IUS CRIMINALE

BOLETÍN DE DERECHO PENAL

Fecha: septiembre 2026
Edición: 11 - Volumen 3
FISCALÍA GENERAL DEL ESTADO
Dirección de Estudios Penales

QUITO - ECUADOR



ENTES FICTICIOS E IRRUPCIÓN TECNOLÓGICA

DEBATE JURÍDICO SOBRE EL DERECHO PENAL FRENTE A LAS NUEVAS REALIDADES

FGE

FISCALÍA GENERAL DEL ESTADO

ECUADOR

Boletín de Derecho Penal IUS CRIMINALE
FISCALÍA GENERAL DEL ESTADO

COMITÉ EDITORIAL

Dr. Carlos Leonardo Alarcón Argudo
Fiscal General del Estado (E)

Mtr. Ximena Coello Martínez
Coordinadora General de Gestión del Conocimiento

Abg. Paula Cisneros Espinosa
Directora de Estudios Penales

COMITÉ ACADÉMICO

Dirección de Estudios Penales

EQUIPO DE DISEÑO EDITORIAL ACADÉMICO

Dirección de Comunicación y Promoción Institucional

Mgs. Amelina Espinosa

Mgs. Andrés Lasso Ruiz

Quito, septiembre de 2026

Contenido de acceso libre.

Los criterios vertidos por los autores no comprometen la opinión institucional.

Todos los derechos reservados. Prohibida la reproducción total o parcial, sin autorización de los autores.

IUS CRIMINALE

BOLETÍN DE DERECHO PENAL

ÍNDICE

Desafíos probatorios de la tecnología *blockchain* en la investigación criminal contemporánea.....1

Hacia una teoría de la imputación penal algorítmica y un modelo de *compliance* tecnológico.....25

La IA como herramienta asistencial en el proceso penal español: potencial, riesgos y límites.....39

La respuesta del sistema judicial ante la inteligencia artificial: enfoque en el sector sanitario.....53



DESAFÍOS PROBATORIOS DE LA TECNOLOGÍA BLOCKCHAIN EN LA INVESTIGACIÓN CRIMINAL CONTEMPORÁNEA

Isabel M.ª Villar Fuentes[1]

1. Introducción

La eclosión de tecnologías disruptivas inherentes a la Cuarta Revolución Industrial representa un avance trascendental para la sociedad en todos sus ámbitos, abarcando desde la medicina y la industria hasta la propia Administración Pública y la Administración de Justicia. No obstante, este progreso tecnológico también ha sido instrumentalizado por la criminalidad, que, de forma recurrente, adapta y emplea estas nuevas herramientas para sus fines ilícitos. De hecho, la delincuencia organizada suele ser pionera en la adopción de innovaciones tecnológicas con el objetivo de perpetrar, ocultar y financiar delitos, así como para blanquear los capitales derivados de estos.

Este escenario impone a los Estados el desafío constante de actualizar sus mecanismos de persecución penal, garantizando en todo momento el escrupuloso respeto a las garantías procesales. En consecuencia, resulta imperativo que los ordenamientos jurídicos, tanto a nivel nacional como internacional, desarrollen marcos normativos capaces de equilibrar la eficacia en la investigación criminal con la salvaguarda del debido proceso.

El presente trabajo propone una reflexión analítica sobre la utilización de la tecnología *blockchain* (cadena de bloques) en diversas tipologías delictivas. Para ello, se formula una clasificación de los ilícitos perpetrados a través de estas plataformas, prestando especial atención al blanqueo de capitales y a la financiación del terrorismo. Ante la gravedad de estos delitos, la Unión Europea ya ha adoptado medidas normativas para regular los criptoactivos y establecer obligaciones a los proveedores de servicios, facilitando así su detección y persecución.

Finalmente, dado que las peculiaridades técnicas y operativas de *blockchain* generan notables obstáculos para la investigación y el enjuiciamiento, este estudio analiza las vías procesales de acceso a las fuentes de prueba en el sistema penal español.

1 Profesora Titular Derecho Procesal, Facultad de Derecho, Universidad de Cádiz, España.

2. Blockchain

Los antecedentes de esta tecnología fueron planteados por Haber y Stornetta en 1991 como un mecanismo para realizar un sellado de tiempo (*time stamp*) en documentos digitales. El reto principal consistía en estampar una marca temporal en los datos de forma independiente al soporte, garantizando la inalterabilidad de los documentos —impidiendo la modificación de un solo bit— y asegurando que fuera imposible registrar una fecha u hora distintas a las reales[2].

Aunque la tecnología *blockchain* nace estrictamente vinculada al ámbito financiero —en concreto, con el diseño de criptomonedas desarrollado por Nakamoto[3]—, rápidamente se ha revelado como una herramienta multifuncional, segura e inmutable. En esencia, *blockchain* funciona como un registro; no se limita a grabar una transacción aislada, sino que compila una secuencia completa e inalterable de las mismas. Por este motivo, se la define habitualmente como una "tecnología de libro de registro digital"[4] o como una base de datos descentralizada. Esta última está distribuida en diferentes ordenadores, estructurada en bloques enlazados mediante criptografía compleja, lo que permite organizar y proteger transacciones interrelacionadas[5].

Desde un punto de vista operativo, *blockchain* opera mediante algoritmos computacionales programados para autoejecutarse cuando se cumplen las condiciones preestablecidas. La arquitectura de esta cadena de bloques permite prescindir de terceros de confianza, ya que los archivos no se almacenan en servidores externos, sino que la base de datos se distribuye entre los distintos terminales (nodos) que componen la red.



2 Stuart Haber y W. Scott Stornetta, "How to Time-Stamp a Digital Document", *Journal of Cryptology* 3, n.º 2 (1991), 99.

3 Juan Pablo Valencia Ramirez, "Derecho, tecnologías e innovación: blockchain y contratos inteligentes", *Revista de Investigación en Tecnologías de la Información Journal* 8 (julio-diciembre 2020), 47.

4 Letícia Melo, "Régimen jurídico de blockchain: una prueba atípica", *Revista de Bioética y Derecho Perspectivas Bioéticas*, n.º 468 (julio-diciembre 2020), 105.

5 Juan Jorge Almonacid Sierra y Yeisson Coronel Ávila, "Aplicabilidad de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado", *Revista de Derecho Privado, Universidad Externado de Colombia*, n.º 38 (enero-junio 2020), 132.

La base de datos de *blockchain* se aloja en distintos terminales denominados nodos, en función de los agentes involucrados en la operación desarrollada con esta tecnología, bien por ser partes, bien por ser terceros interesados en la información (tal es el caso de los registros públicos en *blockchain*). Dicha base de datos está compuesta por bloques de premisas / condiciones / estipulaciones. Se habla de bloques pues podríamos decir que se encuentran compactadas cada una de ellas en un eslabón. La premisa de cada eslabón debe perfeccionarse para que pueda ser cerrada, sin posibilidad de ser alterado su contenido, con carácter de inmutabilidad y, a la vez, abrirse un siguiente eslabón con otra premisa consecuente a la anterior y así de forma sucesiva.

El cierre de cada uno de estos eslabones (bloques) solo se produce bajo dos condiciones: en primer lugar, si la premisa / condición / estipulación se perfecciona por el nodo autorizado para operar, y, en segundo lugar, si la labor de verificación certifica tal perfeccionamiento, esta función corresponde a los nodos autorizantes. Solo entonces cuando se ha producido este control, el eslabón (bloque) se cierra y a través de un enlace se vincula al siguiente, momento en el que se abre para proceder a la siguiente operación. El modo de proceder estos eslabones / bloques sucesivos, responde al patrón *if* ("si" condicional), si sucede y se verifica la acción del primer bloque, *then* (entonces) se abre el siguiente.

Dicho esto, hay que analizar cómo se materializan estas dos condiciones expuestas. En primer lugar, la realización de la premisa / condición / estipulación se debe perfeccionar en el bloque donde está diseñada y prevista por parte del nodo autorizado para operar (por ejemplo, la llegada de una mercancía a un punto determinado). El nodo autorizado perfecciona la premisa con su clave privada, y a través de la clave pública incorpora la misma a la cadena de bloques. Esta primera condición queda registrada en el eslabón correspondiente, de modo que ese bloque contiene la información de la fecha y hora de la misma, mediante un sellado de tiempo, que genera un *hash* (código alfanumérico).

Pero no es suficiente tal registro para que pueda quedar cerrado ese bloque, sino que precisa de las verificaciones de los nodos autorizantes. Estos nodos autorizantes componen la red entre iguales P2P (*peer to peer)* que verifican y aprueban todas y cada una de las transacciones[6]. La red de nodos autorizantes comprueba y certifica las operaciones realizadas por las partes en cada bloque, y comprueba que el *hash* generado no se ha modificado a través de códigos encriptados, que solo se cierran tras producirse la verificación de todos ellos (todos los nodos autorizantes). Solo cuando esto sucede queda cerrado el bloque y permite abrir el siguiente.

Esta labor de los nodos autorizantes o verificadores, que, en el caso de bitcoin, recibe coloquialmente el nombre de *minería*, es costosa[7], pues son necesarios muchos mineros que, a la vez, obtienen unos ingresos por esa labor de comprobación y certificación. Sin embargo, la verificación, no siempre está planteada con multitud de nodos autorizantes, ni de forma retribuida[8]. Esta cuestión viene condicionada por el carácter público, privado o semipúblico de la cadena de bloques, así como por el hecho de ser autorizada (*permissioned*) o no.

6 Alex Tapscott y Don Tapscott, *La revolución del BLOCKCHAIN. Descubre cómo esta nueva tecnología transformará la economía global* (Barcelona: Deusto, 2016), 24 y ss.

7 Mads Von Haller Grønbæk, "Blockchain 2.0, Smart contracts and challenges", Computers & Law, The SCL Magazine (junio/julio 2016), 2. "Las comisiones de la minería son denominadas fees y son calculadas, no por la cuantía de bitcoin transaccionada sino por los bytes que ocupan en blockchain. Este sistema de comisiones utilizado por bitcóin es el que se utiliza también por otras plataformas de criptomoneda como son Ethereum o Litecoin".

8 Javier Ibáñez Jiménez, *Consorcio Red Alastria (Origen y reforma de la primera blockchain de España)* (Madrid: Editorial Reus, 2020), 15-20. "Se trata de la primera blockchain o red de registros distribuidos nacional creada en el mundo de forma colaborativa por multitud de instituciones, organizaciones y empresas con el propósito de realizar operaciones e intercambiar datos, y experimentar con la tecnología de registro distribuido, en un ámbito de país. Esta red está tiene el carácter de asociación de derecho privado sin ánimo de lucro".

3. Clases de blockchain

Se pueden distinguir tres tipos principales de cadenas de bloques, en función de las posibilidades de acceso de terceros en ellas y de los permisos que permiten la intervención en las mismas.



3.1. Cadenas de bloques públicas

Las cadenas de bloques públicas se caracterizan por el libre acceso, de modo que no se puede ocultar ninguna de las operaciones y son autorizadas o libres; cada nodo está autorizado para realizar las operaciones pertinentes y funcionan por un "depósito de confianza en los nodos autorizantes (validadores) de quienes promuevan las transacciones que contienen los datos que se registran"[9].

Dentro de las cadenas de bloques públicas, sin embargo, se encuentran algunas no autorizadas, como es el caso de las utilizadas en las criptomonedas. Por ejemplo, Bitcoin o Ethereum, en estas cadenas la labor de los nodos autorizantes (mineros) es cuantiosa y remunerada.

3.2. Cadenas de bloques privadas

Encontramos también las cadenas de bloques privadas, donde el acceso está restringido a unos nodos autorizados que son los únicos que pueden realizar transacciones. Estas cadenas son las que habitualmente son utilizadas por las cadenas de suministro y el almacenamiento de datos. Un ejemplo de ellas es Morpheus Network[10], la cual es una cadena de suministro con tecnología *blockchain* y sustentada a través de contratos inteligentes. Morpheus Network combina las cadenas privadas que, a la vez, se integran en una cadena global pública y autorizada. Se encuadra en el sistema de cadena de bloques privada, de tal modo que los usuarios deben estar autorizados por la red de *blockchain* y solo pueden entrar si reciben invitación. Una gran ventaja de las cadenas de bloque privadas es que los participantes en la misma se encuentran en una "lista blanca" que obvia la necesidad de la minería y sus costes[11].

9 Javier Ibáñez Jiménez, *Consorcio Red Alastria (Origen y reforma de la primera blockchain de España)*, 16.

10 Puede ser consultado en https://morpheus.network/.

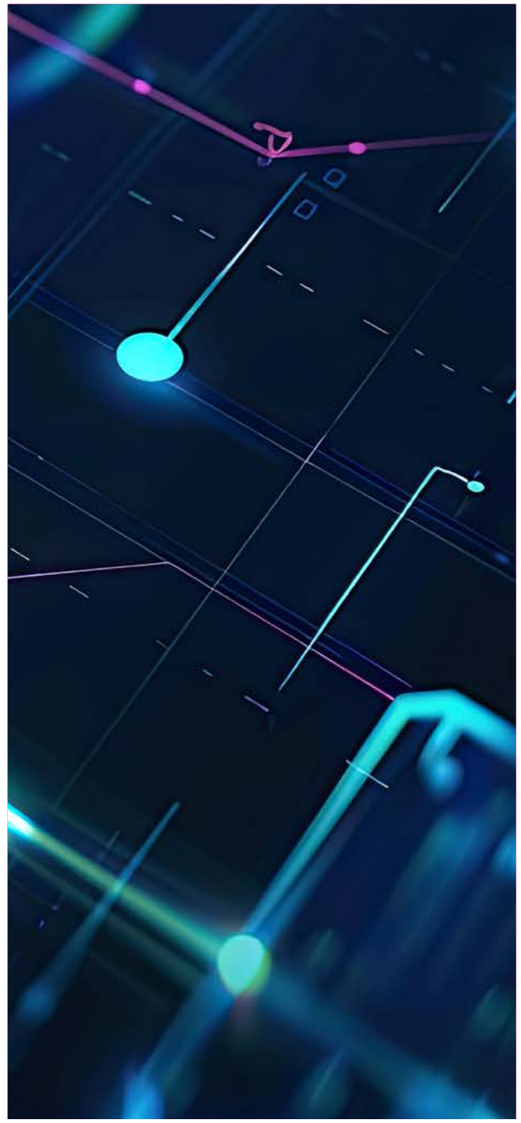
11 Juan Pablo Valencia Ramírez, "Derecho, tecnologías e innovación: blockchain y contratos inteligentes", 48. "Las Blockchain privadas donde los participantes están en una 'lista blanca', no se necesitan mecanismos de consenso costosos como la prueba de trabajo; no existe el riesgo de un ataque Sybil, de esta forma se elimina la necesidad de un incentivo económico para la minería y posibilita una gama más amplia de protocolos de consenso para elegir".

Los usuarios interactúan con la cadena a través de unos nodos, utilizando una clave privada para firmar su operación, que al finalizarla es redirigida a la red con su clave pública. Al entrar en la red con la clave pública, la operación firmada con la clave privada conecta con su *peer* y comprueba su validez[12]. La certeza del origen, la autenticación y la integridad del contenido firmado con la clave privada quedan garantizadas con la criptografía[13], solo entonces queda incorporada la operación u operaciones[14], que se hayan acordado previamente al bloque, el cual se cierra y genera un sellado en el tiempo.

3.3. Cadenas de bloques mixtas

Por último, la versión mixta son las cadenas públicas (*permissioned blockchain*), las cuales solo dan acceso a determinados nodos para realizar transacciones, a la vez que no ocultan las mismas.

4. Características de *blockchain*



4.1. Autoejecutable

La tecnología de cadena de bloques se programa, tal y como hemos visto, para que cada uno de sus bloques se ejecute, conforme se cierra el anterior. Esta característica es especialmente notable en los "contratos inteligentes", donde se produce una "ejecución automática e instantánea una vez se ha cumplido la condición desencadenante de esa ejecución, los convierten en contratos

12 Konstantinos Christidis y Michael Devetsikiotis, "Blockchains and Smart contracts for the IoT", IEEE Access 4 (2016), 2293. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), 3, https://bitcoin.org/bitcoin.pdf. Se señala que los pasos para hacer funcionar la red son los siguientes: "1) Las nuevas transacciones se difunden a todos los nodos; 2) Cada nodo recopila las nuevas transacciones en un bloque; 3) Cada nodo trabaja para encontrar una prueba de trabajo difícil para su bloque; 4) Cuando un nodo encuentra una prueba de trabajo, difunde el bloque a todos los nodos; 5) Los nodos aceptan el bloque solo si todas las transacciones que contiene son válidas y no se han gastado ya; 6) Los nodos expresan su aceptación del bloque trabajando en la creación del siguiente bloque en la cadena, utilizando el hash del bloque aceptado como hash anterior. Los nodos siempre consideran que la cadena más larga es la correcta y seguirán trabajando para extendiéndola. Si dos nodos difunden simultáneamente versiones diferentes del siguiente bloque, algunos nodos pueden recibir uno u otro primero. En ese caso, trabajan en la primera que han recibido, pero guardan la otra rama por si se alarga. El empate se romperá cuando la siguiente prueba de trabajo y una de las ramas se haga más larga; los nodos que estaban trabajando en la otra rama cambiarán a la más larga" (disponible en: https://bitcoin.org/bitcoin.pdf, consultado el 15/12/2022) (traducción hecha por la autora).

13 Juan Jorge Almonacid Sierra y Yeisson Coronel Ávila, "Aplicabilidad de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado", 133. Afirman que "la criptografía es uno de los elementos esenciales de la tecnología blockchain y consiste en un procedimiento algorítmico con clave mediante la cual se transforma un mensaje en secreto, descifrable mediante una clave del algoritmo empleado".

14 Konstantinos Christidis y Michael Devetsikiotis, "Blockchains and Smart contracts for the IoT", 2293. Los nodos que realizan la comprobación y devuelven al bloque la operación verificada criptográficamente son denominados vulgarmente mineros.

automáticos y autónomos, pues no precisan de mayor intervención humana que la inicial aceptación de las condiciones pactadas"[15].

4.2. Inmutable

La inmutabilidad de *blockchain* se sustenta en la ventaja, referida *supra*, que supone la desaparición de operadores intermedios que tengan que verificar cada una de las operaciones o transacciones que se vayan realizando. No es precisa la intervención de terceros, no hay intermediarios, sino que las transacciones se llevan a cabo entre las partes involucradas *peer to peer* (P2P), lo cual supone un valor para la formalización de contratos.

A su vez, es inmutable, pues cada una de las transacciones registradas, por los nodos autorizados genera un *hash* inalterable. La inmutabilidad viene respaldada por el procedimiento que otorga seguridad de los nodos autorizantes o verificadores. El *hash* es verificado por los nodos autorizantes que, mediante cifrados criptográficos comprueban que el *hash* no se ha modificado y solo entonces se cierra el bloque que permite la apertura del siguiente. Al estar conectados cada uno de los bloques por un enlace que provoca la apertura del ulterior, cuando el que le antecede se cierra tras la verificación, tiene el carácter de autoejecutable, sin posibilidad de interferir en la ejecución del mismo.

4.3. Descentralizada

Se trata de una tecnología descentralizada, pues no existe una autoridad (tercero) que aloje y administre las operaciones, sino que estas se encuentran en la propia cadena, a la cual tienen acceso todos sus nodos. Los controles de verificación se llevan a cabo por los nodos autorizantes, con una tecnología *peer to peer* (P2P). El carácter de tecnología descentralizada se sustenta también en el hecho de tener acceso, todos los nodos, a toda la información de la cadena de bloques; de ahí el concepto de "registro". Por esta razón, *blockchain*, ya lo hemos señalado, es conocida también como "libro de registros", pues sin un tercero que almacene y certifique los contenidos, la propia cadena los alberga en cada uno de sus bloques. El "libro de registros", a su vez, tiene una copia en todos y cada uno de los nodos (terminales) que participan en la cadena de bloques, tanto como autorizados, como autorizantes. Estos rasgos distintivos de las cadenas de bloques le otorgan un potencial de explotación y aprovechamiento en todos los ámbitos, al cual le queda mucho recorrido y que precisa de una normativa que lo regule de forma cohesionada, evitando las fragmentaciones.

4.4. Anónima o pseudoanónima

La cadena de bloques vemos que es un "libro de registros", de modo que cualquier usuario de la misma tiene acceso en cualquier momento a todas las transacciones realizadas. Esta característica parece colisionar con un eventual anonimato de los nodos, pero la trazabilidad de las operaciones realizadas por cada uno de ellos no alcanza la rastreabilidad de su identidad personal.

15 Sonia Calaza López, "Blockchain y Smart contracts: ¿un ecosistema digital seguro al margen de la ley?", en *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, dirigido por Ignacio Colomer Hernández (Pamplona: Thomson Reuters Aranzadi, 2022), 238.

La huella que permanece en *blockchain* es la de la clave pública, mientras que la clave privada solo es conocida por el titular. Sin embargo, se puede hablar de "pseudoanonimato", pues en los casos de transacciones sospechosas, el uso de un *software* podría permitir enlazar el número clave con la identidad del inversor[16].

5. Marco normativo

5.1. Unión Europea

5.1.1. Identificación electrónica y servicios de confianza

El sellado en el tiempo que realiza en *blockchain*, en cada una de las operaciones efectuadas por los nodos autorizados puede suponer una evidencia de la ejecución de las mismas. El *time stamp* identifica el nodo autorizado que la realiza y el momento exacto en el cual se produce. Esta cuestión plantea un eventual papel relevante a nivel probatorio. Por esta razón, se ha planteado la posible equiparación del sellado en el tiempo de *blockchain* y la firma cualificada del Reglamento 910 / 2014 eIDAS[17].

El Reglamento eIDAS supone un cambio importante en el ámbito probatorio, pues atribuye

> [...] a los documentos electrónicos para cuya producción o comunicación se haya utilizado un servicio de confianza cualificado una ventaja probatoria. A este respecto, se simplifica la prueba, pues basta la mera constatación de la inclusión del citado servicio en la lista de confianza de prestadores cualificados de servicios electrónicos regulada en el artículo 22 del Reglamento 910 / 2014.[18]

La cuestión que se plantea es si es posible una equiparación del valor probatorio de los documentos electrónicos realizados con un servicio de confianza del Reglamento eIDAS con el sellado en el tiempo de la cadena de bloques. Los Estados miembros de la Unión Europea no tienen una postura uniforme en esta cuestión, la ausencia de servicios de certificación de confianza (debido a la descentralización) en *blockchain* es un óbice, para algunos Estados que están examinando el cumplimiento de garantías de esos servicios de sellado en *blockchain*.

Es el caso de Francia, que no es partidaria de regular *blockchain* como prueba debido a las dudas sobre su validez, al no contar con un tercero servidor de confianza, pero sí permite a los jueces evaluar por sí mismos el valor probatorio de estos datos, confirmando así que su naturaleza digital no puede ser la única razón para rechazarla[19]. Otros Estados miembros tienen posturas intermedias y están estudiando la posibilidad

16 Giovanni Paolo Accinni, "Cybersecuriti e criptovalute. Profili di rilevanza penale dolo la Quinta Direttiva", *Sistema Penale*, fascicolo 5 (2020), 213.

17 Reglamento (UE) 910 / 2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 sobre identificación electrónica y servicios de confianza para las transacciones electrónicas (eIDAS).

18 España, Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, *Boletin Oficial del Estado* 298, 12 de noviembre de 2020, sección III. En virtud de este Reglamento, en España la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, en su artículo 3, Efectos jurídicos de los documentos electrónicos establece: "1. Los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable. 2. La prueba de los documentos electrónicos privados en los que se hubiese utilizado un servicio de confianza no cualificado se regirá por lo dispuesto en el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Si el servicio fuese cualificado, se estará a lo previsto en el apartado 4 del mismo precepto".

19 Así lo establece el Reglamento 910 / 2014 "eIDAS" en su artículo 35: "1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado".

de reconocer los efectos de documento electrónico con servicios de confianza a los datos con sellados en el tiempo de *blockchain*[20].

La homologación, de *blockchain* con la firma electrónica cualificada y la equiparación de sus estándares de calidad y fiabilidad sí ha sido reconocida en Italia en la Ley 12 / 19[21]. Italia equipara el tratamiento jurídico de los sellos en el tiempo de los libros de contabilidad distribuidos como *blockchain* con los sellos de tiempo electrónicos definidos por el "eIDAS"[22].

5.1.2. Tecnologías de registro descentralizado

Ante el elevado número de transacciones realizadas con base en *blockchain*, la Unión Europea ha publicado el Reglamento de Tecnologías de Registro Descentralizado[23]. Este reglamento define las tecnologías de registro descentralizado como "una tecnología que permite el funcionamiento y el uso de registros descentralizados" y el registro descentralizado como "un repositorio de información que lleva registros de operaciones y se comparte a través de un conjunto de nodos de red TRD y está sincronizado entre dichos nodos, utilizando un mecanismo de consenso"[24].

El Reglamento de Tecnologías de Registro Descentralizado (TRD) destaca, entre las finalidades del mismo, garantizar "la continuidad y la transparencia, disponibilidad, fiabilidad y seguridad continuas de sus servicios y actividades, incluida la fiabilidad de los contratos inteligentes utilizados en la infraestructura del mercado basada en la TRD"[25].

En esta línea, en 2018, la Comisión cooperó en el establecimiento de una Infraestructura Europea de Servicios de *Blockchain* (EBSI)[26] y reconoció la importancia de la seguridad jurídica y de un régimen normativo claro en áreas relacionadas con las aplicaciones basadas en cadenas de bloques. De este modo, actualmente está desarrollando un marco legal favorable a la innovación en las áreas de activos digitales, *tokenización*[27] y

20 España, Alemania o Inglaterra se encuentran en fase de análisis, para reconocer a los datos en la cadena de bloques, la eficacia de documento electrónico realizado con servicios de confianza, aunque reconocen la viabilidad de ser introducidos como prueba y la evaluación judicial de su valor probatorio o el modo de verificarlos de forma cualificada.

