o menos complejos, creados o no específicamente para ser empleados en el marco de un proceso penal.

Concretamente en relación con la paridad de armas que ha de regir el proceso penal -acusación y defensa deben poder alegar y probar, conociendo previamente los elementos esenciales de la causa-, si no fuera posible acceder y conocer el "código fuente" del algoritmo que gobierna el sistema IA -generalmente protegido por el derecho de propiedad intelectual y creado para fines ajenos al enjuiciamiento penal-, sería casi imposible cuestionar o impugnar los resultados/datos que proporciona el sistema y que se podrían utilizar como prueba en una causa penal.

Se produciría así lo que en este punto QUATTROCOLO califica de "asimetría o desequilibrio cognoscitivo"[21], ya que generalmente una parte -la pública, el Ministerio Fiscal-, tendrá acceso a la tecnología más moderna y dispondrá de medios económicos que de forma habitual no estarán al alcance del particular investigado / acusado, quien por tanto no tendrá opciones reales de rebatir o impugnar los resultados que ofrezca la "prueba algorítmica". La inaccesibilidad del código fuente o la imposibilidad de conocer características esenciales del *software* protegido, impedirán a la defensa cuestionar la exactitud y fiabilidad de la prueba incriminatoria.

En definitiva, si no hay suficiente transparencia -acceso al código fuente, *inputs* y *outputs* del *software*- no podrá asegurarse la necesaria y suficiente paridad de armas entre acusación y defensa, el justo equilibrio procesal entre ambas posiciones[22]. Incluso suponiendo que se tuviera acceso a tal información, sería preciso además que las partes pudieran disponer de peritos en la materia que certificaran -o no- la fiabilidad del sistema IA y de sus resultados en ese concreto supuesto[23].

---

siquiera previsibles por los técnicos que lo configuraron. Vid. más ampliamente KEARNS, M. / ROTH, A.: *El algoritmo ético, op. cit.* esp. pp. 101 y ss. y p. 262; MITCHEL, J. y otros: "Machine learning for determining accurate outcomes in criminal trials", *Law, Probability and Risk*, núm. 19, 2020, pp. 43 y ss.

[21] Cuestión desarrollada con más detalle en "Equitá del processo…", *op. cit.*, p. 12, y *Artificial Intelligence…, op. cit.*, esp. pp. 73 y ss.

[22] También NIEVA FENOLL pone de relieve la importancia que la "desclasificación de los algoritmos" tiene como garantía del sistema y del derecho de defensa: no es posible elaborar una mínima estrategia de defensiva si no se puede conocer cómo decide "la máquina". Véase más ampliamente *Inteligencia artificial y proceso judicial*, Madrid, 2018, esp. pp. 139 y ss.

[23] Va todavía más allá QUATTROCOLO, pues advierte de que podría producirse una compleja y confusa "batalla entre expertos" -peritos que concluyen la fiabilidad del sistema IA, frente a otros que la niegan-, lo que obligaría al juez a erigirse en árbitro de una discusión sobre materias que toda probabilidad le resultan absolutamente ajenas e incomprensibles. Vid. "Equitá del processo…", *op. cit*., p. 16.

Por lo que respecta al uso de sistemas IA en la fase de valoración de los medios de prueba, entendemos que éstos no podrán reemplazar al juez-persona en esta tarea de valoración libre, conjunta y racional de toda la prueba lícita practicada en la causa[24], pues es éste -el juez o tribunal competente para el enjuiciamiento- el que en definitiva tiene que formar su convicción más allá de toda duda razonable. Si bien es claro que los actuales y futuros instrumentos de inteligencia artificial pueden ser de gran ayuda en esas tareas muchas veces muy complejas, no es menos cierto que tal función de valoración de *toda* la prueba practicada es estrictamente jurisdiccional, y por tanto indelegable[25].

En todo caso, ya los analistas de esta materia vienen haciendo referencia a las posibles utilidades de la IA en este punto[26]: ayuda a la determinación de la credibilidad que ha de otorgarse a las declaraciones de testigos o de las propias partes; ayuda al esclarecimiento de la posible autoría o de la voluntariedad del consentimiento reflejado en la redacción de un documento, con base en el lenguaje usado o en un estilo de escritura; ayuda en la valoración de un dictamen pericial, detectando fallos o incoherencias en el mismo; reconstrucción virtual de hechos delictivos complejos, etc. etc.

Especial mención requiere también la utilidad de los sistemas IA en los supuestos en que el acervo probatorio es extraordinariamente abundante. No es raro, por ejemplo, que en la investigación y prueba de la llamada "delincuencia económica" se tengan que revisar millones de documentos o *terabytes* de información. Así, para que las pesquisas puedan tener finalmente alguna utilidad y no se eternicen, será necesario que el análisis de la documentación se realice de forma selectiva, y que no se incurra en diligencias

---

[24] Siempre interesante la lectura de los trabajos de J. FERRER BELTRÁN; en este punto, en particular, *La valoración racional de la prueba,* Madrid, 2007, *passim.*

[25] Vid. art. 22 del citado Reglamento (UE) 2016/679 -RGPD-, y también la mencionada *Carta ética* del CEPEJ: toda persona tiene derecho a no estar sometida a una decisión que produzca efectos jurídicos o tenga consecuencias significativas sobre ella, fundada exclusivamente en un tratamiento automatizado de datos destinados a valorar ciertos aspectos de su personalidad. Reseñable también que en Italia, el Decreto legislativo de 18 de mayo de 2018, núm. 51, en su art. 8, haya establecido la prohibición expresa de decisiones basadas únicamente en un tratamiento automatizado, incluida la "*profilazione*/perfilado", que produzcan efectos negativos sobre el interesado, salvo que lo autorice el Derecho de la UE o específicas disposiciones legales, y siempre y cuando éstas establezcan garantías adecuadas para los derechos y las libertades del interesado. En todo caso, se garantiza el derecho de obtener la intervención humana por parte del titular de tratamiento. Vid. los comentarios de MALDONATO, L.: "Algoritmi predittivi e discrezionalitá…", *op. cit.,* pp. 401 y ss., esp. p. 403.

[26] Vid. con mucho más detalle las explicaciones de NIEVA FENOLL, J.: *Inteligencia artificial…, op. cit.,* pp. 79 y ss. Por su parte, BUENO DE MATA, F.: "Macrodatos, inteligencia artificial y proceso: luces y sombras", *Revista General de Derecho Procesal,* núm. 51, 2020, pp. 1 y ss., esp. pp. 22 y ss., se refiere al uso de los sistemas IA como una suerte de "prueba de indicios virtual", pues entiende el autor que se trataría de una prueba indirecta, al no recaer sobre los hechos constitutivos del delito. Más recientemente, ARMENTA DEU, T.: *Derivas de la Justicia. Tutela de los derechos y solución de controversias en tiempos de cambios,* Madrid, 2021.

abusivas en forma de *fishing expedition*. Como bien destaca en este punto DE SOUSA MENDES[27], esos instrumentos informáticos -v.gr.: *Data mining*-, que se utilizan desde hace tiempo en otros campos, son perfectamente aplicables también al ámbito jurídico, y deberían considerarse indispensables si se pretende llevar a cabo una investigación mínimamente eficiente en este contexto tan complejo.

No menos importante que el uso estrictamente jurisdiccional de los sistemas IA es el empleo siempre creciente de estas herramientas por las Fuerzas y Cuerpos de seguridad en sus tareas de prevención y persecución de la delincuencia más grave y, desde luego, de la ciberdelincuencia. Como es evidente, la utilización de esos sistemas IA por la policía también podrá repercutir sobre el eventual proceso penal ulterior.

Entre los usos actuales más relevantes, podemos mencionar a modo de ejemplo los siguientes[28]: los sistemas de identificación biométrica -sobre los que volveremos *infra*-; los que permiten la elaboración de patrones con fines predictivos o para la investigación de ciertos delitos, como los que se cometen a través de la *Darknet -v.gr.* el intercambio de pornografía infantil-, o la violencia sexual y de género[29], los incendios forestales, o el *online child grooming,* entre otros muchos; los sistemas que ayudan a la determinación de zonas de patrullaje preferente -y que posibilitan una mejor utilización de los recursos personales y materiales disponibles-; los que permiten detectar denuncias falsas -v.gr.: *VeriPol*[30]-; los que sirven para determinar el riesgo de revictimización -v.gr.: *VioGen*[31]-; los que detectan posibles procesos de captación y radicalización de internos, principalmente musulmanes, en los Centros penitenciarios; o las herramientas que pueden indicar el tipo de desenlace más probable en los supuestos de desaparición de personas, los cuales, al mismo tiempo, ayudar a dirigir la búsqueda policial en un sentido u otro.

