

EL DERECHO A UN PROCESO CON TODAS LAS GARANTÍAS ANTE LOS CAMBIOS DE PARADIGMA DE LA INTELIGENCIA ARTIFICIAL

VALENTINA FAGGIANI¹

*Profesora Titular de Derecho Constitucional
Universidad de Granada*

TRC, n.º 50, 2022, pp. 517-546
ISSN 1139-5583

SUMARIO

I. La naturaleza polivalente y contradictoria de la IA. II. El complejo desarrollo de un nuevo concepto de «justicia compartida»: entre impulsos a la innovación tecnológica y perfiles de inconstitucionalidad. III. ¿Puede el «juez algoritmo» sustituir al «juez persona» *ex arts. 24 y 117 CE*? ¿Y en su caso en qué medida? IV. La progresiva recepción del *fair trial* algorítmico en la UE. V. Las interacciones entre IA y justicia penal en el Derecho de la UE. VI. El impacto de la PRIA: aportaciones, déficits procesales y necesarias modificaciones. VII. La tutela judicial efectiva como centro del sistema de justicia en el Estado de Derecho ante las tendencias disolventes y diluyentes derivadas de la IA.

I. LA NATURALEZA POLIVALENTE Y CONTRADICTORIA DE LA IA

El Estado Constitucional de Derecho está siendo puesto a prueba por el desarrollo irrefrenable de la Inteligencia Artificial (IA). La denominada «cuarta revolución industrial (4.0)»² y la consiguiente «transformación» o las «derivadas»

1 Este trabajo ha sido realizado en el ámbito del Proyecto-Acción Jean Monnet, LUDELOR, Lucha contra la delincuencia organizada, 2020-2022, ref. 620390-EPP-1-2020-1-ES-EPPJMO-PROJECT.

2 MAYER-SCHÖNBERGER, V. y CUKIER, K., *Big Data: A Revolution that Will Transform How We Live Work and Think*, New York: Houghton Mifflin Harcourt, 2013. En doctrina, como pone de relieve PÉREZ ESTRADA, M.J., *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*, Valencia: Tirant lo Blanch, 2022, pp. 26 y 27, se está utilizando también el concepto de «convergencia tecnológica».

tecnológicas³, que está llevando consigo, están produciendo la transición de la sociedad analógica a la sociedad «digital»⁴. En este nuevo «contexto algorítmico»⁵, el «Código como ley» se convierte en la regla básica, a la que le corresponde definir las libertades y controlar el ciberespacio⁶. No obstante, la ubicuidad de la IA, su carácter omnipresente, no produce solo indudables ventajas sino también considerables riesgos para la democracia.

El nuevo espacio de control social dominado por una suerte de colaboración entre las grandes empresas multinacionales y los Estados para elaborar una infraestructura funcional a las exigencias del mercado, y en la que se está produciendo una «difuminación» entre datos públicos y privados⁷, monopolizándolos, ha determinado un cambio importante en los elementos básicos del modelo de Estado Constitucional, una «torsión tecnológica»⁸, desde el reparto de poderes a las fuentes del Derecho, al contenido y alcance de los derechos fundamentales, hacia su privatización.

Tampoco la justicia penal⁹, concebida por tradición como instrumento de *extrema ratio*, capaz de incidir en el bien más importante del individuo, es decir su libertad personal (art. 17 CE), ha estado inmune a estas transformaciones, a estos cambios de paradigma, pues también los sistemas penales se están viendo afectados ante la IA en su centro, que es la tutela judicial efectiva.

Por su parte, la crisis sanitaria derivada del Covid-19 ha acelerado este proceso. La pandemia ha mostrado de forma evidente no solo nuestra capacidad de resiliencia sino sobre todo la necesidad de promover el proceso de digitalización de la justicia y de los mecanismos de cooperación judicial en la UE. Tres son los

3 ARMENTA DEU, T., *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambios*, Madrid: Marcial Pons, 2021, p. 23, entiende el término «derivas» en el sentido de «sin dirección o propósito fijo», a merced de las circunstancias», más que «desvío de su verdadero rumbo».

4 BUENO DE MATA, F., «Macrodatos, inteligencia artificial y proceso: luces y sombras», *Revista General de Derecho Procesal*, n. 51, 2020, pp. 1-31. El autor individualiza las fases de desarrollo de «un modelo de e-justicia»: «a) Primera fase. Creación de un patrimonio digital jurídico, con el fin de llegar al objetivo de tener una Administración con 'papel cero'. b) Segunda fase: gestión procesal informatizada. c) Tercera fase: tecnología interconectada entre los ciudadanos y los operadores jurídicos en una ventanilla judicial única. d) Cuarta fase: aplicación de inteligencia artificial a la fase de decisión del proceso. Nos referimos aquí al uso de sistemas expertos dentro del sistema judicial que puedan ofrecer soluciones y respuestas a través de la inteligencia artificial. El debate ético se centraría en hasta qué punto usaríamos este modelo y si las máquinas pudieran a llegar suplir la decisión de un operador jurídico o únicamente servirían de apoyo a las decisiones de este último» (pp. 12 y 13).

5 BALKIN, J.B., «The Path of Robotics Law», *California Law Review Circuit*, vol. 6, 2015, pp. 45-60, habla de «sociedad algorítmica». La definición de Inteligencia Artificial fue elaborada por primera vez en 1956 por John McCarthy, y a continuación TURING, A., publicó «Computing Machinery and Intelligence», *Mind*, n. 49, 1950, pp. 433-460, sobre las máquinas pensantes.

6 LESSIG, L., *The Code version 2.0*, Cambridge: Basic Books, 2006.

7 BUENO DE MATA, F., *cit.*, p. 8.

8 CESARI, C., «Editoriale: L'impatto delle nuove tecnologie sulla giustizia penale — un orizzonte denso di incognite», *Revista Brasileira de Direito Processual Penal*, vol. 5, n. 3, 2019, pp. 1167-1188.

9 NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial*, Barcelona: Marcial Pons, 2018.

«ingredientes clave»¹⁰ para poner en marcha una estrategia común: la interoperabilidad, la seguridad online y el desarrollo de la tecnología, sobre todo de la IA, la cual constituye una «promesa extraordinaria»¹¹.

La IA ya ha conseguido penetrar en todos los aspectos de nuestra vida cotidiana. En efecto, puede ofrecer importantes beneficios a los ciudadanos, promoviendo su bienestar, a las empresas en términos de eficiencia, productividad y competitividad, y a la comunidad en su conjunto, permitiendo elaborar respuestas y soluciones alternativas a los principales desafíos sociales: del cambio climático y de la protección del ambiente, a la salud, como en el caso de las vacunas contra el Covid-19, a los sectores de la justicia, la seguridad, el modelo de Estado democrático y la lucha contra la criminalidad organizada¹² y contra el «modelo de *business* digital»¹³.

Por todo lo expuesto, el presente trabajo pretende contribuir al debate sobre esta cuestión, analizando cómo la tutela judicial efectiva, que constituye el centro del sistema de justicia penal en el Estado de Derecho, se está adaptando a la irrupción de las tecnologías de inteligencia artificial también en este ámbito. A tal fin, tras analizar los roles y las funciones, que los algoritmos pueden asumir en las distintas fases de desarrollo del proceso, en virtud de su carácter poliédrico y polifacético, puesto que pueden ser a la vez una eficaz herramienta en la lucha contra el crimen y una peligrosa arma al servicio del crimen¹⁴, se reflexionará sobre la necesidad de un estatuto procesal europeo de la IA. Para ello, se centrará en las razones por las que es necesario regular el «*due process of law* algorítmico», lo cual exige repensar las categorías básicas del Derecho a través del juicio de compatibilidad, y en el estado de la cuestión, haciendo referencia a cómo se está progresivamente regulando y especialmente a la Propuesta de Reglamento de la UE sobre la IA, adoptada en abril de 2021¹⁵, cuyo objetivo es construir un «ecosistema de garantías».

La premisa desde la que se desarrolla este estudio es la naturaleza bifronte y contradictoria de la IA, la cual se puede considerar como un «arma de doble filo»¹⁶ o quizás mejor dicho una «balanza», en la que hay que seguir manteniendo

10 EUROJUST, Press releases, EU Justice and Home Affairs agencies put focus on digitalization, *www.eurojust.europa.eu*, 20.11.2020 (*www.eurojust.europa.eu/eu-justice-and-home-affairs-agencies-put-focus-digitalisation*).

11 PARLAMENTO EUROPEO, Comisión de Libertades Civiles, Justicia y Asuntos de Interior, Proyecto de Informe sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)), 8.6.2020, ponente: Tudor Ciuhodaru, ap. A.

12 ZAVRŠNIK, A., «Criminal justice, artificial intelligence systems, and human rights», *ERA Forum*, 20, 2020, pp. 567-583.

13 COMISIÓN EUROPEA, Comunicación sobre la estrategia de la UE en la lucha contra la trata de seres humanos, 14.4.2021, COM (2021) 171 final, p. 12.

14 FAGGIANI, V., «La inteligencia artificial: ¿una herramienta contra o un arma al servicio del crimen?», SPIEZIA, F. y FAGGIANI, V., *Ataque a Europa: un atlas del crimen para comprender las amenazas, las respuestas y las perspectivas*, Valencia: Tirant lo Blanch, 2022, pp. 219-257.

15 COM/2021/206 final.

16 NACIONES UNIDAS, 14.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal en Kioto, Japón, 20 a 27 de abril de 2020, A/CONF.234/11. Documento de antecedentes preparado por la Secretaría.

el equilibrio. Por una parte, puede ofrecer nuevos recursos, más eficaces, para desarrollar una estrategia común de lucha contra el crimen, puesto que puede proporcionar a la policía y la fiscalía instrumentos de prevención y detección y facilitar la labor de investigación de delitos, también en los supuestos de delincuencia organizada como los delitos financieros, el blanqueo de capitales, la financiación del terrorismo y el cibercrimen, a través del intercambio estructurado de datos e informaciones¹⁷.

Asimismo, puede mejorar el ejercicio de la función judicial, simplificando el trabajo del juez, que podría apoyarse en tales aplicaciones para elaborar el contenido de la sentencia. Piénsese, por ejemplo, en la búsqueda de precedentes sobre asuntos concretos parecidos a aquello del que está conociendo y sobre el que tiene que decidir, en aquellos en los que la evaluación se fundamente en elementos numéricos y de carácter técnico-científico, o en la elaboración de documentos concernientes a asuntos más sencillos.

Sin embargo, por otra, dependiendo de cómo se utilice, la IA así como la tecnología en general puede afectar a la comunidad en su conjunto, vulnerando no solo los derechos fundamentales y las garantías procesales de un número indeterminado e indeterminable de personas, que pueden verse mermados por la opacidad («efecto caja negra»), la complejidad, la imprevisibilidad¹⁸, sino también intereses generales, como el orden y la seguridad públicos. Esta otra cara de la moneda vacía de contenido, matiza y devalúa la Tutela Judicial Efectiva, afectando no solo al Sistema de Justicia Penal, que constituye un sector de especial riesgo¹⁹, sino al propio Estado de Derecho.

Piénsese, por ejemplo, en el impacto de las aplicaciones de IA empleadas por los cuerpos y las fuerzas de seguridad y el poder judicial, como los algoritmos para predecir la reincidencia²⁰, que se caracterizan por importantes sesgos raciales o de género. Asimismo, pueden vulnerar nuestros derechos fundamentales los instrumentos de video-vigilancia, a través de los sistemas de reconocimiento facial, de la voz y del habla o de identificación de las matrículas. Y por último, no se puede soslayar que la IA puede ser utilizada para cometer delitos por su increíble capacidad de potenciar el alcance y los efectos del crimen²¹, convirtiéndose en parte

17 Sobre el rol de la IA en la lucha contra la criminalidad organizada, *vid.*: FAGGIANI, V., «La lotta contro il crimine attraverso gli algoritmi: contraddizioni e profili di (in)costituzionalità dell'applicazione dell'IA alla giustizia penale», GARRIDO CARRILLO, F.J. (Dir.); FAGGIANI, V. (Coord.), *Respuesta institucional y normativa al crimen organizado. Perfiles estratégicos para una lucha eficaz*, Cizur Menor: Thomson Reuters Aranzadi, 2022, pp. 245-282.