21 Ley 11 de febrero de 2019, n. 12: "el almacenamiento de un documento informático a través del uso de tecnologías basadas en registros distribuidos, produce los efectos legales de la validación electrónica del tiempo de conformidad con el art. 41 del Reglamento de la UE n.° 910 / 2014".

22 Omar Puertas Álvarez, Oriol Valentí i Vidal y Laura Díaz Vallespinós, "Unlocking Blockchain Evidence in International Arbitration", *Spain Arbitration Review, Revista del Club Español del Arbitraje*, n.º 43 (2022), 20.

23 Reglamento (UE) 2022 / 858 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) n.º 600 / 2014 y (UE) n.º 909 / 2014 y la Directiva 2014 / 65 / UE. El Reglamento 2022 / 858 es de aplicación desde el 23 de marzo 2023, aunque algunos apartados del art. 8 lo son de aplicación desde el 22 de junio 2022.

24 Art. 2, apartados 1) y 2) del Reglamento de Tecnologías de Registro Descentralizado 2022/858. Este art. 2, en sus apartados 3), 4) y 5) plantea otras definiciones de interés sobre estas tecnologías basadas en blockchain: "3) 'mecanismo de consenso': las normas y procedimientos mediante los cuales se llega a un acuerdo de validación de una operación entre los nodos de red TRD; 4) 'nodo de red TRD': un dispositivo o proceso que forma parte de una red y que posee una copia completa o parcial de los registros de todas las operaciones en un registro descentralizado; 5) 'infraestructura del mercado basada en la TRD': un sistema multilateral de negociación basado en la TRD, un sistema de liquidación basado en la TRD o un sistema de negociación y liquidación basado en la TRD."

25 Reglamento de Tecnologías de Registro Descentralizado 2022/858, pág. 3.

26 European Blockchain Services Infrastructure, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home. La Comisión en el marco del Observatorio y Foro Blockchain de la UE crea la Asociación Europea de Blockchain (EBP), y coopera en el establecimiento de una Infraestructura Europea de Servicios de Blockchain (EBSI) el 10 abril 2018 UE y Noruega, posteriormente se unieron 8 países más. La infraestructura europea de servicios de blockchain (EBSI) consiste en una red peer-to-peer de nodos interconectados que ejecutan una infraestructura de servicios basada en blockchain. Cada miembro de la European Blockchain partnership (EBPS), los 27 países de la UE, Noruega, Liechtenstein y la Comisión, ejecutará al menos un nodo.

27 Sergio Nasarre Aznar, "Naturaleza jurídica y régimen civil de los 'token' en 'blockchain'", en *La tokenización de bienes en blockchain: Cuestiones civiles y tributarias*, coordinado por Rosa María García Teruel (Pamplona: Thomson Reuters Aranzadi, 2020), 47. Rosa María García Teruel, coord., *La tokenización de bienes en blockchain: Cuestiones civiles y tributarias* (Pamplona: Thomson Reuters Aranzadi, 2020), 77. Hace referencia a la flexibilidad de nuestro ordenamiento civil para que todo lo susceptible de tener valor económico, disponible y transmisible, sea patrimonializado

contratos inteligentes que protege a los consumidores y brinda seguridad jurídica a las empresas. La Comisión apoya firmemente un marco paneuropeo que espera evitar la fragmentación legal y reglamentaria.

5.1.3. Blanqueo de capitales y financiación terrorismo a través de *blockchain* (criptomonedas)

La Directiva 2018 / 843 para la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, consciente de la necesidad de combatir tanto el blanqueo de capitales como la financiación del terrorismo en el entorno de las criptomonedas, incluye las monedas virtuales en su regulación, las cuales son definidas como

> [...] representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos.[28]

De igual modo, se refiere al "proveedor de servicios de custodia de monederos electrónicos: una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales"[29].

La Directiva 2018 / 843 establece una obligación específica, en aras de la persecución del blanqueo de capitales y financiación del terrorismo a los servicios centralizados prestadores de servicios. El art. 18 bis de esta Directiva fija, a estos operadores, las siguientes obligaciones:

> a) obtención de información adicional sobre el cliente y el titular o titulares reales; b) obtención de información adicional sobre el propósito y la índole prevista de la relación de negocios; c) obtención de información sobre la procedencia de los fondos y la fuente de ingresos del cliente y del titular o titulares reales; d) obtención de información sobre los motivos de las transacciones previstas o realizadas; e) obtención de la aprobación de los órganos de dirección para establecer o mantener la relación de negocios.[30]

En esta línea, viene a colación destacar también la Directiva *Whistelblowing*[31], pues enfatiza el importante papel que juegan "las personas que trabajan para una organización pública o privada o están en contacto con ella en el contexto de sus actividades laborales" por ser "a menudo las primeras en tener conocimiento de amenazas o perjuicios para el interés público"[32]. En el art. 2.1. *ii*) de esta Directiva se incluyen las denuncias referidas a "servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo", dentro del ámbito de aplicación de la misma.

y por ende pueda ser tokenizado." Los tokens pueden representar derechos sobre tipos de activos patrimoniales, tanto digitales, como físicos, haciéndolos fácilmente transmisibles y rastreables; lo que no puede hacer es crearlos, porque su creación depende del Derecho (art. 1089 CC para las fuentes de obligaciones y art. 609 CC)".

28 Unión Europea, Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, Diario Oficial de la Unión Europea L 156, 19 de junio de 2018, art. 1.2.d).

29 Unión Europea, Directiva (UE) 2018/843, art. 1.2.d).19).

30 Unión Europea, Directiva (UE) 2018/843, art. 1.11.1.

31 Directiva (UE) 2019 / 1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

32 Considerando (1) Directiva 2019 / 1937.

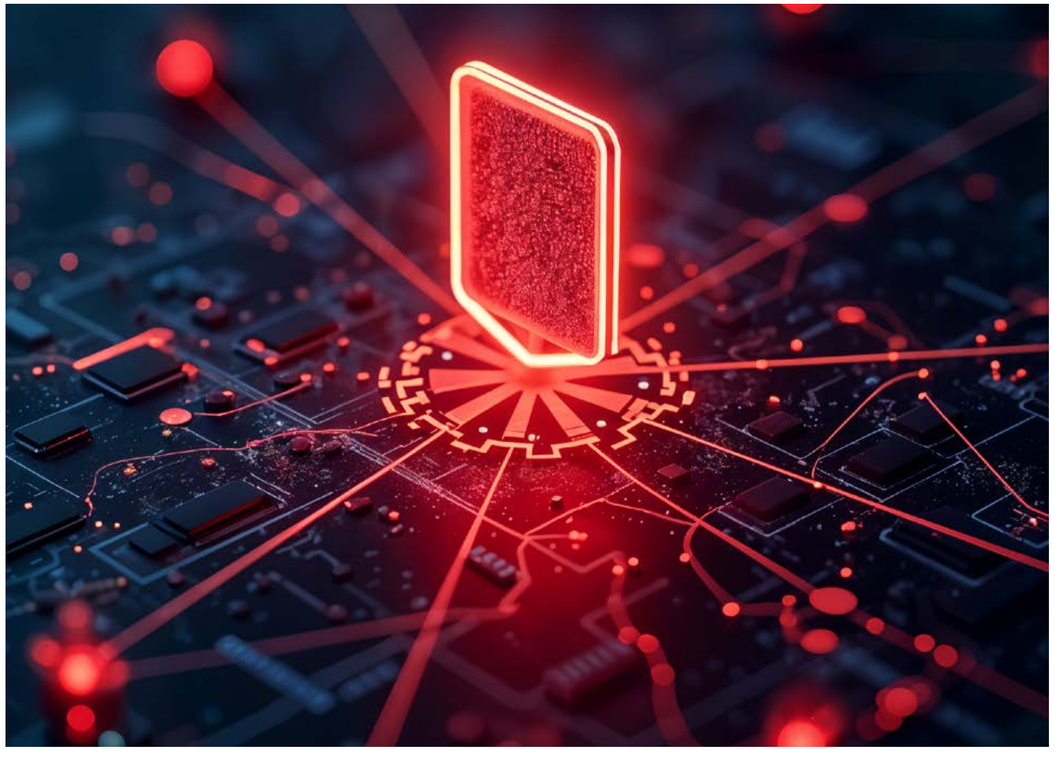
5.1.4. Mercados de criptoactivos

El Reglamento MICA define el criptoactivo como "una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar"[33]. Mayor concreción en el concepto de criptomoneda lo ofrecía la Directiva 2015 / 849[34], que lo definía

> [...] como una representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda de curso legal, que no tiene la consideración de moneda o divisa, pero es aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos.[35]

El nuevo Reglamento MICA impone unos requisitos, tanto a los emisores de criptoactivos, como a los proveedores de servicios de criptoactivos. Los emisores de criptoactivos están obligados a proporcionar información completa y transparente sobre los criptoactivos que emiten, así como a cumplir condiciones de divulgación y transparencia. Respecto a los proveedores de servicios, determina la obligación de estar registrados como tales y cumplir las normas de blanqueo de capitales.

6. Delitos en *blockchain*



33 Unión Europea, Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937, Diario Oficial de la Unión Europea L 150, 9 de junio de 2023, art. 3.5).

34 Directiva 2015 / 849, de 20 de mayo relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.

35 Unión Europea, Directiva (UE) 2018/843, art. 1.2.d).

6.1.Blockchain sede de actividad delictiva

En este caso, encontramos una actividad delictiva "clásica" que de algún modo se beneficia del soporte de la cadena de bloques. Las características de *blockchain* ofrecen unas posibilidades notorias en la actividad delincuencial, especialmente en todo lo concerniente a tráfico ilegal de bienes y servicios; tal es el caso de tenencia y distribución de pornografía infantil, distribución de sustancias, distribución de obras de arte robadas, o distribución en delitos contra la propiedad industrial / intelectual. En estos casos, *blockchain* se aloja en redes privadas, en muchos casos en la *dark web*, lo cual dificulta el acceso a estas cadenas de bloques; sin embargo, más adelante veremos las posibles diligencias de investigación adecuadas, en estos casos.

6.2. Delitos basados en criptomonedas

Como señalábamos, al principio, el punto de partida de la tecnología *blockchain* es el desarrollo de criptoactivos[36]. Los datos sobre las actividades ilícitas asociadas a criptomonedas ponen en evidencia el reto en el que se encuentra la comunidad internacional. En Europa el desglose de estas actividades revela un 57,6 % de estafas, un 31,8 % de robos, un 3,1 % de *ransomware*, un 2,8 % de fraude, un 1,9 % de red oscura, un 1,5 % de cibercrimen y el 1,4 % restante en diversas modalidades delictivas[37].

El abordaje del problema del delito cibernético, más concretamente de los delitos fiscales y financieros que utilizan criptomonedas, finanzas descentralizadas, *peer-to-peer*, pagos y mezcla de servicios, precisa de una acción global. Con este objetivo el Servicio Interno de Impuestos (IRS) de Estados Unidos lanza un programa piloto en América Latina[38], Australia, Europa y Asia. La investigación criminal del IRS persigue con esta acción brindar herramientas a las autoridades locales para combatir el delito cibernético, particularmente los que se cometen con criptomonedas, finanzas descentralizadas (DeFi), plataformas de pagos *peer-to-peer* (persona a persona) y servicios de mezcla de criptoactivos (*mixers*).

6.2.1. Delitos comunes con criptomonedas

Este grupo de delitos se corresponde también con delincuencia común como fraude, apuestas ilegales, pornografía infantil, compraventa de bienes o servicios ilegales, extorsión, cuya diferencia se encuentra en la sustitución del dinero tradicional por la criptomoneda. En estos supuestos, cabe destacar los ataques de "secuestro de datos"[39] (*ransomware*) a empresas e instituciones estatales, mediante la introducción de virus informáticos, en cuyo caso los rescates se solicitan normalmente en bitcoin.

La ventaja de recibir un rescate en criptomoneda radica en la posibilidad de una fácil desaparición del dinero y el "pseudoanonimato" de sus receptores.

36 El precursor de estos criptoactivos fue Bitcoin, puesto en circulación en 2009, junto con Ethereum concentra más del 80 % de esta moneda.

37 Banco de España, Informe de estabilidad financiera, "Especial criptoactivos" (Primavera 2022).

38 En el periodo de junio a septiembre de 2023, el IRS tiene un agente especial en Bogotá para desarrollar su objetivo.

39 Esta actividad delictiva está experimentando un ascenso muy significativo recientemente, hasta alcanzar en 2023 un 65 % de incremento, respecto a 2022 (https://www.chainalysis.com/es/, consultado el 17 / 07 / 2023).

6.2.2. La criptomoneda como elemento esencial del delito

En este caso, no se trata de delincuencia clásica que sustituye la moneda clásica por la criptomoneda en la comisión del ilícito. Las criptomonedas han permitido una actividad delictiva específica para ser desarrollada gracias a la misma. Es el caso del robo de criptomonedas, el blanqueo de capitales y la financiación del terrorismo internacional.

- Robo de criptomonedas

  Los fenómenos de robo de criptodivisas se practican, tanto en las monederas electrónicas de los usuarios, como en las plataformas de inversión. Las transferencias de criptomonedas a direcciones de monederos asociadas a estafas de suplantación han crecido un 49 % desde el 2022[40]. Otra modalidad de robo de criptomoneda se está desarrollando mediante ataques masivos a los operadores de servicios de estas monedas.

- Blanqueo de capitales y financiación del terrorismo

  La lucha contra el blanqueo de capitales y la financiación del terrorismo es consecuencia de una nueva realidad en el mundo criminal y de la ciberseguridad. Se ha hecho evidente que los aspectos económicos del delito han adquirido una importancia nuclear, razón por la cual deben tomarse todas las medidas necesarias de forma globalizada. Se interpreta en el considerando (4) de la Directiva 2018 / 843 que "la prevención del blanqueo de capitales y de la financiación del terrorismo no puede ser eficaz si el entorno no es hostil para los delincuentes que buscan refugio para sus finanzas a través de estructuras opacas"[41].

  En este sentido, en el caso de la financiación del terrorismo, el considerando (8) de la Directiva 2018 / 843 expone: "los grupos terroristas pueden ser capaces de transferir dinero hacia el sistema financiero de la Unión o dentro de las redes de monedas virtuales ocultando transferencias o gozando de cierto grado de anonimato en esas plataformas", por lo que señala preciso regular "los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias, así como a los proveedores de servicios de custodia de monederos electrónicos"[42].

El terrorismo islámico ha sido una de las primeras organizaciones criminales en advertir la potencialidad de su financiación a través de Bitcoin, en concreto *Al Qaeda* e *Isis*. Ambas organizaciones han llevado a cabo mensajes de captación de ayuda financiera en Occidente, a través de redes sociales como *WhatsApp* o *Telegram*[43].

Los beneficios del uso de las criptomonedas no se circunscriben solo al anonimato, sino que la rapidez de los pagos y el bajo coste de los *exchanges* son dos cualidades de las criptomonedas muy valoradas[44]. Prueba de ello, es que la reutilización de capitales ilícitos en el sector de las criptomonedas representa uno de los principales canales de ciberdelincuencia. El Grupo de Acción Financiera Internacional (GAFI) destacó como principales ventajas obtenidas por los criminales en el blanqueo de capitales con criptomonedas:

a. el anonimato asociado al diseño de los AV (que incluso puede incrementarse mediante el recurso a herramientas como los "mezcladores" o "conmutadores" ("Mixers" o "Tumblers");
b. la posibilidad de que una misma persona controle múltiples "monederos virtuales";
c. el carácter descentralizado de la mayoría de las criptomonedas (que supone la inexistencia de un órgano de supervisión que pueda ser alcanzado por la normativa de ALA / CFT); y,
d. el alcance global de muchas de ellas, entre otros.[45]

De hecho, constituye una forma de invertir el producto del delito que proporciona a los sindicatos criminales un mayor anonimato y menores riesgos que los esquemas tradicionales. La meta 4 del ODS 16 identifica los aspectos económicos de los delitos como uno de los elementos esenciales a los cuales dirigir el esfuerzo en la lucha contra la criminalidad. Concretamente se afirma, entre otras cosas, la conveniencia de "fortalecer la recuperación y devolución de los activos robados y luchar contra todas las formas de delincuencia organizada". A este respecto cabe destacar la inquietud a nivel internacional y, más en concreto, de la Unión Europea, en orden a la necesidad de combatir el enriquecimiento fruto de la actividad criminal mediante la figura del decomiso, que debería extenderse sobre todos los "efectos que provengan del mismo y de los bienes, medios o instrumentos con que se haya preparado o ejecutado, así como de las ganancias provenientes del delito, cualesquiera que sean las transformaciones que hubieren podido experimentar"[46].

En esta línea, en América Latina[47], el Grupo de Acción Financiera de Latinoamérica (GAFILAT) tiene como objetivo prevenir y combatir el lavado de activos, el financiamiento del terrorismo y de armas de destrucción masiva. Ante el incremento de lavado de dinero a través de activos digitales, GAFILAT ha elaborado la "Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales"[48]. Esta guía destaca no solo la necesidad de una acción conjunta, a nivel mundial, para el decomiso de criptomoneda, sino también incide en el problema del "posible uso de criptomonedas para facilitar la financiación del terrorismo, en especial como medio para canalizar en forma (semi) anónima donaciones o aportes hacia organizaciones terroristas".

En la ciberdelincuencia, los criptoactivos son una forma de invertir el producto del delito y ofrecen a los grupos delictivos un mayor anonimato y menores riesgos que los sistemas tradicionales, al tiempo que permiten el movimiento de grandes sumas de dinero a jurisdicciones más conformes o menos preparadas para luchar contra el blanqueo de capitales.

40 Información obtenida de https://www.chainalysis.com/es/ (consultado el 17/07/2023).

41 Unión Europea, Directiva (UE) 2018/843, considerando (4).

42 Unión Europea, Directiva (UE) 2018/843, considerando (8).

43 Daniele Maria Barone, "Criptovalute e Jihad", *Periodico del Ministero della Difesa*, fasc. 1 (2019). Al Qaeda, que entró en una crisis de liquidez tras la muerte de su líder Osama Bin Laden, ha lanzado un llamamiento en su revista web al-Haqiqa (La Verdad) invitando a los lectores a utilizar Bitcoins para financiar la organización. El recordatorio fue lanzado por ISIS, a través de un banner publicitario en una de sus webs de información, en enero de 2018.

44 Joseph B. Walton y Gurpreet Dhillon, "Understanding Digital Crime, Trust, and Control in Blockchain Technologies", *AMCIS 2017 Proceedings* 36 (2017), 17.

45 Grupo de Acción Financiera Internacional (GAFI), *Guidance for a risk-based approach: Virtual currencies* (junio 2015), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.

46 España, Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, *Boletín Oficial del Estado* 281, 24 de noviembre de 1995, art. 127.

47 Colombia es uno de los países donde se lleva a cabo mayor volumen de blanqueo de capital y cuenta con organismos como la Unidad de Información y Análisis Financiero (UIAF), desde 1999.

48 "Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales" diciembre/2021.

El blanqueo de capitales puede ser operado, bien en plataformas legales, desconocedoras del mecanismo fraudulento existente o a través de plataformas al servicio del crimen, que encubren su actividad ilícita bajo la apariencia de legalidad. Estas dos modalidades corresponden a los servicios centralizados que implican la existencia de un intermediario en la negociación y los protocolos descentralizados; este intermediario no está presente, respectivamente.

- Plataformas legales-servicios centralizados de criptomonedas

  La utilización de plataformas legales de criptomoneda para el blanqueo de capitales pone de relieve el papel de los "intermediarios especializados" de las mismas. Los proveedores de monederos (*wallet providers*) son empresas que proporcionan a los usuarios monederos electrónicos, es decir, mecanismos para guardar, almacenar y transferir bitcoin u otras criptomonedas. En concreto, además de proporcionar el monedero electrónico, el proveedor de monederos guarda las claves privadas de la cuenta, facilita las operaciones de usuarios e intercambiadores y, en última instancia, actúa como intermediario[49]. El funcionamiento de estas carteras de criptomoneda se basa en la máxima *know your client*, razón por la cual la identificación de los clientes que operan, así como las cantidades y frecuencia de las mismas, deben ser controlados por los operadores de los servicios correspondientes. Como se refiere anteriormente, los proveedores de monederos electrónicos están obligados, en virtud de la Directiva 2018 / 843 a prestar esta información y a conservarla, preservando siempre los datos de sus clientes conforme al Reglamento General de Protección de Datos. De igual modo, deben comunicar las operaciones dudosas a la autoridad competente del Estado miembro y a la UIF (Unidad de Información Financiera)[50] con una previsión de fuertes sanciones tanto administrativas como penales o disuasorias.

  El papel de estos intermediarios es fundamental para la gestión del riesgo de blanqueo de capitales: la casuística, de hecho, de que los usuarios rara vez adoptan conductas ilícitas por su cuenta, sino que tienden a confiar en la "profesionalidad" de los intermediarios[51].

- Plataformas de servicios descentralizadas

  Mayor dificultad en la identificación de los sujetos (persona física o jurídica) se encuentra en las transacciones realizadas a través de servicios descentralizados. En estos casos no existe la figura del intermediario, razón por la cual, al desaparecer el proveedor de monedero electrónico, la información a la cual están obligados a dispensar por la Directiva 2018 / 843, no es accesible. El panorama se ve agravado, si se tiene en cuenta que, tanto en España, como en la zona euro, los servicios descentralizados de criptomonedas monopolizan más del 50 % de la actividad negociadora de estos.

49 Giovanni Paolo Accinni, "Cybersecuriti e criptovalute. Profili di rilevanza penale dolo la Quinta Direttiva", 247.

50 Art. 7.4.f) de la Directiva 2018 / 843: "comunicará la estructura institucional y los procedimientos generales de su sistema de lucha contra el blanqueo de capitales y la financiación del terrorismo, incluidos, entre otros, las UIF, las autoridades tributarias y las fiscalías, así como los recursos humanos y financieros asignados, en la medida en que esta información esté disponible".

51 Giovanni Paolo Accinni, "Cybersecuriti e criptovalute. Profili di rilevanza penale dolo la Quinta Direttiva", 223.

7. Acceso a la fuente de prueba

7.1.Blockchain privadas o al servicio del crimen



En la fase de instrucción, de averiguación en el proceso penal, la actividad delincuencial desarrollada a través de *blockchain*, sin duda, plantea ciertas dificultades. Las propias características mencionadas de descentralización y "pseudoanonimato" suponen trabas en la investigación del delito. En el proceso penal español, las diligencias de investigación tecnológica ofrecen ciertas posibilidades de acceso y averiguación de la información, incluso en los casos de *blockchain* privadas.

En concreto, tres de estas diligencias de investigación tecnológica de la Ley de Enjuiciamiento Criminal española son especialmente adecuadas para esta finalidad.

7.1.1. Identificación mediante número IP (art. 588 ter k, LECrim[52])

La identificación del IP desde el que se están realizando las actividades en una plataforma *blockchain* se revela, en principio, como un medio eficaz, sin embargo, no está desprovisto de dificultades. La cadena de bloques no tiene un nodo centralizado, sino que, por el contrario, tiene diversos nodos que operan dentro de la cadena. Esta característica puede plantear una ventaja, puesto que todo el "libro de registros", con la totalidad de las transacciones es accesible desde todos los nodos de la cadena de bloques, de tal modo que la identificación de la IP de uno de ellos y el posterior acceso al terminal y al sospechoso:

Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara

52 Ley de Enjuiciamiento Criminal.

> la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.[53]

Este acto de investigación electrónica regula también el deber de colaboración por parte de los prestadores de servicios de telecomunicaciones o de servicios de la sociedad de la información, así como quien facilite las comunicaciones a través de teléfono u otro sistema de comunicación telemática. Este deber consiste en prestar asistencia y colaboración al juez, Ministerio Fiscal y policía judicial. A su vez, aquellos que colaboren deben guardar secreto y en todo caso, si se incumplen estos deberes, puede ser delito de desobediencia[54].

Sin embargo, el acceso a la información individualizada de cada una de las transacciones requiere del apoyo de otra diligencia de investigación tecnológica del Capítulo V: "La interceptación de las comunicaciones telefónicas y telemáticas" de la Ley de Enjuiciamiento Criminal, que se expone a continuación.

7.1.2.Registro remoto de dispositivos de almacenamiento masivo de información (art. 588 *septies* a y b LECrim)

El juez puede autorizar la utilización de datos de identificación, códigos o *software*, para, de forma remota y telemática, acceder, sin conocimiento del titular, a los contenidos de ordenadores y sistemas informáticos. El ámbito de aplicación de esta diligencia de investigación tecnológica está limitado a delitos dolosos con pena máxima, al menos de tres años, delitos de organizaciones criminales y delitos de terrorismo, supuestos que se identifican con los supuestos que se están analizando.

Esta diligencia permite utilizar e instalar *software* de forma remota en los terminales investigados, a modo de *spyware* (programa espía) diseñado para recopilar datos de una computadora u otro dispositivo y reenviarlos a un tercero sin el permiso ni el conocimiento del usuario.

> 1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un *software*, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:
>
> a) Delitos cometidos en el seno de organizaciones criminales.
>
> b) Delitos de terrorismo.
>
> c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
>
> d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
>
> e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.[55]

Sin embargo, no todos los programas de investigación forense precisan ser instalados en los equipos informáticos investigados; es el caso de Chainalysis Reactor[56], utilizado por los cuerpos policiales de todo el mundo. Este programa rastrea las transacciones sospechosas de criptomonedas, de manera directa e indirecta: directa cuando se hace una transacción vinculada directamente a un delito o algún suceso irregular, e indirecta cuando se analiza el histórico de una billetera virtual, con la que se hace la transacción, y se detectan vinculaciones con asuntos ilícitos.

7.1.3. Agente encubierto informático (art. 282 *bis* 6 LECrim)

En la investigación de las actividades ilícitas en *blockchain* privadas al servicio del crimen, el agente encubierto informático supone una herramienta valiosa.