---

[27] En su trabajo "A representaçao do conhecimento jurídico, inteligencia artificial e os sistemas de apoio à decisao jurídica", en *Inteligência Artificial & Direito*, Coimbra, 2020, pp. 51 y ss., esp. pp. 60 y 61.

[28] Vid. más ampliamente el trabajo de GONZÁLEZ ÁLVAREZ y otros: "Policía predictiva en España. Aplicación y retos futuros", *Behavior & Law Journal*, 2020, vol. 6, núm. 1, pp. 26 y ss.

[29] Sobre el uso de la IA en la estrategia de lucha contra este tipo de delitos, véase LLORENTE SÁNCHEZ-ARJONA: "*Big data*, inteligencia artificial y violencia de género", *Diario La Ley*, núm. 49, 2021, pp. 1 y ss.

[30] NIEVA FENOLL, *Inteligencia artificial…, op. supra cit.*, p. 87, puso de relieve que ya la Policía española introdujo en 2017 el uso de esta aplicación de inteligencia artificial, conocida como "VeriPol", que sirve para detectar palabras reveladoras del posible engaño en denuncias por el robo de teléfonos móviles, con base en datos y análisis de estadísticas previas sobre denuncias falsas.

[31] El sistema *VioGen,* de seguimiento integral en los casos de violencia de género, puesto en marcha por la Secretaría de Estado de Seguridad del Mº del Interior ya en el año 2007. Sobre sus utilidades, vid. más ampliamente LLORENTE SÁNCHEZ-ARJONA, M.: "*Big data*, Inteligencia Artificial…", *op. cit*., esp. pp. 7 y ss.

En todo caso, si bien no es posible delegar en estos sistemas predictivos, o de ayuda a la investigación en general, las decisiones finales de carácter policial, tampoco puede despreciarse el valor de sus utilidades. Coinciden los expertos en la necesidad de extender el uso de la llamada "cultura analítica prospectiva", también en este campo. Su uso correcto facilita y agiliza la labor policial y, desde luego, puede incrementar la eficiencia de la estrategia en la prevención y lucha contra las formas delictivas más graves[32].

II.- LA NECESIDAD DE SU ARMONIZACIÓN EN EL CONTEXTO DEL ESPACIO DE LIBERTAD, SEGURIDAD Y JUSTICIA DE LA UNIÓN EUROPEA, A FIN DE PODER GARANTIZAR LA MÁXIMA EFICACIA DE LA COOPERACIÓN POLICIAL Y JUDICIAL TRANSFRONTERIZA

Todos estos sistemas IA a los que hemos hecho referencia, y otros muchos que seguro vendrán, podrán emplearse como *apoyo* a la función jurisdiccional, en la investigación y enjuiciamiento de hechos delictivos. Su utilidad es incuestionable, pero a nuestro juicio no deberían llegar a reemplazar la parte esencial de la tarea que realiza un juez o un tribunal; esto es, la toma de decisiones, ya sean de finalización de la causa -absolución / condena- o intermedias -v.gr.: sobre medidas cautelares, o las relativas a la obtención, admisión y valoración de pruebas-, o en fase de ejecución de condena -v.gr: pertinencia del traslado de presos, calificación en grados penitenciarios, concesión de permisos, etc.-. Todas estas resoluciones han de corresponder, en sentido estricto, al titular o titulares de los órganos jurisdiccionales respectivamente competentes. Además, no se vería satisfecho el requisito de jurisdiccionalidad, intrínseco a este tipo de decisiones, si el órgano competente se limitara a "validar" la propuesta o solución que en el supuesto concreto le pudiera ofrecer el sistema IA[33].

---

[32] Coincidimos en este punto con las conclusiones que alcanzan GONZÁLEZ ÁLVAREZ y otros, *op. supra cit.*, esp. p. 38.

[33] Ya destacó GASCÓN INCHAUSTI -vid. su trabajo "Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial", en *La justicia digital en España y en la Unión Europea,* J. Conde y G. Serrano (Dirs.), Barcelona, 2019, pp. 191 y ss., p. 204- que, debido a la dificultad intrínseca de la toma de decisiones en ciertos escenarios complejos, es comprensible la tendencia humana a tratar de delegar esas decisiones o parte de ellas en un tercero -perito- o bien en una "máquina", que gozaría de una cierta "apariencia de mejor condición", al menos por su apariencia de mayor objetividad, lo que puede conducir a que esos sistemas tengan una repercusión sobre el sentido de la decisión que, si bien no puede decirse que sea "automático", sería desde luego muy determinante. Afirmaba también GASCÓN, *op. supra cit*. p. 205, que en tales casos se produciría un claro peligro para la efectividad del derecho de defensa, e incluso el riesgo de cierta inversión de la carga probatoria, pues no será sencillo cuestionar en un caso concreto el fundamento científico, metodológico o empírico del sistema de inteligencia artificial y la fiabilidad de sus resultados. Insiste igualmente GIALUZ en que el juez deberá evitar lo que se denomina "*automation complacency*" o "*automation bias*", es decir, la tendencia humana a ignorar o a no buscar información adicional que pueda contradecir la solución generada por el

Es destacable también la repercusión que el uso policial y jurisdiccional de estas herramientas puede tener en la efectividad de la cooperación transfronteriza en el contexto normativo y geográfico del "espacio de libertad, seguridad y justicia" de la Unión Europea. Como es sabido, ésta se fundamenta en el reconocimiento mutuo de resoluciones judiciales, y su funcionamiento fluido depende en gran medida de la confianza mutua entre las autoridades implicadas en la cooperación, así como del grado de aproximación previa que exista entre las legislaciones estatales[34].

Podemos hacer referencia a varios supuestos que resultarían ilustrativos de cómo puede afectar la falta de esa suficiente armonización previa en la regulación del uso de sistemas IA, a la eficacia de tal cooperación transfronteriza en el contexto de la Unión Europea.

Así, por ejemplo, podría repercutir negativamente sobre la utilización en un Estado UE de pruebas obtenidas en otro/s Estados miembros haciendo uso de sistemas IA, a través de una orden europea de investigación[35] o de la futura orden europea de entrega y conservación de pruebas electrónicas[36]; o sobre la concesión o denegación de la solicitud de traslado de personas condenadas, cuando la determinación judicial de las

---

ordenador, que es aceptada como "la correcta"; vid. "Quando la giustizia penale incontra…", *op. cit.,* pp. 19 y ss. Vid. también UBERTIS, G.: "Intelligenza artificiale…", *op. cit.*, p. 12, y las advertencias que el autor realiza sobre el riesgo del "mito tecnológico" de la IA, que podría inducir al juez a no desmarcarse del resultado ofrecido por la máquina.

[34] Desde la perspectiva procesal, véase ARANGÜENA / DE HOYOS / RODRÍGUEZ-MEDEL (Dirs.): *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Cizur Menor, 2015.

ARANGÜENA / DE HOYOS (Dirs.): *Garantías procesales de investigados y acusados. Situación actual en el ámbito de la Unión Europea,* Valencia, 2018; ARANGÜENA / DE HOYOS / HERNÁNDEZ: *Procedural Safeguards for Suspects and Accused Persons in Criminal Proceedings,* Springer, 2020, y DE HOYOS SANCHO, M.: "El principio de subsidiariedad y la autonomía procesal de los Estados de la Unión Europea", *Revista Jueces para la Democracia*, núm. 96, 2019, pp. 36 y ss.