18 COMISIÓN EUROPEA, Libro Blanco sobre la Inteligencia Artificial - un enfoque europeo orientado a la excelencia y la confianza, 19.2.2020, COM (2020) 65 final.

19 COM(2020) 65 final.

20 TOLAN, S.; MIRON, M.; GÓMEZ, E. y CASTILLO, C., «Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia», Best Paper Award, International Conference on AI and Law (ICAIL), 2019, 10 pp.

21 FEDOTOV, Y., «In Just Two Decades, Technology Has Become A Cornerstone Of Criminality», *Huffington Post UK*, 23.10.2017.

integrante del «*modus operandi* de los delincuentes y los grupos delictivos organizados»²², estando dichos mecanismos programados para delinquir²³.

Por todo ello, este dualismo, que caracteriza el binomio IA-Justicia penal/lucha contra la criminalidad en la «era de la interdependencia digital»²⁴, requiere estudiar cómo este fenómeno puede transformar el modelo de justicia penal constitucionalmente garantizado, los riesgos susceptibles de poner a prueba la democracia pluralista y la respuesta que debería y o podría ofrecer el ordenamiento jurídico, siendo cada vez más urgente la necesidad de regular este espacio²⁵.

II. EL COMPLEJO DESARROLLO DE UN NUEVO CONCEPTO DE «JUSTICIA COMPARTIDA»: ENTRE IMPULSOS A LA INNOVACIÓN TECNOLÓGICA Y PERFILES DE INCONSTITUCIONALIDAD

La progresiva aplicación de la IA a las actividades de *law enforcement*, tanto en la fase de «*predictive policing*» (fase de la investigación)²⁶ como de «*predictive justice*» (fase de elaboración de la decisión del juez), exige desarrollar y delimitar un nuevo concepto de «justicia compartida», basado en una suerte de colaboración entre las autoridades de policía, los fiscales y el juez-persona, quien tiene que seguir ostentando el monopolio del ejercicio del *ius puniendi*, y las máquinas.

En particular, los sistemas de *predictive justice* relacionan factores de riesgo y características individuales, automatizándolos, al fin de verificar la peligrosidad

22 NACIONES UNIDAS, 14.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal en Kioto, cit., 63.

23 MASSARO, A., «Intelligenza artificiale, diritto e giustizia penale: coordinate ricostruttive», MASSARO, A., *Intelligenza artificiale e giustizia penale*, Roma: Università Roma Tre, 2020, pp. 11-38.

24 Naciones Unidas, «La era de la interdependencia digital», Informe del Panel de Alto Nivel del Secretario General sobre la cooperación digital», www.un.org/es/, junio de 2019.

25 BARONA VILAR, S., «Inteligencia Artificial o la Algoritmización de la vida y de la justicia: ¿solución o problema?», *Revista Boliviana de Derecho*, n. 28, 2019, pp. 18-49, habla de la «robotización judicial» o la «Justicia robot». De la misma autora, v. también la obra: *Claves de la justicia penal: feminización, inteligencia artificial, supranacionalidad y seguridad*, Valencia: Tirant lo Blanch, 2019.

26 En Italia, por ejemplo, se introdujo *KeyCrime*, en España se adoptaron VeriPol y VioGén, este último para responder a casos de violencia de género. Al respecto, *vid.* CINELLI, V. y MANRIQUE GAN, A., «El uso de programas de análisis predictivo en la inteligencia policial. Una comparativa europea», *Revista de estudios en seguridad internacional*, vol. 5, n. 2, 2019, pp. 1-19; GONZÁLEZ ÁLVAREZ, J.L.; SANTOS HERMOSO, J. y CAMACHO-COLLADOS, M., «Policía predictiva en España: aplicación y retos futuros», *Behavior & Law Journal*, vol. 6, n. 1, 2020, pp. 26-41; GONZÁLEZ ÁLVAREZ, J.L.; LÓPEZ OSSORIO, J.J. y MUÑOZ RIVAS, M., La valoración policial del riesgo de violencia contra la mujer pareja en España — Sistema VioGén, Ministerio de Interior, Secretaría de Estado de Seguridad, Gabinete de Coordinación y Estudio, Madrid, septiembre de 2018. Disponible en: www.interior.gob.es. Para una crítica a VioGén *vid.*: ETICAS FOUNDATION, The External Audit of VioGén System, eticasfoundation.org/es/, 8.3.2022. En particular, sobre el impacto de los mecanismos de «*predictive policing*» véase GUZMÁN FLUJA, V. C., «Ideas para un debate sobre la predicción del crimen», en CALAZA LÓPEZ, S. y LLORENTE SÁNCHEZ-ARJONA, M. (dirs.), *Inteligencia artificial legal y administración de justicia*, Cizur Menor: Thomson Reuters Aranzadi, 2022, pp. 289-338.

social y calcular el nivel de reincidencia. Si bien los algoritmos de evaluación del riesgo, basados en un software, pueden reducir los tiempos y los costes de los procedimientos, simplificando los procesos decisorios, conforme a un modelo matemático-estadístico, los aspectos positivos tienen que ser ponderados con los negativos.

De hecho, son numerosas las perplejidades que estos tipos de mecanismos despiertan desde el punto de vista de la protección de los derechos fundamentales y especialmente de la cláusula del *due process of law*, siendo muy invasivos. Ante todo, a pesar de haber sido configurados como meros instrumentos de auxilio, para facilitar la actividad del órgano juzgador, careciendo de carácter vinculante para la decisión, los *risk assessment tools* producen un desplazamiento, una delegación, del juez en la máquina, a la que realmente se puede imputar la decisión. Esta recoge los datos necesarios y decide el nivel de reincidencia de una persona detenida, la sanción y, en su caso, la duración y la eventual aplicación de medidas alternativas o la suspensión condicional de la pena, pudiendo por lo tanto atacar directamente la libertad personal.

Se ha hablado al respecto de un fenómeno de «de-responsabilización de los jueces»²⁷ y del consiguiente problema desde el punto de vista del respeto de la independencia e imparcialidad del pronunciamiento por la influencia que puede tener el algoritmo en el proceso decisorio. Alejarse u oponerse a la evaluación del programa requeriría a los jueces un mayor esfuerzo y la asunción de mayores responsabilidades. Este condicionamiento de la voluntad por la IA impone reflexionar sobre la necesidad de dotar a los órganos jurisdiccionales de mayores garantías para proteger su autonomía respecto a la decisión algorítmica, puesto que atendiendo al «requisito de jurisdiccionalidad»²⁸ no pueden limitarse a ratificar la solución de la máquina.

En la misma línea, es muy preocupante el impacto endo-procesal en los derechos de la defensa, al producirse una serie de violaciones a cascada en la esfera jurídica de la persona juzgada por el algoritmo. Ante todo, el efecto *black box* (caja negra) impide conocer, por la opacidad de estos sistemas, los códigos desde los que se deduce el algoritmo y sus efectos en la decisión, violando el derecho a ser informado de forma clara e inteligible del contenido de la acusación.

La imposibilidad de comprender tales datos y por lo tanto de acceder y contestar la validez científica de las pruebas elaboradas de forma automática se refleja directamente en el respeto del principio de contradicción y de igualdad de armas. Asimismo, tales sistemas pueden vulnerar el derecho al silencio y a

27 Según BASILE, F., «Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine», *Diritto Penale e Uomo*, 2019, pp. 28 y 29, nos encontramos entre un fenómeno de «deresponsabilización del hombre y responsabilización de la máquina». Al respecto, v. también LIPTAK, A., «Sent to Prison by a Software Program's Secret Algorithms», *The New York Times*, 1.5.2017 (<http://nyti.ms/2qoe8FC>).

28 DE HOYOS SANCHO, M., «El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea», *RGDP*, n. 55, 2021, p. 11.

no auto-incriminarse, la presunción de inocencia, el derecho a una sentencia individualizada y motivada, y no se puede soslayar que la ausencia de mecanismos de control externo priva al interesado de la posibilidad de impugnar la decisión.

Por lo que se refiere al principio de igualdad es importante considerar que estos protocolos están creados para encasillar de forma automática a las personas en determinados grupos²⁹, lo cual conlleva resultados discriminatorios (*bias*)³⁰. Y por último, se anula el derecho a la protección de datos personales, que se ve privado de contenido. El dominio de los datos personales pasa a las empresas, que en la mayoría de los casos no están dispuestas a compartir secretos, cubiertos por la propiedad industrial, impidiendo a los ciudadanos comprender cómo dichos sistemas funcionan y controlarlos. En este sentido, la opacidad, que los caracteriza, y la falta de colaboración por parte de los productores, que ostentan los derechos de propiedad intelectual-industrial, son contrarias al principio de transparencia, al control externo de la calidad y a la confianza de los resultados obtenidos.

Todos estos déficits procesales han sido puestos de relieve en el conocido caso *Loomis*, el *leading case* en la materia, resuelto por el Tribunal Supremo de Wisconsin (2016)³¹. El recurrente invocaba la violación del derecho a un proceso equitativo por el uso de Compas (*Correctional Offender Management Profiling for Alternative Sanctions*), un sistema de justicia predictiva utilizado en los Estados Unidos para ayudar a los jueces en la toma de decisiones³².

En este caso, sin embargo, el Tribunal Supremo no apreció la violación del *due process of law*, sino que desestimó el recurso, considerando que el algoritmo había sido aplicado correctamente, que era posible confrontar los datos utilizados para la evaluación y que las partes habían podido defenderse. El interesado, en su opinión, había podido controlar los *input* y había sido informado de los *output*³³.

29 HUQ, A.Z., «Racial Equity in Algorithmic Criminal Justice», *Duke Law Journal*, vol. 68, 2019, pp. 1043-1134.

30 Sobre la discriminación algorítmica, v. MIRÓ LLINARES, F., «Inteligencia artificial y Justicia Penal: Más allá de los resultados lesivos causados por robots», *Revista de Derecho Penal y Criminología*, n. 20, 2018, pp. 87-130; DE MIGUEL BERIAIN, I. y PÉREZ ESTRADA, M.J., «La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados», *Revista de Derecho de la UNED*, n. 25, 2019, pp. 531-561.

31 *State v. Loomis* - 2016 WI 68, 371 Wis. 2d 235, 881 N.W.2d 749.

32 GIALUZ, M., «Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei *risk assessment tools* tra Stati Uniti e Europa», *Diritto penale contemporaneo*, 29.5.2019, p. 21. Entre los peligros, que caracterizan estos mecanismos, el A. hace hincapié en la necesidad de evitar que se abra el camino hacia una «*forma inaccettabile di determinismo penale, per cui dal diritto penale del fatto — sancito dall'art. 25, comma 2, Cost. — si passi a un inaccettabile diritto penale del profilo d'autore, nel quale la pericolosità di un soggetto viene desunta esclusivamente dagli schemi comportamentali e dalle decisioni assunte in una determinata comunità nel passato. Ovviamente, questo sarebbe contrario al principio di individualizzazione del trattamento sanzionatorio, desumibile dall'art. 27, co. 1 e 3, Cost. 122, nonché, del canone di individualizzazione del trattamento cautelare, ricavabile dagli artt. 13 e 27, co. 2, Cost.*».

33 BRENNER, M., y otros, «Constitutional Dimensions of Predictive Algorithms in Criminal Justice», *Harvard Civil Rights-Civil Liberties Law Review*, vol. 55, Issue 1, 2020, pp. 267-310.

No era por lo tanto necesario que recibiera también una explicación sobre la ponderación de los intereses y sobre la correspondiente evaluación. Sin embargo, observó que si bien el juez puede tener en cuenta la previsión del riesgo realizada por el algoritmo, tal decisión no es vinculante³⁴.