> El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 *ter* a.
>
> El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.[57]

Las actividades ilícitas en estas *blockchain*, muchas veces alojadas en la *dark web*, son difícilmente detectables para la investigación, razón por la cual, el agente encubierto informático es, prácticamente, el único medio posible para acceder a las mismas. La lucha contra la criminalidad organizada, especialmente la cibercriminalidad ha puesto de manifiesto, a nivel internacional, la necesidad de utilizar medios adecuados y eficientes. La lucha contra la criminalidad, de forma más concreta el tráfico de drogas y la necesidad de desarrollar las herramientas necesarias para combatirla, ha dado lugar al reconocimiento de la necesidad de medidas especiales de investigación encubierta, tanto en el plano internacional como en la UE.

De este modo, la Convención de Naciones Unidas de 20 de diciembre de 1988 contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas, en su art. 2.1, señala que: "[l]as Partes adoptarán las medidas necesarias, comprendidas las de orden legislativo y administrativo, de conformidad con las disposiciones fundamentales de sus respectivos ordenamientos jurídicos internos".

En este sentido, la Convención de Naciones Unidas de 15 de noviembre de 2000 contra la Delincuencia Organizada Transnacional, en su art. 20, compele a la utilización de técnicas especiales de investigación, las operaciones encubiertas, entre otras:

53 España, Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, *Gaceta de Madrid* 260, 17 de septiembre de 1882, art. 588 ter k.

54 España, Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, art. 588 ter e.

55 España, Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, art. 588 septies a.

56 Chainalysis tiene clasificados más de 29 tipologías de peligrosidad que se distribuyen en 4 niveles de alerta: nivel bajo, intermedio, alto y severo. En el nivel intermedio se puede encontrar transacciones sospechosas entre particulares; en el nivel alto se encuentran compras en la darknet, tiendas fraudulentas y transacciones vinculadas a estafas. También la plataforma detecta si las criptomonedas intercambiadas provienen de una jurisdicción de alto riesgo, como pueden ser países como Rusia, Venezuela o Irán. Consultado de: https://www.chainalysis.com/.

57 España, Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, art. 282 bis 6.

> [c]ada Estado Parte adoptará, dentro de sus posibilidades y en las condiciones prescritas por su derecho interno, las medidas que sean necesarias para permitir el adecuado recurso a la entrega vigilada y, cuando lo considere apropiado, la utilización de otras técnicas especiales de investigación, como la vigilancia electrónica o de otra índole y las operaciones encubiertas, por sus autoridades competentes en su territorio con objeto de combatir eficazmente la delincuencia organizada.[58]

En la Unión Europea, el Convenio de asistencia judicial en materia penal de 29 de mayo de 2000, refiere a las investigaciones encubiertas como investigaciones de actividades delictivas por parte de agentes que actúan infiltrados o con una identidad falsa, investigación que habrá de realizarse conforme a la normativa interna del Estado en cuyo territorio se adelante la investigación. El mismo Convenio señala que los agentes encubiertos deberían tener una formación específica, y podría recurrirse a ellos en particular para que se infiltraran en una red delictiva con vistas a obtener información o a ayudar a identificar y detener a los miembros de esa red.

7.2.Blockchain públicas – operadores de servicios de criptomoneda

7.2.1. Unión Europea

La investigación de criptoactivos con fines de blanqueo de capital o financiación del terrorismo en *blockchain* públicas, esto es, desarrolladas por operadores de servicios de "monederos electrónicos" (*wallets*), cuenta con mecanismos regulatorios en la Unión Europea.

El Banco Central Europeo define, en 2012, las criptodivisas como "un tipo de moneda digital no regulada, que es controlada por sus desarrolladores y utilizada y aceptada por los miembros de una comunidad digital específica"[59] y vaticinó los riesgos que podrían ocasionarse con su llegada. Los cambios que se anunciaban en los mercados financieros y más concretamente en el ámbito del blanqueo de capitales y financiación del terrorismo, sin embargo, no fueron abordados de forma inmediata. Por el contrario, la Directiva 2015 / 849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo[60], no tuvo en cuenta en su esfera de actuación las criptomonedas.

Esta cuestión queda subsanada con la Directiva 2018 / 843, referida en el marco regulatorio de la Unión Europea al incluir tres conceptos y cuestiones nucleares para el control e investigación de blanqueo de capitales y financiación del terrorismo con criptomonedas: "monedas virtuales", "proveedor de servicios de custodia de monederos electrónicos" y sus obligaciones y la necesaria identificación de terceros países de alto riesgo.

La Directiva 2018 / 843 incorpora al art. 3. de la Directiva 2015 / 849 los puntos 18 y 19. El nuevo punto 18 de este artículo define "monedas virtuales" como

> […] representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos.[61]

La entrada en escena de las monedas virtuales, a efectos de control del blanqueo de capitales, supone una baza fundamental en lo concerniente a las vías de acceso a la información de eventuales ilícitos.

> Los recientes atentados terroristas han revelado la aparición de nuevas tendencias, especialmente en lo que se refiere a la manera en que se financian y ejecutan las operaciones de los grupos terroristas. Algunos servicios basados en tecnologías modernas están ganando popularidad como sistemas de financiación alternativos si bien permanecen fuera del ámbito de aplicación del Derecho de la Unión o se benefician de exenciones de requisitos jurídicos que podrían haber dejado de estar justificadas.[62]

La Directiva 2018 / 843 en su *considerando* (9) advierte "el anonimato de las monedas virtuales permite su posible uso indebido con fines delictivos", razón por la cual despliega diversas medidas en aras de combatir eficientemente esos fines delictivos a través de las criptomonedas. El legislador europeo es consciente de que las actuaciones que establece no suponen una solución definitiva, pues el ámbito de actuación en estas monedas se constriñe a aquellas que se realicen a través de los proveedores de servicios, pero le consta que siguen produciéndose transacciones fuera de estos operadores. Estas transacciones son las referidas en el apartado anterior, desarrolladas en *blockchain* privadas o al servicio del crimen.

En relación con la moneda virtual operada mediante los proveedores de servicios, esta Directiva añade en el art. 3 la definición de "proveedor de servicios de custodia de monederos electrónicos" como "una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales". Lo más destacable en el tema que nos ocupa son las obligaciones que detalla la Directiva 2018 / 843 para estos proveedores de servicios de monederos electrónicos.

Las obligaciones originales previstas en la Directiva 2015 / 849 para las entidades se circunscribían a

> […] que apliquen las medidas de diligencia debida con respecto al cliente no solo a todos los nuevos clientes, sino también, en el momento oportuno, a los clientes existentes, en función de un análisis del riesgo, en particular cuando cambien las circunstancias pertinentes de un cliente.[63]

Cabe mencionar, en este aspecto, que deberán identificar a todos los clientes, sean persona física o jurídica, así como cualquier indicio sospechoso de ilicitud.

La Directiva 2018 / 843 refuerza estas obligaciones en aquellos casos en los que se produzca, en las transacciones, uno de los siguientes presupuestos:

58 Organización de las Naciones Unidas, *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, Resolución 55/25 de la Asamblea General, 15 de noviembre de 2000, art. 20.

59 Banco Central Europeo, *Virtual currency schemes* (Frankfurt am Main: European Central Bank, 2012), 6 y 29, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

60 Directiva (UE) 2015 /8 49 del Parlamento Europeo y del Consejo de 20 de mayo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, modificada por la Directiva 2018 / 843.

61 Unión Europea, Directiva (UE) 2018/843, art. 1.3.

62 Unión Europea, Directiva (UE) 2018/843, considerando (2).

63 Unión Europea, Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión, *Diario Oficial de la Unión Europea* L 141, 5 de junio de 2015, art. 60.c).

> i) que sean transacciones complejas, ii) que sean de un importe inusitadamente elevado, iii) que se lleven a cabo en una pauta no habitual, iv) que no tengan una finalidad económica o lícita aparente. En particular, las entidades obligadas deberán reforzar el grado y la naturaleza de la supervisión de la relación de negocios, a fin de determinar si tales transacciones o actividades parecen sospechosas.[64]

Toda la información a la cual están obligados los proveedores de servicios de custodia de monederos electrónicos deberá ser trasladada a las Unidades Internacionales de Finanzas (UIF) de cada uno de los Estados miembros, información que podrá ser solicitada, en cualquier momento, no solo por la UIF, sino por los órganos judiciales de cada Estado competentes: "[d]ebe garantizarse la confidencialidad completa relativa a tales investigaciones y a las solicitudes de información por parte de las UIF y las autoridades competentes distintas de las autoridades procesales"[65].

La investigación judicial de los ilícitos desarrollados a través de criptomonedas no solo se canaliza gracias a la información obligada de los proveedores de servicios, sino que, como hemos visto en el anterior apartado, podrá valerse de otros medios. "Además, pueden tenerse en cuenta otros procesos de identificación remota o electrónica segura, que la autoridad nacional competente haya regulado, reconocido, aprobado o aceptado a escala nacional"[66], que es el caso de la legislación procesal española, ya referida.

Por último, debemos referir los riesgos en las transacciones con terceros países: "los medios más habitualmente utilizados por los delincuentes para blanquear el producto de actividades ilícitas, incluidos, cuando estén disponibles, aquellos que se utilizan, en particular, en las transacciones entre Estados miembros y terceros países"[67]. A ello, se añaden los especiales peligros que se adivinan cuando las transacciones se realizan con terceros países de alto riesgo, calificados como tales, en función del "marco jurídico e institucional del tercer país en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo"[68].

Por tanto, los Estados miembros están obligados a la transposición de estas dos directivas de prevención de blanqueo de capital y financiación del terrorismo y, como consecuencia de ello, a instaurar todas y cada una de las prevenciones de las mismas. En el caso de España, son recogidas por el Real Decreto-Ley 7 / 2021, de 27 de abril de *Proveedores de servicios de salvaguardia o custodia de claves criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento y la transferencia de monedas virtuales.*

Como mencionábamos anteriormente, no se soluciona de raíz el problema de acceso a la fuente de prueba en los ilícitos con criptomonedas, pero qué duda cabe, que las obligaciones de los servicios de monederos electrónicos suponen un avance importante en la investigación criminal.

64 Unión Europea, Directiva (UE) 2018/843, art. 1.10.b).

65 Unión Europea, Directiva (UE) 2018/843, considerando (20).

66 Unión Europea, Directiva (UE) 2018/843, considerando (22).

67 Unión Europea, Directiva (UE) 2018/843, art. 6.2.c).

68 Unión Europea, Directiva (UE) 2018/843, art. 9.2. a).

Conclusiones

Las tecnologías de registro descentralizado solo acaban de empezar a desarrollarse e implantarse y aún queda mucho recorrido para las mismas. Por esta razón el legislador debe prestar una especial atención, a estas plataformas, tanto en el proceso civil, como en el proceso penal, a efectos de acceso a la fuente de prueba cuando se aloja en una cadena de bloques, como en el medio probatorio adecuado en el proceso.

La actividad delictiva radicada en *blockchain* presenta una mayor dificultad a la hora de ser investigada, pues las tecnologías disruptivas al servicio del crimen ponen en jaque a la actividad policial y judicial.

Las dos esferas delincuenciales en *blockchain*, de una parte, la delincuencia que se sirve en la comisión de los ilícitos de las oportunidades y ventajas de las cadenas de bloques, y de otra, la actividad que tiene en estas cadenas la base y fundamento del delito precisan diligencias específicas y eficaces.

En el primer supuesto, las diligencias de investigación tecnológica tienen el reto de desplegar correctamente sus posibilidades, entre las cuales especialmente idóneo es el uso de programas informáticos. La instalación remota de *spyware*, por parte de los cuerpos policiales en terminales sospechosos es una baza importante, junto con los programas que permiten la desencriptación de las operaciones realizadas en *blockchain*.

En el caso de actividades criminales con criptomonedas realizadas con operadores de servicios de monederos electrónicos, el papel de estas entidades y las obligaciones de información a las UIF, así como la conservación de las informaciones son fundamentales para el conocimiento de los posibles ilícitos.

Sin embargo, la actualización y celeridad de las autoridades competentes, tanto a nivel internacional, como de cada uno de los Estados, en las herramientas y medidas de averiguación son el reto global de la sociedad internacional. En esta línea, el legislador debe facilitar adaptar los marcos normativos a los nuevos escenarios tecnológicos, siempre con el debido respeto y protección de las garantías procesales.

Bibliografía

Accinni, Giovanni Paolo. "Cybersecuriti e criptovalute. Profili di rilevanza penale dolo la Quinta Direttiva". Sistema Penale, fascicolo 5 (2020).

Almonacid Sierra, Juan Jorge y Yeisson Coronel Ávila. "Aplicabilidad de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado". Revista de Derecho Privado, Universidad Externado de Colombia, n.º 38 (enero-junio 2020).

Banco de España. Informe de estabilidad financiera, "Especial criptoactivos". Primavera 2022.

Barone, Daniele Maria. "Criptovalute e Jihad". Periodico del Ministero della Difesa, fasc. 1 (2019).

Calaza López, Sonia. "Blockchain y Smart contracts: ¿un ecosistema digital seguro al margen de la ley?". En Uso de la información y de los datos personales en los procesos: los cambios en la era digital, dirigido por Ignacio Colomer Hernández. Pamplona: Thomson Reuters Aranzadi, 2022.

Christidis, Konstantinos y Michael Devetsikiotis. "Blockchains and Smart contracts for the IoT". IEEE Access 4 (2016): 2292-2303. doi:10.1109/ACCESS.2016.2566339.

España. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Gaceta de Madrid 260, 17 de septiembre de 1882.

España. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. *Boletín Oficial del Estado* 298, 12 de noviembre de 2020.

García Teruel, Rosa María, coord. La tokenización de bienes en blockchain: Cuestiones civiles y tributarias. Pamplona: Thomson Reuters Aranzadi, 2020.

Grupo de Acción Financiera Internacional (GAFI). Guidance for a risk-based approach: Virtual currencies. Junio 2015. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.

Haber, Stuart y W. Scott Stornetta. "How to Time-Stamp a Digital Document". Journal of Cryptology 3, n.º 2 (1991): 99-111.

Ibáñez Jiménez, Javier. Consorcio Red Alastria (Origen y reforma de la primera blockchain de España). Madrid: Editorial Reus, 2020.

Melo, Letícia. "Régimen jurídico de blockchain: una prueba atípica". Revista de Bioética y Derecho Perspectivas Bioéticas, n.º 468 (julio-diciembre 2020).

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System". 2008. https://bitcoin.org/bitcoin.pdf.

Nasarre Aznar, Sergio. "Naturaleza jurídica y régimen civil de los 'token' en 'blockchain'". En La tokenización de bienes en blockchain: Cuestiones civiles y tributarias, coordinado por Rosa María García Teruel. Pamplona: Thomson Reuters Aranzadi, 2020.

Organización de las Naciones Unidas. Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Resolución 55/25 de la Asamblea General, 15 de noviembre de 2000.

Puertas Álvarez, Omar, Oriol Valentí i Vidal y Laura Díaz Vallespinós. "Unlocking Blockchain Evidence in International Arbitration". Spain Arbitration Review, Revista del Club Español del Arbitraje, n.º 43 (2022): 15-30.

Tapscott, Alex y Don Tapscott. La revolución del BLOCKCHAIN. Descubre cómo esta nueva tecnología transformará la economía global. Barcelona: Deusto, 2016.

Unión Europea. Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión. Diario Oficial de la Unión Europea L 141, 5 de junio de 2015.

Unión Europea. Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE. Diario Oficial de la Unión Europea L 156, 19 de junio de 2018.

Unión Europea. Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937. Diario Oficial de la Unión Europea L 150, 9 de junio de 2023.

Valencia Ramírez, Juan Pablo. "Derecho, tecnologías e innovación: blockchain y contratos inteligentes". Revista de Investigación en Tecnologías de la Información Journal 8 (julio-diciembre 2020).

Von Haller Grønbæk, Mads. "Blockchain 2.0, Smart contracts and challenges". Computers & Law, The SCL Magazine (junio/julio 2016).

Walton, Joseph B. y Gurpreet Dhillon. "Understanding Digital Crime, Trust, and Control in Blockchain Technologies". AMCIS 2017 Proceedings 36 (2017).

HACIA UNA TEORÍA DE LA IMPUTACIÓN PENAL ALGORÍTMICA Y UN MODELO DE COMPLIANCE TECNOLÓGICO

Nuria Belloso Martín[1]

Resumen

El trabajo analiza el impacto de los usos de sistemas de inteligencia artificial en los modelos contemporáneos de *compliance* penal. Tras una breve comparativa entre los usos de la IA en el sistema de *compliance* en España y en Ecuador, se revisará la teoría de la imputación penal algorítmica, así como la gobernanza algorítmica. Se concluirá con la propuesta de un modelo normativo de *compliance* penal algorítmico.

Abstract

This paper analyses the impact of the use of artificial intelligence systems on contemporary models of criminal compliance. Following a brief comparison of the use of AI in compliance systems in Spain and Ecuador, it will examine the theory of algorithmic criminal liability, as well as algorithmic governance. It will conclude with a proposal for a regulatory model of algorithmic criminal compliance.

Índice: 1. Introducción 2. Inteligencia artificial y transformación del *compliance*: Una mirada comparativa entre España y Ecuador. 2.1. La incorporación de tecnologías de inteligencia artificial en los sistemas de *compliance.* 2.2. Breve referencia comparativa entre España y Ecuador con respecto al uso de inteligencia artificial en *compliance* 3. Teoría de la imputación penal algorítmica 4. Gobernanza algorítmica y *compliance* penal 5. Conclusiones. Hacia un modelo de *compliance* penal algorítmico.

1 Catedrática de la Universidad de Burgos, España.

1. Introducción

En las últimas décadas, el desarrollo de los programas de *compliance* penal ha respondido precisamente a la necesidad de prevenir la criminalidad corporativa mediante sistemas internos de control y supervisión. La introducción de la responsabilidad penal de las personas jurídicas en numerosos ordenamientos jurídicos ha reforzado esta tendencia, situando los modelos de organización y gestión como elementos clave para determinar la imputación penal de la empresa. En este contexto, el *compliance* se ha consolidado como uno de los instrumentos más relevantes para la prevención del delito en el ámbito empresarial. Sin embargo, la incorporación de sistemas de inteligencia artificial (IA) en la gestión empresarial plantea nuevos desafíos que los modelos tradicionales de *compliance* no estaban diseñados para afrontar. Si bien la IA puede ser de gran ayuda para prevenir y detectar posibles infracciones de las normas de cumplimiento y mejorar así la eficiencia en el desempeño de los controles, la aplicación de la IA en el ámbito del *compliance* no está exenta de desafíos y limitaciones.



El problema adquiere especial relevancia en el ámbito del Derecho penal económico, donde las decisiones empresariales suelen adoptarse en contextos organizativos complejos y altamente tecnificados. En estos escenarios, la inteligencia artificial puede convertirse simultáneamente en un instrumento de prevención del delito y, a su vez, en un factor generador de nuevos riesgos delictivos. La utilización de tecnologías algorítmicas puede facilitar la detección de irregularidades dentro de la empresa, pero también puede introducir nuevas formas de opacidad decisional y dilución de responsabilidades.

El presente estudio realizará una breve referencia a la comparativa del estado de la cuestión en España y en Ecuador. Se parte de la hipótesis de que los modelos tradicionales de imputación penal corporativa resultan insuficientes para afrontar los desafíos derivados del uso de inteligencia artificial en el ámbito empresarial. En este sentido, este estudio pretende realizar tres aportaciones sobre el tema. En primer lugar, contribuir al debate doctrinal sobre la responsabilidad penal corporativa al analizar el impacto de la inteligencia artificial en los modelos contemporáneos de *compliance* penal. Mientras que buena parte de los estudios sobre inteligencia artificial se han centrado en los problemas éticos o regulatorios de estas tecnologías, en estas páginas se hará referencia a la cuestión desde la perspectiva específica del Derecho penal económico y la responsabilidad penal de las organizaciones.

En segundo lugar, el artículo desarrolla un marco conceptual para lo que puede denominarse imputación penal algorítmica. Partiendo de la teoría de la imputación objetiva desarrollada por Roxin y de la concepción funcionalista del Derecho penal propuesta por Jakobs, se sostiene que la responsabilidad penal en contextos algorítmicos debe fundamentarse en dos elementos esenciales: la creación de riesgos tecnológicos jurídicamente relevantes y la infracción de deberes organizativos de supervisión tecnológica. En tercer lugar, el trabajo propone un modelo normativo de *compliance* penal algorítmico, orientado a integrar mecanismos de gobernanza tecnológica dentro de los programas de cumplimiento empresarial. Este modelo se estructura en torno a cinco principios fundamentales: gobernanza algorítmica, transparencia tecnológica, supervisión humana significativa, gestión preventiva del riesgo tecnológico y trazabilidad decisional.

De este modo, estas páginas pretenden contribuir al desarrollo de un marco conceptual que permita conectar la teoría del riesgo en el Derecho penal contemporáneo con los desafíos regulatorios planteados por la inteligencia artificial en el ámbito empresarial.

2. Inteligencia artificial y transformación del *compliance*: Una mirada comparativa entre España y Ecuador

El desarrollo del *compliance penal* se encuentra estrechamente vinculado a la evolución del Derecho penal económico y, particularmente, al reconocimiento de la responsabilidad penal de las personas jurídicas[2]. Durante siglos predominó el

2 En España, tras la reforma del Código Penal del año 2010, las personas jurídicas son penalmente responsables de los delitos cometidos en su nombre o por su cuenta por sus representantes legales y administradores, pero, también, por quienes estando sometidos a su autoridad hayan podido realizar los hechos al no haberse ejercido sobre ellos el debido control. Se introdujo así la responsabilidad de las personas jurídicas privadas. En su posterior revisión del año 2015, se introdujeron los planes de prevención de riesgos penales (mecanismos preventivos basados en el compliance) como medida para atenuar o eximir a las empresas de su responsabilidad penal. Asimismo, desde 2021 es obligatorio implementar un canal de denuncias, siguiendo lo establecido en la Directiva (UE) 2019/1937.

principio *societas delinquere non potest*, según el cual únicamente las personas físicas podían ser sujetos de responsabilidad penal. Sin embargo, la creciente complejidad de las estructuras empresariales y el desarrollo de la criminalidad económica llevaron a cuestionar este principio[3]. En la actualidad, numerosos ordenamientos jurídicos reconocen la posibilidad de atribuir responsabilidad penal a las empresas cuando los delitos se cometen en su beneficio o como consecuencia de defectos en sus sistemas de organización y control.

Desde una perspectiva dogmática, diversos autores han señalado que la responsabilidad penal corporativa se fundamenta en la existencia de defectos estructurales de organización que facilitan la comisión de delitos dentro de la empresa[4]. El *compliance* penal se configura como un mecanismo destinado a prevenir la comisión de ilícitos mediante la implantación de sistemas internos de control y supervisión. Entre los elementos esenciales de un programa de *compliance* destacan la identificación de riesgos penales, la elaboración de códigos éticos, la formación interna, los canales de denuncia, la supervisión por parte del *compliance officer* y las auditorías periódicas del sistema. Estos instrumentos buscan promover una cultura corporativa orientada al cumplimiento normativo[5].

En este sentido, el *compliance* penal no debe entenderse únicamente como un instrumento de autorregulación empresarial, sino como un mecanismo de *gobernanza jurídica del riesgo organizativo. Los programas de cumplimiento norm*ativo operan como sistemas institucionales destinados a identificar, prevenir y gestionar riesgos jurídicos derivados de la actividad empresarial.

2.1. La incorporación de tecnologías de inteligencia artificial en los sistemas de *compliance*

La incorporación de tecnologías de inteligencia artificial en los sistemas de *compliance* representa una evolución significativa en los mecanismos de prevención del delito corporativo[6]. Los sistemas de análisis algorítmico permiten procesar grandes volúmenes de datos empresariales y detectar patrones de comportamiento que podrían indicar la existencia de irregularidades.

La implementación de programas de compliance y sistemas de gestión para el buen gobierno de la administración en las empresas permitirán mitigar el riesgo de la comisión de delitos y exonerar a la empresa de la responsabilidad penal de delitos cometidos por directivos o empleados. La forma de evitar o atenuar la pena en caso de comisión de un delito es demostrar que la empresa ha sido diligente, adoptando las medidas necesarias mediante la implantación de un Corporate Compliance o plan de prevención de riesgos penales. Aunque no es obligatorio, la implementación de un programa de compliance puede eximir de responsabilidad penal a la empresa. A lo que se suma que hay varias normativas que hacen alusión indirecta al compliance, como la ley de protección de denunciantes, Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, o la Directiva UE 2019/1937. Vid. Nuria Belloso Martín, "Los códigos de conducta como proyección del liderazgo cívico", en Paloma Durán y Lalaguna, Liderazgo y compromiso cívico en el siglo XXI (Córdoba: Editorial Almuzara, 2025), 197-237; Eduardo Vázquez de Castro, "La inminente obligatoriedad del 'compliance' en las organizaciones como imperativo europeo: protección jurídica de la empresa, del denunciante y del denunciado", Revista Aranzadi de derecho patrimonial, n.° 53 (2020).

3 Vid. Carlos Gómez-Jara Díez, *Corporate Criminal Liability: Prevention, Compliance and Corporate Governance* (Cheltenham: Edward Elgar, 2015), 23-45.

4 Sobre la fundamentación de la responsabilidad penal corporativa en los defectos estructurales de organización, vid. Adán Nieto Martín, Compliance y Derecho penal económico (Valencia: Tirant lo Blanch, 2015), 89-104.

5 Sobre la función preventiva de los programas de compliance en el ámbito del Derecho penal económico, vid. Nieto Martín, Compliance y Derecho penal económico, 89-104; Gómez-Jara Díez, Corporate Criminal Liability, 23-45.

6 Vid. Túlio Felippe Xavier Januário, "Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales", *Estudios Penales y Criminológicos* 44, extra (2023): 1-39. https://dialnet.unirioja.es/ejemplar/657488.

