ESTUDIOS PENALES Y CRIMINOLÓGICOS

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

Artículos Doctrinales

INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD PENAL DE PERSONAS JURÍDICAS: UN ANÁLISIS DE SUS ASPECTOS MATERIALES Y PROCESALES*

ARTIFICIAL INTELLIGENCE AND CORPORATE CRIMINAL LIABILITY: AN ANALYSIS OF THE SUBSTANTIVE AND PROCEDURAL ASPECTS

Túlio Felippe Xavier Januário[1,a]
[1] Becario de la "Fundação para a Ciência e a Tecnologia – FCT". Doctorando en la Facultad de Derecho de la Universidad de Coimbra, Portugal

[a]tuliofxj@gmail.com

Resumen

Partiendo del supuesto de que las empresas asumen un rol de innegable protagonismo en la producción y utilización de los sistemas de inteligencia artificial (IA), abordaremos en el presente trabajo, los aspectos penales y procesales penales de esta relación. Tras un breve estudio del concepto, funcionamiento y limitaciones de esta tecnología, analizaremos las dificultades que impone a la imputación de responsabilidades penales, que acaban justificando la adopción de modelos específicos de responsabilidad de personas jurídicas también en este ámbito. Por otro lado, observaremos que, aun que como usuarias, las personas jurídicas no gozan de libertad irrestricta para emplear la IA en sus programas de cumplimiento, debiendo cumplir con ciertos parámetros legales, especialmente si pretenden obtener beneficios penales a través del *compliance* eficaz.

Palabras clave: derecho penal económico; inteligencia artificial; responsabilidad penal de la persona jurídica; proceso penal de la persona jurídica; cumplimiento.

Abstract

Assuming that companies exercise a role of undeniable relevance in the production and use of artificial intelligence systems (AI), we will address in this paper the criminal and procedural aspects of this relationship. After a brief study of the concept, procedures and limitations of this technology, we will analyze the difficulties it imposes on the attribution of criminal responsibilities, which end up justifying the adoption of specific models of corporate criminal liability also in this area. On the other hand, we will observe that, even as users, legal entities do not have unrestricted freedom to use AI in their compliance programs, and must comply with certain legal parameters, especially if they intend to obtain criminal benefits through effective compliance.

Keywords: economic criminal law; artificial intelligence; corporate criminal responsibility; corporate criminal procedure; compliance.

* El presente trabajo se ha realizado en el marco del proyecto de investigación "Autoria e responsabilidade em crimes cometidos através de sistemas de inteligência artificial" (2020.08615.BD), financiado por la "Fundação para a Ciência e a Tecnologia – FCT".

1. INTRODUCCIÓN

El protagonismo asumido por las personas jurídicas a lo largo del siglo XX y principios del XXI es una constatación prácticamente irrefutable. Las grandes corporaciones se encuentran actualmente en el centro de las más variadas ramas de actividad, siendo responsables de gran parte de la circulación de capitales, la producción y distribución de bienes y la prestación de servicios y, en consecuencia, de la generación de puestos de trabajo.

Sin embargo, en proporción a la progresiva relevancia de estos actores en el contexto global, fue necesario avanzar en las reflexiones sobre la respuesta penal ante eventuales ilícitos relacionados al entorno empresarial[1] . Es decir, dada la creciente preocupación de la sociedad por los delitos típicamente económicos y empresariales[2] , sumada a la complejidad de su tratamiento por parte del sistema de justicia penal[3] , los temas relacionados con la responsabilidad penal de las personas jurídicas[4] se han convertido en objeto no solo

[1] En este sentido, Laura Zuñiga Rodríguez destaca el papel de protagonismo de las personas jurídicas también en el "mundo del crimen", ya que la estructura altamente compleja, especializada y jerárquica que asumen, sumada a su alta concentración de capital, las transforman en importante fuente de riesgo. ZUÑIGA RODRÍGUEZ, L.: *Bases para un modelo de imputación de responsabilidad penal a las personas jurídicas*, Navarra, 2000, p. 80-81.