En cambio, parece diferente el enfoque que se está adoptando en el continente europeo. La *Hague District Court*, en la sentencia de 5 de febrero de 2020, sobre el caso *Systeem Risico Indicatie (SyRI o SyRI i)*, se ha mostrado más preocupada por los derechos de las personas que podrían verse perjudicados por los mecanismos de IA, gestionados por la Administración del Estado para prevenir y combatir contra el fraude fiscal o en el ámbito de la seguridad social³⁵. Según esta decisión SyRI vulnera el respeto de la vida privada (art. 8, par. 2, CEDH), constituyendo un sistema desproporcionado, no necesario en una sociedad democrática, opaco y no verificable.

El presente pronunciamiento ha inaugurado una nueva línea jurisprudencial que puede contribuir a favorecer el diálogo judicial europeo así como el proceso de regulación/progresiva constitucionalización de los principios fundamentales y de las garantías en el uso de la IA, al fin de alcanzar el justo equilibrio entre los distintos intereses en juego: privacidad y protección de datos personales *vs.* lucha contra el fraude.

Tales garantías son fundamentales para reforzar el ejercicio del derecho al recurso efectivo y a un proceso equitativo, siendo tales perfiles estrictamente conectados. El Tribunal de la Haya, sirviéndose de un enfoque multinivel³⁶, estimó que el Estado no hizo públicos, ni reveló a los interesados el modelo de riesgo y los indicadores de los que se compone o puede estar compuesto, en definitiva cómo funciona y el procedimiento decisorio, y que no proporcionó al tribunal información objetivamente verificable para evitar que los ciudadanos encuentren la manera para eludir este programa³⁷.

³⁴ Desde un punto de vista crítico, v. CESARI, C., *op. cit.*, p. 1177; y QUATTROCOLO, S., «Quesiti nuovi e soluzioni antiche?: Consolidati paradigmi normativi vs rischi e paure della giustizia digitale 'predittiva'», *Cassazione Penale*, vol. 59, n. 4, 2019, pp. 1748-1765.

³⁵ *Rechtbank Den Haag*, sent. del 5 febbraio 2020, SyRI, ECLI:NL:RBDHA:2020:865 (<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878>). Vid. GESLEY, J., «Netherlands: Court Prohibits Government's Use of AI Software to Detect Welfare Fraud», *Global Legal Monitor*, 13.5.2020; NG, Y. F.; O'SULLIVAN, M.; PATERSON, M. y WITZLEB, N., «Revitalising public law in a technological era: rights, transparency and administrative justice», *University of New South Wales Law Journal*, vol. 43, n. 3, 2020, pp. 1-37; y LAZCOZ MORATINOS, G. y CASTILLO PARRILLA, J.A., «Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI», *Revista Chilena de Derecho y Tecnología*, vol. 9, n. 1, 2020, pp. 207-225.

³⁶ El respeto de la vida privada es un derecho humano fundamental, protegido por el art. 8 CEDH y el art. 17 PIDCP, el cual se encuentra estrictamente vinculado a la dignidad y a la libertad y a la noción de autonomía procesal. Y por lo que se refiere al Derecho de la UE, que es el más desarrollado y completo, la protección de este derecho se deduce de la interpretación sistemática de la Carta de los derechos fundamentales, el Reglamento UE 2016/679 sobre la protección de datos personales (RGPD) y la Directiva (UE) 2016/680 relativa a la cooperación judicial en materia penal (OJ, L 119/1, 14.5.2016 y OJ L 119, 4.5.2016).

³⁷ Tribunal de Distrito de la Haya, asunto SyRI, ap. 6.49.

III. ¿PUEDE EL «JUEZ ALGORITMO» SUSTITUIR AL «JUEZ PERSONA» EX ARTS. 24 Y 117 CE? ¿Y EN SU CASO EN QUÉ MEDIDA?

La aplicación de la IA a la justicia penal pretende eliminar o al menos reducir determinadas disfunciones y carencias que afectan a la Justicia, como la elevada subjetividad de las decisiones de los jueces, por el amplio margen de apreciación, que les dota de poderes creativos, la sobrecarga de trabajo por la falta de personal y las excesivas dilaciones de los procedimientos, con el fin de desarrollar un sistema más eficiente, de calidad, más previsible, sencillo y seguro³⁸.

Ahora bien, la progresiva aplicación de los algoritmos a las distintas fases del juicio y especialmente a los procesos decisorios plantea varias cuestiones, por las contradicciones y los riesgos que comporta, puesto que su carácter automático, opaco, inaccesible e incontrolable podría distorsionar el sistema.

Por ello, ante todo es necesario preguntarse si la IA puede sustituir al juez y en su caso en qué medida, si es recomendable que se aplique al ámbito de justicia penal y sobre todo si es compatible con el marco constitucional que la decisión adoptada por un programa informático pueda llevar a la cárcel a un individuo, puesto que la función judicial, atendiendo al art. 117 CE, se lleva a cabo «por jueces y magistrados integrantes del Poder Judicial», quienes como sabemos son personas³⁹.

Dicho en otros términos, ¿la decisión adoptada de forma automática y con un cierto grado de autonomía, a través del uso de procesos matemáticos-estadísticos, basados en una secuencia de reglas o instrucciones y en el manejo de una inconmensurable cantidad de datos que se interconectan, puede ser capaz de resolver una controversia de carácter penal? y en su caso ¿su calidad y acierto pueden ser equivalentes a la sentencia elaborada y dictada por el juez-persona?

Es evidente que «el mito del juez robot»⁴⁰ o del órgano jurisdiccional algorítmico, al fin de suplir los déficits humanos en el ejercicio de la función judicial, se coloca en una perspectiva distópica. Si el juez fuera una máquina y no una persona, como ocurre actualmente, a esta le correspondería la función de juzgar y hacer ejecutar lo juzgado (art. 117 CE), asegurando que el proceso sea equitativo (art. 24 CE).

38 KOSTORIS, R., «Predizione decisoria, diversion processuale e archiviazione», *www.sistemapenale.it*, 23.7.2021, p. 3, distingue entre «instrumentos predictivos de la IA para finalidades decisorias y predicciones decisorias». «*I primi, si diceva, dovrebbero fornire elementi su cui basare una decisione, sia di tipo parziale, come avviene in materia cautelare, sia tale da coinvolgere l'intera regiudicanda, fermo restando per il momento in ogni caso il divieto di ricorrere a decisioni completamente automatizzate in materia penale. Le predizioni decisorie tramite IA, dal canto loro, dovrebbero mirare invece a determinare la prevedibilità delle future decisioni su casi simili*».

39 COMISIÓN EUROPEA, Libro Blanco sobre la inteligencia artificial..., cit.

40 MORELLI, A., «Il giudice robot e il legislatore naïf. La problematica applicazione delle nuove tecnologie all'esercizio delle funzioni pubbliche», *Consulta online*, 6.8.2020, pp. 8-9.

Ahora bien, esta idea del «juez algorítmico», en el que delegar completamente el ejercicio de la función judicial⁴¹, es contraria al modelo de justicia penal *ex Costituzione* (arts. 24 y 117 de la CE), pues es incompatible con su planteamiento antropocéntrico, centrado en el principio personalista y en el carácter inviolable de los derechos fundamentales y de las libertades públicas (art. 10 CE). Se trata de un sistema «pensado para el hombre y encomendado al juicio del hombre»⁴², que constituye su centro de imputación. Este, sin embargo, a pesar de no ser perfecto, puede ser sometido a control y verificación.

En cambio, las máquinas carecen de la capacidad de comprender, razonar y argumentar. No tienen, por ejemplo, la misma capacidad de evaluar el caso concreto y de subsumirlo en el supuesto abstracto, considerando todos los elementos; no consiguen discernir, dudar y por consiguiente indagar para encontrar una solución alternativa, no tienen la imaginación, la empatía, la creatividad, la intuición y no sienten las emociones, «la sana consciencia de ‘saber de no saber’» y el sentido común⁴³, que en cambio perciben las personas. Aunque pueden elaborar análisis cuantitativos de un número muy elevado de datos en tiempos record e imitar en cierta medida sentimientos, su automatismo les impide comprender la complejidad de la realidad humana y el conjunto de variables que determinan su evolución.

Además, tampoco el «oráculo algorítmico»⁴⁴ con el mito de la justicia exacta es perfecto, sino todo lo contrario, puesto que puede incurrir en errores. Por ejemplo, un coche autónoma podría no notar una señal de tráfico y atropellar a un peatón, provocando lesiones graves o incluso matando; los software para identificar mensajes de odio o la propaganda terrorista podrían no comprender el tono o la intención de determinadas expresiones. Sin embargo, en tales supuestos es muy complicado descifrar los fallos del sistema, que además no pueden imputarse directamente a la máquina por su naturaleza y características, sino que su responsabilidad recaería más bien en la persona, que los ha elaborado. Por lo tanto, el error cometido por el algoritmo en la mayoría de los casos no puede identificarse, como el del ser humano, planteando problemas bajo el perfil del respeto del principio de publicidad del proceso y de transparencia, de la oralidad y en definitiva del contradictorio. Estos son solo algunos de los impedimentos absolutos a la sustitución total del juez persona por el juez-máquina, pues el robot no posee calidades que, en cambio, caracterizan al primero y que son fundamentales para el correcto desempeño de la función judicial.

41 LUCIANI, M., «La decisione giudiziaria robotica», *Rivista dell'Associazione Italiana dei Costituzionalisti*, n. 3, 2018, pp. 872-893.

42 MANES, V., «L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia», *dis-crimen.it*, 15.5.2020, p. 2.

43 CASONATO, C., «Intelligenza artificiale e diritto costituzionale: prime considerazioni», *Diritto pubblico comparato ed europeo*, núm. especial, 2019, pp. 101-130.

44 CONTISSA, G.; LASAGNI, G. y SARTOR, G., «Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo», *Diritto di internet*, 2019, pp. 619-634.

En la misma línea, se ha puesto de relieve que una de las principales razones por las que se pretende remplazar al hombre por la IA se halla en la necesidad de garantizar que los procesos sean más rápidos, al fin de asegurar el derecho a un proceso sin dilaciones indebidas (art. 24 CE y art. 6 CEDH). No obstante, no puede olvidarse, como observa M. LUCIANI, que la «rapidez no puede ir en detrimento de la calidad, lo cual plantea serios problemas de legitimidad constitucional, porque la jurisdicción tiene que satisfacer un derecho fundamental como el derecho de defensa»⁴⁵. Esto implica la necesidad de una equivalencia cualitativa entre la decisión algorítmica y la decisión del juez⁴⁶.

Asimismo, se ha hecho referencia a la exigencia de certeza jurídica, puesto que la justicia predictiva debería eliminar el carácter excesivamente subjetivo de la evaluación del juez. Sin embargo, es cierto que la máquina no sería capaz de aplicar correctamente la normativa y de desarrollar un proceso garantista. El hecho de que el algoritmo tome la decisión o de que el juez se pronuncie, atendiendo al algoritmo, puede ser problemático desde el punto de vista de la capacidad de seleccionar los datos, relacionando el supuesto concreto a la norma típica, problemas que se complican cuando se requiere un margen de discrecionalidad en la interpretación de conceptos jurídicos indeterminados, como el orden público, la seguridad o la salud⁴⁷.

No obstante, si bien la IA, especialmente en el ámbito de justicia penal, no puede sustituir al juez, quien tiene que seguir pronunciando la decisión final, es innegable que puede convertirse en un importante instrumento de apoyo y asesoramiento en el proceso decisorio, en vista del desarrollo de un sistema de «justicia compartido»⁴⁸. Por consiguiente, aunque los principios contenidos en las Constituciones impiden atribuir el ejercicio de la función jurisdiccional a un robot, que es una máquina, estas aplicaciones pueden adquirir una función instrumental y de auxilio en el ejercicio de la función de *iuris dictio*⁴⁹.

Es decir, la decisión sería emitida por el juez, que seguiría manteniendo el control, aunque este podrá acudir a las herramientas de IA para formular el contenido de la sentencia⁵⁰. Piénsese, por ejemplo, en la importante función desarrollada por plataformas, que se basan en motores de búsqueda inteligentes, con el objetivo de analizar las distintas fuentes normativas y jurisprudenciales y el material científico doctrinal. Tales mecanismos facilitan el acceso a un alto nivel

45 LUCIANI, M., *cit.*, p. 874.

46 Ídem.