[35] Sobre el instrumento, véase el compendio titulado *Orden europea de investigación y prueba transfronteriza en la Unión Europea,* Dir.: I. GONZÁLEZ CANO, Valencia, 2019, y en particular los trabajos que, en relación con la admisión de la prueba transfronteriza, firman respectivamente en dicha obra, ARMENTA DEU, T., y LARO GONZÁLEZ, M.E., pp. 767 y ss. Vid. también, DE HOYOS SANCHO, M.: "Orden europea de investigación: avanzando hacia la integración en materia procesal penal", en *Claves de la Justicia Penal*, Ed.: S. Barona Vilar, Valencia, 2019, pp. 343 y ss. Más recientemente, LLORENTE SÁNCHEZ-ARJONA, M.: *La Orden Europea de Investigación y su incorporación al Derecho español,* Valencia, 2020; ARANGÜENA FANEGO, C.: "Orden europea de investigación: régimen de sustitución de la medida solicitada", *InDret,* núm. 2, 2021; DE HOYOS SANCHO, M.: "Algunas dificultades en la aplicación práctica de la Orden Europea de Investigación", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Dir. V. Moreno Catena, Valencia, 2021, pp. 511 y ss.

[36] Actualmente en fase de Propuesta de Reglamento del Parlamento europeo y del Consejo sobre órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, de 17 de abril de 2018, COM (2018) 225 final. Vid. los trabajos de FUENTES SORIANO, O.: "Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación de pruebas electrónicas", en *Era digital, sociedad y derecho,* Dir.: O. Fuentes Soriano, Valencia, 2020, pp. 281 y ss., y de LARO GONZÁLEZ, E.: "El Reglamento E-evidence: instrumento adicional a la Orden europea de investigación", *La Ley Probática*, núm. 3, enero-marzo 2021.

posibilidades de reinserción social se pueda fundamentar precisamente en el resultado de un sistema IA -reconocimiento mutuo de sentencias que condenan a penas privativas de libertad[37]-; o sobre la posible sustitución de la prisión provisional por otra medida cautelar menos gravosa para el investigado / acusado[38], cuando la determinación judicial del riesgo de fuga o de reiteración delictiva se basó en la previsión ofrecida por un sistema IA; o sobre la eficacia transfronteriza de una orden europea de protección de víctimas[39], en los casos en que la previsión del riesgo de revictimización se hubiera basado en el resultado ofrecido por un sistema IA. Incluso tal falta de armonización en el uso de sistemas IA podría incidir en la apreciación del motivo de "vulneración de derechos fundamentales" en el Estado requirente, que podría invocarse como causa de denegación del reconocimiento y ejecución, entre otros instrumentos, de una orden europea de detención y entrega[40].

Además de su posible repercusión sobre la eficacia de la cooperación transfronteriza en materia penal, los instrumentos IA que pueden emplearse en la prevención, investigación y enjuiciamiento de hechos delictivos se califican generalmente como "sistemas de alto riesgo", pues pueden afectar derechos fundamentales de los ciudadanos, como la intimidad, la protección de datos personales, o la no discriminación, e incluso podrían llegar a verse erosionadas las garantías del debido proceso, o la esencia de la tutela judicial efectiva[41], entre otros.

Será preciso por tanto contar, no tardando, con una regulación nacional lo más detallada posible sobre su posible uso policial y jurisdiccional; pero no bastará sólo con

---

[37] Vid. Decisión Marco 2008/909, del Consejo, de 27 de noviembre de 2008, y la transposición en España en el Título III de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, arts. 63 y ss. Más ampliamente, DE HOYOS SANCHO, M.: "El reconocimiento mutuo de resoluciones por la que se impone una pena o medida privativa de libertad", en *Reconocimiento mutuo de resoluciones penales…, op. cit.* pp. 107 y ss.

[38] Sobre este instrumento, ARANGÜENA FANEGO, C.: "Reconocimiento mutuo de resoluciones sobre medidas alternativas a la prisión provisional", en *Reconocimiento mutuo de resoluciones penales…, op. cit.*, pp. 207 y ss.

[39] Vid. Directiva 2011/99/UE y Reglamento UE 606/2013, respectivamente sobre reconocimiento de órdenes de protección dictadas en procesos penales y en materia civil, así como el Título VI de la citada Ley de reconocimiento mutuo de resoluciones penales, arts. 130 y ss. Un estudio de dicho instrumento puede encontrarse en DE HOYOS SANCHO, M.: "La orden europea de protección de víctimas: análisis normativo", en *Reconocimiento mutuo de resoluciones penales…, op. cit.*, pp. 271 y ss.

[40] Vid. art. 3 de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea. Acerca del instrumento, vid. JIMENO BULNES, M.: "La orden de detención europea como instrumento procesal en la lucha contra el terrorismo", *Unión Europea Aranzadi,* núm. 12, 2020.

[41] Así lo destaca MARTÍN DIZ en "Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva *versus* decisoria", en *Justicia algorítmica y neuroderecho,* op. cit, pp. 65 y ss., esp. pp. 75 y ss., y también QUATTROCOLO, S.: *Artificial Intelligence…, op.cit.,* esp. pp. 73 y ss.

esa normativa interna sobre la materia estableciendo las condiciones de su uso en cada Estado y garantizando los derechos de los respectivos ciudadanos.

La delincuencia organizada más grave y, desde luego, prácticamente todo el cibercrimen, es de carácter transfronterizo, por lo que será necesario, a fin de garantizar la operatividad del reconocimiento mutuo de resoluciones penales en que se basa la cooperación judicial y policial en el contexto UE, que exista previamente una mínima, pero suficiente armonización del uso jurisdiccional y policial de los sistemas IA, destacadamente de esos que se califican de "alto riesgo" por poder afectar derechos y libertades fundamentales.

Veremos a continuación en qué términos se está intentando esa armonización o aproximación de las legislaciones nacionales en el referido contexto del "espacio de libertad, seguridad y justicia" de la Unión Europea.

III. LA ARMONIZACIÓN CONTENIDA EN LA PROPUESTA DE REGLAMENTO SOBRE INTELIGENCIA ARTIFICIAL. VALORACIÓN Y CONCLUSIONES

Tras numerosos estudios de grupos de especialistas, de trabajos previos en el contexto del Consejo de Europa, y también en el marco de las propias instituciones de la Unión Europea -entre los más recientes, la *Carta Ética europea sobre el uso de IA en los sistemas judiciales y su entorno* de 2018[42], *Directrices éticas para una IA fiable* de abril 2019[43], o el *Libro Blanco sobre IA* de febrero 2020[44]- se ha publicado, con fecha 21 de abril 2021, una Propuesta de Reglamento del Parlamento europeo y del Consejo para establecer reglas armonizadas en materia de IA[45].

Según puede leerse en la "Exposición de motivos" de esta Propuesta de Reglamento -Apdo. 2.4: *Choice of the instrument*-, se opta por este instrumento normativo -el Reglamento- porque es necesaria una aplicación uniforme de las nuevas reglas, así como de la definición de IA, la prohibición de ciertas prácticas potencialmente peligrosas y la clasificación de sistemas IA en función del riesgo. La aplicación directa del Reglamento reduce la fragmentación normativa, asegura la libre circulación de bienes y

[42] Aprobada por la *Comisión europea para la eficacia de la justicia* -CEPEJ- con fecha de 4 de diciembre de 2018.

[43] Documento elaborado un Grupo independiente de expertos de alto nivel sobre IA, por encargo de la Comisión Europea.

[44] Un estudio de este instrumento prenormativo puede encontrarse en DE HOYOS SANCHO, M.: "El Libro Blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como sector de riesgo", *Revista Española de Derecho Europeo,* núm. 26, 2020, pp. 9 y ss.

[45] *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts* {SEC (2021) 167 final} - {SWD (2021) 84 final} - {SWD(2021) 85 final}.

servicios en el mercado interior, y facilita el desarrollo de un mercado único para sistemas IA, que deberán ser legales, seguros y fiables. De otro lado, también expresamente se indica -Apdo. 2.1: *Legal basis*- que la base normativa de esta Propuesta es, en primer término, el art. 114 TFUE, relativo a la adopción de medidas para garantizar el establecimiento y funcionamiento del Mercado Interior; concretamente en relación con la estrategia del Mercado Único digital en la UE. Además, teniendo en cuenta que esta propuesta de Reglamento contiene normas específicas sobre protección de las personas físicas en relación con el tratamiento de sus datos personales, también tiene por fundamento esta norma en lo dispuesto en el art. 16 TFUE, relativo precisamente a la protección de datos de carácter personal.