Entre las aplicaciones más relevantes cabe destacar el análisis automatizado de transacciones financieras, la monitorización de comunicaciones corporativas, la detección de fraude y el análisis predictivo de riesgos regulatorios. Estas herramientas permiten mejorar significativamente la capacidad de las empresas para detectar conductas ilícitas como el fraude, la corrupción o el blanqueo de capitales[7]. Por ejemplo, como señala Bellver Velda, mediante técnicas de análisis de datos como el *machine learning*, se pueden detectar patrones de comportamiento sospechosos en los registros financieros de una empresa, lo que podría indicar la existencia de prácticas fraudulentas o de blanqueo de capitales; la IA también puede ser útil en el ámbito de la formación y el entrenamiento de los empleados en materia de cumplimiento normativo. Por ejemplo, se pueden crear simulaciones de situaciones reales en las que los empleados deban tomar decisiones éticas y legales, permitiéndoles practicar y adquirir una formación en el tema de una manera más dinámica e interactiva; otra de las posibilidades es la mejora de la eficiencia y la reducción de costos en los procesos de auditoría; y una última posibilidad, entre otras, es la creación de sistemas de alerta temprana que permitan a las empresas detectar y prevenir posibles infracciones normativas de forma proactiva[8].

Ya se han apuntado casos de éxito de uso de la inteligencia artificial en el *compliance.* Uno de esos usos exitosos es el llevado a cabo para detectar y prevenir el lavado de dinero en el sector financiero. Las instituciones financieras utilizan algoritmos de *machine learning* para analizar grandes cantidades de datos financieros y transacciones sospechosas, lo que les facilita identificar patrones y anomalías que podrían indicar actividades ilícitas. Otro ejemplo es el uso de la IA en la detección de fraude y corrupción en contrataciones públicas. Uno de los casos más reseñables es el del Gobierno de Colombia, que ha implementado un sistema de IA para analizar los datos de licitaciones y contratos públicos, con el objetivo de detectar posibles irregularidades o patrones de corrupción. También se puede hacer uso de la IA para analizar y clasificar documentos y registros electrónicos en busca de posibles infracciones. Por ejemplo, una empresa puede utilizar la IA para identificar rápidamente documentos que contengan información confidencial o que puedan estar sujetos a regulaciones específicas, lo que puede ayudar a prevenir la divulgación de aquella sensible o la violación de normas de cumplimiento.

No obstante, como ya hemos adelantado, el uso de inteligencia artificial en los sistemas de *compliance* también plantea importantes desafíos jurídicos especialmente en relación con la transparencia algorítmica, la protección de datos personales y la atribución de responsabilidad por decisiones automatizadas, por lo que habrá que conjugar su aplicación con la adopción de las cautelas necesarias. A ello hay que añadir que una de las limitaciones radica en la propia complejidad de implementar sistemas de IA en la empresa, ya que la incorporación de herramientas puede requerir una importante inversión económica y tecnológica, además de requerir contar con personal altamente cualificado para su correcto funcionamiento.

El *compliance penal* algorítmico debe operar simultáneamente en tres planos: el plano tecnológico, donde se diseñan y supervisan los sistemas de inteligencia artificial (a través de instrumentos como auditoría algorítmica, control de datos, validación del modelo); el plano organizativo, donde se integran los mecanismos de control dentro de la estructura

7 Sobre el uso de herramientas algorítmicas para la detección de irregularidades y el análisis de riesgos corporativos, vid. Cathy O'Neil, *Weapons of Math Destruction* (Nueva York: Crown Publishing, 2016).

8 Javier Bellver Belda, "El uso de la inteligencia artificial en el ámbito del compliance: posibilidades, limitaciones y perspectivas de futuro", *ElDerecho.com*, 19 de julio de 2023, https://elderecho.com/uso-inteligencia-artificial-ambito-compliance-posibilidades-limitaciones.

empresarial (como supervisión del *compliance officer*, protocolos internos); y, por último, el plano jurídico, donde se evalúa la responsabilidad penal derivada del uso de dichas tecnologías (a través de la trazabilidad decisional). En este contexto, la cuestión central consiste en determinar cómo deben adaptarse los criterios tradicionales de imputación penal a los riesgos derivados del funcionamiento de sistemas algorítmicos. Esta cuestión será abordada más adelante, mediante el desarrollo de una teoría de la imputación penal algorítmica.

2.2. Breve referencia comparativa entre España y Ecuador con respecto al uso de inteligencia artificial en *compliance*

Como se ha señalado, el sistema de *compliance* en España introduce la responsabilidad penal de la persona jurídica en el año 2010, y puede **eximir o atenuar responsabilidad penal** si es eficaz. Cuenta con doctrina del Tribunal Supremo y con un alto desarrollo de estándares (como UNE 19601), además de una práctica empresarial consolidada. Ello hace que se haya creado un entorno favorable a la incorporación de la IA. Si se hace una breve comparativa con Ecuador, el concepto de *compliance* cobró relevancia principalmente a partir de la entrada en vigor del Código Orgánico Integral Penal (COIP) el 10 de febrero de 2014, que introdujo la responsabilidad penal de las personas jurídicas. A partir de ahí, contar con programas de cumplimiento normativo puede actuar como atenuante en caso de procesos judiciales, tal como recoge el artículo 49 del COIP. Esta disposición ha impulsado una evolución en la cultura corporativa ecuatoriana, promoviendo la implementación de sistemas de integridad, normas de prevención, dirección y supervisión. Con la reciente regulación específica de compliance, en 2021, podría considerarse que el sistema está aún en fase de desarrollo e interpretación, y se están resolviendo problemas doctrinales y procesales. Ello da como resultado un entorno más incierto para innovaciones como la IA[9].

Como todo sistema, la introducción de IA en el compliance presenta unas ventajas e inconvenientes. Como ventajas, en España cabe reseñar que puede reforzar la eximente penal (art. 31 bis CP), mejora la competitividad empresarial y reputación y es compatible con sistemas certificados y auditorías. También en Ecuador cabe apreciar varias ventajas, como que ofrece una oportunidad de modernizar el sistema, permite suplir carencias estructurales del control interno y facilita convergencia con estándares internacionales.

En cuanto a los inconvenientes y riesgos, por un lado, habría que tomar en consideración problemas generales que, de por sí, presenta la IA, como la falta de transparencia (black box), el riesgo de falsos positivos/negativos, la protección de datos y la dependencia tecnológica. De manera más específica, en España, dada la alta exigencia que se requiere, el sistema debe ser eficaz y no meramente formal. Asimismo, la IA mal implementada puede: no eximir responsabilidad penal y, además, generar responsabilidad adicional (negligencia en supervisión). Con respecto a Ecuador, el problema principal que cabe advertir es la inseguridad jurídica, dada la regulación reciente y poco desarrollada y la falta de criterios jurisprudenciales claros. Asimismo, cabe advertir la baja implantación práctica, en cuanto que el compliance aún no está plenamente integrado en empresas. Ello desemboca en un riesgo de inversión tecnológica sin reconocimiento legal claro y una dificultad probatoria en tribunales.

9 José Roberto Pazmiño Ruiz y Juan Francisco Pozo Torres, "Responsabilidad penal de las personas jurídicas y compliance: caso Ecuador", *Derecho Penal y Criminología* 40, n.° 109 (2019): 89-122. doi:10.18601/01210483.v40n109.04.

En definitiva, en **España**, la IA es una **herramienta estratégica consolidada**, capaz incluso de evitar condenas si se integra correctamente, mientras que, en **Ecuador**, la IA representa más bien una **oportunidad en construcción**, pero con riesgos derivados de falta de desarrollo normativo, escasa cultura de *compliance* e inseguridad interpretativa.



3. Teoría de la imputación penal algorítmica

El surgimiento de tecnologías algorítmicas debe interpretarse a la luz de una transformación más amplia del paradigma regulatorio del Derecho penal. Como ha señalado Beck, las sociedades contemporáneas se caracterizan por la producción sistemática de riesgos derivados del progreso tecnológico[10]. En este contexto, el Derecho penal deja de operar exclusivamente como un mecanismo de reacción frente a daños consumados para asumir progresivamente funciones de **gestión preventiva del riesgo.** Esta evolución ha sido descrita por Silva Sánchez como una de las manifestaciones más significativas de la expansión del Derecho penal en las sociedades contemporáneas[11]. La inteligencia artificial constituye un ejemplo paradigmático de este proceso: los sistemas algorítmicos introducen nuevas formas de riesgo estructural cuya gestión exige adaptar los criterios tradicionales de imputación jurídica.

Uno de los desafíos más complejos que plantea la inteligencia artificial desde la perspectiva del Derecho penal contemporáneo consiste en determinar los criterios de atribución de responsabilidad cuando un sistema algorítmico interviene en la producción de un resultado jurídicamente

10 Ulrich Beck, La sociedad del riesgo: *Hacia una nueva modernidad* (Barcelona: Paidós, 1998).

11 Jesús-María Silva Sánchez, *La expansión del Derecho penal* (Madrid: Civitas, 2001).

relevante. A diferencia de los instrumentos tecnológicos tradicionales, los sistemas de inteligencia artificial –especialmente aquellos basados en aprendizaje automático– pueden generar resultados no previstos de forma directa por sus programadores o usuarios, lo que introduce un elemento de indeterminación en la cadena causal. Los sistemas de inteligencia artificial carecen de personalidad jurídica y no pueden ser considerados sujetos de responsabilidad penal. En consecuencia, cualquier intento de atribuir responsabilidad por los resultados producidos por estos sistemas debe dirigirse necesariamente a personas físicas o jurídicas vinculadas a su diseño, desarrollo o utilización. La cuestión central radica, por tanto, en determinar qué sujetos pueden ser considerados jurídicamente responsables cuando el resultado lesivo se produce a través de procesos decisionales automatizados. La responsabilidad en el uso de la IA en el ámbito del compliance recaería en aquellos que están involucrados en su implementación, supervisión y utilización. Un mal uso de dichos mecanismos y herramientas podría tener consecuencias legales y reputacionales significativas, por lo que es crucial designar un responsable adecuado, una especie de IA Officer, y establecer mecanismos de rendición de cuentas efectivos para garantizar su buen uso y el cumplimiento de las normas y regulaciones aplicables.

Desde la perspectiva de la teoría del delito, esta problemática obliga a replantear algunos de los presupuestos clásicos de la imputación penal. Tradicionalmente, la teoría penal ha situado la acción humana como punto de partida de la imputación[12]. Sin embargo, en contextos tecnológicos complejos caracterizados por la intervención de sistemas automatizados, el resultado lesivo puede derivarse de procesos de decisión en los que la intervención humana es indirecta o mediata. Las empresas deben asumir la responsabilidad, además de por las acciones directas de sus empleados, también por las decisiones que adopten sus sistemas de IA. Por tanto, las organizaciones deben de adoptar políticas de compliance claras de manera que garanticen que sus tecnologías no sean usadas de manera indebida para cometer fraudes, violaciones de derechos o incluso otros delitos como el lavado de dinero o evasión fiscal.

Una de las principales dificultades radica en la incapacidad de los marcos legales actuales para asignar responsabilidad de manera adecuada a las tecnologías autónomas. Aunque el derecho penal empresarial ha avanzado para abordar la responsabilidad penal de las personas jurídicas, la naturaleza intrínsecamente autónoma de los sistemas de IA crea una zona gris donde resulta complejo determinar la responsabilidad por los actos cometidos por estos sistemas. Se abre así una funcionalidad a cumplir, respectivamente, por el compliance y por el Derecho penal empresarial: el compliance debe ir más allá de las exigencias regulatorias tradicionales y convertirse en un mecanismo activo de control de riesgos tecnológicos. Por su parte, al Derecho penal empresarial le corresponde adaptarse rápidamente de manera que pueda asignar responsabilidad a las personas jurídicas por los actos de sus sistemas automatizados[13].

12 Sobre la centralidad de la acción humana como presupuesto de la imputación penal en la teoría clásica del delito, vid. George P. Fletcher, *Rethinking Criminal Law* (Oxford: Oxford University Press, 2000), 441-460.

13 Son varios los ejemplos de herramienta de IA aplicada al compliance penal empresarial que podrían citarse. Entre otras, Compliance Penal, la nueva herramienta de Lefebvre, que valorará posibles riesgos basados en la probabilidad de ocurrencia y de su impacto en la empresa, además de establecer los controles necesarios para evitarlos (Lefebvre, "Compliance penal: una herramienta para implantar un programa de vigilancia y control eficaz de la actividad de la empresa", accedido 15 de abril de 2026, https://lefebvre.es/actualidad/corporativa/compliance-penal-una-herramienta-para-implantar-un-programa-de-vigilancia-y-control-eficaz-de-la-actividad-de-la-empresa/); PrudencIA, que se presenta como la mejor IA para compliance por combinar análisis normativo, automatización legal y gestión de riesgos en una sola plataforma (LexGo, "PrudencIA: La mejor inteligencia artificial para compliance penal, financiero, energético y regulatorio", accedido 15 de abril de 2026, https://lexgoapp.com/guias-legales/compliance-penal/la-mejor-inteligencia-artificial-para-compliance-penal-financiero-energetico-y-regulatorio).

La teoría de la imputación objetiva desarrollada por Claus Roxin ofrece un marco conceptual especialmente adecuado para tratar estos problemas[14]. Según este enfoque, la imputación penal no se fundamenta exclusivamente en la relación causal entre conducta y resultado, sino en la creación de un riesgo jurídicamente desaprobado que se materializa en el resultado típico. De acuerdo con esta perspectiva, la responsabilidad penal surge cuando un sujeto introduce en el mundo social una fuente de peligro jurídicamente relevante y el resultado producido constituye la realización de ese riesgo. De este modo, la introducción de sistemas algorítmicos en procesos empresariales puede ser considerada como la creación de una fuente de riesgo organizativo, especialmente cuando estos sistemas intervienen en ámbitos sensibles como la gestión financiera, la producción de contenidos o la toma de decisiones estratégicas. Desde esta perspectiva, la responsabilidad penal podría fundamentarse en la falta de control sobre la fuente de riesgo tecnológico, especialmente cuando se omiten medidas razonables de supervisión o control del sistema algorítmico[15].

En el ámbito del Derecho penal económico, esta cuestión adquiere especial relevancia, puesto que los sistemas algorítmicos pueden intervenir en ámbitos particularmente sensibles como la gestión financiera, la contratación automatizada, el análisis de datos personales o la producción de contenidos digitales. Desde esta perspectiva, la imputación penal en contextos algorítmicos debe basarse en el principio de control sobre la fuente de riesgo tecnológico. Este criterio permite atribuir responsabilidad a aquellos sujetos que, en virtud de su posición organizativa, poseen la capacidad de introducir, supervisar o modificar el funcionamiento del sistema algorítmico.

En el contexto empresarial, estos sujetos pueden incluir los desarrolladores del sistema, las empresas que diseñan o comercializan la tecnología, las organizaciones que la incorporan a sus procesos productivos y los responsables de supervisión tecnológica dentro de la empresa. No obstante, la atribución de responsabilidad no puede basarse únicamente en la relación causal entre el diseño del sistema y el resultado producido. Resulta necesario analizar también los deberes organizativos de supervisión tecnológica que corresponden a los distintos sujetos implicados. En este punto resulta especialmente relevante la concepción funcionalista del Derecho penal desarrollada por Günther Jakobs[16]. Según Jakobs, la imputación penal puede fundamentarse en la infracción de deberes normativos vinculados al rol que desempeña el sujeto en el sistema social. En el ámbito empresarial, estos deberes se concretan en obligaciones de organización y supervisión destinadas a garantizar que la actividad económica se desarrolle dentro de los límites del ordenamiento jurídico.

La combinación de la teoría de la imputación objetiva de Roxin y la concepción funcionalista de Jakobs permite así formular un modelo de imputación penal algorítmica basado en dos elementos fundamentales: la creación de un riesgo tecnológico jurídicamente relevante mediante la introducción de sistemas de inteligencia artificial en la actividad empresarial; y la infracción de deberes organizativos de supervisión tecnológica destinados a controlar el funcionamiento de dichos sistemas.

En consecuencia, la imputación penal en contextos algorítmicos no debe centrarse exclusivamente en la causalidad entre el funcionamiento del sistema y el resultado

14 Claus Roxin, *Derecho penal: Parte general* (Madrid: Civitas, 1997), 365-372.

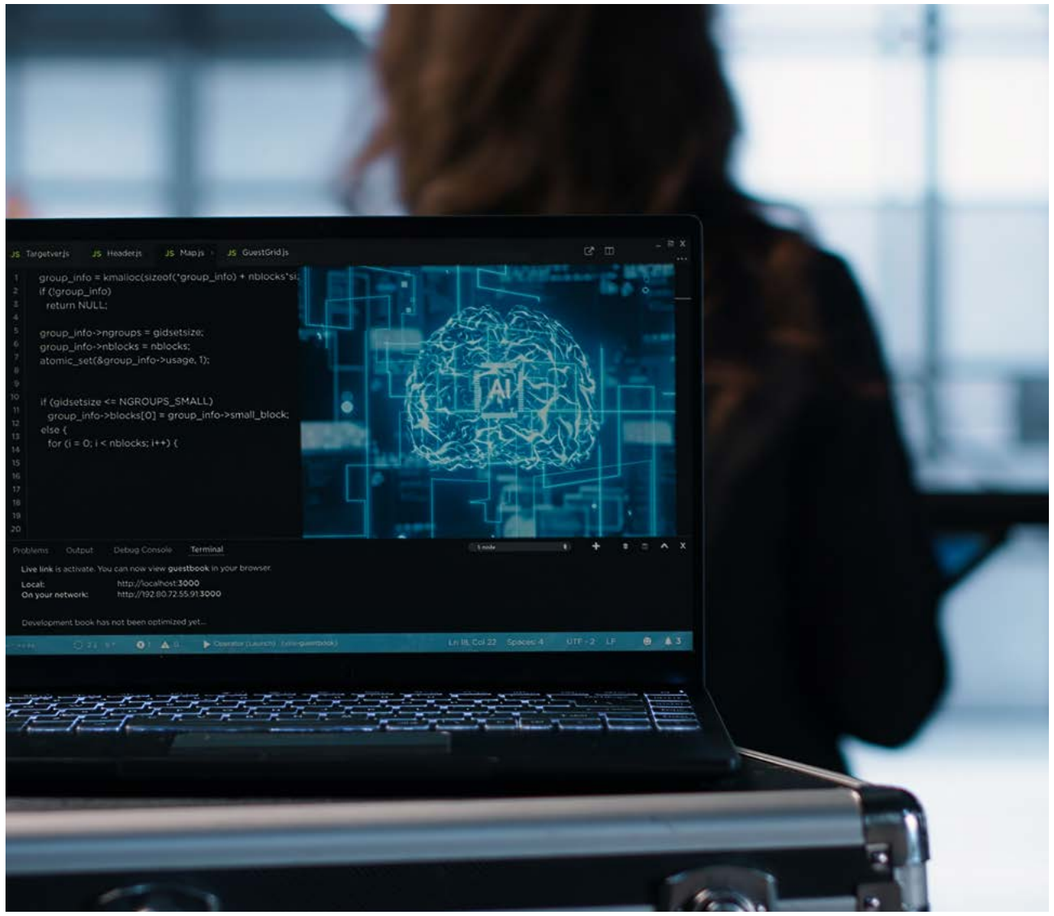
15 Sobre los desafíos que los sistemas de inteligencia artificial plantean para la imputación penal y la responsabilidad jurídica, vid. José Manuel Ríos Corbacho, *Inteligencia artificial y Derecho penal* (Valencia: Tirant lo Blanch, 2020).

16 Günther Jakobs, *Derecho penal: Parte general* (Madrid: Marcial Pons, 1995), 27-35.

producido, sino en la evaluación de las estructuras organizativas destinadas a gestionar el riesgo tecnológico. La responsabilidad penal recaerá así sobre aquellos sujetos que, en virtud de su posición organizativa, poseen el control efectivo sobre la introducción y supervisión de sistemas de inteligencia artificial en el ámbito empresarial[17].

El desarrollo de una teoría de la imputación penal algorítmica no puede limitarse a la identificación de criterios de atribución de responsabilidad ex post. Resulta igualmente necesario analizar los mecanismos institucionales destinados a prevenir la producción de riesgos tecnológicos dentro de las organizaciones. En este contexto, la noción de gobernanza algorítmica adquiere una relevancia central.

4. Gobernanza algorítmica y *compliance* penal



La gobernanza algorítmica puede concebirse como una dimensión específica del *compliance* penal orientada a la gestión del riesgo tecnológico organizativo. Diversos autores han señalado que la implementación de mecanismos de gobernanza algorítmica constituye una condición necesaria para garantizar la rendición de cuentas en entornos de decisión automatizada. La opacidad de muchos sistemas de aprendizaje automático puede dificultar la identificación de las causas que han conducido a una determinada decisión, lo que plantea importantes problemas desde la perspectiva de la responsabilidad jurídica.

Por esta razón, los sistemas de compliance penal deben incorporar herramientas específicas destinadas a garantizar la transparencia y supervisión de los sistemas algorítmicos utilizados por la organización. Entre los mecanismos más relevantes pueden destacarse auditorías algorítmicas destinadas a evaluar el funcionamiento del sistema; controles de calidad sobre los datos utilizados para el entrenamiento de los modelos; evaluaciones de impacto jurídico y ético del uso de sistemas de inteligencia artificial; mecanismos de supervisión humana significativa sobre las decisiones automatizadas; y protocolos internos destinados a garantizar la trazabilidad de los procesos decisionales. La incorporación de estos instrumentos permite integrar el control de los sistemas de inteligencia artificial dentro de los programas de compliance empresarial, transformando estos programas en verdaderos sistemas de gobernanza del riesgo tecnológico.

Cuando una empresa incorpora tecnologías de inteligencia artificial en su actividad productiva, asume la responsabilidad de establecer mecanismos adecuados de supervisión y control sobre el funcionamiento de dichos sistemas. La ausencia de tales mecanismos puede constituir un indicio de defecto organizativo, elemento central en los modelos contemporáneos de imputación penal a las personas jurídicas.

El marco regulatorio europeo de la inteligencia artificial conlleva implicaciones para el *compliance* penal[18]. Como es conocido, el Reglamento (UE) 2024/1689 sobre inteligencia artificial, comúnmente denominado como *Artificial Intelligence Act*, establece un sistema de regulación basado en el nivel de riesgo asociado a los diferentes sistemas de IA[19]. El reglamento distingue cuatro categorías principales de riesgo: sistemas de riesgo inaceptable, sistemas de alto riesgo, sistemas de riesgo limitado y sistemas de riesgo mínimo. Entre los segundos, los sistemas de inteligencia artificial considerados de alto riesgo, están sujetos a obligaciones estrictas, tales como sistemas de gestión de riesgos, requisitos de calidad de los datos, documentación técnica, transparencia algorítmica y supervisión humana obligatoria. Estas obligaciones tienen importantes implicaciones para los programas de *compliance* empresarial. En particular, el *AI Act* refuerza la necesidad de integrar mecanismos de gobernanza tecnológica dentro de los sistemas de cumplimiento normativo. El incumplimiento de las obligaciones establecidas por el *AI Act* podría constituir un indicio relevante de defecto organizativo, elemento central en los modelos de responsabilidad penal corporativa.

Asimismo, el reglamento introduce principios fundamentales para el desarrollo de sistemas de inteligencia artificial confiables, como los ya frecuentemente citados transparencia, trazabilidad, seguridad tecnológica y supervisión humana. Estos principios pueden integrarse en los programas de *compliance penal* como criterios de evaluación del riesgo tecnológico. De este modo, la regulación europea de la inteligencia artificial no solo establece un marco administrativo para el desarrollo de estas tecnologías, sino que también contribuye a configurar los estándares de diligencia organizativa exigibles a las empresas en el ámbito penal.

17 Sobre las nuevas formas de criminalidad asociadas a tecnologías digitales y algoritmos, vid. Eric Hilgendorf y Brian Valerius, *Computer- und Internetstrafrecht* (Heidelberg: Springer, 2020).

18 Paz M. de la Cuesta Aguado, "El Derecho penal frente al Reglamento de Inteligencia Artificial", *Revista Ius Criminale*, n.º 1 (2024): 83-107. https://dialnet.unirioja.es/servlet/articulo?codigo=9972781

19 Sobre el impacto del AI Act en la regulación de sistemas algoritmicos y sus implicaciones jurídicas, vid. Luciano Floridi, *The Ethics of Artificial Intelligence* (Oxford: Oxford University Press, 2023).

5 Conclusiones: Hacia un modelo de *compliance* penal algorítmico

A lo largo de estas páginas se han puesto de relieve las ventajas de usar IA en *compliance* penal, reflejado en la mejora en la prevención del delito. En efecto, la IA permite detectar patrones de fraude, corrupción o blanqueo, refuerza la función preventiva del *compliance* (núcleo del Derecho penal económico); la automatización y la eficiencia (análisis masivo de datos (transacciones, emails, contratos), reduce costes operativos y errores humanos.); la monitorización continua (sistemas de vigilancia en tiempo real, mayor capacidad de reacción frente a riesgos); evidencia documental en cuanto que genera trazabilidad útil en procesos penales (prueba de diligencia debida).

La interacción entre inteligencia artificial y *compliance* penal genera un doble escenario. Por una parte, las tecnologías algorítmicas pueden reforzar significativamente los mecanismos de prevención del delito empresarial mediante herramientas avanzadas de análisis de datos y detección de irregularidades. Por otra, pueden generar decisiones automatizadas cuya lógica interna resulta difícilmente explicable y cuya atribución de responsabilidad plantea importantes desafíos desde la perspectiva del Derecho penal. Ello hace que se proponga el desarrollo de una teoría de la imputación penal algorítmica. En lugar de concebir los sistemas algorítmicos como sujetos autónomos de responsabilidad jurídica, la imputación debe centrarse en las estructuras organizativas que generan y gestionan el riesgo tecnológico.