47 DE LA OLIVA SANTOS, A., «Justicia predictiva», interpretación matemática de las normas, sentencias robóticas y la vieja historia del 'Justizklavier', *El Cronista del Estado Social y Democrático de Derecho*, n. 80, 2019, p. 34.

48 MANES, V., *cit.*, p. 22.

49 DONATI, F., «Intelligenza artificiale e giustizia», *Rivista AIC*, n. 1, 2020, pp. 416-436.

50 Según MANES, V., *cit.*, p. 19, «L'orizzonte, dunque, dovrebbe essere quello che — confermando il perentorio divieto di una decisione basata unicamente su trattamenti automatizzati — ammetta una funzione solo tutoria dell'algoritmo per limitare la fallibilità della decisione giudiziale, nel quadro di una collaborazione uomo-macchina».

de informaciones, considerando normas de distinta naturaleza y procedentes de diferentes ordenamientos y de forma más rápida gracias a Internet⁵¹.

No obstante, el peligro consiste en que las soluciones ofrecidas por la «justicia predictiva» arriesgan no limitarse a tener un valor meramente indicativo sino que asumen una función casi prescriptiva, incidiendo directamente en el proceso de formación de la voluntad del juez y condicionando el contenido de sus decisiones. De esta forma, como afirma F. Donati, se puede producir un efecto circular que facilita la reproducción de las decisiones y la «cristalización» de la jurisprudencia, limitando su evolución⁵².

IV. LA PROGRESIVA RECEPCIÓN DEL *FAIR TRIAL* ALGORÍTMICO EN LA UE

La necesidad de aprovechar al máximo la IA y al mismo tiempo reducir o al menos atenuar los peligros derivados de su aplicación a la justicia penal impone la adopción de estándares mínimos a escala de la Unión, que permitan repensar las categorías jurídicas tradicionales en «clave algorítmica» y consolidar las bases de una política común, estableciendo cuando proceda unas «líneas rojas», con el fin de limitar tanto los poderes privados como los públicos y responder a eventuales incumplimientos.

Para comprender por qué es necesario regular la IA y su impacto es suficiente considerar que solo a través de la previsión de los requisitos y de las modalidades de aplicación de estos sistemas es posible adaptar la justicia penal a la nueva sociedad digitalizada, reforzando la confianza tanto entre los ciudadanos y la administración como entre los Estados miembros, siendo esta la base de la cooperación judicial en la Unión.

Sin embargo, la recepción del «*due process of law* algorítmico» o «*due process of law* tecnológico»⁵³ y el desarrollo de un estatuto procesal de la IA o la adopción de nuevos supuestos delictivos son objetivos muy complejos, articulados y pro-

51 En España, por ejemplo, junto a los motores de búsqueda como *Westlaw* y *LexisNexis*, en los últimos años se han introducido también sistemas predictivos de análisis jurisprudencial, como *Jurimetria*, que permite a los abogados elaborar la estrategia procesal para ganar un caso, indicando la probabilidad de éxito, la trayectoria del juez que está conociendo el caso, y trazar las principales líneas jurisprudenciales y las argumentaciones de las partes. En el contexto europeo la *University college of London*, en 2016, desarrolló un algoritmo capaz de prever el resultado de las controversias ante el TEDH, sistematizando la jurisprudencia y adivinando la solución en el 75% de los casos. Al respecto, v. MEDVEDEVA, M.; VOLS, M. y WIELING., M., «Using machine learning to predict decisions of the European Court of Human Rights», *Artificial Intelligence and Law*, vol. 28, 2020, pp. 237-266; ALETRAS, N.; TSARAPATSANIS, D.; PREOȚIUC-PIETRO, D. y LAMPOS, V., «Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective», *PeerJ Comput. Sci.*, vol. 2, 2016 (<https://peerj.com/articles/cs-93/>).

52 DONATI, F., *cit.*, p. 433.

53 CITRON, D. K., «Technological Due Process», *Washington University Law Review*, vol. 85, Issue 6, 2008, pp. 1249-1313. En este estudio se observa la necesidad de construir un modelo de «*due process*» capaz

gresivos, que requieren la integración y la coordinación entre los distintos niveles de protección de los derechos fundamentales.

Ante todo, se requiere un profundo proceso de reflexión, que permita aclarar la relación entre Derecho e IA, entre Derecho y tecnología⁵⁴, al fin de evitar el efecto «disruptivo»⁵⁵, que estos sistemas y su rápida evolución podrían producir en la justicia penal. Al respecto, es importante observar que la IA y las tecnologías se nutren de datos e informaciones, que inciden en los procesos decisorios, determinando el resultado. En otros términos, el dato se convierte en la norma, atendiendo a la cual se establece el contenido final de la decisión.

El replanteamiento de las categorías jurídicas en clave algorítmica tiene que realizarse atendiendo al «juicio de compatibilidad», bajo el filtro de la proporcionalidad, y adoptando un enfoque multinivel. Dicho «test» pretende medir los efectos de la IA en el Derecho penal, sustantivo y procesal, con el fin de adaptar esta «metamorfosis» a los principios fundamentales de nuestros ordenamientos jurídicos. Este núcleo mínimo irreductible está constituido por la dignidad y los derechos fundamentales, entre los que los derechos procesales adquieren una posición central, siendo instrumentales para la protección de los demás derechos⁵⁶.

de proteger los intereses de los individuos de forma equitativa, responsable y transparente sin renunciar a las ventajas ofrecidas por los sistemas que adoptan decisiones automatizadas (p. 1313).

54 BALAGUER CALLEJÓN, F., «Inteligencia artificial, democracia y derechos», en GUERRA FILHO, W.S.; SANTAELLA, L.; KAUFMAN, D. y CANTARINI, P. (Orgs.), *Direito e Inteligência Artificial: Fundamentos*, Vol. 1 - Inteligência Artificial, Ética e Direito, Rio de Janeiro: Lumen Juris, 2021, pp. 57-82. Y del mismo A., «The Impact of the New Mediators of the Digital Age on Freedom of Speech», *YSEC Yearbook of Socio-Economic Constitutions*, 2022.

55 ARMENTA DEU, T., *op. cit.*, p. 220.

56 Por lo que se refiere al ordenamiento español, los principales parámetros de referencia están constituidos por los arts. 24 y 117 CE relativos al derecho a la tutela judicial efectiva y a un proceso con todas las garantías y al estatuto de los jueces y el art. 18.4 CE, del que se ha deducido el carácter fundamental del derecho a la protección de datos personales. Tales preceptos se encuentran desarrollados por las siguientes leyes: la Ley de Enjuiciamiento Criminal (LeCrim, BOE, n. 260, 17.9.1882), la Ley Orgánica (LO) 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (BOE, n. 294, 6.12.2018), la LO 7/2021 de protección de datos personales tratados para fines de prevención, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (BOE, n. 126, de 27 de mayo de 2021) y por la Ley 3/2020 de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia (BOE, n. 250, de 19 de septiembre de 2020). Por su parte, el marco convencional europeo está integrado por el CEDH, en particular los artículos 5, 6, 7 y 13, y por los Convenios adoptados en el marco del Consejo de Europa y sus respectivos Protocolos, entre los que es interesante mencionar: el Convenio n. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Estrasburgo, 1981); el Convenio n. 164 relativo a los derechos humanos y la biomedicina (Oviedo, 1997); el Convenio n. 185 sobre la ciberdelincuencia (Budapest, 2001); el Convenio n. 50 sobre la elaboración de una farmacopea europea (Estrasburgo, 1964); el Convenio n. 196 para la Prevención del Terrorismo (Varsovia, 2005); el Convenio Europeo para la Represión del Terrorismo (Estrasburgo, 2003); y el Convenio Europeo de Asistencia Judicial en Materia Penal (Estrasburgo, 1959). Y por último, la IA deberá respetar el Derecho de la UE, *in primis*, las disposiciones de la Carta, sobre todo los arts. 47 a 50 en materia de justicia, el art. 6 sobre el derecho a la libertad personal y los arts. 7 y 8 relativos al derecho a la protección de datos personales y al respeto de la vida privada, los dos paquetes de Directivas sobre derechos procesales (la Directiva 2010/64/UE, DOUE L 280/1, 26.10.2010; la Directiva 2012/13/UE, DOUE L 142/1, 1.6.2012; la Directiva 2013/48/UE,

Atendiendo a dicho razonamiento, en estos años se ha intentado suplir la ausencia de una normativa específica en materia de IA, adoptando instrumentos de autorregulación y de *soft law*. Estas dos técnicas han impulsado la progresiva recepción normativa en instrumentos de *hard law*. Autorregulación, *soft law* y *hard law* se retroalimentan y están funcionalmente orientadas a alcanzar el mismo objetivo es decir la configuración de un marco ético, integrado por un conjunto de principios programáticos, que respondan a los riesgos previstos y futuros de la IA, permitiendo un uso de las tecnologías y aplicaciones de IA respetuoso con los valores europeos comunes (art. 2 TUE)⁵⁷.

No obstante, es evidente que no se puede dejar la regulación de este ámbito tan complejo a las empresas, puesto que esto conlleva el riesgo de instrumentalización para sus propios fines⁵⁸. En este sentido, «Si bien la autorregulación puede ser un método complementario de aplicación de ciertos principios y normas, no puede sustituir las obligaciones positivas de los Estados miembros de proteger y salvaguardar eficazmente los derechos humanos, la democracia y el Estado de Derecho»⁵⁹.

Por su parte, los instrumentos de *soft law*, aunque carezcan de fuerza jurídica vinculante, se han convertido pronto en parámetros a seguir, contribuyendo a crear un «marco ético-jurídico» de buena «gobernanza» de la IA, que aunque en este estadio se encuentra «todavía inacabado»⁶⁰ está impulsando su recepción normativa. Este proceso ha culminado con la propuesta de Reglamento sobre la IA de la UE, que permitiría el traspaso definitivo e inequívoco del *soft law* al *hard law*.

Por lo que se refiere de forma más específica al ámbito de la Gran Europa, destaca la Carta Ética sobre el Uso de IA en los sistemas judiciales y su entorno, elaborada en el marco del Consejo de Europa por la Comisión Europea sobre la Eficacia de la Justicia (Cepej). Se trata del primer texto en el que se enuncian los

DOUE L 294/1, 6.11.2013; la Directiva 2016/343, DOUE L 65/1, 11.3.2016; la Directiva 2016/800/UE, DOUE L 132/1, 21.5.2016, y la Directiva (UE) 2016/1919, DOUE L 297/1, 4.11.2016), el RGPD, la Directiva (UE) 2016/680 y la Directiva (UE) 2016/681, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (OJ L 119, 4.5.2016). Este marco representa la base para la institución de una normativa específica capaz de limitar los efectos negativos de tales instrumentos sobre la justicia penal.

57 HERNÁNDEZ PEÑA, J.C., «Gobernanza de la inteligencia artificial en la Unión Europea. La construcción de un marco ético-jurídico aún inacabado», *Revista General de Derecho Administrativo*, n. 56, 2021, 42 pp.

58 BARRIO ANDRÉS, M., «¿Deben los Estados regular la inteligencia artificial?», *Elpais.com*, 26.9.2018; e Id., «Robots, inteligencia artificial y persona electrónica», en DE LA QUADRA-SALCEDO, T., PIÑAR MAÑAS, J.L. (Dir.), *Sociedad Digital y Derecho*, BOE, Ministerio de Industria, Comercio y Turismo y RED.ES, 2018, pp. 113-136.

59 Ad hoc Committee on Artificial Intelligence (CAHAI) policy development group (CAHAI-PDG) Draft Feasibility Study, V.0.5. Strasbourg, 11.11.2020, CAHAI-PDG(2020)01rev2, ap. 135, disponible en: www.coe.int/cahai.

60 HERNÁNDEZ PEÑA, J.C., *cit.*, p. 21 y ss. El autor analiza la creación del marco de gobernanza de la IA en la UE, que se estructura en un trinomio compuesto de en normas éticas, estandarización y regulación *Hard-Law*.

«principios sustanciales y metodológicos»⁶¹, que pueden devenir el centro de una «ciber-justicia» europea.