Debe llamarse la atención sobre el hecho de que ninguno de estos instrumentos aprobados o proyectados en el ámbito de la Unión Europea haga referencia a la importancia que la armonización del uso jurisdiccional y policial de los sistemas IA tiene y tendrá sobre la cooperación transfronteriza en el "espacio de libertad, seguridad y justicia". En todas las "Exposiciones de motivos" o "Considerandos" de esos textos se incluye una alusión directa a la importancia que esta materia tiene para del reforzamiento del Mercado Interior europeo, para la libre circulación de bienes y servicios, o para mejorar la competitividad de las empresas tecnológicas europeas en el mercado global. Nada se dice sobre la notoria la trascendencia que el empleo de sistemas IA puede llegar a tener también sobre el reconocimiento mutuo de resoluciones jurisdiccionales, que está en la base de la cooperación transfronteriza penal y también civil, aunque ésta es evidente, según hemos expuesto *supra.*

Por lo que respecta a la definición de "Sistema de Inteligencia Artificial", el art. 3 de la Propuesta de Reglamento indica que por tal se entenderá "el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el Anexo I y que puede, para un conjunto de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa".

Tal Anexo I se refiere a estrategias de aprendizaje automático a través de una amplia variedad de métodos, incluido el aprendizaje profundo[46], a estrategias basadas en la

[46] Los algoritmos pueden configurarse para seguir aprendiendo mientras se utilizan y a medida que se van nutriendo de nuevos datos, de tal forma que los sistemas IA identifican patrones no predeterminados y general nuevas relaciones entre esos patrones y los nuevos datos, de forma que pueden seguir haciendo sucesivas predicciones o recomendaciones, en principio no previstas específicamente en la programación inicial del algoritmo. Sobre el llamado "aprendizaje automático" -*Machine learning*- y las utilidades de las máquinas emuladoras de funciones cognitivas humanas, vid. las reflexiones de BARONA VILAR, S.: *Algoritmización del Derecho y de la Justicia…, op. cit.*, esp. pp. 95 y ss., y de MARTIN DIZ, F.: "Aplicaciones de inteligencia artificial en procesos penales por delitos relacionados con la corrupción", en *Corrupción: compliance, represión y recuperación de activos,* RODRÍGUEZ GARCÍA, N. y otros (Coords.), Valencia, 2019,

lógica y en el conocimiento, así como a estrategias estadísticas, métodos de búsqueda y optimización.

Esta definición contenida en la Propuesta de Reglamento y completada en el Anexo I, que desde luego es compleja[47], pretende abarcar todas las posibles técnicas y estrategias de IA que se conocen hasta hoy. Entendemos además que el legislador europeo ha tratado de que no quede obsoleta en poco tiempo, lo que desde luego no es tarea sencilla en este específico contexto tecnológico. En todo caso, más clara nos parecía la definición expuesta al inicio de este trabajo, esto es, la reflejada en el citado *Libro Blanco sobre la inteligencia artificial* publicado por la Comisión europea en 2020.

Nos detendremos a continuación en los que, a nuestro juicio, son los contenidos más relevantes de esta Propuesta de Reglamento sobre IA; concretamente en relación con los llamados "sistemas de alto riesgo" que pueden usarse en el contexto de la investigación y enjuiciamiento de hechos delictivos, y en sus correspondientes garantías.

En primer lugar, conviene destacar que el legislador UE ha optado por un marco normativo basado en la clasificación por "niveles de riesgo" de los sistemas IA sobre derechos de los ciudadanos y seguridad de los sistemas, que serían los siguientes: inaceptable, alto, limitado/bajo y mínimo[48].

Se consideran niveles de riesgo "inaceptables" -vid. art. 5: prácticas IA que deben estar prohibidas- los que conllevan aquellos sistemas IA que pueden causar daños físicos o psíquicos, manipular la voluntad y el comportamiento humano o, en general, los que suponen "*social scoring*" -puntuación o clasificación social de una persona por los respectivos gobiernos a partir de datos sobre su comportamiento o características personales, si bien se admiten ciertas excepciones, vid. art. 5.1.c)-.

---

pp. 533 y ss. Fuera de España, véase el trabajo de MITCHEL, J. y otros: "Machine learning for determining…", *op. cit.,* pp. 43 y ss.

[47] Como explica ORTEGA KLEIN, esta definición, que no es precisamente clara, refleja la complejidad de la materia a regular, la dificultad de sintetizar un concepto lo más neutro posible y que abarque todo lo que puede calificarse como IA, por lo que ha sido necesaria la remisión a un Anexo que, además, tendrá que ser objeto de continuas actualizaciones. Vid. "Hacia un régimen europeo de control de la Inteligencia Artificial", *Análisis del Real Instituto Elcano*, 6 de mayo 2021, pp. 1 y ss., esp. p. 3.

[48] Vid. apdo. 5.2.2. de la Exposición de motivos: los sistemas IA de riesgo bajo o limitado serían aquellos que simplemente conllevan obligaciones específicas de información o transparencia, como por ejemplo cuando se utilizan "robots conversacionales" -vid. Exposición de motivos, apdo. 1.1-, en cuyo caso los usuarios tendrían que poder saber que están interactuando con un sistema IA. Serían de riesgo mínimo o nulo la mayoría de las aplicaciones de uso común, como por ejemplo las que nos recomiendan una película o serie en nuestra plataforma de entretenimiento, o las que permiten discriminar emails como *spam*. Este tipo de cuestiones no son objeto de tratamiento en el Proyecto de Reglamento, precisamente por no presentar riesgos para el usuario, si bien se fomentará y facilitará la elaboración de "Códigos de Conducta" destinados a la aplicación voluntaria de los requisitos de garantía, también en esos ámbitos de bajo riesgo, vid. art. 69 de la Propuesta de Reglamento.

También se considera prohibido o generalmente inaceptable el uso de sistemas de identificación biométrica de personas[49] en tiempo real y en lugares accesibles al público, con la finalidad de hacer cumplir la ley -"*real time biometric systems in publicly accessible spaces for the purpose of law enforcement*" [50]-, a menos que -y en esos casos pasarían a ser sistemas permitidos, pero de "alto riesgo"- su uso sea estrictamente necesario para uno de estos objetivos que menciona la propia norma, vid. art. 5.1.d): búsqueda dirigida de víctimas, especialmente de niños desaparecidos; prevenir una amenaza específica, importante e inminente para la vida o la seguridad física de personas, o un ataque terrorista; o bien para la detección, localización, identificación y procesamiento de un autor o sospechoso de haber cometido un delito de los mencionados en el art. 2.2 Decisión Marco 2002/584/JHA[51], castigado al menos en el Estado miembro interesado con penas de tres años de privación de libertad, según la legislación del referido Estado.

Además, para que sea admisible el uso de estos sistemas de identificación biométrica, se deberán tener en cuenta los siguientes elementos -art. 5.2-: gravedad y probabilidad de que efectivamente se produzca la situación de riesgo, daños que podrían causarse si no se usara este sistema de identificación, así como las consecuencias que el empleo de estos sistemas pueda tener sobre los derechos y libertades de todas las personas afectadas[52]. Su utilización ha de contar con las necesarias y proporcionadas

---

[49] De imprescindible consulta sobre esta materia el Informe de la Agencia Europea para los Derechos Fundamentales (FRA), publicado en 2020, sobre *Facial Recognition Technology*: *fundamental rights considerations in the context of law enforcement*, así como las recomendaciones contenidas en el *Study on the use of innovative technologies in the justice field,* Informe Final presentado por la Comisión Europea, con fecha de septiembre 2020, esp. pp. 40 y ss. Véase también, aunque escrito en fecha anterior a la publicación de la Propuesta de Reglamento que nos ocupa, el trabajo de ETXEBERRIA GURIDI, J.F.: "Inteligencia artificial aplicada a la videovigilancia: tecnologías de reconocimiento facial", *Justicia algorítmica y neuroderecho, op. cit.,* pp. 443 y ss.