A partir de este planteamiento dogmático, se propone avanzar hacia un modelo de *compliance* penal algorítmico. Este modelo puede articularse en torno a cinco principios fundamentales: principio de gobernanza algorítmica, principio de transparencia y explicabilidad tecnológica, principio de supervisión humana, principio de gestión preventiva del riesgo tecnológico, principio de trazabilidad y responsabilidad organizativa. El desarrollo de modelos de *compliance* penal algorítmico no constituye únicamente una evolución técnica de los programas de cumplimiento empresarial, sino una condición necesaria para garantizar la responsabilidad jurídica y la gobernanza del riesgo tecnológico en las organizaciones del siglo XXI. Ahora bien, no conviene caer en la tentación de delegar en la IA la creación de políticas de *compliance*. Por mucho que avance la tecnología, no hay inteligencia artificial que pueda sustituir a aquellos profesionales que llevan años diseñando políticas a medida, trabajando de forma individual y sin estandarización de ningún tipo. De nuevo, la centralidad humana se erige en el principio orientador del uso de la IA.

En definitiva, la inteligencia artificial constituye una herramienta de gran potencial para el *compliance* penal, al mejorar la capacidad preventiva, la eficiencia y la trazabilidad de los sistemas de control interno. No obstante, su utilización plantea importantes desafíos jurídicos, especialmente en relación con la imputación de responsabilidad, la transparencia y la protección de derechos fundamentales.

Desde una perspectiva comparada, puede afirmarse que, con relación a España, la IA se integra en un sistema consolidado, donde puede reforzar la eficacia del compliance y contribuir a la exención de responsabilidad penal. En cuanto a Ecuador, la IA representa una oportunidad de modernización, pero su implementación se enfrenta a importantes riesgos derivados de la inseguridad jurídica y la falta de desarrollo doctrinal. En cualquier caso, el futuro del compliance penal pasa por una integración equilibrada de la IA, basada en principios de transparencia, supervisión humana y responsabilidad.

Bibliografía

Beck, Ulrich. *La sociedad del riesgo: Hacia una nueva modernidad*. Barcelona: Paidós, 1998.

Belloso Martín, Nuria. "Los códigos de conducta como proyección del liderazgo cívico". En *Liderazgo y compromiso cívico en el siglo XXI*, coordinado por Paloma Durán y Lalaguna, 197-237. Córdoba: Editorial Almuzara, 2025.

Bellver Belda, Javier. "El uso de la inteligencia artificial en el ámbito del compliance: posibilidades, limitaciones y perspectivas de futuro". *ElDerecho.com*, 19 de julio de 2023. https://elderecho.com/uso-inteligencia-artificial-ambito-compliance-posibilidades-limitaciones.

De la Cuesta Aguado, Paz M. "El Derecho penal frente al Reglamento de Inteligencia Artificial". *Revista Ius Criminale*, n.° 1 (2024): 83-107. https://dialnet.unirioja.es/servlet/articulo?codigo=9972781.

Fletcher, George P. *Rethinking Criminal Law*. Oxford: Oxford University Press, 2000.

Floridi, Luciano. *The Ethics of Artificial Intelligence*. Oxford: Oxford University Press, 2023.

Gómez-Jara Díez, Carlos. *Corporate Criminal Liability: Prevention, Compliance and Corporate Governance*. Cheltenham: Edward Elgar, 2015.

Hilgendorf, Eric y Brian Valerius. *Computer- und Internetstrafrecht*. Heidelberg: Springer, 2020.

Jakobs, Günther. *Derecho penal: Parte general*. Madrid: Marcial Pons, 1995.

Lefebvre. "Compliance penal: una herramienta para implantar un programa de vigilancia y control eficaz de la actividad de la empresa". Lefebvre, accedido 15 de abril de 2026. https://lefebvre.es/actualidad/corporativa/compliance-penal-una-herramienta-para-implantar-un-programa-de-vigilancia-y-control-eficaz-de-la-actividad-de-la-empresa/

LexGo. "PrudencIA: La mejor inteligencia artificial para compliance penal, financiero, energético y regulatorio". LexGo, accedido 15 de abril de 2026. https://lexgoapp.com/guias-legales/compliance-penal/la-mejor-inteligencia-artificial-para-compliance-penal-financiero-energetico-y-regulatorio.

Nieto Martín, Adán. *Compliance y Derecho penal económico*. Valencia: Tirant lo Blanch, 2015.

O'Neil, Cathy. *Weapons of Math Destruction*. Nueva York: Crown Publishing, 2016.

Parlamento Europeo y Consejo de la Unión Europea. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial. *Diario Oficial de la Unión Europea* L, 12 de julio de 2024. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=OJ:L_202401689.

Pazmiño Ruiz, José Roberto y Juan Francisco Pozo Torres. "Responsabilidad penal de las personas jurídicas y compliance: caso Ecuador". *Derecho Penal y Criminología* 40, n.° 109 (2019): 89-122. doi:10.18601/01210483.v40n109.04.

Ríos Corbacho, José Manuel. *Inteligencia artificial y Derecho penal*. Valencia: Tirant lo Blanch, 2020.

Ríos, Susana. "Responsabilidad penal y sistemas de inteligencia artificial". *Revista Electrónica de Ciencia Penal y Criminología*, n.° 24-27 (2022): 1-35. http://criminet.ugr.es/recpc/24/recpc24-27.pdf.

Roxin, Claus. *Derecho penal: Parte general*. Madrid: Civitas, 1997.

Silva Sánchez, Jesús-María. *La expansión del Derecho penal*. Madrid: Civitas, 2001.

Vázquez de Castro, Eduardo. "La inminente obligatoriedad del 'compliance' en las organizaciones como imperativo europeo: protección jurídica de la empresa, del denunciante y del denunciado". *Revista Aranzadi de derecho patrimonial*, n.° 53 (2020).

Xavier Januário, Túlio Felippe. "Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales". *Estudios Penales y Criminológicos* 44, extra (2023): 1-39. https://dialnet.unirioja.es/ejemplar/657488.

LA IA COMO HERRAMIENTA ASISTENCIAL EN EL PROCESO PENAL ESPAÑOL:

POTENCIAL, RIESGOS Y LÍMITES

Lucana Mª Estévez Mendoza[1]

1. Introducción

La inteligencia artificial (IA) se ha convertido en un elemento omnipresente en la vida contemporánea, integrándose de manera silenciosa, pero decisiva, prácticamente en todos los ámbitos de la sociedad.

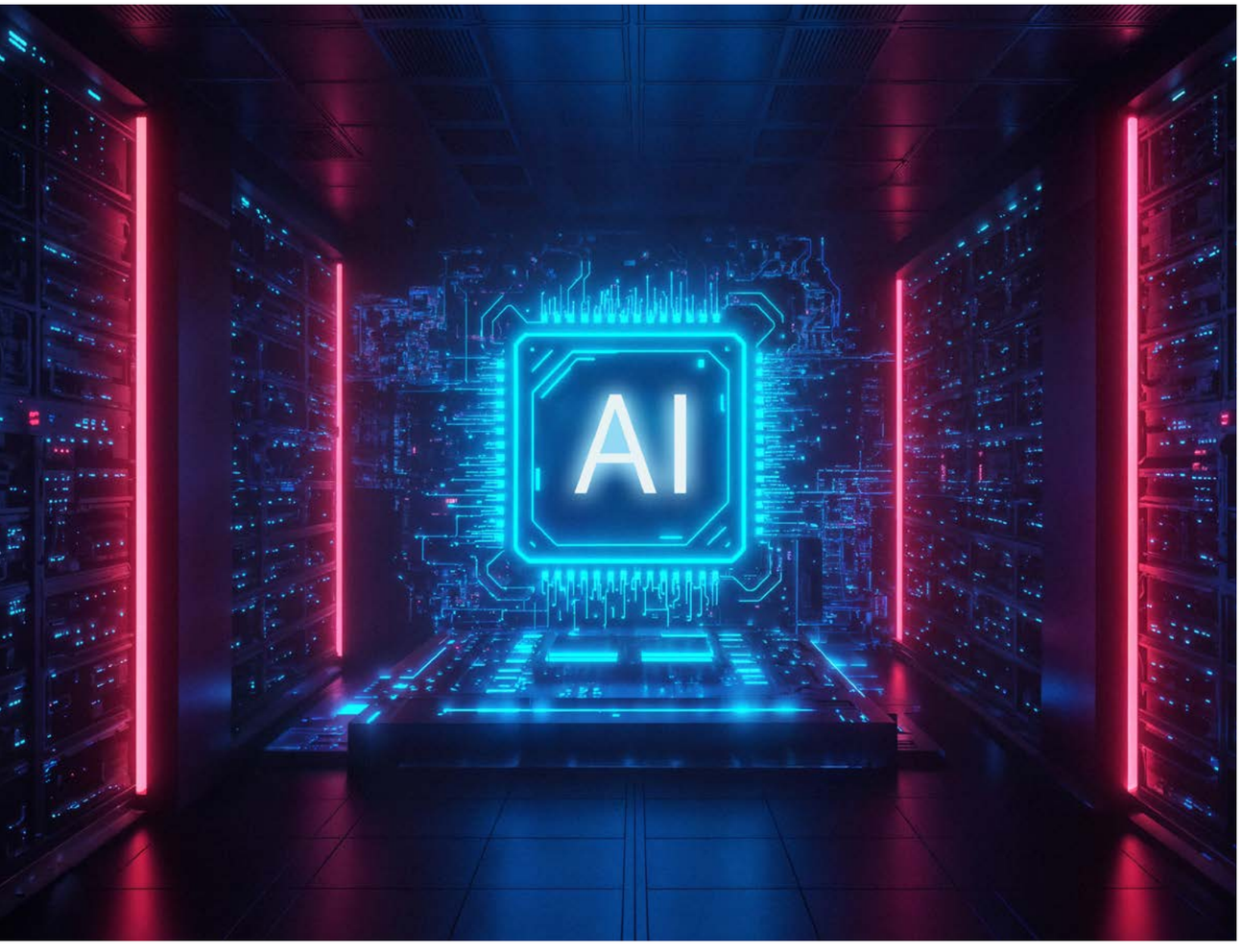
Su expansión no ha dejado al margen al proceso penal, donde emerge, por un lado, como herramienta con un potencial enorme para optimizar y agilizar los trámites procesales en manos del personal de la Administración de Justicia, tanto operadores jurídicos como cuerpos policiales y, por otro lado, como recurso empleado por quienes cometen delitos, ya sea para facilitar nuevas formas de criminalidad o para perfeccionar los métodos tradicionales, pues a nadie escapa ya que la tecnología puede ser instrumentalizada con fines ilícitos. Sirva de ejemplo la existencia de herramientas de generación de contenido, la automatización de ataques informáticos, la suplantación de identidad o la manipulación de evidencias digitales.

1 Profesora de Derecho Procesal, Universidad de Las Palmas de Gran Canaria, España.

Este doble impacto convierte a la IA en un fenómeno que exige un análisis riguroso desde la perspectiva jurídicopenal. Este trabajo se centra únicamente en la vertiente asistencial, no criminal, de la IA en el contexto penal, para lo que se plantea un estudio que considera tanto el potencial de la IA para mejorar la eficacia del sistema penal, como los riesgos que introduce en términos de seguridad, garantías procesales y derechos fundamentales.

Cómo podrían incluirse sistemas de IA en un proceso de naturaleza penal y para qué actuaciones es la cuestión concreta a la que se tratará de dar respuesta, partiendo de un sistema penal formalmente acusatorio o mixto[2], que responde a un modelo en dos fases (investigación y enjuiciamiento), propio del Derecho continental, y de la normativa europea y española que avala el uso de la IA en Justicia, de la que derivan su ámbito de posible aplicación y sus límites.

Para ello, en primer lugar, se realiza una aproximación al concepto de IA y sus clases y, en segundo lugar, se aborda qué papel pueden desempeñar estas herramientas en un proceso penal, concluyendo con una valoración de los riesgos inherentes a la IA que marcan su efectividad.



2 Teresa Armenta Deu, "Debido proceso, sistemas y reforma del proceso penal", *Revista Brasileira de Direito Processual Penal* 1, n.º 1 (2015): 131-133.

2. Aproximación conceptual a la IA y sus tipologías

Desde el punto de vista etimológico, la IA es una expresión compuesta por dos vocablos: inteligencia, formado por los lexemas latinos *"inte"* (entre) y *"legere"* (leer, escoger), que unidos se refieren a una actividad relacionada con la capacidad para comprender y conocer las cosas; y artificial, vinculado al término latino *"artificialis"*, compuesto por *"art"* y *"facere"*, configura un adjetivo que identifica el arte producido por el hombre, consecuencia práctica de un aprendizaje.

En los años 50, cuando se sitúa el origen de la IA, McCarthy la define como "la ciencia y la ingeniería de fabricar máquinas inteligentes, en especial máquinas inteligentes de computación"[3]. Como disciplina científica, se identifica con la "rama que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico"[4].

Desde entonces, según el desarrollo tecnológico de esos programas, ha ido cambiando la concepción sobre qué programas son reflejo del concepto de inteligencia atribuido a las máquinas, en función de la capacidad que las mismas han tenido para resolver problemas en entornos complejos en cada momento[5]. De ahí que se suela afirmar que no es sencillo contar con una definición de IA que permanezca invariable en el tiempo.

Aun así, el Reglamento de Inteligencia Artificial (RIA) de la Unión Europea 2024/1689, de 13 de junio, la define en su artículo 3:

> [...] sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.[6]

Tipológicamente, se distinguen dos modelos de IA: la general o *Strong AI*, que implica la combinación de algoritmos con el fin de crear máquinas que presenten las mismas capacidades que el ser humano[7], y la específica o *Weak AI*, que se refiere a cualquier software capaz de ejecutar una tarea asociada habitualmente a un humano[8]. Más recientemente se asocian a la IA calificativos que responden a las nuevas capacidades que han ido adquiriendo estos sistemas.

La IA generativa da nombre a los sistemas surgidos al evolucionar la computación en el uso de redes neuronales con múltiples capas especializadas[9], en la creación de

3 John McCarthy, Marvin Minsky, Nathaniel Rochester, y Claude Shannon, "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence August 31, 1955", *AI Magazine* 27, n.º 4 (2006): 12.

4 Según la Real Academia Española de la Lengua (RAE), https://dle.rae.es/inteligencia#2DxmhCT.

5 Shane Legg y Marcus Hutter, "A collection of definitions of intelligence", *Frontiers in Artificial Intelligence and Application, Advances in Artificial General Intelligence: Concepts, Architecture and Algorithms* 157 (2007): 17-18.

6 Unión Europea, Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial), *Diario Oficial de la Unión Europea* L 2024/1689, 12 de julio de 2024.

7 Iberdrola, "¿Qué es la Inteligencia Artificial? ¿Somos conscientes de los retos y principales aplicaciones de la Inteligencia Artificial?", Iberdrola, accedido 17 de marzo de 2026, https://www.iberdrola.com/innovacion/que-es-inteligencia-artificial.

8 Jorge Morrel Ramos, "La Inteligencia Artificial en el día a día de un abogado: qué le va a enseñar y cómo lo cambiará", *Revista del Consejo General de la Abogacía*, n.º 108 (2018): 7.

9 Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, y Illia Polosukhin, "Attention is all you need", arXiv:1706.03762 [cs.CL], Cornell University, 12 de junio de 2017.

redes convolucionales, capaces de clasificar objetos, reconocer caras, gente andando o etiquetar fotos[10], entre otras habilidades, y en el desarrollo de redes por adversario (*Generative Adversarial Networks*), que ya no requieren de un humano para que verifique si el modelo de IA es bueno o malo, sino que otra red neuronal se encarga de ello, con los que se avanza hacia otro tipo de máquinas capaces no sólo de hacer predicciones, sino de generar alguna forma de contenido.

La IA agentiva o agéntica es la relativa o perteneciente a los agentes, que proceden del campo informático de los sistemas multiagentes a los que ahora se les incorpora los avances de la IA[11]. El agente se define como la "entidad computacional, como un programa de software o un robot, que percibe y actúa sobre su entorno y es autónomo, ya que su comportamiento depende, al menos parcialmente, de su propia experiencia"[12]. Estos agentes son capaces de tomar decisiones y ejecutar acciones por pasos de manera autónoma[13], resolviendo problemas complejos con una supervisión limitada.

3. La incorporación de la IA en el proceso penal

3.1. Marco normativo de referencia

En un escenario en el que el proceso penal de referencia, entendido como el medio por el que los órganos jurisdiccionales cumplen la función de aplicar el derecho penal objetivo al caso concreto, juzgando y haciendo ejecutar lo juzgado (artículo 117 Constitución Española) sea el español, valorar la incorporación de herramientas de IA en él exige tomar en consideración tanto normativa europea como nacional.

En el plano internacional, es el mencionado Reglamento de IA el que determina qué sistemas son posibles a nivel técnico y cuáles admisibles legalmente, utilizando un criterio basado en el nivel de riesgo que implica la técnica empleada y en la finalidad para la que serán utilizados. Se admite el empleo de herramientas de IA en Justicia en general, sin hacer distinción entre órdenes jurisdiccionales ni establecer especialidades respecto al proceso penal, aunque las considera de alto riesgo (Anexo III).

De manera específica, el apartado 8 a) del Anexo III admite los sistemas de IA

> […] destinados a ser utilizados por una autoridad judicial o en su nombre para ayudar en la investigación e interpretación de los hechos y de la ley, así como en la garantía del cumplimiento del Derecho a su conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios.[14]

El apartado 6 lo permite para otros usos que puedan incidir en el ámbito de actuación de los órganos jurisdiccionales, entre los que recoge los destinados a evaluar el riesgo de que una persona física sea víctima de delitos, a actuar como polígrafos o herramientas similares, a valorar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos, a evaluar el riesgo de comisión delictiva o reincidencia, o a elaborar perfiles de personas físicas durante la detección, la investigación o el enjuiciamiento de delitos.

En el plano interno, el uso de las tecnologías de la información y la comunicación en Justicia se desprende, de manera genérica, del artículo 230 de la Ley Orgánica del Poder Judicial 6/1985, de 1 de julio (LOPJ)[15]. Con independencia de otras normas relativas a la Administración electrónica, clave resulta el Real Decreto Ley 6/2023, de 19 de diciembre[16] por habilitar de manera específica el uso de aplicaciones técnicas de IA como instrumento de apoyo a fines jurisdiccionales y organizativos en su artículo 35.1.k), al admitir actuaciones automatizadas, asistidas y proactivas, en los artículos 56 a 58.

Adicionalmente, ha de tenerse en cuenta la Política de uso de la IA en la Administración de Justicia, del Comité Técnico Estatal de la Administración de Justicia Electrónica (CTEAJE), de 21 de junio de 2024[17], la Instrucción 2/2026 sobre utilización de sistemas de IA en el ejercicio de la actividad jurisdiccional del Consejo General del Poder Judicial (CGPJ)[18] y las orientaciones sobre Inteligencia Artificial agéntica de la Agencia Española de Protección de Datos, de febrero de 2026[19].

3.2. Funciones asistenciales según la fase del procedimiento

La finalidad del proceso penal es la realización del *ius puniendi* del Estado, siendo el proceso la única herramienta para aplicar el derecho penal cumpliendo las garantías requeridas y derivadas del principio de legalidad. A través del proceso, los representantes del poder judicial (jueces y magistrados), juzgan causas y juicios criminales, con excepción de los atribuidos a la jurisdicción militar (artículo 9.3 LOPJ), cometidos por españoles o extranjeros en territorio español, con las salvedades legalmente previstas (artículo 23 LOPJ).

Partiendo de esta premisa, tanto el Reglamento europeo de IA como la Instrucción 2/2026 delimitan el ámbito de aplicación de esta tecnología en el entorno judicial, limitándolo a funciones de ayuda, apoyo, auxilio o asistencia de las autoridades judiciales o, se sobreentiende, que de otro personal al servicio o cooperador de la Administración de Justicia cuando se trate de usos que afecten al ámbito de actuación de los órganos jurisdiccionales, como pueden ser los propios de gestión y tramitación del proceso, pero también labores de investigación propias del proceso penal.

La Instrucción 2/2026 se refiere específicamente a los usos permitidos de los sistemas de IA en el ejercicio de la actividad jurisdiccional en su apartado 6.3, recogiendo como finalidades posibles las siguientes:

10 Miguel Jiménez, "El Supremo de EEUU se inclina a mantener el blindaje de redes sociales por su contenido", *El País*, 23 de febrero de 2023.

11 Ana Gutowska, "¿Qué es un sistema multiagente?", IBM, accedido 17 de marzo de 2026, https://www.ibm.com/es-es/think/topics/multiagent-system.

12 Gerhard Weiss, *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence* (Cambridge: MIT Press, 1999), 28.

13 Patricia Jiménez, "IA agéntica: el siguiente paso en la evolución de la inteligencia artificial empresarial", *Arbentia empowering consulting*, 6 de febrero de 2026, https://www.arbentia.com/blog/ia-agentica-siguiente-paso-evolucion-inteligencia-artificial-empresarial/.

14 Unión Europea, Reglamento (UE) 2024/1689, art. 8.a.

15 España, Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, *Boletín Oficial del Estado* 157, 2 de julio de 1985.

16 España, Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, *Boletín Oficial del Estado* 303, 20 de diciembre de 2023.

17 España Ministerio de Justicia, "Política de uso de la Inteligencia Artificial en la Administración de Justicia", Ministerio de Justicia, accedido 17 de marzo de 2026, https://www.administraciondejusticia.gob.es/documents/7557301/7558184/CTEAJE-NOR-Politica+de+uso+de+la+IA+en+la+AJ+v1.0.pdf/ddc0eda1-950b-e926-b367-be511b16f2f9?t=1733925140122.

18 España, Acuerdo de 28 de enero de 2026, del Pleno del Consejo General del Poder Judicial, por el que se aprueba la Instrucción 2/2026, sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional, *Boletín Oficial del Estado* 27, 30 de enero de 2026.

19 España Agencia Española de Protección de Datos, "Orientaciones para el desarrollo de aplicaciones de IA agéntica", Agencia Española de Protección de Datos, accedido 17 de marzo de 2026, https://www.aepd.es/guias/orientaciones-ia-agentica.pdf.

A. Búsqueda y localización de información jurídica, incluida la identificación de normativa, jurisprudencia y doctrina relevante, así como la recuperación de antecedentes procesales o documentales.

B. Análisis, clasificación y estructuración de información, documentos o datos contenidos en actuaciones judiciales, con fines de organización, comprensión o apoyo al estudio del asunto.

C. Elaboración de esquemas, resúmenes o borradores de trabajo interno, siempre que no tengan carácter decisorio ni sustituyan la redacción personal de resoluciones judiciales.

D. Apoyo a tareas organizativas o auxiliares, relacionadas con la gestión del conocimiento jurídico o con la preparación del trabajo jurisdiccional.[20]

Plantear la modernización del proceso penal en este sentido obliga a pensar en trámites o actuaciones concretas que, respondiendo a estos fines, se podrían automatizar incorporando herramientas de IA atendiendo a las fases que estructuran el proceso penal y la finalidad de cada una, pero sin que ello resulte un condicionante.

3.2.1. En la fase de investigación

La instrucción penal implica el desarrollo de actuaciones destinadas a comprobar la existencia de hechos de carácter delictivo, las circunstancias que lo rodean, la identificación del delincuente y los daños ocasionados por él. Además, suele ser en esta etapa donde se valora la necesidad de adoptar medidas cautelares.

Recibida la *notitia criminis*, vía denuncia o querella, se podría hacer uso de asistentes inteligentes para el manejo de casos, para decidir su admisión o no a trámite, pues se trata de actos procesales de contenido determinado, y la robotización de la gestión de documentación legal podría contribuir a detectar si existen o no causas de inadmisión. Precisamente con el fin de identificar denuncias falsas e inadmitirlas se empleaba en España Veripol[21].

La IA podría incluso preparar un borrador de escrito judicial de admisión o inadmisión en base a algoritmos lógicos capaces de estructurar documentos, que siempre que fuera validado por un juez, magistrado, fiscal o Letrado de la Administración de Justicia, en el ámbito de sus competencias, respetaría el principio de control humano (artículo 14 del RIA y apartados 4 a) y 7.2 de la Instrucción 2/2026).

Con relación a algunas diligencias de investigación se usan, desde hace años en varios países, herramientas de IA con fines diversos, algunos predictivos de conductas delictivas primarias o de reincidencia, otros de evaluación de riesgos, que siendo de reincidencia pueden emplearse en la valoración de la adopción de medidas cautelares, o simplemente para la asignación de recursos o con fines asistenciales de los operadores jurídicos[22]. Sirvan de ejemplo herramientas como[23]: los archiconocidos COMPAS o PREDPOL, con fines predictivos, en Estados Unidos; VICTOR, usado en Brasil para apoyar la toma de decisiones en procesos judiciales, especialmente en la evaluación de riesgos y la clasificación de casos; en Alemania, el sistema OLGA ayuda a jueces y fiscales a acceder a bases de datos sobre crimen organizado, acelerando el análisis de expedientes complejos[24]; en Reino Unido, HART[25]; en Holanda, VALCRI[26] y CAS en Ámsterdam; o VioGen, en España, que evalúa el riesgo de violencia de género y optimiza la distribución de recursos policiales para proteger a las víctimas[27].

El mantenimiento de las existentes, la incorporación de las que operan en otros Estados o el diseño de nuevas herramientas es admisible técnica y legalmente siempre que cumplan los fines descritos y las obligaciones que les impone el Reglamento de IA.

3.3.2. En la fase de enjuiciamiento

La fase de enjuiciamiento se caracteriza porque en ella las partes realizan sus alegaciones y aportan y practican pruebas, correspondiendo a la autoridad judicial su validación y valoración, además de la resolución del caso en sí mismo.

Los roles de los sujetos intervinientes en esta fase están predeterminados, pero nada impide que durante la práctica de las pruebas los jueces o magistrados puedan apoyarse en IA que les ayuden, por ejemplo, en interrogatorios y tomas de declaración a encausados, víctimas, testigos, peritos o incluso en careos[28]. Por sus características, robots capaces de realizar análisis computacionales del movimiento, de mantener conversaciones e interpretar emociones, que asistan pasivamente en tales actuaciones podrían ser de utilidad[29], resultando similar a contar con una especie de polígrafo que incluso podría facilitar al juez un borrador de informe psicofisiológico.