Desde su aprobación, la Carta ha desempeñado un rol muy importante, habiendo impulsado el proceso de concienciación de la sociedad civil así como la recepción normativa de los principios éticos que tienen que informar los mecanismos de IA. De tal forma, ha adquirido la función de parámetro, atendiendo al cual los sujetos privados y públicos, que actúan en este ámbito, deberían conformarse en el desarrollo y en la aplicación de estos mecanismos a la justicia.

En esta senda en diciembre de 2020, el CAHAI, el Comité *ad hoc* sobre la IA del Consejo de Europa, adoptó por unanimidad el estudio de viabilidad de un marco normativo sobre el diseño, el desarrollo y la aplicación de la IA, con un enfoque basado en los derechos humanos, centrandó la atención en los riesgos para la democracia⁶² y el Estado de Derecho⁶³. En el mencionado estudio se explica por qué es necesario un marco normativo, cuáles deberían ser sus elementos constitutivos y se evalúa la oportunidad de adoptar un instrumento jurídico internacional bajo la forma de Convención, de Convenio marco o de otra medida, con el fin de favorecer la armonización.

En particular, en el presente estudio, se observa que la adopción de una convención favorecería un uso responsable con el fin de crear un sistema de gobernanza para la administración y los tribunales así como las fuerzas del orden y las administraciones públicas y contribuir y promover una estrategia común para la lucha contra la criminalidad organizada, que ayude a identificar la corrupción dentro de las entidades públicas, así como detectar y defenderse de ciberataques⁶⁴.

V. LAS INTERACCIONES ENTRE IA Y JUSTICIA PENAL EN EL DERECHO DE LA UE

La adopción de una acción política y normativa europea que facilite la armonización⁶⁵ está dirigida a desarrollar un «ecosistema de garantías» y de «confianza

61 BARBARO, C., «Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari», *www.questionegiustizia.it*, 7.12.2018; y QUATTROCOLO, S., «Intelligenza artificiale e giustizia: nella cornice della carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche», *lalegislazionepenale.eu*, 18.12.2018, pp. 1-12.

62 CAHAI, Feasibility Study, Strasbourg, 17 December 2020 CAHAI (2020) 23, www.coe.int/cahai.

63 BARBARO, C., «Lo studio di fattibilità di un nuovo quadro normativo sulla concezione, lo sviluppo e l'applicazione dei sistemi di Intelligenza Artificiale sulla base delle norme del Consiglio d'Europa. Il lavoro del Comitato Ad hoc sull'intelligenza artificiale del Consiglio d'Europa (CAHAI)», *www.questionegiustizia.it*, 28.4.2021.

64 CAHAI, Feasibility Study, ap. 39.

65 FAGGIANI, V., *Los derechos procesales en el espacio europeo de justicia penal. Técnicas de armonización*, Cizur Menor: Thomson-Reuters Aranzadi, 2017.

exclusivo»⁶⁶, basado en un planteamiento antropocéntrico, enfocado en el ser humano, que respete la dignidad, los derechos y los valores europeos⁶⁷. De lo contrario, existe un riesgo de fragmentación no solo del mercado interior sino del reconocimiento mutuo de las sentencias y de las decisiones judiciales y por lo tanto de la cooperación judicial en materia penal.

En unos pocos años, la UE ha conseguido pasar de la elaboración de documentos de *soft law*, como el Libro Blanco sobre la inteligencia artificial —Un enfoque europeo para la excelencia y la confianza (2020)⁶⁸, a la aprobación de la propuesta de Reglamento sobre un enfoque europeo a la IA, de 21 de abril de 2021, y poco después del Reglamento (UE) 2021/784 del 29 de abril de 2021 sobre la lucha contra la difusión de contenidos terroristas online⁶⁹, que establece la remoción⁷⁰ o el bloqueo de contenidos terroristas online, contra el uso impropio de los servicios de *hosting*⁷¹.

El presente Reglamento prevé el uso de sistemas automatizados para identificar tales mensajes⁷², es decir de esta forma los algoritmos deciden si proceder a la remoción de un determinado contenido, marcando los límites entre mensajes, que están amparados por la libertad de expresión, y aquellos que en cambio tienen carácter terrorista o pueden ser instrumentalizados por tales grupos.

Tales mecanismos no están exentos del riesgo de realizar una evaluación errónea, pues siguen siendo opacos, no transparentes y en muchas ocasiones no consiguen percibir matices o el contexto, no siendo siempre capaces de distinguir, por ejemplo, el adoctrinamiento y la propaganda o de reconocer el tono del mensaje: no obstante, dicha medida parece muy oportuna y puede jugar un rol importante contra esta forma de criminalidad. Su aplicación está empezando a dar sus frutos.

En España, por ejemplo, el CITCO (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado) del Ministerio de Interior participó en mayo de 2022 en una operación de Europol, que ha involucrado a varios países, a través de la cual se ha conseguido la retirada de 1.124 contenidos ilícitos de corte terrorista y violento de internet, como los «*nasheed*», los cánticos del Estado Islámico que instan a la comisión de ataques⁷³.

66 COMISIÓN EUROPEA, Comunicación, Una estrategia europea para los datos, Bruselas, 19.2.2020, COM/2020/66 final.

67 COMISIÓN EUROPEA, Crear confianza en la inteligencia artificial antropocéntrica, 8.4.2019, COM(2019) 168 final.

68 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*, n. 76, 2020, pp. 9-43.

69 OJ L 172, 17.5.2021.

70 Art. 3 Reglamento (UE) 2021/784.

71 Art. 7 Reglamento (UE) 2021/784.

72 Art. 7.1 Reglamento (UE) 2021/784.

73 MINISTERIO DE INTERIOR, España participa en una operación de Europol que logra la retirada de 1.124 contenidos ilícitos de internet, www.interior.gob.es, Madrid, 21.5.2022.

En esta línea, en enero de 2022, la Comisión presentó el texto de una Declaración de Derechos y Principios Digitales⁷⁴, que debería ser firmada por el PE, la Comisión y el Consejo. Este documento de *soft law* está dotado de interesantes virtualidades. En la Exposición de motivos se pone de relieve su «carácter declarativo», sin valor jurídico vinculante, reafirmando que se mueve en el respeto del «Derecho primario de la UE, en particular el TUE, el TFUE, la CDFUE y la jurisprudencia del TJUE, así como en el Derecho derivado» y «el pilar europeo de derechos sociales»⁷⁵, que constituyen sus bases. No obstante, con el paso del tiempo, debido al avance de la tecnología, podría convertirse a todos los efectos en una Carta de derechos para el espacio digital, que se yuxtapondría a la CDFUE, a modo de Protocolo, integrándola a través de la recepción de nuevos derechos y adaptándola a la nueva realidad digital⁷⁶.

Por lo que se refiere de forma más específica a los algoritmos y a los sistemas de IA, a los que este documento hace referencia en el Capítulo III, se reconoce la necesidad de construir un entorno digital justo sobre la base de información objetiva, transparente y fiable, «en el que los derechos fundamentales estén protegidos y las responsabilidades de las plataformas» «bien definidas».

VI. EL IMPACTO DE LA PRIA: APORTACIONES, DÉFICITS PROCESALES Y NECESARIAS MODIFICACIONES

La PRIA, presentada el 21 de abril de 2021, podría convertirse en el primer instrumento normativo común para el desarrollo, la comercialización y el

⁷⁴ Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, Bruselas, 26.1.2022, COM(2022) 28 final.

⁷⁵ De forma parecida, también en España se ha elaborado una Carta de los derechos digitales, atendiendo a los objetivos de la Agenda España Digital 2025, por un grupo de expertos constituido por la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) del Ministerio de Asuntos Económicos y Transformación Digital (19.11.2020) (https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf). A pesar de ser un documento de *soft law*, puede asumir un importante valor de herramienta interpretativa, impulsando un proceso de reflexión sobre estas cuestiones y su posterior recepción en un texto normativo *ad hoc*, jurídicamente vinculante. En este documento se intenta conjugar la perspectiva antropocéntrica y la protección de los derechos fundamentales con las exigencias derivadas del desarrollo de la tecnología y de la dimensión digital. A tal fin, no se pretende «descubrir derechos digitales», para que «sean algo distinto de los derechos fundamentales ya reconocidos o que las nuevas tecnologías y el ecosistema digital se erijan por definición en fuente de nuevos derechos», sino «concretar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros» (Carta de derechos digitales: consideraciones previas).

⁷⁶ Según DE PASQUALE, P., «Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?», *DUE. Osservatorio europeo*, marzo, 2022, p. 5, dicho documento «nascerrebbe come 'sovrastuttura' rispetto all'alluvionale sedimentazione di norme nazionali, stratificatesi nel corso del tempo; a cui andrebbero ad aggiungersi i diritti che, al momento della sua adozione, saranno 'inediti'. Più precisamente, essa non soltanto avrebbe la funzione di innovare, ma altresì di rendere espliciti una serie di principi e diritti».

uso de la IA, dotando a la UE de un propio modelo de *governance*, vinculante para los Estados miembros, también en su relaciones con terceros países. Se trata de una medida muy ambiciosa, horizontal, basada en un enfoque de riesgo, cuyo objetivo es responder a la rápida evolución de la tecnología, garantizando la sostenibilidad del mercado interior, sin menoscabar los derechos fundamentales.

La aproximación es tanto preventiva, puesto que se indican *ex ante* los requisitos que los mecanismos de IA tienen que satisfacer antes de ser puestos en el mercado, así como *ex post* para permitir a las autoridades públicas intervenir cuando surjan riesgos imprevistos.

Por su parte, el uso del reglamento está funcionalmente orientado a alcanzar la armonización de este ámbito y asegurar la correcta y uniforme interpretación y aplicación de tales normas, evitando que los Estados miembros intervengan de forma automática, descoordinada y fragmentada. Además, dicha fuente normativa, al contrario de la directiva, tiene una eficacia inmediata y directa, no requiriendo ser transpuesta en el ámbito de los Estados miembros (art. 288 TFUE).

Ahora bien, a pesar del considerable esfuerzo mostrado por la UE, la propuesta no está exenta de problemas y perfiles de incompatibilidad con el marco europeo y constitucional de los Estados Miembros. De hecho, presenta aspectos controvertidos, que afectan a la justicia penal, y que deberían ser reconsiderados, puesto que conllevan el riesgo de desencadenar violaciones reiteradas y sistemáticas de los derechos fundamentales, encerrando y bloqueando a la ciudadanía en un bucle sin salida. Y todo ello, evidentemente, es contrario al núcleo mínimo, al corazón del Estado de Derecho.

Por lo expuesto, en el presente trabajo, se ha preferido poner de relieve las deficiencias, los límites y las lagunas de la PRIA, más que abordar los aspectos positivos, que ya han sido sobradamente comentados por la doctrina, pues tales defectos podrían perjudicar el éxito de esta normativa, consolidando un sistema disfuncional.

Estas insuficiencias interesan básicamente los siguientes perfiles: a) la ausencia de una referencia explícita a la cooperación judicial en materia penal y al impacto de la IA en este ámbito; b) el reconocimiento de una mera prohibición relativa del reconocimiento biométrico en «tiempo real» en «espacios de acceso público», con la previsión de excepciones amplias y generales para actividades de *law enforcement*; c) y la no inclusión de los mecanismos de justicia predictiva y de elaboración de perfiles en los sistemas de riesgo inaceptable, que en cambio deberían estar incluidos en el art. 5 PRIA.

Vamos por lo tanto por puntos. La primera laguna que se observa y que podría ser corregida en el proceso de negociación concierne a los objetivos de la PRIA, entre los que no aparece ninguna mención explícita, como observa De

Hoyos Sáncho, M., a la cooperación judicial en materia penal⁷⁷. El silencio del legislador europeo no está justificado, puesto que el desarrollo del mercado interior va de la mano de la existencia de un sistema de protección de los derechos fundamentales efectivo, que se fundamenta en la cooperación judicial, constituyendo su *conditio sine qua non*.