[2] En el concepto de "criminalidad empresarial", en el mismo sentido que Schünemann, englobamos los delitos económicos cometidos por actuación para una empresa, mediante la cual se lesionan bienes jurídicos ajenos, incluidos los intereses de los trabajadores de la persona jurídica. En cuanto a los delitos económicos, podemos destacar diferentes concepciones. Desde una comprensión más restringida, sostenida por Bajo Fernández, pueden ser conceptualizados como ilícitos cometidos en detrimento del orden económico. Schünemann, por su parte, parte de un concepto más amplio, entendiendo como delitos económicos todos los actos punibles penal o administrativamente cometidos en el ámbito de la vida económica o estrechamente relacionados con ella. Para Klaus Tiedemann, el derecho penal económico debe abarcar no sólo las transgresiones del llamado "derecho económico administrativo", que ampara la actividad de regulación e intervención del Estado en la Economía, sino también los delitos cometidos contra bienes jurídicos supraindividuales relacionados con la vida económica y los hechos delictivos relacionados con el denominado "derecho penal patrimonial clásico", siempre que estén dirigidos contra bienes jurídicos colectivos o que constituyan abuso de medidas e instrumentos de la vida económica. Ver detalladamente: SCHÜNEMANN, B.: "Cuestiones básicas de dogmática jurídico-penal y política criminal sobre la criminalidad empresarial", en *Anuario de derecho penal y ciencias penales*, v. 41, n. 2, 1988, p. 529-531; BAJO FERNÁNDEZ, M.: "El derecho penal económico: un estudio de derecho positivo español", en *Anuario de derecho penal y ciencias penales*, v. 26, n. 1, 1973, p. 96; TIEDEMANN, K.: "El concepto de derecho economico, de derecho penal economico y de delito económico" en *Revista Chilena de Derecho*, v. 10, n. 1, 1983, p. 61-62; CANESTRARO, A. C., JANUÁRIO, T. F. X., "Programas de compliance e branqueamento de capitais: implicações da lei nº 83/2017, de 31 de agosto, no regime jurídico de Portugal" en *Revista Científica do CPJM*, v. 1, n. 3, 2022, p. 74; SOUSA, S. A., *Questões fundamentais de direito penal da empresa,* Coimbra, 2019, p. 19-22.

[3] Entre estas dificultades, se destaca el fenómeno conocido como "irresponsabilidad organizada". Las personas jurídicas contemporáneas, marcadas notablemente por la descentralización de la toma de decisiones y la complejidad de su estructura interna, acaban convirtiéndose en una suerte de "escudo" frente a la identificación de los autores de determinadas conductas ilícitas. En otras palabras, la "organización de responsabilidades" puede convertirse en "irresponsabilidad organizada". Ver: SCHÜNEMANN, B.: "Cuestiones básicas de dogmática jurídico-penal y política criminal sobre la criminalidad empresarial", en *Anuario de derecho penal y ciencias penales*, v. 41, n. 2, 1988, p. 553; GÓMEZ-JARA DÍEZ, C.: *A responsabilidade penal da pessoa jurídica: teoria do crime para pessoas jurídicas,* São Paulo, 2015, p. xi; CANESTRARO, A. C., KASSADA, D. A., JANUÁRIO, T. F. X.: "Nemo tenetur se detegere e programas de compliance: o direito de não produzir prova contra si próprio em face da Lei n. 13.303/16", en SAAD-DINIZ, E., BRODT, L. A., TORRES, H. A. A., LOPES, L. S. (orgs.), *Direito penal econômico nas ciências criminais,* Belo Horizonte, 2019, p. 313.

[4] En este sentido, al enumerar las razones que acreditan la necesidad de la responsabilidad penal de las personas jurídicas, Adán Nieto Martín argumenta que: "resulta necesario recuperar el terreno de la eficacia perdida" de los instrumentos estatales frente al creciente poder de las corporaciones en el contexto de globalización y mayor

de cambios legislativos en diversos países, sino también de interminables y controvertidas discusiones doctrinales y jurisprudenciales[5] .

Más recientemente, ese cuadro ha sufrido las repercusiones de un nuevo contexto, al que convencionalmente se ha venido a llamar "Revolución 4.0"[6] . Es decir, en las bases del creciente desarrollo de nuevas tecnologías como la inteligencia artificial (IA), vuelven a encontrarse las grandes corporaciones, reavivando algunos debates sobre las respuestas penales más adecuadas a los daños causados con intervención de estas tecnologías.

Pero los significativos impactos de los sistemas de la IA en el ámbito empresarial no se limitan a los casos en que estas entidades se insertan en la cadena de producción. También son relevantes las hipótesis en las que son destinatarias de estas tecnologías, tal como en el frecuente empleo de la IA en los programas de cumplimiento, ya sea en las tareas de supervisión de los empleados o para ayudar en las actividades de *due diligence* y de investigaciones internas.