Sistemas de IA basados en analítica predictiva son ya empleados por los jueces en la toma de decisiones. Si bien hasta ahora nada impedía recurrir a IA generalistas, no diseñadas específicamente para la Administración de Justicia, en España, tal práctica queda prohibida por la Instrucción 2/2026, al establecer que en el ejercicio de la actividad jurisdiccional "única y exclusivamente" se podrán utilizar sistemas de IA facilitados por el CGPJ o por las Administraciones competentes, para dar cabida a las Comunidades Autónomas. Ello excluye la posibilidad de hacer uso de IA específicas como Justicio.es por ser de acceso abierto y no pertenecer a las entidades mencionadas[30].

Ahora bien, sí podrían utilizarse sistemas de IA que cumplan los requisitos y exigencias legales, en la búsqueda de jurisprudencia precedente (caso de HJ en el seno de Tribunal

20 España, Acuerdo de 28 de enero de 2026, Instrucción 2/2026, art. sexto.

21 Veripol fue presentada en 2018 como un algoritmo capaz de detectar denuncias falsas de robo con violencia, con una precisión de más del 90%. Se estuvo usando durante seis años, aunque en 2024, tras la publicación del Reglamento europeo de IA su uso se descartó, por no cumplir con las exigencias que le imponen como sistema de alto riesgo. Ter García, Carmen Torrecillas, Adrián Maqueda, y David Cabo, "La Policía Nacional deja de usar Veripol, su IA estrella para detectar denuncias falsas", Civio, 19 de marzo de 2025, https://civio.es/transparencia/2025/03/19/la-policia-nacional-deja-de-usar-veripol-su-ia-estrella-para-detectar-denuncias-falsas/.

22 Lucana Estévez Mendoza, "Prevención e investigación de delitos en España: ¿un nuevo terreno para la IA?", en *FODERTICS 8.0: estudios sobre tecnologías disruptivas y justicia*, coord. Irene González Pulido y dir. Federico Bueno de Mata (Granada: Comares, 2020), 259-272.

23 Xulio Ferreiro Baamonde, "La utilización de herramientas de Inteligencia Artificial en el proceso penal bajo el prisma de la propuesta de reglamento de inteligencia artificial", en *Desafíos del derecho procesal del siglo XXI: prueba prohibida, inteligencia artificial y digitalización de la administración de justicia*, coord. Agustín Pérez Cruz Martín, Sonia Calaza López y José María Roca Martínez (Madrid: Dykinson, 2024), 69-110.

24 Fair Trial, "Automating injustice: the use of artificial intelligence & automated decision-making systems in criminal justice in Europe", Fair Trial, accedido 17 de marzo de 2026, https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf.

25 Marion Oswald, Jamie Grace, Sheena Urwin, y Geoffrey C. Barnes, "Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality", *Information & Communications Technology Law* 27, n.º 2 (2018): 223-250.

26 Timothy Revell, "AI detective analyses police data to learn how to crack cases", *NewScientist*, 10 de mayo de 2017, https://www.newscientist.com/article/mg23431254-000-ai-detective-analyses-police-data-to-learn-how-to-crack-cases/.

27 Lara Cuevas Esteban, "Predicción de la reincidencia a partir del sistema policial de valoración del riesgo de Violencia de Género (VdG)" (tesis doctoral, Universidad Autónoma de Madrid, 2025), https://repositorio.uam.es/entities/publication/4be28be1-7740-4662-857d-6c72199b9512.

28 Lucana Estévez Mendoza, "La pregunta simbiótica: ¿robots en el proceso penal español?", 40-145.

29 Mirian Guardiola Salmerón, "Retos, desafíos y nuevas oportunidades", *Revista del Consejo General de la Abogacía Española*, n.º 108 (2018): 10.

30 Ver respecto a esta herramienta Justicio, "Acerca de Justicio", Justicio, accedido 17 de marzo de 2026, https://justicio.es/acerca.

Constitucional), para llevar a cabo la determinación de la pena, tanto de prisión como de multa o indemnizaciones, o la cuantificación de las costas, siempre que el cálculo fuera luego validado por la persona competente, así como para obtener borradores de resoluciones judiciales o procesales supervisados. De hecho, en Cataluña hay en marcha un proyecto piloto en este sentido, denominado IA4Justice[31], que generando borradores de sentencias ha supuesto un ahorro de 12.000 horas de trabajo y 552.000€ por cada 20 jueces, al reducir el tiempo de redacción medio de 2 horas a 20 minutos[32].

3.2.3. A lo largo de todo el proceso



La asignación de casos a los tribunales competentes se realiza por sistema de reparto que, en ocasiones, está automatizado. No obstante, se podría trabajar para detectar casos relacionados o conexos, con el fin de acumularlos o considerarlos durante las instrucciones. Un *bot* podría desempeñar esta tarea según los casos abiertos por demarcaciones territoriales más o menos amplias e incluso a nivel nacional, agilizando el proceso y evitando duplicidades de manera más fiable que la que se emplea en la actualidad (de forma manual), incrementando incluso las posibilidades de identificación.

Las IA podrían asumir, en todas las fases del proceso, tareas características del personal de auxilio judicial, tales como la práctica y gestión de actos de comunicación. Éstos se podrían automatizar y gestionar telemáticamente, como hacen en Estados Unidos sistemas tipo *Gina* para cuestiones de tráfico o *Jury Chat Bot* con relación al jurado[33]. Asimismo, podrían apoyar la labor de los funcionarios de los cuerpos tanto de Gestión Procesal como de Tramitación Procesal y Administrativa[34].

Otras tareas que se podrían automatizar pueden ser las de control del orden en las salas de los tribunales, las de vigilancia, las de archivo de autos y expedientes judiciales, bajo la supervisión del Letrado de la Administración de Justicia. Éstas podrían ser asumidas, tanto por su capacitación operativa como por su cualificación, por robots tipo el androide Anbot[35]. Esa función de policía que podría asumir sería trasladable a otras fases del proceso penal, como la ejecución de sentencias de privación de libertad, asistiendo a agentes de la autoridad en casos concretos o, incluso, en supuestos de ejecución de embargos y lanzamientos, vinculados a condenas por ejercicio de acciones civiles derivadas de delitos.

31 Ayllen Gil Seaton, "Eficiencia organizativa y el uso de la IA en los tribunales españoles", *IurisCrimPol, Blog de Estudios de Derecho y Ciencia Política*, Universidad Oberta de Cataluña, 10 de octubre de 2025.

32 Sergi Llanas, "Cataluña impulsa un plan para agilizar la resolución de sentencias judiciales con Inteligencia Artificial", *El País*, 13 de marzo de 2025.

33 Jeff J. Horn, "Artificial Intelligence in the Courts", *Our Latest Blog, Horn Law Group*, n.º 8 (2020).

34 Javier Ercilla García, "Agentes de Inteligencia Artificial en la Administración de Justicia española: marco normativo y potencial de implementación", *La Ley Digital, Derecho Digital e Innovación*, n.º 22 (2024): 13-21.

35 Deusartificial, "AnBot, El Robot Chino", Deusartificial, 27 de noviembre de 2019, https://deusartificial.com/anbotel-robot-chino/.

4. Ventajas, riesgos y límites

La aplicación de esta tecnología en la justicia penal lleva aparejada considerables ventajas, como la eficacia, el equilibrio entre el hombre y la máquina y poder disponer de herramientas a la altura de la época actual para apoyar el trabajo de jueces y magistrados, como si de un aparato ortopédico que les ayuda a trabajar mejor se tratara. Sin embargo, al mismo tiempo plantea riesgos diversos.

Por un lado, su uso puede ocasionar una pérdida de autonomía del usuario, por la dependencia que puede generar, viéndose éste condicionado por la propuesta o predicción que la IA pueda dar. Además, conlleva una falta de adecuación a los cambios legislativos y jurisprudenciales, por el tiempo de aprendizaje que requieren. Para minimizar este riesgo, la normativa nacional exige proporcionalidad, uso responsable, independencia y responsabilidad judicial, en tanto que impone un control humano real y consciente, como principios de utilización de la IA en el ejercicio de la actividad jurisdiccional (apartados a, c y h de la Instrucción 2/2026). Cuestión distinta es que queda pendiente articular cómo controlar tal responsabilidad y las posibles sanciones derivadas de un uso erróneo o automático de las herramientas por parte de los operadores jurídicos. Por otro lado, conlleva problemas vinculados a la transparencia, la equidad, la ética, y la protección de los derechos fundamentales que se hace necesario abordar.

La equidad algorítmica, entendida como la ausencia de sesgos[36], no sólo es un objetivo que controla el Reglamento de IA a través de las exigencias impuestas a la creación y distribución de sistemas de IA, especialmente de alto riesgo, sino que reitera la normativa nacional al introducir como principio de actuación su prevención, obligando a adoptar cautelas para identificar la existencia de sesgos y tratar de corregirlos.

La transparencia algorítmica[37] exige explicabilidad, garantizar que las decisiones ejecutadas por sistemas algorítmicos puedan ser auditadas, evaluadas y explicadas por sus responsables para que sus procesos de toma de decisiones sean comprensibles, especialmente cuando tienen consecuencias significativas para las personas, como sucede en el marco de un proceso penal. El Reglamento de IA establece requisitos estrictos al respecto, imponiendo a los desarrolladores la obligación de proporcionar explicaciones claras y accesibles sobre cómo sus algoritmos toman decisiones.

El respeto a los derechos fundamentales resulta esencial, convirtiéndose en otro de los principios de utilización de los sistemas de IA en justicia. De manera particular se debe velar por no afectar a la tutela judicial efectiva, la igualdad ni la protección de datos personales. Ahora bien, para ello quizás haga falta el diseño de nuevas garantías de protección o la reformulación de las existentes.

36 BBVA, "Equidad algorítmica, clave para crear una inteligencia artificial responsable", BBVA, 30 de julio de 2024, https://www.bbva.com/es/innovacion/equidad-algoritmica-clave-para-crear-una-inteligencia-artificial-responsable/.

37 Gabriele Vestri, "Cinco claves para entender la transparencia algorítmica en el sector público", IDP-Observatorio de Derecho Público, 30 de marzo de 2023, https://idpbarcelona.net/cinco-claves-para-entender-la-transparencia-algoritmica-en-el-sector-publico/.

Conclusiones

No se puede negar que la automatización de determinados procesos, a través de instrumentos de IA, puede mejorar el trabajo de los tribunales, agilizar los procedimientos al procesar millones de datos en milésimas de segundos y gestionar tareas legales de carácter repetitivo, eliminar trámites innecesarios, reducir plazos e incluso simplificar la prueba, permitiendo obtener resultados que incrementen la eficiencia procesal y la eficacia judicial.

El potencial de la IA es sin duda enorme e incalculable, de ahí que los retos a asumir en el futuro sean también considerables, apotropaicos, como ya he señalado en alguna ocasión anterior, pero no por ello inasumibles. En esa tarea lo que no debe olvidarse es que la incorporación y desarrollo de herramientas de IA en el proceso penal empieza a ser una realidad, pero que su eficacia y compatibilidad con las garantías procesales y derechos fundamentales exige aún, en España, abordar diferentes cuestiones:

La primera, aclarar si los principios rectores generales diseñados para el personal con funciones jurisdiccionales son trasladables, *mutatis mutandi*, a la labor de los cuerpos policiales que actúan en relación con la Administración de Justicia o si requieren de concreción o complemento, dada la especificidad de las funciones que éstos desarrollan.

La segunda, que el personal de la Administración de Justicia en disposición de usar herramientas de IA asuma la responsabilidad de realmente utilizar única y exclusivamente programas específicos creados para ellos por las autoridades competentes en el ejercicio de las funciones que le son propias.

La tercera, que jueces, magistrados, Letrados de la Administración de Justicia y resto de funcionarios intervinientes en la función jurisdiccional controlen de manera real la validación de las decisiones asistidas, pues ello será clave para que operadores jurídicos y justiciables confíen en el nuevo paradigma procesal que se vislumbra.

La cuarta, que sea el Derecho el que lidere el proceso de transformación tecnológica, pero en equilibrio con los expertos en tecnología, pues abusar de la regulación puede dejar al margen la innovación, y dar prioridad a las ciencias de la computación puede pasar por alto las premisas del Estado de Derecho en que se pretende que convivan.

En definitiva, para todo ello se requiere tiempo, conciencia, formación y capacitación, pues solo de esa forma la sociedad judicial se acostumbrará a trabajar con las máquinas como lo está haciendo el resto de los sectores, trabajando por encontrar el lugar que cada uno debe ocupar que, de momento, no pasa por contar con jueces robot en sentido estricto, que resuelvan conflictos de manera autónoma, algo que si bien de momento en Europa y en España es impensable, dadas las restricciones legales existentes para ello, podría no ser imposible en el futuro.

Bibliografía

Armenta Deu, Teresa. "Debido proceso, sistemas y reforma del proceso penal". *Revista Brasileira de Direito Processual Penal* 1, n.º 1 (2015): 121-139.

BBVA. "Equidad algorítmica, clave para crear una inteligencia artificial responsable". BBVA. 30 de julio de 2024. https://www.bbva.com/es/innovacion/equidad-algoritmica-clave-para-crear-una-inteligencia-artificial-responsable/.

Cuevas Esteban, Lara. "Predicción de la reincidencia a partir del sistema policial de valoración del riesgo de Violencia de Género (VdG)". Tesis doctoral, Universidad Autónoma de Madrid, 2025. https://repositorio.uam.es/entities/publication/4be28be1-7740-4662-857d-6c72199b9512.

Deusartificial. "AnBot, El Robot Chino". Deusartificial. 27 de noviembre de 2019. https://deusartificial.com/anbotel-robot-chino/.

Ercilla García, Javier. "Agentes de Inteligencia Artificial en la Administración de Justicia española: marco normativo y potencial de implementación". *La Ley Digital, Derecho Digital e Innovación*, n.º 22 (2024): 1-34.

España. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *Boletín Oficial del Estado* 157, 2 de julio de 1985.

España. Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. *Boletín Oficial del Estado* 303, 20 de diciembre de 2023.

España Ministerio de Justicia. "Política de uso de la Inteligencia Artificial en la Administración de Justicia". Ministerio de Justicia. Accedido 17 de marzo de 2026. https://www.administraciondejusticia.gob.es/documents/7557301/7558184/CTEAJE-NOR-Politica+de+uso+de+la+IA+en+la+AJ+v1.0.pdf/ddc0eda1-950b-e926-b367-be511b16f2f9?t=1733925140122.

España. Acuerdo de 28 de enero de 2026, del Pleno del Consejo General del Poder Judicial, por el que se aprueba la Instrucción 2/2026, sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional. *Boletín Oficial del Estado* 27, 30 de enero de 2026.

España Agencia Española de Protección de Datos. "Orientaciones para el desarrollo de aplicaciones de IA agéntica". Agencia Española de Protección de Datos. Accedido 17 de marzo de 2026. https://www.aepd.es/guias/orientaciones-ia-agentica.pdf.

Estévez Mendoza, Lucana. "La pregunta simbiótica: ¿robots en el proceso penal español?". En *El impacto de las tecnologías disruptivas en el derecho procesal*, dirigido por Federico Bueno de Mata, 245-268. Valencia: Aranzadi Thomson Reuters, 2022.

————. "Prevención e investigación de delitos en España: ¿un nuevo terreno para la IA?". En *FODERTICS 8.0: estudios sobre tecnologías disruptivas y justicia*, coordinado por Irene González Pulido y dirigido por Federico Bueno de Mata, 189-210. Granada: Comares, 2020.

Fair Trial. "Automating injustice: the use of artificial intelligence & automated decision-making systems in criminal justice in Europe". Fair Trial. Accedido 17 de marzo de 2026. https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf.

Ferreiro Baamonde, Xulio. "La utilización de herramientas de Inteligencia Artificial en el proceso penal bajo el prisma de la propuesta de reglamento de inteligencia artificial". En

Desafíos del derecho procesal del siglo XXI: prueba prohibida, inteligencia artificial y digitalización de la administración de justicia, coordinado por Agustín Pérez Cruz Martín, Sonia Calaza López y José María Roca Martínez, 315-342. Madrid: Dykinson, 2024.

García, Ter, Carmen Torrecillas, Adrián Maqueda, y David Cabo. "La Policía Nacional deja de usar Veripol, su IA estrella para detectar denuncias falsas". Civio. 19 de marzo de 2025. https://civio.es/transparencia/2025/03/19/la-policia-nacional-deja-de-usar-veripol-su-ia-estrella-para-detectar-denuncias-falsas/.

Gil Seaton, Ayllen. "Eficiencia organizativa y el uso de la IA en los tribunales españoles". *IurisCrimPol, Blog de Estudios de Derecho y Ciencia Política*, Universidad Oberta de Cataluña. 10 de octubre de 2025.

Guardiola Salmerón, Mirian. "Retos, desafíos y nuevas oportunidades". *Revista del Consejo General de la Abogacía Española*, n.º 108 (2018): 10-13.

Gutowska, Ana. "¿Qué es un sistema multiagente?". IBM. Accedido 17 de marzo de 2026. https://www.ibm.com/es-es/think/topics/multiagent-system.

Horn, Jeff J. "Artificial Intelligence in the Courts". *Our Latest Blog, Horn Law Group*, n.º 8 (2020).

Iberdrola. "¿Qué es la Inteligencia Artificial? ¿Somos conscientes de los retos y principales aplicaciones de la Inteligencia Artificial?". Iberdrola. Accedido 17 de marzo de 2026. https://www.iberdrola.com/innovacion/que-es-inteligencia-artificial.

Jiménez, Miguel. "El Supremo de EEUU se inclina a mantener el blindaje de redes sociales por su contenido". *El País*. 23 de febrero de 2023.

Jiménez, Patricia. "IA agéntica: el siguiente paso en la evolución de la inteligencia artificial empresarial". Arbentia empowering consulting. 6 de febrero de 2026. https://www.arbentia.com/blog/ia-agentica-siguiente-paso-evolucion-inteligencia-artificial-empresarial/.

Legg, Shane, y Marcus Hutter. "A collection of definitions of intelligence". *Frontiers in Artificial Intelligence and Application, Advances in Artificial General Intelligence: Concepts, Architecture and Algorithms* 157 (2007): 17-24.

Llanas, Sergi. "Cataluña impulsa un plan para agilizar la resolución de sentencias judiciales con Inteligencia Artificial". *El País*. 13 de marzo de 2025.

McCarthy, John, Marvin Minsky, Nathaniel Rochester, y Claude Shannon. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence August 31, 1955". *AI Magazine* 27, n.º 4 (2006): 12-14. https://doi.org/10.1609/aimag.v27i4.1904.

Morrel Ramos, Jorge. "La Inteligencia Artificial en el día a día de un abogado: qué le va a enseñar y cómo lo cambiará". *Revista del Consejo General de la Abogacía*, n.º 108 (2018): 7-8.

Oswald, Marion, Jamie Grace, Sheena Urwin, y Geoffrey C. Barnes. "Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality". *Information & Communications Technology Law* 27, n.º 2 (2018): 223-250.

Revell, Timothy. "AI detective analyses police data to learn how to crack cases". *NewScientist*. 10 de mayo de 2017. https://www.newscientist.com/article/mg23431254-000-ai-detective-analyses-police-data-to-learn-how-to-crack-cases/.

Unión Europea. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea* L 2024/1689, 12 de julio de 2024.

Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, y Illia Polosukhin. "Attention is all you need". arXiv:1706.03762 [cs.CL], Cornell University. 12 de junio de 2017.

Vestri, Gabriele. "Cinco claves para entender la transparencia algorítmica en el sector público". IDP-Observatorio de Derecho Público. 30 de marzo de 2023. https://idpbarcelona.net/cinco-claves-para-entender-la-transparencia-algoritmica-en-el-sector-publico/.

Weiss, Gerhard. *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence*. Cambridge: MIT Press, 1999.



LA RESPUESTA DEL SISTEMA JUDICIAL ANTE LA INTELIGENCIA ARTIFICIAL:

ENFOQUE EN EL SECTOR SANITARIO[1]

Elena Atienza Macías[2]

1. Contextualización de la problemática objeto de estudio

En la actualidad, es innegable que las máquinas no solo desempeñan un papel de apoyo, sino que, en numerosos casos, sustituyen a los seres humanos —en concreto, en lo que respecta al orbe sanitario— en funciones propias de cuidadores, profesionales sanitarios, médicos y especialistas, así como en las dinámicas de toma de decisiones dentro del ámbito de la salud.

En este contexto, el sector de la sanidad y los cuidados se configura como un espacio proclive para la expansión de la innovación en sistemas robóticos[3]. Asimismo, la Inteligencia Artificial (IA) ha transformado la arquitectura del mundo contemporáneo y sus efectos se extienden de manera significativa al entorno sanitario.

Este modelo imperante forjará —o, mejor, está ya forjando, dado que la robótica no pertenece al futuro, ya forma parte del presente[4]—, una serie de múltiples y multidisciplinares problemáticas jurídicas y de política sanitaria. Entre dichos desafíos, la responsabilidad por los daños generados por robots y el tratamiento de datos personales se vuelven particularmente relevantes. Se abordarán estos temas a lo largo de este trabajo. La aplicación adecuada de la normativa existente, la necesidad

1 El presente trabajo ha sido desarrollado durante la estancia de investigación de la Dra. ATIENZA MACÍAS en la *Universidade Católica Portuguesa,* concretamente en el centro de investigación *Católica Research Centre for the Future of Law,* del Campus de Lisboa (Portugal) durante el periodo julio-agosto de 2025 en el contexto de las ayudas Ramón y Cajal 2021 del Plan Estatal de Investigación Científica, Técnica y de Innovación para el período 2021-2023, en el marco del Plan de Recuperación, Transformación y Resiliencia, y por la que se aprueba la convocatoria de tramitación anticipada correspondiente al año 2021, en concreto la Ayuda Ramón y Cajal con Referencia RYC2021-033628-I. Asimismo, la presente investigación se ha elaborado en el marco del Proyecto de Investigación "El Derecho Penal ante los retos actuales de la Biomedicina (DERPEBIO)". Referencia: PID2022-136743OB-I00. Proyectos de Generación de Conocimiento 2022. Entidades financiadoras: MCIN / AEI / y FEDER Una manera de hacer Europa y en el marco del Módulo Jean Monnet "EU-Biolaw: European Biolaw as a toolbox to promote EU values (Project 101176018 - ERASMUS-JMO-2024-HEI-TCH-RSCH)". Los puntos de vista y opiniones expresados a lo largo del presente texto son exclusivamente responsabilidad de la autora y no reflejan necesariamente la posición de la Unión Europea. La Unión Europea queda exenta de cualquier responsabilidad al respecto.

2 Investigadora Postdoctoral Ramón y Cajal del Ministerio de Ciencia e Innovación. Profesora de Derecho Constitucional. Facultad de Derecho, Universidad de Deusto, Campus Donostia-San Sebastián.

3 Como sostiene Erica Palmerini, "Robótica y derecho: sugerencias, confluencias, evoluciones en el marco de una investigación europea", *Revista de Derecho Privado*, n.º 32 (2017): 55.

4 Comenta la Profa. Minero Alejandre que actualmente vivimos en la era de la inteligencia artificial, en la que se ha denominado "cuarta revolución industrial" o "revolución industrial 4.0" en donde ya no nos resulta sorprendente —y comenta un ejemplo que nos viene al caso—, el uso de la Inteligencia Artificial en la Medicina, mediante robots cirujanos. Vid. Gemma Minero Alejandre, "Robots y derecho civil. Algunas cuestiones a tener en cuenta desde la perspectiva europea", en FODERTICS 8.0: estudios sobre tecnologías disruptivas y justicia, dir. Federico Bueno de Mata y coord. Irene González Pulido (Granada: Comares, 2020), 55-6.

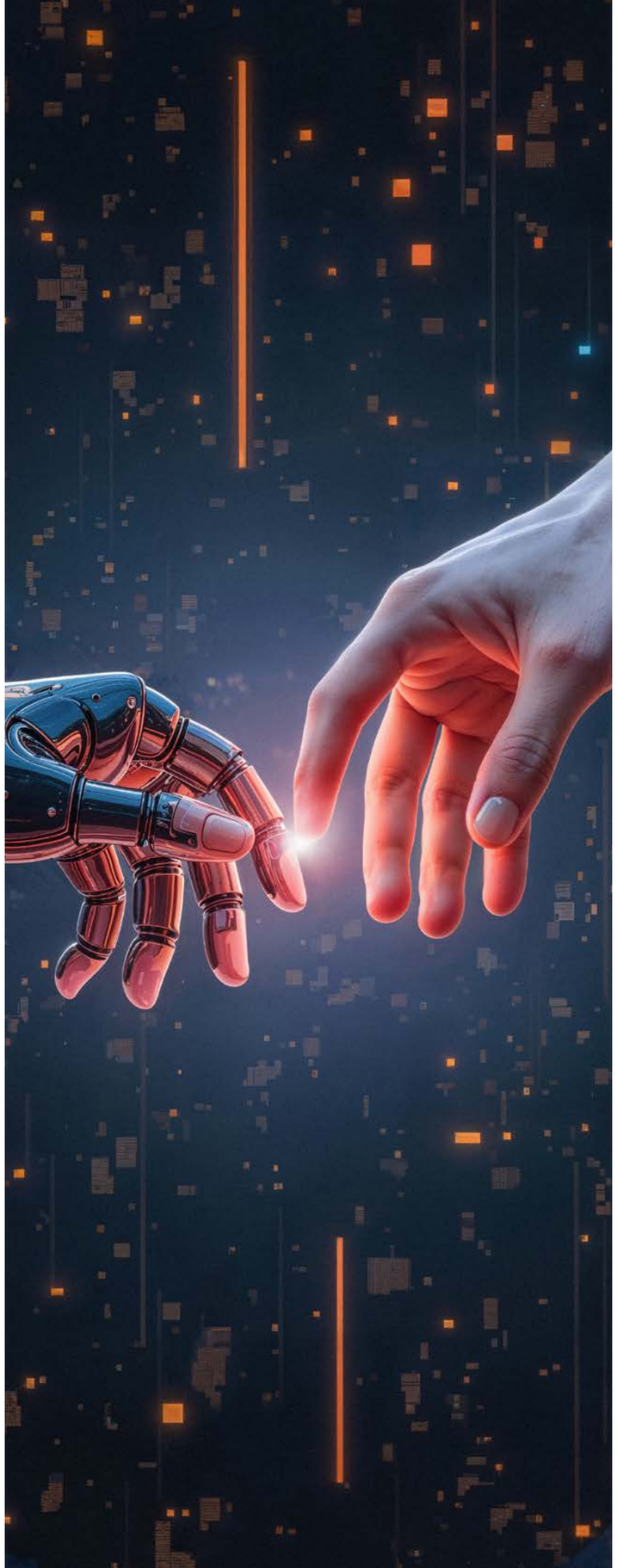
de nuevas leyes y la formulación de alternativas de políticas sanitarias acertadas requieren una atención suficiente en aras de asegurar una utilización provechosa de los robots y de la Inteligencia Artificial.