[50] Por datos biométricos se entiende en la norma -vid. art. 3, apdo. 33-, los datos personales resultantes de un procesamiento técnico específico, relacionado con las características físicas, fisiológicas o de comportamiento de una persona, que permiten o confirman la identificación única de esa persona física, tales como imágenes faciales, o datos dactiloscópicos.

[51] Se trata de los ya conocidos como treinta y dos "eurodelitos", que permiten eludir el control de doble incriminación en relación con la orden europea de detención y entrega, si estuvieran castigados en el Estado miembro emisor con pena o medida de seguridad privativa de libertad de un máximo de al menos tras años, tal y como se definen en el Derecho del Estado miembro emisor. Entre esos delitos se cuentan tipos tan graves como la pertenencia a organización delictiva, el terrorismo, la trata de seres humanos, la explotación sexual de niños, el tráfico de armas, etc., etc.

[52] Como bien destaca EXTEBERRÍA GURIDI, los sistemas de videovigilancia unidos a las nuevas herramientas IA, no sólo pueden afectar a la protección de datos de carácter personal, sino que los riesgos se extienden también a otras esferas de los derechos y libertades de los ciudadanos. Por ejemplo, el sometimiento a un escrutinio intenso mediante cámaras de un concreto espacio público puede resultar ser un elemento disuasorio para el ejercicio de ciertos derechos en ese espacio, como el derecho de reunión, de manifestación, o incluso la propia libertad de circulación. De otro lado, es evidente que estos sistemas IA de identificación biométrica remota pueden estar basados en algoritmos que alberguen deficiencias en su configuración, de

salvaguardas, y además deben estar bien concretadas sus condiciones de uso; en particular, límites temporales, geográficos y personales.

Por otro lado, debe llamarse la atención sobre el hecho de que la norma que nos ocupa exige de forma expresa -vid. art. 5.3- que el uso de estos sistemas de identificación biométrica cuente con una autorización previa por parte de una "autoridad judicial" o por una "autoridad administrativa independiente" del Estado miembro en que se vaya a usar, la cual, en caso de extrema urgencia, podría obtenerse posteriormente.

Según el apartado 8º de la Exposición de Motivos de esta Propuesta de Reglamento, la noción de "sistema de identificación biométrica remota" ha de entenderse de manera funcional; es decir, se trataría de un sistema IA destinado a la identificación de personas físicas a distancia, mediante la comparación de sus datos biométricos -facciones, modo de caminar, etc.-, captados en un lugar de acceso público, con los contenidos en una base de datos de referencia, y sin que se sepa previamente si la persona estará presente en ese lugar accesible al público donde se localiza el sistema IA, y si podrá ser identificada.

La norma distingue entre identificación biométrica remota que puede realizarse en "tiempo real", de aquella otra que se efectuaría "*ex post*". En el primer caso, -vid. art. 3, apdo. 37-, la captura de datos biométricos, la comparación con la base de datos y la identificación de la persona ocurren de manera instantánea o casi instantánea; se usarían secuencias de video que se están grabando en ese momento en un lugar de acceso público[53]. En la llamada identificación "*ex post*" -vid. art. 3, apdo. 38-, los datos biométricos se han captado previamente, de forma que la comparación e identificación del sujeto se hace posteriormente, con un retraso que ya es "significativo" -*significant delay*-. Las imágenes o secuencias de video se habrían obtenido entonces de cámaras de TV de circuito cerrado o de dispositivos privados.

Por *publicly accesible space* en el que se van a obtener las grabaciones y los datos biométricos, se entiende en el Proyecto de Reglamento IA -vid. Exposición de Motivos, apdo. 9- un espacio físico accesible al público, independientemente de si se aplican ciertas condiciones de acceso, o si es de propiedad pública o privada. Aunque para acceder a ese espacio hicieran falta tickets de entrada, o hubiera restricciones por edad, también se consideraría a estos efectos un "espacio de acceso público". Por tanto, las

manera que puedan hacer aflorar sesgos raciales o de género, con un elevado peligro de consecuencias discriminatorias, o bien dar como resultados porcentajes considerables de "falsos positivos o negativos". Vid. más ampliamente su trabajo "Inteligencia artificial aplicada…", *op. cit.*, pp. 448, 457 y 464. Sobre el posible "sesgo de género" en las decisiones alcanzadas por sistemas IA, vid. MARTÍNEZ GARCÍA, E.: "Justicia e inteligencia artificial sin género", en *Justicia algorítmica…, op. cit.,* pp. 209 y ss.

[53] La calidad de este tipo de imágenes puede no ser muy buena, por lo que aumenta la probabilidad de que se produzcan "falsas coincidencias".

calles, las partes relevantes de edificios gubernamentales, la mayoría de las infraestructuras de transporte, cines, teatros, centros comerciales…, también son espacios de acceso público en este sentido. No obstante, deberá concretarse "*case-by-case*", destaca la Propuesta de Reglamento.

De otro lado, en este punto debe tenerse también muy en cuenta lo dispuesto en el Reglamento (UE) 2016/679, sobre protección de datos de personas físicas y libre circulación de esos datos -RGPD-, especialmente lo dispuesto en su art. 9 : prohibición de tratamiento de datos personales de carácter biométrico y sus posibles excepciones. En semejantes términos, el art. 10 del Reglamento (UE) 2018/1725, sobre protección de las personas físicas en relación con el tratamiento de datos personales por instituciones, órganos u organismos UE y libre circulación de tales datos, así como el art. 10 de la Directiva (UE) 2016/680, sobre protección de las personas físicas en lo relativo al tratamiento de datos personales en ámbito penal.

Según esta normativa de referencia, se permitirá el tratamiento de los datos biométricos que permitan identificar de manera unívoca a una persona, si lo autoriza el Derecho de la Unión Europea o del Estado miembro, si fuera necesario para proteger intereses vitales del interesado o de otra persona física, por razones de un interés público esencial, o bien si el tratamiento se refiere a datos que el interesado hubiera hecho públicos de forma manifiesta.

Continuando con el análisis de los demás sistemas de "riesgo alto" que se contienen en el Título III de la Propuesta de Reglamento que nos ocupa, arts. 6 y ss., debe destacarse que entre ellos se encuadrarían la mayoría de los que pueden usarse en el orden penal. Esta categoría de sistemas se identificarían con una serie de criterios genéricos - *Classification rules for high-risk AI systems,* vid. art. 6- , si bien se adjunta además un listado de los mismos[54], en el Anexo III.

En relación con la aplicación de sistemas IA a la prevención, investigación y enjuiciamiento de los hechos delictivos, nos interesan ahora particularmente algunos de los mencionados en los apartados 6º y 8º del referido Anexo III[55].

El apartado 6º es el relativo al "*Law enforcement*"[56], es decir, a las herramientas IA que pueden emplearse por las autoridades competentes para "el cumplimiento de la ley"

[54] Listado que la Comisión puede ir ampliando, con base en una serie de criterios que también se apuntan en el apdo. 2º del art. 7.

[55] El listado de sistemas IA "*high risk*" en este Anexo III comienza -vid. apdo. 1º- con una referencia a los sistemas de identificación biométrica remota, a pesar de que, según hemos visto, en el articulado de la Propuesta de Reglamento éstos se posicionan como "sistemas prohibidos" o generalmente "inaceptables".

[56] Vid. definición en art. 3, apdo. (41): 'law enforcement' means activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal

en términos generales, entre las cuales se mencionan las siguientes: a) los sistemas IA usados por las autoridades para realizar una evaluación del riesgo individual en relación con personas físicas -"*individual risk assessments*", a fin de poder determinar su riesgo de comisión delictiva o de reincidencia, así como el riesgo de ser víctimas potenciales de hechos delictivos; b) el uso de polígrafos y herramientas similares, o de aquellas que detectan el estado emocional de una persona; d) los sistemas IA destinados a ser usados por las autoridades competentes para la evaluación de la fiabilidad de pruebas en el curso de una investigación o enjuiciamiento por hechos delictivos; e) los sistemas IA destinados a ser usados para predecir y prevenir la comisión o repetición de delitos, actuales o potenciales, con base en la elaboración de perfiles de personas físicas, o en la evaluación de rasgos de la personalidad, características o comportamientos delictivos pasados de personas concretas o grupos de personas, f) los sistemas IA destinados a ser usados por las autoridades encargadas de la aplicación de la ley para establecer perfiles de personas -"*profiling*"- según art. 3.4 Directiva 2016/680[57], en el curso de detección, investigación o enjuiciamiento de hechos delictivos. g) los sistemas IA usados para el análisis del delito - "*crime analytics*"- en relación con personas físicas, que permiten a la policía la búsqueda de grandes conjuntos de datos complejos en distintas fuentes o en diferentes formatos, a fin de identificar patrones desconocidos o descubrir relaciones ocultas entre esos datos.