Ante este escenario, partimos de la hipótesis de que las personas jurídicas tienden a asumir un papel destacado en los casos en que la intervención de la IA asume relevancia penal, ya sea por causar el daño, o por la información que almacena y que puede ser de interés a las investigaciones. Dicho esto, el objetivo del presente artículo es precisamente analizar las posibles consecuencias materiales y procesales de la IA en la responsabilidad penal de las personas jurídicas. A partir de la metodología deductiva aplicada al análisis de la doctrina y jurisprudencia española y portuguesa, responderemos a las siguientes cuestiones: en el caso de delitos con intervención de IA, ¿sería penalmente responsable la persona jurídica que la produjo? ¿Cómo se estructuraría el sistema de imputación? Además, ¿la información almacenada por la IA podría ser utilizada como prueba en un proceso penal? ¿Seríamos capaces de evaluar su fiabilidad y asegurarnos de que no se han obtenido con vulneración de los derechos de los visados?

2. INTELIGENCIA ARTIFICIAL: CONCEPTO, LIMITACIONES Y DIFICULTADES IMPUESTAS AL DERECHO PENAL

Para que podamos comprender mejor las reverberaciones de la IA en el entorno empresarial es necesario, en un primer momento, aproximarnos a qué es exactamente esta tecnología y cuáles son sus particularidades que justifican la atención que ha recibido por parte de los juristas.

---

complejidad tecnológica que acompaña a la llamada "sociedad del riesgo". NIETO MARTÍN, A.: *La responsabilidad penal de las personas jurídicas: un modelo legislativo,* Madrid, 2008, p. 38.

[5] Destacamos, por ejemplo, los debates iniciales sobre la adecuación de la responsabilidad penal de las personas jurídicas. Para algunos de los argumentos refractarios a este instituto, ver en detalle: GRACIA MARTÍN, L.: "Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica", en *Revista Electrónica de Ciencia Penal y Criminología,* n. 18-05, 2016; GRECO, L.: "Por que é ilegítimo e quase de todo inconstitucional punir pessoas jurídicas", en BUSATO, P. (org.), *Responsabilidade penal de pessoas jurídicas: seminario Brasil – Alemanha,* Florianópolis, 2018.

[6] "Los desarrollos de la tecnología y los avances científicos, especialmente en los años finales del Siglo XX y en el Siglo XXI, fueron dando paso a una nueva etapa de industrialización, en la se combinan digitalización, conectividad, automatización, robotización e inteligencia artificial. Esta etapa es la que se ha denominado como la de la industria del 4.0". BARONA VILAR, S.: *Algoritmización del derecho y de la justicia: de la inteligencia artificial a la Smart Justice,* Valencia, 2021, p. 58.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

La literatura demuestra cómo la pretensión de reproducir algunas de las capacidades humanas en máquinas es algo que ronda la imaginación de las personas desde mucho antes de que la tecnología fuera capaz de tanto. Un ejemplo de esto se puede encontrar en la mitología griega, concretamente en el robot de bronce llamado "Talos". Mencionado como el guardián de la isla de Creta, poseería habilidades de combate cuerpo a cuerpo, además de ser capaz de detectar embarcaciones extranjeras y hundirlas arrojando piedras[7] .

Sin embargo, fue en el período posterior a la Segunda Guerra Mundial cuando comenzaron a realizarse estudios más directamente relacionados con la IA. Las investigaciones realizadas por Alan Turing, orientadas a la decodificación de mensajes durante la guerra, se mencionan generalmente como fundamentales para el desarrollo del tema[8] . Pero el origen de la terminología "inteligencia artificial" se atribuye a John McCarthy, concretamente en el ámbito del texto "*A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*", de 1955. En ese momento, se consideraba como "la ciencia y la ingeniería de producir máquinas inteligentes, especialmente programas informáticos", relacionándose "con la función similar de usar computadoras para comprender la inteligencia humana" y no limitándose, sin embargo, a "métodos biológicamente observables"[9] .

Luego de décadas de avances científicos y tecnológicos en la materia, la comprensión actual de su concepto se puede subdividir en dos categorías: i) en la *inteligencia artificial como sistema*, podemos incluir *softwares* y *hardwares* que, para lograr un determinado objetivo, analizan su entorno a través de la recolección e interpretación de datos y toman una decisión en base a reglas simbólicas preestablecidas o en su propio "aprendizaje" alcanzado con experiencias anteriores. Estos sistemas pueden actuar tanto en el entorno físico como en el digital y tienen la capacidad de adaptar sus algoritmos (y en consecuencia su comportamiento) de forma autónoma, a partir de un análisis de las consecuencias de sus acciones anteriores; ii) como *disciplina científica*, la inteligencia artificial engloba diversas técnicas y metodologías, como el *machine learning*, el *machine reasoning* y la robótica, integrándolas en sistemas ciberfísicos[10] .