Desde este enfoque, los robots ya están automatizando diversas tareas físicas que tradicionalmente llevan o, han llevado a cabo, los profesionales sanitarios. Tal es el caso de la entrega de mercancías, administración y reparto de medicamentos entre los pacientes, monitorización de constantes vitales, seguimiento de los pacientes, monitorización para determinar si el paciente toma la medicación prescrita, ayuda a la movilidad, entre otras funciones.

Un caso ilustrativo es "ROBEAR". Se trata de un robot experimental, del tamaño de un humano, especializado en cuidados de auxiliar de enfermería (comúnmente llamado "robot enfermero") con el que, en efecto, se puede levantar a un paciente de una silla de ruedas. Este tipo de robots quedaría encuadrado (tal y como señala García Portero[5]) dentro de los robots de atención y cuidado que se encuentran en pleno apogeo dado el creciente envejecimiento de la población. Ciertamente, las personas mayores de sesenta y cinco años constituyen un colectivo de creciente peso demográfico y económico en la sociedad europea.

Debe precisarse que estos robots asistenciales surgen no sólo para el cuidado de ancianos, sino también para personas con cierto tipo de discapacidad; teniendo, ciertamente, un mayor potencial en lo que atañe a tareas físicas, pero también pueden tener su transcendencia en lo que se refiere a tareas de índole psicológica.

5 Roberto García Portero, "Los robots en la sanidad", en *Derecho de los robots*, dir. Moisés Barrio Andrés (Madrid: Wolters Kluwer, 2018), 208.



A la luz de lo anterior, más allá de la esfera física, la Inteligencia Artificial está, en efecto, alcanzando un logro cuantificable en la realización de diversas tareas intelectuales en los campos de la psicoterapia, el diagnóstico médico y la toma de decisiones, es decir, aspectos relativos a la asistencia sanitaria que, históricamente, se hallaban dentro del feudo de los expertos clínicos humanos.

Constituyó un hito importante —en el contexto de la crisis sanitaria mundial por la COVID-19— un modelo de sistema de Inteligencia Artificial que fue capaz de elaborar diagnósticos médicos: nos referimos al robot capacitado para el diagnóstico de la COVID-19. La principal ventaja de estas plataformas basadas en la Inteligencia Artificial se refiere a que son capaces de acelerar el proceso de diagnóstico y tratamiento de enfermedades como la COVID-19[6]. Éste es el caso del robot, denominado OPENTRONS, que permite el procesamiento de muestras para hacer pruebas PCR de forma masiva y diagnosticar al mayor número de personas afectadas por la COVID-19[7].

Estos logros iniciales apuntan hacia el impacto previsto que la robótica y la Inteligencia Artificial tendrán en las próximas décadas en el sistema sanitario, sus numerosas industrias, profesionales y cuidadores, así como en los pacientes y los familiares sometidos a su uso. Al mismo tiempo, varias características de los robots y la Inteligencia Artificial crearán nuevos desafíos para el cuidado de la salud, que requerirán una cuidadosa reflexión sobre los límites apropiados de delegar las tareas y la toma de decisiones humanas a las máquinas. Además de su potencialmente enorme impacto en los mercados laborales, los robots y la IA nos están obligando a repensar varios conceptos éticos y jurídicos tradicionales, incluyendo el sistema de responsabilidad y resarcimiento.

A medida que avanzamos por el camino de la automatización, vale la pena hacer un balance de los diversos robots e inteligencias artificiales actualmente implantadas y en desarrollo en el sector de la salud. Esto nos ayudará a identificar, anticipar y comprender mejor algunos de los desafíos éticos, jurídicos, políticos y sociales que estas tecnologías están generando.

Este capítulo se focaliza en la exploración de las principales consideraciones jurídicas que surgen, destacando la necesidad de diversas reformas de la doctrina jurídica y las estructuras reguladoras. Dado que los robots y la Inteligencia Artificial son un componente emergente –más que establecido en la prestación de asistencia sanitaria–, este capítulo pretende provocar, desafiar e inspirar al lector a pensar de forma crítica sobre lo que seguramente será uno de los puntos álgidos en los debates sobre legislación y políticas sanitarias en los próximos decenios.

6 Si bien lo analizaremos más ampliamente en el epígrafe posterior relativo a esta enfermedad. V. Maria Tsikala Vafea, Eleftheria Atalla, Joanna Georgakas et al., "Emerging technologies for use in the study, diagnosis, and treatment of patients with COVID-19", *Cellular and Molecular Bioengineering* 13, n.º 4 (2020): 249-57.

7 En época álgida de la Covid-19, veíamos cómo el Centro de Diagnóstico Biomédico (CDB) del Hospital Clínic de Barcelona incorporaba un nuevo robot para la realización de pruebas masivas de PCR. La llegada de este específico robot era posible gracias al esfuerzo colectivo de varias entidades privadas y públicas en el marco de la iniciativa *Covichain Robots*. La incorporación del robot respondía a la necesidad de dinamizar la realización de test de coronavirus y resolver el cuello de botella que suponía el procesamiento de las muestras. Se trataba de robots que cuentan con la última tecnología bajo las características *open source*, lo que permite adaptarlos a los protocolos establecidos en cada hospital. El robot, denominado OPENTRONS, permite el procesamiento de muestras para hacer pruebas PCR de forma masiva y diagnosticar al mayor número de personas afectadas por la COVID-19. De una forma rápida, eficaz y fiable, permite procesar un máximo de 2.400 muestras diarias. Veíamos la noticia "El Clínic incorpora un robot para la realización de pruebas masivas PCR para la COVID-19", información disponible en: https://www.clinicbarcelona.org/noticias/el-clinic-incorpora-un-robot-para-la-realizacion-de-pruebas-masivas-pcr-para-la-covid-19 [Última consulta: 28 de enero de 2026].

2. Matices y fronteras de figuras afines: robots, máquinas, Inteligencia Artificial, robótica…

Hasta este punto, hemos recurrido a un uso alternativo de un modo no del todo preciso que requiere de los términos *máquinas, Inteligencia Artificial, robótica y robots.* Conviene dar su sitio a cada uno de estos conceptos.

Los robots son un clásico de la ciencia ficción, tanto en la literatura como en el cine. Desde que el escritor checo Karel Capek acuñara el término en las primeras décadas del siglo XX para describir unas máquinas trabajadoras o serviles, han protagonizado infinidad de novelas y películas con diferentes roles (desde unos fieles escuderos del ser humano como el mítico C3PO que actuaba, en algunas ocasiones, como robot cirujano en *Star Wars*[8] a aniquiladores de la humanidad, véase *Blade Runner* o *Terminator*). En efecto, "robot", que podríamos traducir como "esclavo" o "trabajador forzado", es recogido décadas después por el cine y la literatura, siendo la voz más ampliamente aceptada y popularizada.

Empero, es relevante señalar que no es "robot" el término más antiguo, recayendo este mérito en el vocablo "androide", recogido ya por San Alberto en 1270, y popularizado por el autor francés Auguste Villiers en su novela *L'Ève future* en 1886. Cuando nos referimos a "androide" aludimos genéricamente a una entidad mecánica de aspecto antropomorfo.

En otro plano, en un uso sutilmente más preciso, encontramos el término "sistemas ciber-físicos", definido por la Unión Europea[9] como: sistemas robóticos inteligentes, vinculados con el Internet de las cosas, o sistemas técnicos de ordenadores en red, robots e inteligencia artificial, que interactúan con el mundo físico. Nótese que esta definición aporta un paso más al indicar que no se trata de máquinas autónomas aisladas, sino aquellas que entran en interacción directa con el mundo que las rodea, sea a través de sensores (interacción con factores ambientales) o con personas (interacción con factores humanos).

Siguiendo lo planteado en el párrafo anterior, robot es un término utilizado, por ende, para describir una maquinaria que interactúa con el mundo físico para realizar tareas específicas. Es, en definitiva, una máquina programable que puede realizar automáticamente una serie de acciones complejas, una serie de funciones mecánicas[10]. Respecto a versiones afines que responden al neologismo como el de "bots", precisar que la diferencia esencial entre un bot y un robot reside en la existencia de una parte física. Así como un bot es sustancialmente software, el robot precisa de un hardware. Mientras que los robots son máquinas programables que pueden ejecutar acciones automáticamente, los bots son programas que pueden ejecutar acciones automáticamente[11]. Primo hermano de los robots serían los "cobots", término que hace referencia a la contracción entre "collaborative" y "robot". Se trata de robots colaborativos que complementan el trabajo humano o colaboran con el mismo para el desarrollo de una tarea[12].

Para poner fin a este apartado decir que la fórmula "Inteligencia Artificial o AI" delimita una realidad capaz de analizar datos y actuar en consecuencia en la consecución de un fin, programado de antemano. Esto es, sumamos a los rasgos ya vistos (movilidad, sometimiento a órdenes e interacción con el mundo físico, o captación de información del medio), la capacidad de análisis, elaboración de razonamientos y actuación conforme a los mismos. En la definición más moderna que la Unión Europea[13] propone para el término, se define del siguiente modo:

> Los sistemas de inteligencia artificial (IA) son sistemas de software (aunque también pueden incluir hardware) diseñados por humanos, dado un objetivo complejo, para actuar en una dimensión digital o física, mediante la percepción de su entorno y a través de la adquisición de información, interpretación de los datos estructurados o no estructurados, el razonamiento con base en ese conocimiento, o el procesamiento de información, como consecuencia de lo cual son capaces de decidir la mejor acción para conseguir el objetivo dado. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y pueden adaptar su comportamiento analizando como el entorno se ve afectado por sus acciones anteriores.[14]

Como disciplina científica, la Inteligencia Artificial incluye aproximaciones y técnicas, como la robótica[15] (que incluye control, percepción, uso de sensores y mecanismos de acción, así como la integración de todas las otras técnicas en sistemas ciber-físicos), el *machine learning* (del cual el aprendizaje profundo y el aprendizaje reforzado son ejemplos específicos), así como el razonamiento mecánico, que incluye planear, programar, representar conocimiento y razonamientos, así como búsqueda y optimización.

El punto de partida de la inteligencia artificial nos permite construir progresiones, también terminológicas, de la misma. Así, es comúnmente aceptado el uso de conceptos como Inteligencia Artificial general o fuerte (*strong Artificial Intelligence*) e Inteligencia Artificial débil (*narrow Artificial Intelligence*), para referirnos a aquélla que puede llevar a cabo acciones tradicionalmente asignadas a seres humanos, en el primer caso, y a la que está diseñada solo para realizar un rango muy limitado de acciones, en el segundo.

3. Tecnologías robóticas en el sector sanitario: marco conceptual

El sector de la salud de la UE se enfrenta a una demanda creciente de servicios debido al envejecimiento de la población, el aumento de las enfermedades crónicas, las limitaciones presupuestarias y la escasez de trabajadores cualificados. Los avances tecnológicos en los campos de la robótica y la IA pueden ofrecer innumerables oportunidades para hacer frente a esos desafíos, lo que se traducirá en importantes ahorros de costos. Junto con la integración de las tecnologías digitales, la aplicación de la robótica y la IA podría conducir a mejoras en el diagnóstico médico, las intervenciones quirúrgicas, la prevención y el tratamiento de enfermedades y el apoyo a la rehabilitación

8 Con este cuño cinematográfico se inicia la obra monográfica de obligada consulta en esta materia elaborada por Aimee Van Wynsberghe, "Introduction", *Healthcare Robots, Ethics, Design and Implementation* (Farnham: Ashgate, 2015), 1-4.

9 *Vid. Ethical Aspects of Cyber-Physical Systems - Scientific Foresight study*, Unidad de Prospectiva Científica (Scientific Foresight Unit (STOA) del Parlamento Europeo, 2016.

10 De referencia la monografía de Javier Ercilla García y su capítulo sobre "Bots, Robots Cobots y otros autómatas", en *La robotización como "causa técnica" de despido objetivo* (Cizur Menor (Navarra): Aranzadi, 2020), 61.

11 Javier Ercilla García, *La robotización como "causa técnica" de despido objetivo* (Cizur Menor (Navarra): Aranzadi, 2020), 53-66.

12 Javier Ercilla García, *La robotización como "causa técnica" de despido objetivo*, 64-6.

13 El Informe aludido determina la inteligencia en un examen de racionalidad, refiriéndose este a la capacidad de elegir el mejor curso de acción para conseguir un fin, dados ciertos criterios que deben ser optimizados (y que son preconfigurados ex ante), y la disponibilidad de recursos. V. Comisión Europea - High-Level Expert Group on Artificial Intelligence, A definition of AI: Main Capabilities and Disciplines, 2019.

14 Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial, *A Definition of AI: Main Capabilities and Disciplines. Definition developed for the purpose of the AI HLEG's deliverables* (Comisión Europea, 2019), https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

15 Ahonda en ello Manuel Iglesias Cabero, "Aproximación al concepto de robótica", en *Robótica y responsabilidad. Aspectos legales en las diferentes áreas del Derecho* (A Coruña: Colex, 2017), 13-20.

y los cuidados a largo plazo. La IA y las soluciones digitales también podrían contribuir a procesos de gestión del trabajo más eficaces y automatizados, ofreciendo al mismo tiempo una formación continua a los trabajadores de la salud y la atención sanitaria[16].

Los robots para el cuidado han sido definidos en la literatura como aquellos robots diseñados para su uso en el hogar, el hospital u otros entornos para ayudar, apoyar o proporcionar cuidado a los enfermos, discapacitados, ancianos o personas vulnerables[17] o en el cuidado de las personas en general[18].

Previo a explorar la tipología de robots sanitarios, merece la pena hacer un paréntesis explicativo. Viene reclamándose desde la doctrina[19] que el Derecho está obligado a proporcionar una ordenación avanzada que permita estimular el desenvolvimiento de la robótica y de la Inteligencia Artificial a la par que garantice un desarrollo armonizado con los valores propios de las Constituciones y de la Carta de los Derechos Fundamentales de la Unión Europea. Entre las distintas iniciativas reguladoras, cabe destacar la significativa Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica[2021].

Y es que, fue, precisamente, dicha Resolución del Parlamento Europeo de 2017 la que señalaba los tres grandes ámbitos de aplicación de la robótica en el campo del sector salud: el quirúrgico, el rehabilitador/protésico y el asistencial o de cuidados. De esta forma, entre algunas de las aplicaciones más interesantes para los sectores de la salud y la atención sanitaria se encuentran las siguientes:

a. *Robots quirúrgicos*. Cirugía robótica que permite intervenciones más precisas, menos invasivas y remotas, basándose en la disponibilidad y evaluación de grandes cantidades de datos. Nos referimos, en concreto a que existen robots diseñados para la práctica quirúrgica. Dado su inicial éxito comercial resulta un ejemplo paradigmático el robot DA VINCI, distribuido por la empresa homónima, a la sazón propietaria de multitud de patentes que protegen la tecnología del robot diseñado para ayudar en operaciones quirúrgicas[22].

b. *Robots protésicos y rehabilitadores*. Sistemas de rehabilitación que apoyen la recuperación de los pacientes, así como su tratamiento a largo plazo en el hogar en lugar de en un centro de atención de la salud. Dentro de los primeros encontramos una amplia gama, como los destinados a la rehabilitación de funciones corporales dañadas o la sustitución de miembros, la rehabilitación cognitiva y también se incluirían aquí los exoesqueletos u otros elementos que pueden llevarse o implantarse en el cuerpo y, en su caso, las prótesis biónicas avanzadas[23].

c. *Robots de atención y cuidado.* Robots de atención y asistencia social que permiten satisfacer las crecientes demandas de atención a largo plazo de una población envejecida afectada por múltiples morbilidades.

16 Zrinjka Dolic, Rosa Castro y Andrei Moarcas, *Robots in healthcare: a solution or a problem? Study for the Committee on Environment, Public Health, and Food Safety, Policy Department for Economic, Scientific and Quality of Life Policies* (Luxemburgo: European Parliament, 2019), https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/638391/IPOL_IDA(2019)638391_EN.pdf.

17 Shannon Vallor, "Carebots and Caregivers: Sustaining the Ethical Ideal of Care in the Twenty-First Century", *Philosophy and Technology* 24, n.º 3 (2011): 251-68.

18 Aimee Van Wynsberghe, *Healthcare Robots, Ethics, Design and Implementation* (Farnham: Ashgate, 2015), 61-2.

19 Moisés Barrio Andrés, "Del Derecho de Internet al Derecho de los Robots", *Diario La Ley* (on-line), n.º 16, Sección Ciberderecho, 13 de marzo de 2018.

20 Resolución del Parlamento Europeo de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica [P8_TA(2017)0051]. Disponible en: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.pdf [Ultima consulta: 27 de enero de 2026].

21 A esta Resolución del Parlamento Europeo sobre robótica de febrero de 2017, le ha dedicado la doctrina especial atención y sendos monográficos. Así, partiendo de esta resolución, la obra coral coordinada por Rogel Vide propone un recorrido por cuestiones como la creatividad por parte de robots o androides, la consideración de estos como personas, la inteligencia artificial, el control y fallos de los robots y su responsabilidad civil. Vid. AA.VV., *Los robots y el Derecho*, coord. Carlos Rogel Vide (Madrid: Reus, 2018).

22 Con buen juicio comenta Juan García-Prieto Cuesta, "¿Qué es un robot?", en Derecho de los robots, dir. Moisés Barrio Andrés (Madrid: Wolters Kluwer, 2018), 43. Más en profundidad: v. Jonathan Douissard, Monika E. Hagen y P. Morel, "The da Vinci Surgical System", en Bariatric Robotic Surgery, ed. Carlos Eduardo Domene, Keith C. Kim, Ramón Vilallonga Puy y Paula Volpe (Cham: Springer, 2019), 13-27.

4. La tecnología robótica ante una crisis sanitaria



Experiencias pasadas como la pandemia por la COVID-19 –que causó una crisis sanitaria y económica sin precedentes– han exigido respuestas inmediatas de los agentes gubernamentales, los científicos y los profesionales de la medicina. Con recursos limitados y la necesidad inmediata de suministros médicos, apoyo de salud y tratamientos, la crisis demandó soluciones innovadoras. De esta forma, se propusieron nuevos usos de las tecnologías emergentes para satisfacer las crecientes demandas. Con recursos limitados y la necesidad inmediata de suministros médicos, apoyo sanitario y tratamientos, la crisis exigió soluciones innovadoras. Las tecnologías emergentes contribuyeron al estudio de la COVID-19, al desarrollo de herramientas de diagnóstico y tratamientos avanzados y a la respuesta a la escasez de suministros médicos. El uso innovador de las tecnologías emergentes tuvo un profundo impacto en nuestra capacidad de responder a aquella crisis mundial y debería seguir utilizándose para ayudar a mejorar los resultados. Entre dichas tecnologías innovadoras se incluyeron los robots.

No en vano, los robots son una tecnología prometedora para realizar muchas tareas como rociar, desinfectar, limpiar, tratar, detectar una temperatura corporal demasiado alta o la ausencia de mascarilla, y entregar bienes y suministros médicos como fue en el caso de la

23 Belén Andreu Martínez, "Robótica en el ámbito sanitario y de los cuidados: implicaciones para la privacidad y la protección de datos", *Dilemata, Revista Internacional de Éticas Aplicadas*, n.º 30 (2019): 81.

pandemia por COVID-19[24].

De forma semejante, ya durante el brote de Ébola de 2015 se identificaron tres grandes áreas en las que la robótica podía marcar la diferencia: la atención clínica (por ejemplo, la telemedicina y la descontaminación), logística (por ejemplo, la entrega y la manipulación de los residuos) y el reconocimiento (por ejemplo, vigilancia del cumplimiento de las cuarentenas voluntarias)[25].

En definitiva, los acontecimientos vividos han demostrado que la colaboración entre los investigadores médicos y los ingenieros es esencial en pro del desarrollo de formas rápidas y menos costosas con el propósito de hacer frente a pandemias como las aludidas. Y es que muchos de los robots utilizados en la atención sanitaria tienen atributos sociales, interactuando con los pacientes para proporcionarles compañía, terapia y una capacidad ampliada para vigilar los signos vitales y otras funciones relacionadas con la salud. A medida que los robots sean más capaces de imitar los gestos faciales, las voces, las expresiones, el lenguaje y las emociones de los humanos, la gente desarrollará cada vez más vínculos sociales con ellos. Esto, a su vez, establecerá el tipo de confianza necesaria para la delegación de ciertas tareas y la toma de decisiones previamente realizadas por cuidadores y médicos humanos. Ya se están diseñando robots para optimizar la interacción con los pacientes con demencia y autismo, proporcionando el nivel óptimo de compromiso social para facilitar el aprendizaje, acompañamiento y, en algunos casos, aumentar la capacidad de independencia de esas poblaciones de pacientes[26].

Otra estrategia para imbuir de sociabilidad a los robots es la telepresencia. Los robots de telepresencia son robots semiautónomos que pueden ser operados a distancia pero que también pueden realizar algunas operaciones por sí mismos. el propósito de estos robots es dar una sensación de presencia tanto al teleoperador como a los que se encuentran en el mismo lugar que el robot. Estos robots utilizan las telecomunicaciones para vigilar la salud y proporcionar servicios de apoyo a los pacientes externos y a otras personas que necesitan atención, sin atarlos a una institución.

La encarnación física de estos robots suele incluir un cuerpo hecho de plástico y metal y una "cara" (por lo general una pantalla que proyecta la cara del operador a distancia). Así, por ejemplo, es famoso THE GIRAFF, un robot de telepresencia dirigido a las poblaciones de edad avanzada que utiliza una variedad de sensores caseros inteligentes para medir los cambios en la presión sanguínea de los pacientes y detectar cuándo se desmayan. Paralelamente posee una interfaz parecida a un skype para conectar al paciente con sus cuidadores y familiares.

Algunos de los robots sociales más efectivos hasta la fecha son máquinas mucho más simples, quizás el más conocido de estos es PARO, un robot de compañía socialmente asistido que se asemeja a una foca bebé, que utiliza sensores táctiles, de luz, auditivos, de temperatura y de postura para percibir a las personas y reaccionar a su entorno. PARO proporciona apoyo terapéutico de manera muy similar a la terapia animal: reduciendo el estrés, promoviendo la relajación y estimulando la interacción entre pacientes y cuidadores.

Este tipo de robots sociales que brindan "acompañamiento" tuvieron un papel crucial en tiempos de la COVID-19 con los largos periodos de cuarentenas que se requirieron; que resultaron especialmente contraproducentes para la salud mental de las personas de edad avanzada y más vulnerables que por ser personas de riesgo tuvieron que ser más rigurosos en sus confinamientos[27]. Su virtualidad reside en que realizan labores de acompañamiento y, dada su no característica humana la no transmisión del virus parece garantizada.

5. La Inteligencia Artificial y la dinámica del Derecho



Cabe esperar que la prestación de cuidados utilizando robots sea susceptible de provocar algún tipo de daño. Así, en Estados Unidos ya se han acreditado casos de daños tras una cirugía con el robot DA VINCI[28] anteriormente comentado. Establecer la responsabilidad en tales casos presentará cuestiones jurídicas novedosas.

24 V. Maria Tsikala Vafea, Eleftheria Atalla, Joanna Georgakas et al., "Emerging technologies for use in the study, diagnosis, and treatment of patients with COVID-19", *Cellular and Molecular Bioengineering* 13, n.º 4 (2020) y V. Saeed H. Alsamhi y Brian Lee, "Blockchain-Empowered Multi-Robot Collaboration to Fight COVID-19 and Future Pandemics", *IEEE Access* 9 (2020).

25 Muchas de estas aplicaciones han sido exploradas activamente en China. V. Guang-Zhong Yang, Bradley J. Nelson, Robin R. Murphy et al., "Combating COVID-19—The role of robotics in managing public health and infectious diseases", *Science Robotics* 5, n.º 40 (2020), https://robotics.sciencemag.org/content/5/40/eabb5589.

26 Ian R. Kerr, Jason Millar y Noel Corriveau, "Robots and Artificial Intelligence in Health Care", en *Canadian Health Law and Policy*, 5.ª ed., ed. Joanna Erdman, Vanessa Gruben y Eric Nelson (Toronto: LexisNexis Canada, 2017), 257-80. En esta línea, Cfr. Alexander P. Henkel, Martina Čaić, Marah Blaurock et al., "Robotic transformative service research: deploying social robots for consumer well-being during COVID-19 and beyond", *Journal of Service Management* 31, n.º 6 (2020) y Brian Scassellati y Marynel Vázquez, "The potential of socially assistive robots during infectious disease outbreaks", *Science Robotics* 5, n.º 44 (2020).