En este sentido, es muy importante remarcar que la IA puede simplificar las actividades de contraste del crimen, permitiendo prever la comisión del delito, identificar con mayor facilidad al culpable o a la víctima y garantizar la concreta operatividad de los instrumentos de reconocimiento mutuo de las sentencias y resoluciones judiciales, como la orden europea de detención y la orden europea de investigación. Por ello, el refuerzo de la cooperación judicial en materia penal debería estar contemplado de forma expresa entre los objetivos de la PRIA, junto al desarrollo del «mercado interior».

En segundo lugar, por lo que se refiere al sistema de «líneas rojas», fijado en la PRIA para atenuar los efectos perjudiciales sobre los derechos fundamentales, la sistemática, que se articula en cuatro niveles o escalas de riesgo (riesgo inaceptable que comporta la prohibición del sistema, alto riesgo, riesgo mediano o limitado y riesgo bajo o mínimo) parece correcta. No obstante, tanto los tipos de mecanismos subsumibles en las distintas categorías de riesgo, así como las posibles excepciones y la formulación de las disposiciones, es bastante mejorable.

El primer nivel de riesgo incluye los sistemas de máximo peligro, los cuales están prohibidos porque se consideran inaceptables. Se considera que estas herramientas violan la dignidad, los derechos fundamentales y, en general, los valores de la UE (art. 2 TUE) y pueden manipular a las personas, incidiendo en el libre arbitrio y aprovechando las debilidades de los colectivos especialmente vulnerables, como los niños o las personas con discapacidad.

Se pueden reconducir a este escalón, por ejemplo, los juegos, que utilizan los asistentes vocales para incitar a la violencia, los comportamientos peligrosos sobre los menores y los de control social de los gobiernos, como los *social score*, usados en China para controlar a los ciudadanos y facilitar el desarrollo de sistemas de vigilancia masiva⁷⁸. Estos últimos sistemas, sin embargo, deberían ser prohibidos no solo para las autoridades públicas, como prevé la propuesta, sino también para los privados.

77 DE HOYOS SANCHO, M., «Delincuencia organizada e inteligencia artificial. Estrategias y propuestas normativas en el contexto de la Unión Europea desde la perspectiva procesal», en GARRIDO CARRILLO, F.J. (Dir.) y FAGGIANI, V. (Coord.), *Respuesta institucional y normativa al crimen organizado. Perfiles estratégicos para una lucha eficaz*, cit., p. 302 y 303; y también v. ID, «El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea», *RGDP*, *op. cit.*, p. 11.

78 Sobre la PRIA, v. COTINO HUESO, L.; CASTILLO, J. A.; SALAZAR, I.; BENJAMINS, R.; CUMBRERAS, M. y ESTEBAN, A. M., «Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Artificial Intelligence Act)», *Diario La Ley*, 2.7.2021. Asimismo, v. CASONATO, C. y MARCHETTI, B., «Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale», *BioLaw*, 29.9.2021.

No obstante, el aspecto más controvertido está representado por las herramientas de identificación biométrica «en tiempo real» en los «espacios de acceso público»⁷⁹ para actividades de *law enforcement*⁸⁰. La PRIA, en principio, veta dichos sistemas en el art. 5; sin embargo, la negativa no es absoluta porque a continuación se prevé la posibilidad de excepcionar la regla, cuando esté justificado por la necesidad de perseguir un interés público relevante. Se admiten la búsqueda de potenciales víctimas del delito, con la inclusión de los menores desaparecidos; la existencia de amenazas para la vida o la incolumidad física de las personas físicas o un ataque terrorista; y la detección, localización e identificación de los autores o sospechosos de haber cometido delitos graves⁸¹ o de llevar a cabo la acción penal contra ellos⁸².

Ante todo, se observa que de por sí el uso de la IA para el reconocimiento automático de las características humanas, tales como la cara pero también la forma de andar, las huellas digitales, el ADN, la voz y otros datos biométricos o del comportamiento en espacios de acceso público debería ser prohibido de forma generalizada y en cualquier tipo de contexto⁸³. El uso-abuso de una innumerable cantidad de datos personales, de información sensible y de la imagen no es solo susceptible de vulnerar los derechos fundamentales de un número indiscifrable de personas, sino que las máquinas se sirven de tales datos para alimentarse y aprender, entrenándose con ellos y adquiriendo de esta forma una mayor autonomía.

Ahora bien, el legislador europeo, salvo que modifique la PRIA —lo cual sería deseable—, de momento, ha optado por un veto relativo, que prevé un conjunto de excepciones, cuya formulación podría revelarse contraproducente, pues la excesiva extensión de las mallas de dichas derogaciones y por lo tanto de la discrecionalidad de los Estados en este ámbito podría vaciar la prohibición del uso de estos mecanismos de contenido y de eficacia práctica⁸⁴.

79 ETXEBERRIA GURIDI, J.F., «Sistemas biométricos y su aplicación», en BARONA, S., *Justicia poliédrica en periodo de mudanza: Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad*, Valencia: Tirant lo Blanch, 2022, pp. 455-482.

80 Art. 5 PRIA.

81 El art. 5.1, d, iii) reenvía al art. 2, ap. 2, de la Decisión Marco 2002/584/JAI del Consejo.

82 Art. 5.2 PRIA.

83 En este sentido, *vid.* EDPB-EDPS, *Joint Opinion 5/2021, on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18.6.2021, 32. En la misma línea, el Parlamento Europeo en la Resolución, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)), aps. 26 y 27, pide lo siguiente: a. la «prohibición permanente del uso de análisis automatizados o el reconocimiento en espacios accesibles al público de otras características humanas, como los andares, las huellas dactilares, el ADN, la voz y otras señales biométricas y de comportamiento»; y b. posponer la introducción de «sistemas de reconocimiento facial para fines coercitivos con funciones de identificación, a menos que se utilicen estrictamente para fines de identificación de víctimas de delitos, hasta que» no sean conformes con el marco constitucional. De lo contrario, en su opinión, los sistemas no deberían utilizarse ni desplegarse.

84 Art. 5.3 PRIA.

Otra confirmación se puede encontrar, a continuación, en la disposición que atribuye a los Estados miembros la facultad de autorizar totalmente o parcialmente, en el ámbito del propio ordenamiento, la identificación biométrica remota «en tiempo real» en espacios accesibles al público para actividades de *law enforcement*, especificando los requisitos y el procedimiento para la solicitud, la expedición, el ejercicio de las autorizaciones, las actividades de control y los objetivos⁸⁵. Y al respecto es evidente el riesgo de que se produzca un cuadro fragmentado.

Asimismo, no se debería distinguir entre reconocimiento biométrico a distancia o no, sino que se debería considerar cualquier tipo de sistema, que actúe sin el consentimiento del interesado. Y por último y más en general, el cumplimiento de los requisitos formales no aseguraría el respeto de los derechos fundamentales⁸⁶.

En la misma línea, parece incorrecta la inclusión en los sistemas de IA de segundo nivel, es decir de alto riesgo, y no en el primer nivel, de aquellos destinados a la identificación biométrica remota en tiempo real y a posteriori de personas físicas, que pueden provocar resultados distorsionados y efectos discriminatorios en relación a la edad, etnia, sexo o discapacidad, así como los mecanismos utilizados en la lucha contra el crimen por las autoridades de *law enforcement* (anexo III)⁸⁷.

Estas últimas aplicaciones, en particular, pueden ser muy intrusivas y dotan a las autoridades de penetrantes poderes, legitimándoles a vigilar o a privar a una persona de la libertad. Además, pueden perjudicar no solo el principio de igualdad bajo el perfil de la prohibición de discriminar, sino también el derecho a un recurso efectivo y a un proceso equitativo, el derecho de defensa y la presunción de inocencia, que pueden ser vulnerados, sobre todo cuando los algoritmos no sean suficientemente transparentes, comprensibles y documentados⁸⁸.

Por todo ello, se considera que la prohibición *ex art.* 5 debería ser extendida también a los sistemas de IA de *law enforcement* para comprobar el riesgo de reincidencia o para prever la comisión o la repetición de un delito real o potencial sobre la base de la elaboración de perfiles o de la evaluación de los

85 Art. 5.4 PRIA. El uso de estos sistemas de *high risk* está subordinado a la autorización preventiva de la autoridad judicial o administrativa independiente del Estado Miembro, en el cual se usarán estos sistemas, expedida previa solicitud motivada y atendiendo lo previsto en el derecho interno. Dicha solicitud puede ser presentada a posteriori en una situación de urgencia debidamente justificada, en la que deberán explicarse las razones por las que dicho trámite no ha podido realizarse.

86 De acuerdo con POLLICINO, O. y PAOLUCCI, F., «La proposta di regolamento sull'intelligenza artificiale: verso una nuova governance europea», *Privacy&*, 3, 2021, «Il ragionamento alla base della proposta sembra omettere che quando si monitorano aree aperte, gli obblighi previsti dalla normativa UE sulla protezione dei dati devono essere soddisfatti non solo per i sospetti, ma per tutti coloro che in pratica sono monitorati, onde instaurare pericolosi meccanismi di sorveglianza di massa. Resta dunque centrale il ruolo del sistema a tutela dei dati personali fornito dal GDPR che costituisce un limite all'utilizzo discrezionale delle tecnologie biometriche».

87 Anexo III, relativo a los sistemas de IA de alto riesgo (art. 6.2.1 PRIA).

88 Considerando n. 38 PRIA.

rasgos o de las características de la personalidad o de un comportamiento criminal pasado, porque condiciona la decisión de las autoridades de policía o del juez a la máquina, que en definitiva es quien puede llevar a la cárcel a una persona⁸⁹.

La PRIA considera también de alto riesgo para la democracia, el Estado de Derecho y los derechos fundamentales, en particular el derecho a un recurso efectivo y a un proceso equitativo, los mecanismos de IA usados en el ámbito de la administración de la justicia y de los procesos democráticos. Es suficiente pensar en los posibles prejuicios, en los errores y la opacidad, que pueden caracterizar los *softwares* de auxilio a las autoridades judiciales en la interpretación y la aplicación de la ley a una serie concreta de hechos⁹⁰.

En cambio, no deben considerarse de alto riesgo los sistemas de IA aplicados en los procedimientos administrativos por las autoridades fiscales y aduaneras⁹¹ y aquellos que desarrollan actividades administrativas meramente auxiliares, que no perjudican la administración de la justicia, como en el caso de la anonimización o de la pseudonimización de documentos, decisiones o datos judiciales, la comunicación entre el personal, las tareas administrativas o la asignación de personal y recursos⁹². Ahora bien, como se puede observar fácilmente, se trata de sistemas completamente distintos respecto a aquellos usados en las actividades de *law enforcement*, los cuales se limitan a coadyuvar al individuo, pues simplifican la realización de tareas repetitivas y reiterativas de por sí caracterizadas por un cierto automatismo y no requieren una intervención más intelectual.

En definitiva, aunque la PRIA represente una propuesta indudablemente muy ambiciosa, que pretende enfrentarse a la IA y a su extrema complejidad, por su carácter de por sí anárquico, tendente a superar las barreras y a rechazar la regulación, también es cierto que es bastante mejorable. De ahí, la importancia de la fase de tramitación y negociación de la propuesta, anterior a su definitiva adopción. Es en esta sede donde se podrá jugar el partido para modificar los aspectos más controvertidos de esta normativa, elevando el estándar de protección de los derechos fundamentales. Mientras tanto, les corresponde sobre todo a los Estados adoptar medidas internas para adaptarse y estar preparados a este fenómeno tecnológico muy fascinante, con un halo mágico, pero al mismo tiempo misterioso, ambiguo y controvertido.

89 EDPB-EDPS, *Joint Opinion 5/2021*, cit., 34.

90 Considerando n. 40 PRIA.

91 Considerando n. 38 PRIA.

92 Considerando n. 40 PRIA.

VII. LA TUTELA JUDICIAL EFECTIVA COMO CENTRO DEL SISTEMA DE JUSTICIA EN EL ESTADO DE DERECHO ANTE LAS TENDENCIAS DISOLVENTES Y DILUYENTES DERIVADAS DE LA IA

La protección procesal constituye el instrumento para otorgar efectividad y dotar de contenido y concreción a los demás derechos. Por ello, la tutela judicial *ex art.* 24 CE, que se puede considerar como base para el respeto de los demás derechos fundamentales, se convierte en el centro del sistema de justicia penal, siendo indispensable para su efectividad y para que se pueda confiar en él⁹³.