En el apartado 8º del Anexo III que nos ocupa, encontramos una referencia, calificándolos también como sistemas IA de "alto riesgo", a los que pueden utilizarse en el contexto de la "Administración de justicia y procesos democráticos", que serían aquellos instrumentos destinados a ayudar a la autoridad judicial a investigar e interpretar los hechos y la ley, para la aplicación de ésta a un conjunto concreto de hechos. Entendemos que bajo este epígrafe tendrían cabida numerosos instrumentos que pueden ser útiles para la obtención de fuentes de prueba, así como para la valoración de los correspondientes medios probatorios.

El legislador UE ha entendido que todos estos son sistemas de "riesgo alto", pues pueden conllevar peligros para la salud y la seguridad, y en general para los derechos fundamentales de las personas. Para su empleo tendrían que cumplir con una serie de

offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.

[57] Según lo dispuesto en el art. 3.4 de la Directiva 2016/680, sobre protección de las personas físicas y tratamiento de sus datos personales para prevenir, investigar, detectar o enjuiciar infracciones penales o de ejecución de sanciones penales, y libre circulación de dichos datos, se entiende por "elaboración de perfiles" toda forma de tratamiento automatizado de datos personales consistente en utilizar dichos datos para evaluar aspectos personales, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. Sobre esta cuestión, vid. ARMENTA DEU, T.: *Derivas de la justicia, op. cit.,* pp. 272 y ss.

requisitos "horizontales" de fiabilidad, y seguir unos procedimientos de evaluación de ese cumplimiento antes de su posible utilización.

Se distinguen además en la Propuesta de Reglamento los sistemas IA de "alto riesgo", que en términos generales estarían prohibidos, y que para ser empleados tendrían que verificarse previamente por un tercero independiente -v.gr.: sistemas de identificación biométrica remota-, de aquellos otros sistemas también de "alto riesgo", pero para cuyo uso bastaría una "declaración responsable" del proveedor del sistema IA -*Conformity assessment*-, en el sentido de que cumple con los requisitos establecidos; véase lo dispuesto en el art. 19[58]. Se trataría entonces de una especie de "cumplimiento normativo" - *Compliance tools*[59] - , que se requeriría *v.gr*. para los sistemas IA que podrían usarse con fines predictivos, tanto por la policía, como en el ámbito jurisdiccional.

Pues bien, llegados a este punto, puesto que los sistemas IA a los que venimos haciendo referencia se emplean y se van a seguir empleando de manera creciente, y puesto que tal uso ha de favorecer la ingente tarea de prevención, investigación y enjuiciamiento de hechos delictivos, es preciso referirnos a la determinante cuestión de las garantías o requisitos que debe reunir la configuración y el uso de estos sistemas IA de "riesgo alto". Estas cuestiones también se abordan en la Propuesta de Reglamento que analizamos; concretamente, en el Capítulo II del Libro III, arts. 8 y ss., y son las que resumimos a continuación:

> *Risk managemente system*, art. 9: habrá de establecerse y documentarse un sistema continuo, regular y actualizado de evaluación y mitigación de riesgos, durante todo el ciclo de vida del sistema IA.
>
> *Data and data governance*, art. 10: ha de exigirse una alta calidad del conjunto de datos -*high quality data*- que alimentan o con los que se "entrena" el sistema. Se deberá examinar periódicamente el conjunto de datos para evitar desviaciones -*biases*-, sesgos o discriminaciones, identificar posibles "*data gaps*" o "*shortcomings*" -lagunas o defectos- y establecer cómo pueden ser resueltos éstos.
>
> *Technical documentation*, art. 11: toda la documentación técnica sobre el sistema IA deberá elaborarse antes de que se comercialice o se ponga en servicio, y se mantendrá actualizada. Deberá permitir evaluar su funcionamiento y el cumplimiento de las finalidades previstas.

[58] Llama la atención sobre esta diferencia HUERGO LORA, A.: "El proyecto de Reglamento sobre la Inteligencia Artificial", *Almacén de Derecho*, 17 de abril 2021.

[59] Vid. Exposición de motivos, apdo. 2.3.

Record-keeping, art. 12: todos estos sistemas IA han de tener la capacidad de grabar de forma automática los registros, y de asegurar un nivel adecuado de trazabilidad de los resultados alcanzados. Además, deberá poderse identificar a la persona física implicada en la verificación de los resultados.

Transparency and provision of information to users, art. 13: el diseño y funcionamiento de los sistemas IA debe ser lo suficientemente transparente como para permitir a los usuarios interpretar el resultado y emplearlo de forma adecuada. Las instrucciones de uso han de incluir información relevante, concisa, clara y completa, que además sea accesible y comprensible para los usuarios. Deberán explicar las características del sistema IA, sus posibles usos, su nivel de precisión, solidez y ciberseguridad. Habrán de advertir sobre posibles riesgos, tanto en su uso debido como en condiciones de uso indebido, aquellos que sean razonablemente previsibles. También deberán contener información sobre las medidas de supervisión humanas, necesidades de mantenimiento y de actualización del sistema, entre otros extremos relevantes.

Human oversight, art. 14: deberán establecerse medidas de supervisión humana, que puedan prever y minimizar los riesgos del sistema. Destaca en particular la medida contenida en el apartado 4. d) de este artículo, en el que se indica que la persona encargada de la supervisión debe ser capaz de decidir, en cualquier situación, la no utilización del sistema IA, o bien ignorar el "*output*" que éste ofrece.

Accuracy, robustness and cybersecurity, art. 15: este tipo de sistemas IA deben ser diseñados y desarrollados de forma que, a la vista de su específica finalidad, tengan un nivel adecuado de precisión, robustez y ciberseguridad, a lo largo de todo su ciclo de vida útil. Los niveles de precisión del sistema deben estar explicitados en las instrucciones de uso. Además, han de ser sistemas resilientes en caso de que se produzcan errores, fallos o incoherencias en el propio sistema o en el entorno en que operan, en particular por su interacción con personas físicas o con otros sistemas. Si son sistemas IA que continúan su aprendizaje tras su puesta en marcha, debe asegurarse que los ciclos de retroalimentación no lleven a resultados erróneos -*feedback loops*-. Deben ser seguros para prevenir y controlar ataques que pretendan manipular el conjunto de datos de entrenamiento del sistema, o entradas que tuvieran por objeto provocar errores en su funcionamiento.

Es igualmente reseñable el hecho de que el Proyecto de Reglamento añada también una serie de obligaciones que tendrán los usuarios de sistemas IA de "alto riesgo"; por ejemplo, seguir en todo momento las instrucciones de uso, conservar los registros generados automáticamente, respetar toda la normativa vigente sobre protección de datos, entre otros extremos[60].

Finalizaremos nuestro análisis con algunas valoraciones adicionales y conclusiones sobre el instrumento aquí abordado.

Podemos convenir que esta normativa europea llegará tarde, pues es muy poco probable que entre en vigor antes del año 2023; sin embargo, como se ha expuesto, los sistemas IA ya se están utilizando desde hace mucho tiempo en distintos ámbitos públicos y privados, incluso los calificados de "alto riesgo".

De otro lado, aunque el instrumento normativo elegido es un Reglamento, lo que desde luego favorece el grado de armonización que pretende alcanzarse en la Unión, es indudable que éste necesitará normas nacionales de desarrollo y, además, esta regulación de carácter horizontal y general va a requerir ser complementada por otras normativas sectoriales mucho más específicas.