27 A este propósito responde el Proyecto SPRING, financiado con fondos europeos, que pretende abordar este desafío mediante la creación de robots sociales asistenciales que realizan interacciones multipersonales y diálogo de dominio abierto. Gracias a la tecnología desarrollada en el marco del citado proyecto, los robots sociales "entenderán a diversos individuos y situaciones grupales y tomarán las decisiones adecuadas como la identificación de pacientes que han estado esperando solos por mucho tiempo o que pueden estar nerviosos. En última instancia, los robots sociales interactuarán en conversaciones cara a cara con los pacientes, sus familiares, el personal y grupos de personas completos". Hemos de destacar la naturaleza "sin contacto y sin el uso de las manos" de la tecnología de SPRING -con una gran demanda- ya que reduce el riesgo y la propagación de infecciones. Esto es fundamental porque, aunque el proyecto fue inicialmente puesto en marcha para ayudar a personas de edad avanzada, puede ser beneficioso para la gestión de brotes como el de la pandemia por Covid-19. El proyecto SPRING (*Socially Pertinent Robots in Gerontological Healthcare*) desarrolla métodos y algoritmos para Inteligencia Artificial conversacional, visión artificial, procesamiento de audio, aprendizaje automático e interacción humano-robot, junto con el análisis del comportamiento humano y el control sensomotriz de robots. Los socios del proyecto validan su tecnología en un hospital de día para personas mayores y evalúan la aceptación por parte de los pacientes y el personal sanitario. Información disponible en https://cordis.europa.eu/article/id/418037-how-to-use-robots-to-tackle-future-global-health-crises-like-covid-19/es [Última consulta: 25 de enero de 2026].

28 El sistema quirúrgico da Vinci está diseñado para mejorar las cirugías mínimamente invasivas proporcionando a los cirujanos una mayor precisión y visualización y permitiendo procedimientos que de otro modo se considerarían demasiado difíciles sin un instrumento robótico. Cuando se realizan de forma experta, estos procedimientos robóticos mínimamente invasivos pueden ayudar a proporcionar a los pacientes recuperaciones optimizadas en comparación con las cirugías abiertas tradicionales. La cirugía robótica, específicamente con dispositivos como el Sistema Quirúrgico da Vinci, ha experimentado una rápida expansión y crecimiento desde principios de la década de 2000. Sin embargo, a medida que aumenta la frecuencia de los procedimientos robóticos, también lo hacen las quejas por el mal funcionamiento del sistema y los informes de lesiones de los pacientes que, en efecto, pueden dar lugar a demandas contra las partes interesadas, entre las que se incluyen el fabricante del dispositivo, el hospital o las instituciones y su personal, así como los cirujanos y sus asociados. Cada uno de estos interesados que participan en la cirugía robótica tiene la responsabilidad de mantener el más alto nivel de capacitación y atención disponible para ayudar a un paciente a lograr un buen resultado.
A todo ello responden Elizabeth M. Hechenbleikner y Brian P. Jacob, "Medicolegal Issues in Robotic Surgery", en *Robotic-Assisted Minimally Invasive Surgery,* ed. Shawn Tsuda y Omar Yusef Kudsi (Cham: Springer, 2019), 27-34. En nuestro país también se ha pronunciado la doctrina: Tomás Gabriel García Micó, "Litigación asociada a la cirugía robótica con el da vinci (Da Vinci's Robotic Surgery Litigation)", *InDret*, n.º 4 (2014).

Uno de los escollos más comunes en la normativización de lo atinente a la robótica en el contexto sanitario reside en el encuentro de una armonía entre el fomento de la innovación tecnológica (de hecho el marco regulatorio debe resultar un incentivo a la innovación sanitaria no un sistema que oprima o ralentice la innovación) y al mismo tiempo la garantía de que las nuevas tecnologías robóticas no supongan riesgos irrazonables para la salud y la seguridad o para la protección de los derechos y valores fundamentales[29]. En este sentido, es necesaria la adopción de precauciones especiales en la interacción de sistemas de inteligencia artificial y robots con personas especialmente vulnerables, esto es, ancianos, niños, discapacitados.

La bisagra que contribuye a lograr este equilibrio es el régimen de la responsabilidad, que debe hacer frente a los posibles efectos adversos en la utilización de los robots[30]. Destacan como aspectos jurídicos fundamentales de este sector, junto al instituto de la responsabilidad, en segundo lugar, la seguridad y comercialización y en tercero, todo lo concerniente a la privacidad y protección de datos.

5.1. Responsabilidad de los robots y la Inteligencia Artificial

La cuestión de la responsabilidad cuando un robot causa daños o lesiones es, al igual que la mayoría de las aplicaciones robóticas, un asunto radial que atañe a todos los robots empleados en sanidad. En concordancia con el criterio de clasificación de los robots sanitarios seguido en el epígrafe tercero relativo a *Tecnologías robóticas en el sector sanitario:*

En primer lugar, la introducción de *robots en la cirugía* genera un nuevo riesgo: la posibilidad real de que un paciente pueda ser lesionado por el robot independientemente de las acciones del cirujano.

Un segundo plano se refiere a los *robots protésicos*. Los riesgos asociados al uso de prótesis robóticas pueden ser especialmente altos, dado que son sistemas extremadamente sofisticados tecnológicamente hablando, se utilizan en un gran número de actividades cotidianas y pueden emplearse de formas que el fabricante no contempló originariamente.

Así, en el caso de los *robots de atención y cuidado*, no es aventurado pensar que un robot que traslade a una persona de edad avanzada de una cama a una silla de ruedas, por ejemplo, pueda lesionar a este anciano si no funciona correctamente. Si esto ocurriera, ¿quién sería responsable de indemnizar a la persona lesionada? El sujeto responsable del daño podría ser el desarrollador del robot, el fabricante, el vendedor, la empresa encargada de su mantenimiento, o incluso el propio usuario por interactuar con el robot de una manera prohibida por el fabricante.

Bajo esta perspectiva, es la institución de la responsabilidad por productos defectuosos —como "régimen de responsabilidad civil especial"— el que se nos antoja[31] más oportuno

29 Así lo aseveran Ronald Leenes, Erica Palmerini, Bert-Jaap Koops et al., "Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues", *Law, Innovation and Technology* 9, n.º 1 (2017): 14.

30 De nuevo, interesantes reflexiones presenta Roberto García Portero, "Los robots en la sanidad", 218.

31 Joaquín Ataz López, "Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial", Càtedra Jean Monnet Working Paper 4/2020, agosto 2020, 34. Véase también del mismo "Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial", en *Derecho de daños*, coord. Mariano José Herrador Guardia (Madrid: Francis Lefebvre, 2020), 317-75. El prof. Ataz se refiere a Sánchez del Campo quien sólo contempla este tipo de responsabilidad (Vid. Alejandro Sánchez del Campo Redonet, *Reflexiones de un replicante legal: Los retos jurídicos de la robótica y las tecnologías disruptivas* (Cizur Menor (Navarra): Thomson Reuters – Aranzadi, 2016), 24 y ss.).

al hilo de los daños causados por robots o dispositivos robotizados. El marco jurídico de la responsabilidad por productos defectuosos existente en Europa se contiene aún en la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por daños causados por productos defectuosos, modificada por la Directiva 1999/34/CE del Parlamento Europeo y del Consejo, de 10 de mayo de 1999.

Su implementación española se encuentra hoy día en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre (en adelante, TRLGDCU) e instituye a este respecto un régimen de responsabilidad estricta[32].

El artículo 136 del TRLGDCU proporciona una noción legal de producto, a efectos de la aplicación de este régimen de responsabilidad civil, lo suficientemente amplia como para encajar en ella a los robots[33]. Producto es, a tenor del artículo 136 TRLGDCU— "cualquier bien mueble, aun cuando esté unido o incorporado a otro bien mueble o inmueble, así como el gas o la electricidad".

El artículo 137 del TRLGDCU establece el concepto legal de "producto defectuoso"

1. Se entenderá por producto defectuoso aquél que no ofrezca la seguridad que cabría legítimamente esperar, teniendo en cuenta todas las circunstancias y, especialmente, su presentación, el uso razonablemente previsible del mismo y el momento de su puesta en circulación.

2. En todo caso, un producto es defectuoso si no ofrece la seguridad normalmente ofrecida por los demás ejemplares de la misma serie.

3. Un producto no podrá ser considerado defectuoso por el solo hecho de que tal producto se ponga posteriormente en circulación de forma más perfeccionada.[34]

En lo que respecta a las causas de exoneración de responsabilidad recogidas en el art. 140 TRLGDCU, el fabricante puede *evitar* la responsabilidad por un producto defectuoso si por un lado, dadas las circunstancias del caso, es posible presumir que el defecto no existía en el momento en que se puso en circulación el producto (apartado b del precepto en cuestión) y otro motivo se refiere a que el estado de los conocimientos científicos y técnicos en el momento en que el fabricante puso en circulación el producto no era tal que permitiera descubrir la existencia del defecto (apartado e del citado precepto).

También puede haber ocasiones en las que un usuario se haya lesionado por un mal uso de un robot de atención y cuidado o de un robot protésico, en vez de por un defecto en el robot, y en estos casos la forma de reconducir los daños será mediante la imposición de un seguro de responsabilidad civil obligatorio, que debería ser suscrito por el propietario del robot.

32 Expone con tino interesantes reflexiones Silvia Díaz Alabart, *Robots y responsabilidad civil* (Madrid: Reus, 2018), Capítulo IV. "¿Pueden los robots, en su caso, ser considerados productos defectuosos, y por tanto sometidos a la regulación vigente sobre éstos?".

33 Joaquín Ataz López, "Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial", 35.

34 España, *Texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias*, Real Decreto Legislativo 1/2007, Boletín Oficial del Estado 287, Suplemento, 30 de noviembre de 2007, art. 137.

Ha de significarse, además, que hay otros factores a considerar en la producción de cualquier acción dañosa. Tomando como ejemplo la cirugía robótica, en ella los cirujanos, el hospital, los equipos de mantenimiento, los desarrolladores de software y los responsables de los sistemas informáticos podrían tener un posible protagonismo o participación en la causación del daño al paciente.

De lo anterior se deduce que la responsabilidad de incorporar dispositivos tecnológicos al cuerpo humano se divide en dos: por un lado, la resultante de una incorrecta intervención quirúrgica y, por otro, la derivada de un producto defectuoso[35]. Y es que ya se trate de una reclamación en el marco de la responsabilidad por productos defectuosos o de una acción de responsabilidad civil contractual o extracontractual en el caso de daños a terceros, en bastantes ocasiones puede ser difícil probar la naturaleza defectuosa de la compleja tecnología robótica.

En este ámbito, se plantea desde la Unión Europea y EURON (*EUropean RObotics research Network*) el rastreo y grabación de la actividad de los robots (caja negra) y, asimismo el hecho de brindar una "identificación única" a cada robot[36]. En este sentido, se ha propuesto que los robots sanitarios deberían *ex lege* estar dotados —haciendo un símil aeronáutico— de una "caja negra"[37] en la que todos los datos relativos a los movimientos del robot, los datos ambientales, las órdenes dadas por el operador, entre otros datos, quedarían perfectamente registrados.

A la vista del planteamiento anterior, este mecanismo permitiría clarificar y resolver los litigios. Paralelamente, también podría permitir a los fabricantes intuir cómo el algoritmo de aprendizaje del robot originó cambios en el comportamiento del sistema. Habida cuenta de las elevadas capacidades de procesamiento existentes y el tratamiento del *big data* hace que sea realmente peliagudo para las personas llegar a conocer cómo el robot ha adoptado una determinada decisión y cuál es la base que la conforma.

5.2. Cuestiones conexas a la seguridad y comercialización

Hemos venido contando con un aparato normativo que ha regulado la fabricación y comercialización de los robots en el sector salud y, con este fin, fueron dictadas, en sede europea, dos nucleares directivas. En primer lugar, la Directiva 90/385/CEE del Consejo de 20 de junio de 1990 relativa a la aproximación de las legislaciones de los Estados Miembros sobre los productos sanitarios implantables activos. Esta directiva armonizaba la legislación nacional sobre productos sanitarios implantables activos en aras de asegurar a los pacientes unas normas de seguridad, valga la redundancia, que se implantasen con alcance forma universal. Igualmente, permitía que los productos se pudiesen emplear en cualquier país de la Unión. En segundo lugar, la Directiva 93/42/CEE del Consejo, de 14 de junio de 1993, relativa a los productos sanitarios. Esta norma armonizaba la legislación nacional sobre productos sanitarios promoviendo la confianza del público en el sistema. Asimismo, habilitaba a que los productos se pudiesen usar en cualquier país de la UE[38].

En la actualidad, la regulación clave en la órbita europea se recoge en el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo de 5 de abril de 2017 sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) núm. 178/2002 y el Reglamento (CE) núm. 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo, aludidas en líneas anteriores.

Según el artículo 1.1. del Reglamento 2017/745, se establecen normas relativas a la introducción en el mercado, la comercialización o la puesta en servicio de productos sanitarios para uso humano y accesorios de dichos productos en la Unión. El presente Reglamento también es de aplicación a las investigaciones clínicas referentes a los productos sanitarios y accesorios que se desarrollan en la Unión.

En España, la regulación vigente se contiene en el Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios y por el que se deroga el Real Decreto 1591/2009 y el Real Decreto 1616/2009, con las excepciones recogidas en las disposiciones transitorias y en la disposición derogatoria de la norma. Este Real Decreto establece los requisitos nacionales aplicables para la introducción en el mercado, comercialización y puesta en servicio de los productos sanitarios en España. Esta normativa se aplica a: o productos sanitarios de uso humano y sus accesorios o productos sin finalidad médica enumerados en el anexo XVI del Reglamento UE de 2017.

Reza el artículo 1 del meritado Real Decreto 192/2023 que tiene por *objeto* regular los productos sanitarios de uso humano y sus accesorios, los productos sin finalidad médica, y en particular:

a. La autoridad competente y las garantías sanitarias.

b. Los procedimientos para el otorgamiento de las licencias previas de funcionamiento de instalaciones.

c. Los requisitos y las actuaciones de los organismos notificados.

d. El reprocesamiento de productos sanitarios de un solo uso.

e. La comercialización y puesta en servicio en España.

f. El comercio en el mercado de la Unión Europea y en el mercado exterior.

g. Las investigaciones clínicas.

h. El sistema de vigilancia.

i. La inspección y control del mercado y medidas de protección de la salud.[39]

Bajo este paraguas normativo, los robots protésicos quedan incardinados en el mismo en tanto en cuanto engloba expresamente a los productos sanitarios que dependen de una fuente de energía eléctrica (o de cualquier otra fuente de energía) para su funcionamiento que están destinados a ser introducidos total o parcialmente, quirúrgica

35 Marc Abraham Puig Hernández, "Ciborgs: el cuerpo humano, los dispositivos tecnológicos y la libertad", *Cuadernos Electrónicos de Filosofía del Derecho*, n.º 40 (2019): 221.

36 Así lo sugiere la Coordinadora del Departamento Jurídico del Instituto Nacional de Ciberseguridad de España: María José Santos González y, lo refleja doctrinalmente en su trabajo "Regulación legal de la robótica y la inteligencia artificial: retos de futuro", *Revista Jurídica de la Universidad de León*, n.º 4 (2017): 36.

37 Utiliza el vocablo "black-box" el Informe del Parlamento Europeo *Liability for Artificial Intelligence and other emerging digital technologies* de 2019, 33, a propósito de la característica opacidad de este tipo de dispositivos. https://op.europa.eu/es/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1

38 Es clave el trabajo de Roberto García Portero, "Los robots en la sanidad", 218-21.

39 España, *Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios,* Boletín Oficial del Estado 69, 22 de marzo de 2023, art. 1.

o médicamente, en el cuerpo humano y que están destinados a permanecer después del procedimiento[40].

En un semblante distinto, la subsunción de los robots de atención y cuidado resulta más incierta. La definición de "producto sanitario" en el Reglamento (UE) 2017/745 es la siguiente:

1. Producto sanitario: todo instrumento, dispositivo, equipo, programa informático, implante, reactivo, material u otro artículo destinado por el fabricante a ser utilizado en personas, por separado o en combinación, con alguno de los siguientes fines médicos específicos:

   - diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad,

   - diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad,

   - investigación, sustitución o modificación de la anatomía o de un proceso o estado fisiológico o patológico,

   - obtención de información mediante el examen *in vitro* de muestras procedentes del cuerpo humano, incluyendo donaciones de órganos, sangre y tejidos, y que no ejerce su acción principal prevista en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales mecanismos.

Los robots quirúrgicos claramente entran dentro de la citada normativa sobre productos sanitarios. Si bien ciertos robots asistenciales podrían quedar amparados en esta definición, los robots cuidadores con otras funciones, como ordenar la vivienda del paciente no quedarían incluidos en esta conceptualización y, por consiguiente, este tipo de robots no estarían sujetos a los requisitos de la regulación europea y española sobre productos sanitarios. Es por ello, que, en su defecto, nos remitimos a la norma ISO 13482:2014 (de la *International Organization for Standardization*) que ha sido desarrollada, *ex professo*, para esta modalidad de robots de atención y cuidado. En esta norma expresamente se abarcan tres tipos de robots asistenciales: robots de servicio móvil, los asistentes físicos, que ayudan a realizar determinadas tareas, proporcionando un suplemento o aumentando las propias capacidades y los robots que tienen como finalidad transportar personas[41].



40 De nuevo, Roberto García Portero, "Los robots en la sanidad", 218-21.

41 Eduard Fosch-Villaronga, *Robots, Healthcare, and the Law. Regulating automation in personal care* (Oxfordshire: Routledge, 2020), 58.

5.3. Privacidad y protección de datos relativos a la salud (sensibles o especialmente protegidos)

Es muy probable que los robots empleados con fines sanitarios almacenen grandes cantidades de datos de carácter personal muy íntimos. Esta tipología de datos, en el contexto de la normativa de protección de datos recibe la designación de datos sensibles o especialmente protegidos, en los que los datos de salud quedan subsumidos.

Desde luego, los datos que pueden llegar a implicar mayor información son los que se obtienen de una finalidad de asistencia social, en tanto en cuanto se refieren a toda índole de datos sobre el estilo de vida o hábitos de la persona en su vida cotidiana. Así las cosas, se podrían contemplar, entre otros, datos de geolocalización, monitorización de constantes vitales, gestión de alarmas médicas, monitorización para determinar si el paciente toma la medicación prescrita, reconocimiento de voz, grabación de sonidos, almacenamiento de la información a medida que el usuario la va dando a través del diálogo con el robot y, eventualmente, podría incluir en un futuro —tal y como apunta Andreu Martínez— un sistema de computación afectiva (ej. análisis de la gestualidad de la persona de cara al reconocimiento, gestión y generación de emociones)[42].

Paralelamente es reseñable que, en el contexto de estos nuevos sistemas de robótica se requerirá el almacenamiento de los datos sobre el estado y las enfermedades del paciente, así como la tan traída y llevada "historia clínica", los medicamentos y otros datos concernientes a la salud con el fin de que el robot pueda llevar a cabo su cometido.

En suma, los aspectos concernientes a la privacidad y protección de datos a nivel europeo están regulados (y, por tanto ahí nos remitimos) en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).



42 Belén Andreu Martínez, "Robótica en el ámbito sanitario y de los cuidados: implicaciones para la privacidad y la protección de datos", 79-92.

Bibliografía

Alsamhi, Saeed H. y Brian Lee. "Blockchain-Empowered Multi-Robot Collaboration to Fight COVID-19 and Future Pandemics". *IEEE Access* 9 (2020): 44173-44197. doi:10.1109/ACCESS.2020.3032450.

Andreu Martínez, Belén. "Robótica en el ámbito sanitario y de los cuidados: implicaciones para la privacidad y la protección de datos". *Dilemata, Revista Internacional de Éticas Aplicadas*, n.º 30 (2019): 167-185.

Ataz López, Joaquín. «Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial». En *Derecho de daños*, coordinado por Mariano José Herrador Guardia, 337-372. Madrid: Francis Lefebvre, 2020.

Atienza Macías, Elena. "Algunas respuestas jurídicas a la posible vulneración de derechos fundamentales por sistemas de Inteligencia Artificial". En *Derecho e Inteligencia Artificial. El jurista ante los retos de la era digital*, dirigido por Inmaculada Herbosa Martínez y David Fernández de Retana Gorostizagoiza, 125-152. Pamplona: Aranzadi, 2023.

Atienza Macías, Elena y Miguel Vieito Villar. "La inteligencia artificial en el contexto sanitario: algunas reflexiones éticas y jurídicas. Especial referencia al papel de los robots ante la pandemia de la Covid-19 y su alcance en las personas mayores". En *Soluciones tecnológicas para los problemas ligados al envejecimiento: cuestiones éticas y jurídicas*, dirigido por Itziar Alkorta Idiakez y coordinado por Elena Atienza Macías, 169-210. Madrid: Dykinson, 2020.

Díaz Alabart, Silvia. *Robots y responsabilidad civil*. Madrid: Reus, 2018.

Dolic, Zrinjka, Rosa Castro y Andrei Moarcas. *Robots in healthcare: a solution or a problem? Study for the Committee on Environment, Public Health, and Food Safety, Policy Department for Economic, Scientific and Quality of Life Policies*. Luxemburgo: European Parliament, 2019.

Douissard, Jonathan, Monika E. Hagen y P. Morel. "The da Vinci Surgical System". En *Bariatric Robotic Surgery*, editado por Carlos Eduardo Domene, Keith C. Kim, Ramón Vilallonga Puy y Paula Volpe, 19-29. Cham: Springer, 2019.

Ercilla García, Javier. *La robotización como "causa técnica" de despido objetivo*. Cizur Menor (Navarra): Aranzadi, 2020.

España. *Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios*. Boletín Oficial del Estado 69, 22 de marzo de 2023.

España. *Texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias*. Real Decreto Legislativo 1/2007. Boletín Oficial del Estado 287, Suplemento, 30 de noviembre de 2007.

Fosch-Villaronga, Eduard. *Robots, Healthcare, and the Law. Regulating automation in personal care*. Oxfordshire: Routledge, 2020.

García Micó, Tomás Gabriel. "Litigación Asociada a La Cirugía Robótica Con El Da Vinci (Da Vinci's Robotic Surgery Litigation)". *InDret*, n.º 4 (2014): 1-32.

García Portero, Roberto. "Los robots en la sanidad". En *Derecho de los robots*, dirigido por Moisés Barrio Andrés, 189-214. Madrid: Wolters Kluwer, 2018.

García-Prieto Cuesta, Juan. "¿Qué es un robot?". En *Derecho de los robots*, dirigido por Moisés Barrio Andrés, 29-60. Madrid: Wolters Kluwer, 2018.

Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial. *A Definition of AI: Main Capabilities and Disciplines. Definition developed for the purpose of the AI HLEG's deliverables*. Comisión Europea, 2019. https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

Hechenbleikner, Elizabeth M. y Brian P. Jacob. "Medicolegal Issues in Robotic Surgery". En *Robotic-Assisted Minimally Invasive Surgery*, editado por Shawn Tsuda y Omar Yusef Kudsi, 531-545. Cham: Springer, 2019.

Henkel, Alexander P., Martina Čaić, Marah Blaurock y Monika Okan. "Robotic transformative service research: deploying social robots for consumer well-being during COVID-19 and beyond". *Journal of Service Management* 31, n.º 6 (2020): 1131-1148. doi:10.1108/JOSM-05-2020-0145.

Herbosa Martínez, Inmaculada. "Encaje de los sistemas de IA en la definición de producto en la legislación de productos defectuosos: Análisis de la legislación vigente con la vista puesta en la Propuesta de Directiva del Parlamento europeo y del Consejo de 28 de septiembre de 2022 (COM/2022/495)". *Indret: Revista para el Análisis del Derecho*, n.º 3 (2024): 1-41.

Iglesias Cabero, Manuel. *Robótica y responsabilidad. Aspectos legales en las diferentes áreas del Derecho*. A Coruña: Colex, 2017.

Kerr, Ian R., Jason Millar y Noel Corriveau. "Robots and Artificial Intelligence in Health Care". En *Canadian Health Law and Policy*, 5.ª ed., editado por Joanna Erdman, Vanessa Gruben y Eric Nelson, 543-578. Toronto: LexisNexis Canada, 2017.

Leenes, Ronald, Erica Palmerini, Bert-Jaap Koops, Andrea Bertolini, Pericle Salvini y Federica Lucivero. "Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues". *Law, Innovation and Technology* 9, n.º 1 (2017): 1-44. doi:10.1080/17579961.2017.1304921.

Minero Alejandre, Gemma. "Robots y derecho civil. Algunas cuestiones a tener en cuenta desde la perspectiva europea". En *FODERTICS 8.0: estudios sobre tecnologías disruptivas y justicia*, dirigido por Federico Bueno de Mata y coordinado por Irene González Pulido, 31-50. Granada: Comares, 2020.

Palmerini, Erica. "Robótica y derecho: sugerencias, confluencias, evoluciones en el marco de una investigación europea". *Revista de Derecho Privado*, n.º 32 (2017): 53-97. doi:10.18601/01234366.n32.04.

Tsikala Vafea, Maria, Eleftheria Atalla, Joanna Georgakas, Fotini Shehadeh, Eleftherios Mylona, Markos Kalligeros y Fadi Shehadeh. "Emerging technologies for use in the study, diagnosis, and treatment of patients with COVID-19". *Cellular and Molecular Bioengineering* 13, n.º 4 (2020): 249-257. doi:10.1007/s12195-020-00629-w.

Vallor, Shannon. "Carebots and Caregivers: Sustaining the Ethical Ideal of Care in the Twenty-First Century". *Philosophy and Technology* 24, n.º 3 (2011): 251-268. doi:10.1007/s13347-011-0015-x.

Van Wynsberghe, Aimee. *Healthcare Robots, Ethics, Design and Implementation*. Farnham: Ashgate, 2015.

Yang, Guang-Zhong, Bradley J. Nelson, Robin R. Murphy, Howie Choset, Henrik Christensen, Steven H. Collins, Paolo Dario, Ken Goldberg, Koji Ikuta, Neil Jacobstein, Danica Kragic, Russell H. Taylor y Marcia McNutt. "Combating COVID-19—The role of robotics in managing public health and infectious diseases". *Science Robotics* 5, n.º 40 (2020): eabb5589. doi:10.1126/scirobotics.abb5589.



FGE

FISCALÍA GENERAL DEL ESTADO

ECUADOR

Fiscalía General del Estado
Dirección de Estudios Penales
Quito - Ecuador