El derecho a un juicio con todas las garantías, junto al principio de legalidad, según el cual el proceso legislativo tiene que ser transparente, responsable, democrático y pluralista, la certeza del Derecho y la prohibición de arbitrariedad del poder ejecutivo, constituyen parte integrante del núcleo, de la esencia, de la democracia⁹⁴. No se trata de meros requisitos procedimentales, sino de instrumentos necesarios e íntimamente interconectados, de cuya efectividad depende que el Estado de Derecho pueda seguir siendo «la columna vertebral de toda democracia constitucional moderna»⁹⁵, el eje de las sociedades abiertas y plurales, caracterizadas por el fenómeno de la globalización, en cuanto valor común de la UE y patrimonio constitucional de los Estados miembros (art. 2 TUE). De hecho, los derechos son efectivos si se pueden accionar ante un órgano jurisdiccional. Se trata de un índice de calidad del nivel de democracia existente en un determinado ordenamiento⁹⁶.

La tutela judicial efectiva, que representa el centro, el corazón del sistema de justicia penal en un Estado de Derecho, uno de sus elementos constitutivos, está

93 Sobre el art. 24 CE *vid.*: AGUIAR DE LUQUE, L., «Las garantías constitucionales de los derechos fundamentales en la Constitución Española», *Revista de Derecho Político*, n. 10, 1981, pp. 1-23; CORDÓN MORENO, F., *Las Garantías constitucionales del proceso penal*, Pamplona: Aranzadi, 1999; DE LA OLIVA SANTOS, A., *Los verdaderos tribunales en España: legalidad y derecho al juez predeterminado por la Ley*, Madrid: Centro de Estudios Ramón Areces, 1992; Díez-PICAZO GIMÉNEZ, I., «Artículo 24: garantías procesales», ALZAGA VILAAMIL, O. (dir.), *Comentarios a la Constitución de 1978*, vol. III, Madrid: Edersa/Cortes Generales, 1996, pp. 19-123; Díez-PICAZO GIMÉNEZ, L.M., *Régimen Constitucional del Poder Judicial*, Madrid: Civitas, 1991; Díez-PICAZO y PONCE DE LEÓN, L., «El Poder Judicial: breves reflexiones sobre veinticinco años de experiencia», *Revista Española de Derecho Constitucional*, año 24, n. 71, 2004, pp. 35-46; FIGUERUELO BURRIEZA, A., «En torno al concepto de tutela efectiva de los jueces y tribunales (Art. 24.1 de la C.E.)», *Revista de Estudios Políticos*, n. 33, 1983, pp. 207-220; GIMENO SENDRA, V., *Fundamentos de Derecho Procesal*, Madrid: Civitas, 1981; PICÓ I JUNOY, J., *Las garantías constitucionales del proceso*, Barcelona: Bosch, 2011.

94 CRAIG, P., «Formal and Substantive Conceptions of the Rule of Law: An Analytical Framework», *Public Law*, n. 3, 1997, pp. 467-487.

95 Comunicación de la Comisión al Parlamento Europeo y al Consejo, Un nuevo marco de la UE para reforzar el Estado de Derecho, Estrasburgo, 11.3.2014 COM (2014) 158 final, en particular p. 2.

96 FAGGIANI, V., «Le crisi sistemiche dello stato di diritto e i loro effetti sulla cooperazione giudiziaria nell'UE», *Diritto Penale Contemporaneo*, n. 2, 2019, pp. 195-228; e ID, «La 'rule of law backsliding' como categoría interpretativa del declive del constitucionalismo en la UE», *Revista Española de Derecho Europeo*: n. 71, 2019, pp. 57-99.

siendo puesta a prueba ante el reto de la IA, cuyos mecanismos han empezado a ser aplicados tanto en la fase de *law enforcement* así como en el proceso decisorio, especialmente a través de los mecanismos de *predictive justice*. Este «hecho tecnológico»⁹⁷ sin duda muy atractivo, intrigante y terriblemente inquietante, se caracteriza por una complejidad científica y tecnológica extrema, en muchos casos muy difícil de conjugar con las ciencias jurídicas, y por zonas de sombra para nosotros inaccesibles, que crean espacios de impunidad.

La posibilidad para las máquinas de reproducir comportamientos humanos y adoptar decisiones autónomas, que afectan directamente a la libertad personal, nos sitúa en una realidad que supera la ciencia ficción, pues la difusión de los mecanismos de vigilancia masiva o los sistemas de reconocimiento biométrico de las personas está al orden del día, situándonos en un escenario muy parecido al del Gran Hermano de George Orwell. En la misma línea, el mito distópico del juez robot ya no parece una posibilidad tan lejana como hace unos años. En este nuevo contexto, el Código, los algoritmos, es decir esta secuencia de reglas e instrucciones, que se nutren de millones de datos, se convierte en la Ley, en la regla básica. A esta le corresponde definir las libertades y controlar el ciberespacio, incidiendo en los aspectos estructurales de nuestros Ordenamientos Jurídicos.

El impacto, dependiendo de su uso, puede ser tanto positivo como negativo. La IA se podría definir como un «arma de doble filo», pues de su carácter ubicuo, mutable y omnipresente derivan no solo innegables ventajas sino también considerables riesgos para la seguridad, las empresas, la economía y la democracia. En este sentido, aunque podría mejorar la «*governance* judicial», eliminando el margen de subjetividad que caracteriza la decisión judicial y las dilaciones de los procedimientos, es indiscutible que la administración de justicia sobre todo penal es un «sector de riesgo» desde el perfil del respeto de los derechos fundamentales y de las garantías procesales.

Se trata, en definitiva, de una «balanza» en la que tenemos que intentar mantener el equilibrio, porque aunque podría eliminar barreras espacio-físicas y temporales, haciendo mucho más rápidos los procesos de toma de decisiones y otorgándoles eficacia, y podría proporcionar nuevos instrumentos, adaptando algunos ámbitos a las exigencias de una sociedad tecnológica, sí es cierto que puede vaciar de contenido, matizar y devaluar la Tutela Judicial Efectiva, afectando no solo al sistema de justicia penal, sino al propio Estado de Derecho, en su núcleo mínimo irreductible.

Por todo ello, en el presente trabajo se ha avanzado y profundizado en el binomio Inteligencia Artificial - Justicia Penal a fin de comprender cuáles son las potencialidades y los riesgos de los mecanismos de IA y su compatibilidad al

97 *Vid.* Anteproyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia, por la que se transpone al ordenamiento jurídico español la Directiva (UE) 2019/1151, de 20 de junio de 2019, Exposición de motivos, 1.

marco constitucional. Este análisis se ha desarrollado desde la premisa de que la «protección procesal» constituye la base para la concreción de todos los demás derechos fundamentales, dotándolos de efectividad. Esto significa que la Tutela Judicial Efectiva sigue siendo el eje, el elemento de unidad del Sistema Jurídico, el cual permite su mantenimiento y la supervivencia. Es necesario reinterpretar este derecho fundamental y sus múltiples facetas, adaptándolo a las nuevas exigencias derivadas de la sociedad tecnología y del Internet de las cosas, a fin de que no se vea privado de contenido, obligando a las personas a renunciar a sus propios derechos.

Dicho en otros términos, aunque vivamos en un contexto en el que todo fluye de forma incesante, con una velocidad irrefrenable, que impone cambios y movimientos continuos, existen principios, que constituyen límites materiales inderogables e intangibles, que tampoco la IA puede diluir y difuminar hasta menoscabar su contenido esencial. Uno de estos principios básicos es precisamente el derecho a la tutela judicial efectiva y a un juicio ante un Juez-Persona independiente e imparcial *ex arts. 24 y 117 CE*.

Tales preceptos representan una frontera infranqueable a la atribución del ejercicio de la función jurisdiccional a un robot, que es una máquina, puesto que sus razonamientos automáticos imposibilitan la correcta subsunción del supuesto concreto a la norma típica, que tuviera en cuenta todas las circunstancias del caso. Además, se prescindiría de aquella empatía y sexto sentido que son fundamentales en todos los procesos de evaluación. Al respecto, no se puede soslayar que la interpretación es de por sí una operación dotada de un margen de subjetividad y discrecionalidad, que dependiendo de los casos será más o menos amplia.

Ahora bien, de todo lo expuesto, la primera conclusión que se extrae se refiere a la necesidad de regular la IA y su impacto en los distintos ámbitos del Derecho, y al respecto tenemos que ser conscientes de que la IA solo puede avanzar y nunca ir hacia atrás, dependiendo solo de nosotros saber utilizar sus ventajas y limitar los efectos perjudiciales, que no son pocos⁹⁸. Regular y, en su caso, limitar y controlar dichos ámbitos produce dos efectos entre ellos interrelacionados.

En primer lugar, la institución de un marco normativo representa una garantía para el ciudadano tanto frente a las empresas que se han convertido en las propietarias, en las dueñas de los datos, como frente al correcto ejercicio de los poderes públicos que utilizan cada vez más estas herramientas. Y en segundo lugar, de esta forma, se pone en marcha un interesante proceso de progresiva transformación del modelo de Estado, que se convierte, en palabras de BARRIO, en un «Estado algorítmico de Derecho»⁹⁹, basado en la regulación de los sistemas

98 BARONA VILAR, S., «Inteligencia Artificial o la Algoritmización de la vida y de la justicia: ¿solución o problema?», *Rev. Boliv. de Derecho*, cit., p. 46.

99 BARRIO ANDRÉS, M., «Retos y desafíos del Estado algorítmico de Derecho», *Análisis del Real Instituto Elcano (ARI)*, 82, 9.6.2020.

caracterizados por la presencia de procesos, que incluyen la IA así como otras técnicas de automatización.

Ahora bien, el proceso de normativización de este espacio y de su impacto transversal en todos los aspectos de nuestras vidas requiere alcanzar una ponderación equilibrada de los distintos intereses en juego. Este proceso necesita antes una fase de reflexión en la que replantear las principales categorías jurídicas en clave algorítmica, a través del juicio de compatibilidad de los mecanismos de IA al marco constitucional, bajo el test de proporcionalidad. Solo de esta forma, se pueden alcanzar soluciones de síntesis, que faciliten el acercamiento recíproco de la IA al Derecho y del Derecho a la IA, en un proceso circular de retroalimentación mutua. Por otra parte, esta reformulación tiene que ser multinivel.

Por todo ello, ya no son suficientes ni los instrumentos de autorregulación, los «códigos de conductas» adoptados por las empresas privadas, las cuales producen y explotan los mecanismos de IA, no teniendo por lo tanto interés en una normativa que los pueda limitar, ni los instrumentos de *soft law*, como la Carta Ética sobre el Uso de IA en los sistemas judiciales y su entorno de 2018, que si bien hayan contribuido a desarrollar el marco que podría convertirse en el punto de referencia de una futura ciber-justicia a nivel europeo, carecen de eficacia jurídica vinculante.

Por su parte, la adopción de la Propuesta de Reglamento de la UE para armonizar la IA, aunque representa el avance más importante en el proceso de recepción normativa de un ámbito tan complejo, deberá ser sometido a un proceso de negociación, que podrá prolongarse entre uno y tres años. Mientras tanto, los Estados tienen que seguir adaptándose a este nuevo contexto de forma simultánea aunque coordinada con los ámbitos supraestatales, siendo cada vez más necesaria la interacción entre los distintos niveles de regulación, al fin de crear una conciencia común que sienta las bases para reformas amplias y transversales.

En cuanto al ámbito interno, iniciativas como la propuesta francesa de Ley Constitucional sobre la Carta de IA y Algoritmos n. 2585 del 15 de enero de 2020¹⁰⁰ son positivas para avanzar en este proceso, aunque ahora ya se advierte la necesidad de una mayor concreción, dando un paso más incisivo. Italia por ejemplo en la Ley n. 205/2021 de 3 de diciembre ha suspendido la instalación y la utilización de herramientas de video-vigilancia con sistemas de reconocimiento facial que usan datos biométricos en lugares públicos o abiertos al público por parte de autoridades públicas o sujetos privados hasta que se regule dicha materia y de todas formas no más allá del 31 de diciembre de 2023, a la espera del Reglamento de la UE¹⁰¹. Se trata sin duda de un importante avance.