Por ejemplo, en el ámbito jurisdiccional, que principalmente nos ocupa, será imprescindible aprobar la correspondiente regulación que permita el uso procesal de este tipo de sistemas IA en cuestiones para las que ya se viene empleando dentro y fuera de nuestras fronteras, y en otras muchas utilidades que seguro surgirán: previsión del riesgo de reincidencia delictiva o de fuga, de revictimización, posibilidades de reinserción social, determinación de la futura solvencia económica de una persona, presupuestos y efectos de la identificación biométrica remota, uso de sistemas IA para la obtención de fuentes de prueba, como ayuda en la valoración judicial de medios probatorios en los distintos órdenes jurisdiccionales[61], posibilidad -o no- de que se adopten decisiones judiciales "automatizadas", en todo o en parte[62], etc., etc.

---

[60] Véase con más detalle el contenido del art. 29 de esta Propuesta de Reglamento.

[61] Teniendo bien presente que la "eficiencia tecnológica" no puede ser un criterio autosuficiente sobre la fiabilidad de la prueba, ni reemplazar la necesaria valoración y juicio humano. Vid. más ampliamente, KEARNS, M. y ROTH, A.: *El algoritmo ético, op. cit.* esp. pp. 101 y ss.

[62] Vid. el art. 22 del Reglamento 2016/679 -RGPD-, sobre el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre una persona o le afecte significativamente, así como el más reciente art. 14 de la L.O. 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales: *Artículo 14. Mecanismo de decisión individual automatizado:* "1. Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del

Esta regulación sectorial más específica tendrá que adaptar e incorporar todas las garantías que de forma muy genérica se contienen actualmente en la Propuesta de Reglamento IA, y que finalmente encontrarán reflejo en el previsible Reglamento, a las especificidades de su uso en ámbitos más concretos: proceso civil, penal, administrativo, laboral, actuaciones policiales, etc. De otro lado, será preciso avanzar en la llamada *Estrategia Europea de Datos*, que incluye una gestión responsable de los mismos, cumpliendo además con los llamados "principios FAIR"[63]. Además, habrá que armonizar también los aspectos esenciales relativos a la responsabilidad civil que pudiera derivarse del uso de sistemas IA[64].

Por último, aunque no por ello menos relevante, la necesaria creación del "ecosistema de confianza" en la Unión Europea en materia de Inteligencia Artificial[65], la implantación de un marco jurídico destinado a lograr una IA fiable y respetuosa de los derechos y garantías fundamentales[66], repercutirá también sobre el éxito de la imprescindible cooperación judicial y policial transfronteriza en los supuestos cada vez más frecuentes en que se hayan podido usar sistemas IA, cuestión esta que, según ya

---

interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada. 2. Las decisiones a las que se refiere el apartado anterior no se basarán en las categorías especiales de datos personales contempladas en el artículo 13, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. 3. Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13". Véase más ampliamente, GUZMÁN FLUJA, V.: "Proceso penal y justicia automatizada", *op. cit.,* pp. 1 y ss.

[63] Acrónimo de "Fáciles de encontrar, Accesibles, Interoperables y Reutilizables". Véase el Informe final y Plan de acción del Grupo de expertos en datos FAIR de la Comisión europea: *Turning FAIR into reality, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.*

[64] Materia esta desde luego de enorme trascendencia práctica, y que ya se abordó en el *Informe sobre el marco de seguridad y responsabilidad civil de la Inteligencia Artificial, el Internet de las cosas y la robótica,* adjunto al Libro Blanco sobre IA. *https://ec.europa.eu/transparency/regdoc/rep/1/2020/ES/COM-2020-64-F1-ES-MAIN-PART-1.PDF*

En fechas más recientes la DG Justicia de la Comisión europea ha publicado un estudio muy completo de Derecho comparado sobre responsabilidad civil por Inteligencia artificial, que puede consultarse en https://op.europa.eu/es/publication-detail/-/publication/8a32ccc3-0f83-11ec-9151-01aa75ed71a1. Sobre esta cuestión, en nuestro país, vid. el trabajo de NÚÑEZ ZORRILLA, M.C.: *Inteligencia artificial y responsabilidad civil derivada de daños ocasionados por robots autónomos con inteligencia artificial*, Madrid, 2019, y con referencia al contexto europeo, de la misma autora: "Los nuevos retos de la UE en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial", *Revista Española de Derecho Europeo*, núm. 66, 2018, pp. 9 y ss.

[65] Al que ya se refería expresamente el *Libro Blanco sobre IA*, donde se insistía además en el "enfoque antropocéntrico" como objetivo político en sí mismo, que sirviera de guía para hacer frente a los principales riesgos que hay que salvar cuando se hace uso de los sistemas IA: opacidad en la toma de decisiones, discriminaciones de género u otro tipo, intromisión en la intimidad y posible uso con fines delictivos.

[66] Además de todos los que se mencionan expresamente en la Propuesta de Reglamento, habrá que tener siempre presente el respeto al debido proceso o proceso con todas las garantías, los derechos de defensa e igualdad de partes, la presunción de inocencia y la protección de la privacidad.

se ha indicado, ni siquiera encuentra mención en el Proyecto de Reglamento que analizamos.

Esta normativa UE está claramente centrada en la mejora del mercado interior y de la competitividad; en definitiva, en las libertades económicas comunitarias, y no tanto en reforzar el "espacio de libertad, seguridad y justicia", a pesar de que nos parecen objetivos perfectamente compatibles. Confiamos en que tras este importante esfuerzo regulatorio en la Unión[67], el texto del Reglamento que finalmente se apruebe sí tenga en consideración también este aspecto.

IV. REFERENCIAS BIBLIOGRÁFICAS

ARANGÜENA FANEGO, C.: "Reconocimiento mutuo de resoluciones sobre medidas alternativas a la prisión provisional", en *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Cizur Menor, 2015.

ARANGÜENA FANEGO, C.: "Orden europea de investigación: régimen de sustitución de la medida solicitada", *InDret,* núm. 2, 2021.

ARANGÜENA, C./ DE HOYOS, M. / RODRÍGUEZ-MEDEL, C. (Dirs.): *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Cizur Menor, 2015.

ARANGÜENA, C. / DE HOYOS, M. (Dirs.): *Garantías procesales de investigados y acusados. Situación actual en el ámbito de la Unión Europea,* Valencia, 2018.

ARANGÜENA, C. / DE HOYOS, M. / HERNÁNDEZ, A.: *Procedural Safeguards for Suspects and Accused Persons in Criminal Proceedings,* Springer, 2020.

ARMENTA DEU, T.: *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambios*, Madrid, 2021.

BACHMAIER, L.: "The Handling of Digital Evidence in Spain", en *Digital Forensic Evidence. Towards common European Standards in Antifraud Administrative and Criminal Investigations,* CAIANIELLO, M. / CAMON, A. (Eds.): Milano, 2021.

BARONA VILAR, S. (Dir.): *Claves de la Justicia Penal*, Valencia, 2019.

BARONA VILAR, S. (Ed.): *Justicia algorítmica y neuroderecho,* Valencia, 2021.

BARONA VILAR, S.: "Una Justicia 'digital' y 'algorítmica' para una sociedad en estado de mudanza", *Justicia algorítmica y neuroderecho,* Valencia, 2021.

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

[67] Que bien destaca BARONA VILAR, S.: *Algoritmización del Derecho y de la Justicia, op. cit.*, esp. pp. 149 y ss.

BUENO DE MATA, F.: “Macrodatos, inteligencia artificial y proceso: luces y sombras”, *Revista General de Derecho Procesal,* núm. 51, 2020, pp. 1 y ss.

BURCHARD, Ch.: “L’intelligenza artificiale come fine del Diritto penale? Sulla trasformazione algorítmica della societá”, *Riv.it.dir.proc.pen.,* vol. 62, núm. 4, 2019, pp. 1909 a 1942.

CAIANIELLO, M. / CAMON, A. (Eds.): *Digital Forensic Evidence. Towards common European Standards in Antifraud Administrative and Criminal Investigations.),* Milano, 2021.

DE HOYOS SANCHO, M.: “El reconocimiento mutuo de resoluciones por la que se impone una pena o medida privativa de libertad”, en *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Cizur Menor, 2015.

DE HOYOS SANCHO, M.: “La orden europea de protección de víctimas: análisis normativo”, en *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Cizur Menor, 2015.

DE HOYOS SANCHO, M.: “El principio de subsidiariedad y la autonomía procesal de los Estados de la Unión Europea”, *Revista Jueces para la Democracia*, núm. 96, 2019, pp. 36 y ss.

DE HOYOS SANCHO, M.: “El Libro Blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como sector de riesgo”, *Revista Española de Derecho Europeo,* núm. 26, 2020.

DE HOYOS SANCHO, M.: “Algunas dificultades en la aplicación práctica de la Orden Europea de Investigación”, en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Dir. V. Moreno Catena, Valencia, 2021, pp. 511 y ss.

DE MIGUEL BERIAIN, I.: “Does the use of risk assessments in sentences respect the right to due process? A critical analysis of the Wisconsin v. Loomis ruling”, *Law, Probability and Risk,* Vol. 17, núm. 1, marzo 2018, pp. 45 a 53.

DE SOUSA MENDES, P.: “A representaçao do conhecimento jurídico, inteligencia artificial e os sistemas de apoio à decisao jurídica”, *Inteligência Artificial & Direito*, Coimbra, 2020, pp. 51 y ss.

ETXEBERRIA GURIDI, J.F.: “Inteligencia artificial aplicada a la videovigilancia: tecnologías de reconocimiento facial”, *Justicia algorítmica y neuroderecho,* S. Barona Vilar (Ed.), Valencia, 2021, pp. 443 y ss.

FAIR TRIALS: *Regulating AI for Use in Criminal Justice Systems in the EU*, informe publicado en noviembre 2020. https://www.fairtrials.org

FERRER BELTRÁN, J.: *La valoración racional de la prueba,* Madrid, 2007.

FUENTES SORIANO, O.: “Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación

de pruebas electrónicas", en *Era digital, sociedad y derecho,* Dir.: O. Fuentes Soriano, Valencia, 2020, pp. 281 y ss.

GASCÓN INCHAUSTI, F.: "Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial", en *La justicia digital en España y en la Unión Europea,* J. Conde y G. Serrano (Dirs.), Barcelona, 2019, pp. 191 y ss.

GIALUZ, M.: "Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei *Risk Assessment Tools* tra Stati Uniti ed Europa", *Diritto Penale Contemporaneo*, 29 mayo 2019, pp. 1 y ss., esp. pp. 12 y ss.

GONZÁLEZ ÁLVAREZ, J.L., SANTOS HERMOSO, J., CAMACHO-COLLADOS, M.: "Policía predictiva en España. Aplicación y retos futuros", *Behavior & Law Journal*, 2020, vol. 6, núm. 1, pp. 26 y ss.

GONZÁLEZ CANO, M.I. (Dir.): *Orden europea de investigación y prueba transfronteriza en la Unión Europea,* Valencia, 2019.

GUZMÁN FLUJA, V.: "Proceso penal y justicia automatizada", *Revista General de Derecho Procesal*, núm. 53, 2021.

HUERGO LORA, A.: "El proyecto de Reglamento sobre la Inteligencia Artificial", *Almacén de Derecho*, 17 de abril 2021. https://almacendederecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial

JIMENO BULNES, M.: "La orden de detención europea como instrumento procesal en la lucha contra el terrorismo", *Unión Europea Aranzadi,* núm. 12, 2020.

KEARNS, M. / ROTH, A.: *El algoritmo ético. La ciencia del diseño de algoritmos socialmente responsables,* Madrid, 2020.

LARO GONZÁLEZ, E.: "El Reglamento E-evidence: instrumento adicional a la Orden europea de investigación", *La Ley Probática*, núm. 3, enero-marzo 2021.

LLORENTE SÁNCHEZ-ARJONA, M.: *La Orden Europea de Investigación y su incorporación al Derecho español,* Valencia, 2020.

LLORENTE SÁNCHEZ-ARJONA, M.: "Big data, inteligencia artificial y violencia de género", *Diario La Ley*, núm. 49, 2021, pp. 1 y ss.

MALDONATO, L.: "Algoritmi predittivi e discrezionalitá del giuidice: una nuova sfida per la giustizia penale", *Diritto Penale Contemporaneo*, 2/2019, pp. 391 y ss.

MARTÍN DIZ, F.: "Aplicaciones de Inteligencia Artificial en procesos penales por delitos relacionados con la corrupción", en Sánchez Bernal, J. y otros (Eds.): *Corrupción: compliance, represión y recuperación de activos,* Valencia, 2019, pp. 533 y ss.

MARTÍN DIZ, F.: "Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva *versus* decisoria", en *Justicia algorítmica y neuroderecho,* S. Barona Vilar (Ed.), Valencia, 2021.

MARTÍNEZ GARCÍA, E.: "Justicia e inteligencia artificial sin género", *Justicia algorítmica y neuroderecho,* S. Barona Vilar (Ed.), Valencia, 2021, pp. 209 y ss.

McKAY, C.: "Predicting risk in criminal procedure: actuarial tools, algorithms, AI and judicial decisión-making", *Current Issues in Criminal Justice,* 32:1, 2020, pp. 22 a 39.

MITCHEL, J y otros: "Machine learning for determining accurate outcomes in criminal trials", *Law, Probability and Risk*, núm. 19, 2020, pp. 43 y ss.

MORENO CATENA, V. (Dir.): *Nuevos postulados de la cooperación judicial en la Unión Europea*, Valencia, 2021.

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

NÚÑEZ ZORRILLA, M.C.: "Los nuevos retos de la UE en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial", *Revista Española de Derecho Europeo*, núm. 66, 2018, pp. 9 y ss.

NÚÑEZ ZORRILLA, M.C.: *Inteligencia artificial y responsabilidad civil derivada de daños ocasionados por robots autónomos con inteligencia artificial*, Madrid, 2019.

OCCHIUZZI, B.: "Algoritmi predittivi: alcune premesse metodologiche", *Diritto Penale Contemporaneo*, 2/2019, pp. 391 y ss.

ORTEGA KLEIN, A.: "Hacia un régimen europeo de control de la Inteligencia Artificial", *Análisis del Real Instituto Elcano*, 6 de mayo 2021, pp. 1 y ss.

PEREZ ESTRADA, M.J.: "El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías", en *Claves de la Justicia Penal,* S. Barona Vilar (Dir.), Valencia, 2019, pp. 235 y ss.

PILLADO GONZÁLEZ, E.: "Algoritmos predictivos del comportamiento y proceso penal de menores", *Justicia algorítmica y neuroderecho,* Ed.: S. Barona Vilar, Valencia, 2021.

PLANCHADELL GARGALLO, A.: "Inteligencia artificial y medidas cautelares", *Justicia algorítmica y neuroderecho,* Ed.: S. Barona Vilar, Valencia, 2021.

PRETRIAL JUSTICE INSTITUTE: *Updated Position on Pretrial Risk Assessment Tools*, 7 de febrero de 2020, https://www.pretrial.org/wp-content/uploads/Risk-Statement-PJI-2020.pdf

QUATTROCOLO, S.: "Intelligenza artificiale e giustizia: nella cornice della Carta ética europea, gli spunti per un'urgente discussione tra scienze penali e informatiche", en www.lalegislazionepenale.it, 22 marzo 2018.

QUATTROCOLO, S.: "Equitá del processo penale e *automated evidence* alla luce della Convenzione europea dei diritti dell'uomo", *Revista ítalo-española de Derecho Procesal,* vol. 2, 2109, pp. 1 y ss.

QUATTROCOLO, S.: *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, Springer, 2020.

SIGNORATO, S.: “Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo”, en *Rivista di Diritto Processuale*, 2/2020, pp. 605 y ss.

SUSSKIND, R.: *On line Courts and the Future of the Justice*, Oxford University Press, 2019.

THE LAW SOCIETY: *Algorithms in the Criminal Justice System,* junio 2019, en https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report

UBERTIS, G.: “Intelligenza artificiale, giustizia penale, controllo umano significativo”, en *Sistema penale*, texto presentado en Milán el 15 octubre 2020, en http://www.ristretti.it/commenti/2020/novembre/pdf3/articolo_ubertis.pdf