100 *Proposition de loi constitutionnelle n. 2585 relative à la Charte de l'intelligence artificielle et des algorithmes* Enregistré à la Présidence de l'Assemblée nationale le 15 janvier 2020 (https://www.assemblee-nationale.fr/dyn/15/textes/l15b2585_proposition-loi).

101 *Legge 3 dicembre 2021, n. 205, conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di*

Por lo que se refiere a España, la Declaración de Derechos Digitales ha constituido el paso previo hacia la adopción de una regulación en términos estrictos. En la misma línea, merece una valoración positiva la LO 7/2021, que, reformando la LOPJ, se ocupa de los datos personales objeto de tratamiento automatizado en las distintas fases de la justicia penal¹⁰². Dicha Ley ha llegado tras la condena del TJUE a España con sentencia de 25 de febrero de 2021 asunto C658/19¹⁰³, por haber incumplido el plazo de transposición de la Directiva (UE) 2016/680, no haber comunicado esas disposiciones a la Comisión Europea y haber persistido en ello.

Por su parte, el Anteproyecto de ley de eficiencia digital del servicio público de justicia, por la que se incorpora al ordenamiento jurídico español la Directiva UE 2017/1131 sobre la utilización de herramientas y procesos digitales en el ámbito del derecho de sociedades¹⁰⁴, aunque manifieste el compromiso de España para adaptar la administración de justicia a la nueva dimensión tecnológica, tal y como ha sido redactado y planteado, presenta una serie de cuestiones, que deberían ser revisadas, como el Consejo General del Poder Judicial (CGPJ) ha puesto correctamente de relieve¹⁰⁵.

Nadie discute la necesidad de introducir modelos y técnicas de IA a la tramitación electrónica de los procedimientos judiciales y en particular al dictado de las resoluciones judiciales, puesto que la tutela judicial efectiva no puede comprenderse desconectada de la realidad¹⁰⁶. No obstante, su recepción requiere considerar y medir la «oportunidad», habida cuenta del «estado tecnológico y procesal», pero también «normativo» actual, y la compatibilidad con los principios *ex arts.* 117 CE y 24.1 CE. Tales preceptos imponen establecer los debidos controles, realizar las evaluaciones pertinentes y fijar un conjunto de garantías para la correcta configuración, el uso y el éxito de dichos mecanismos en el desarrollo de la función

pubbliche amministrazioni e in materia di protezione dei dati personali (GU Serie Generale n. 291 del 7.12.2021). No obstante, el art. 9, co. 12, de dicha Ley relativo a la protección de datos personales establece una excepción a la prohibición en los siguientes casos: «*I commi 9, 10 e 11 non si applicano ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018*».

102 *Vid.* en particular los arts. 13 y 14 de la LO 7/2021. Sobre dicha medida, véase ESPARZA LEIBAR, I., «Derecho fundamental a la protección de datos de carácter personal en el ámbito jurisdiccional e inteligencia artificial. En especial 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», en CALAZA LÓPEZ, S. y LLORENTE SÁNCHEZ-ARJONA, M. (dirs.), *Inteligencia artificial legal y administración de justicia*, cit., pp. 181-209.

103 STJUE, de 25 de febrero de 2021, *Comisión Europea c. Reino de España*, asunto C 658/19, ECLI:EU:C:2021:138.

104 OJ L 186, 11.7.2019.

105 Acuerdo adoptado por el Pleno del CGPJ en su reunión del día 24 de febrero de 2022, Informe del CGPJ al Anteproyecto de la Ley de Eficiencia Digital.

106 *Vid.* art. 57 Anteproyecto de la Ley de Eficiencia Digital y ap. 51 del Informe del CGPJ.

jurisdiccional, a fin de salvaguardar su ejercicio, que se encuentra «consustancial y ontológicamente anudad[o] a la naturaleza humana, con independencia, imparcialidad, exclusividad y con exclusivo sometimiento al imperio de la ley»¹⁰⁷.

Desde el punto de vista de la oportunidad, no se puede soslayar que se trata de un ámbito que podríamos calificar, tal y como ha sido indicado por la Comisión Europea en la PRIA, de «alto riesgo», lo cual conlleva la necesidad de que tales sistemas reúnan determinados requisitos y sean sometidos a adecuadas comprobaciones. Por ello, si no se quiere esperar que la UE adopte la PRIA, se deberían por lo menos atender las pautas contenidas en la Propuesta de Reglamento, para no tener que volver a adaptar a posteriori este ámbito, tan complejo y de primaria importancia para la protección de todos los demás derechos fundamentales.

El auspiciado objetivo de la «vertebración» de la tecnología en el proceso requiere una ponderación equilibrada, no se puede tensionar la función jurisdiccional de forma excesiva y sin límites, arriesgando convertirla «en una mera actividad tecnológica alejada de los principios estructurales del proceso, que se verían desplazados». Dicho en otros términos, el proceso no debería plegarse y someterse a la tecnología, todo lo contrario estos recursos deberían adquirir una función instrumental, apoyando pero no reemplazando la actividad humana¹⁰⁸.

En segundo lugar, es clave su recepción en los distintos espacios de protección de los derechos fundamentales. En dicho marco, la adopción de la PRIA impulsaría de forma extraordinaria la incorporación de la IA en los ordenamientos de los Estados miembros y también representaría un ejemplo para los Estados terceros.

Y por último, por lo que se refiere a la regulación en los ordenamientos internos de los Estados de la UE, se considera que el reconocimiento constitucional de la IA sería oportuno, puesto que otorgaría un plus de tutela. Además, dicha reforma debería contener una referencia explícita al impacto en la justicia. En este sentido, se comparte con F. BALAGUER CALLEJÓN la necesidad de introducir una «Constitución del Algoritmo», que impulse la regulación y el desarrollo de la IA, adaptando el ordenamiento y fijando los principios a los que tiene que conformarse. La «Constitución del algoritmo» debe entenderse «en el doble sentido de constitucionalizar el algoritmo y de digitalizar la Constitución»¹⁰⁹, como la

107 Informe del CGPJ n. VII, Conclusión novena.

108 En los apartados 137 y 138 del Informe del CGPJ se critica el art. 35 del Anteproyecto, donde se prevé que el uso de SIC orientado al dato permita o facilite «la aplicación de técnicas de inteligencia artificial para los fines anteriores u otros que sirvan de apoyo a la función jurisdiccional, a la tramitación y conclusión, en su caso, de procedimientos judiciales, y a la definición y ejecución de políticas públicas, de acuerdo con la ley». Al respecto, el CGPJ ha considerado esta previsión como «una habilitación en blanco para el empleo de técnicas de inteligencia artificial con incidencia en la tramitación de los procesos y el ejercicio de la función jurisdiccional», que revela un entendimiento de la aplicación de las técnicas de inteligencia artificial en el ámbito jurisdiccional acrítico o no problemático que dista mucho de ser la aproximación adecuada a esta cuestión.

109 BALAGUER CALLEJÓN, F., «La Constitución del Algoritmo. El difícil encaje de la Constitución analógica en el mundo digital», GOMES, A.; ALBERGARIA, B. y CANOTILHO, M. (Coord.), *Direito*

base desde las que partir si se quiere controlar estos factores de poder y el eventual ejercicio prejudicial para los derechos fundamentales¹¹⁰.

La modificación del texto constitucional, en virtud de la cristalización de estos principios en la Ley superior del Estado y de la fuerza que esto le otorgaría tanto hacia los poderes públicos como hacia los particulares, permitiría adaptarla al nuevo contexto digital, en el que vivimos, y así evolucionar.

La previsión de la dimensión tecnológica tendría el objetivo de hacer frente a dichas amenazas, las cuales pueden atentar contra la democracia y los elementos constitutivos del Estado de Derecho, entre los que el derecho a la tutela judicial efectiva sigue representando la base, el centro del que dependen todos los demás. En la misma línea se apuesta por el desarrollo legislativo de la aplicación de la IA a la justicia, porque la dotaría de una mayor concreción y permitiría su aplicación práctica. No obstante, el afán para la modernización y la digitalización en aras a una supuesta eficacia y eficiencia¹¹¹ no puede ser a costa de los principios estructurales de nuestros ordenamientos.

TITLE: *The right to due process before the paradigm changes of AI*

ABSTRACT: *This study analyses how the effective judicial protection, which constitutes the heart of the justice system in the rule of law, is adapting to the irruption of artificial intelligence technologies. Therefore, after focusing on the roles and functions that algorithms can assume in the different phases of criminal justice, by virtue of their polybedral and multi-faceted character, it will reflect on the need for a European procedural statute of AI. To this end, it will consider why it is necessary to regulate the «algorithmic due process of law», which requires rethinking the basic categories of law, through compatibility judgement, and the state of the issue, referring to how it is progressively being regulated and especially to the Proposal for an EU Regulation on AI, adopted in April 2021, which aims to build an «ecosystem of guarantees».*

RESUMEN: *El presente trabajo analiza cómo la tutela judicial efectiva, que constituye el centro del sistema de justicia en el Estado de Derecho, se está adaptando a la irrupción de las tecnologías de inteligencia artificial. A tal fin, tras analizar los roles y las funciones que los algoritmos pueden asumir en las distintas fases de la justicia penal, en virtud de su carácter poliédrico y polifacético, se reflexionará sobre la necesidad*

Constitucional: diálogos en homenaje a 80.º aniversario de J. J. Gomes Canotilho, La Constitución del algoritmo. El difícil encaje de la constitución analógica en el mundo digital, Belo Horizonte: Fórum, 2021, pp. 1-14.

110 Sobre la IA como objeto constitucional, *vid.* SÁNCHEZ BARRILAO, J.F., *Inteligencia y seguridad como objeto constitucional. El CNI y la comunidad de inteligencia ante los nuevos retos de la sociedad del riesgo*, Madrid: CEPC, 2019. Del mismo autor, *vid.* también «El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional», *Estudios de Deusto*, vol. 64, n. 2, 2016, pp. 225-258; e *Id.*, «Los fundamentos del 'progreso informático' en la Unión Europea», *Revista de Derecho Político*, n. 98, 2017, pp. 335-368.

111 Al respecto BARONA VILAR, S., habla del proceso de liquefacción del modelo de justicia penal, «Mutación de la justicia en el siglo XXI. Elementos para una mirada poliédrica de la tutela de la ciudadanía», en BARONA VILAR, S., *Justicia poliédrica en periodo de mudanza: Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad*, Valencia: Tirant lo Blanch, 2022, pp. 31-62, o también de un proceso penal «líquido» o «liquidable», más cèlere pero también menos garantista, *Id.*, «Justicia penal líquida (desde la mirada de Bauman)», *Teoría y derecho: revista de pensamiento jurídico*, n. 22, 2017, pp. 64-91.

de un estatuto procesal europeo de la IA. Para ello, se centrará en las razones por las que es necesario regular el «due process of law algorítmico», lo cual exige repensar las categorías básicas del Derecho, a través del juicio de compatibilidad, y en el estado de la cuestión, haciendo referencia a cómo se está progresivamente regulando y especialmente a la Propuesta de Reglamento de la UE sobre la IA, adoptada en abril de 2021, cuyo objetivo es construir un «ecosistema de garantías».

KEY WORDS: *Algorithmic fair trial, artificial intelligence, «shared justice», rule of law, Proposal for an EU regulation on the harmonisation of AI.*

PALABRAS CLAVE: *Fair trial algorítmico, inteligencia artificial, justicia compartida, Estado de Derecho, Propuesta de reglamento de la UE para la armonización de la IA.*

FECHA DE RECEPCIÓN: 15.06.2022

FECHA DE ACEPTACIÓN: 20.09.2022

CÓMO CITAR / CITATION: Faggiani, V. El derecho a un proceso con todas las garantías ante los cambios de paradigma de la inteligencia artificial, *Teoría y Realidad Constitucional*, 50, 517-546.