---

[7] MAYOR, A.: *Gods and Robots: myths, machines and ancient dreams of technology,* Princeton, 2018, p. 7. Ver también: JANUÁRIO, T. F. X. "Considerações preambulares acerca das reverberações da inteligência artificial no direito penal", en COMÉRIO, M. S., JUNQUILHO, T. A. (orgs.), *Direito e tecnologia: um debate multidisciplinar,* Rio de Janeiro, 2021, p. 295 y ss.

[8] SHABBIR, J., ANWER, T.: "Artificial intelligence and its role in near future", en *Journal of Latex Class Files*, v. 14, n. 8, 2015, p. 3; PEIXOTO, F. H., SILVA, R. Z. M., *Inteligência artificial e direito*, Curitiba, 2019, p. 24.

[9] MCCARTHY, J.: *What is Artificial Intelligence?,* Stanford, 2007; MCCARTHY, J., MINSKY, M. L., ROCHESTER, N., SHANNON, C. E.: "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955", en *AI Magazine,* v. 27, n. 4, 2006, p. 14. Ver también: JANUÁRIO, T. F. X.: "Vulnerabilidad e hiposuficiencia 4.0: la protección jurídico-penal de los consumidores en la era de la inteligencia artificial", en FONTESTAD PORTALÉS, L. (dir.), PÉREZ TORTOSA, F. (coord.), *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI,* A Coruña, en curso de publicación. Es importante mencionar que parte de la doctrina contempla con reservas la caracterización de estas tecnologías como inteligentes. En ese sentido, explica Martín Diz: "Personalmente, acepto esta catalogación, ya prácticamente consolidada, con bastantes reservas, puesto que por muy perfecta que sea la máquina, su datificación, programación y algoritmos, nunca dispondrá, por ejemplo, de sentimientos o emociones, ni siquiera de consideraciones sociales, éticas o morales, al nivel que las posee el ser humano; estas cualidades, de una manera u otra, salen a la luz cuando recurre a su inteligencia —humana— para afrontar problemas y determinar soluciones". Ver: MARTÍN DIZ, F.: "La disrupción de la inteligencia artificial en el proceso judicial: avances y retrocesos", en RAMÍREZ CARVAJAL, D. M. (coord.), *Justicia Digital: una mirada internacional en época de crisis,* Medellín, 2020, p. 526-527.

[10] THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE: *A Definition of AI: Main Capabilities and Scientific Disciplines: Definition Developed for the Purpose of the Deliverables of the High-Level Expert*

El uso de estos sistemas ya es una realidad en varias áreas de actividad. Un primer ejemplo lo encontramos en el ámbito del mercado de capitales, más concretamente en las denominadas negociaciones algorítmicas de alta frecuencia (*high-frequency trading*). Estas son técnicas de negociación algorítmica[11] , que pueden ser utilizadas en estrategias de mercado lícitas o ilícitas[12] , y que se caracterizan por la búsqueda de la máxima reducción del periodo de latencia[13] y por la emisión, modificación y cancelación de un número muy elevado de órdenes de compra y venta en un corto período de tiempo, en base a la información de mercado obtenida y procesada por el algoritmo[14] .

Es decir, en un sector donde la velocidad es fundamental, el uso de algoritmos capaces de procesar la información necesaria sobre el mercado en muy poco tiempo y de tomar decisiones de forma autónoma sobre la compra o venta de determinadas acciones puede poner a los agentes que hacen uso de ellos en una posición de innegable ventaja sobre otros operadores, lo que implica, para el mercado, beneficios pero también riesgos[15] .

Group, Brussels, 2018, p. 7. Ver también: JANUÁRIO, T. F. X.: "Vulnerabilidad e hiposuficiencia 4.0: la protección jurídico-penal de los consumidores en la era de la inteligencia artificial", en FONTESTAD PORTALÉS, L. (dir.), PÉREZ TORTOSA, F. (coord.), *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI,* A Coruña, en curso de publicación. Para un análisis detallado de la evolución del concepto de inteligencia artificial, así como algunas definiciones importantes relacionadas con esta tecnología, ver también: VALLS PRIETO, J.: *Inteligencia artificial, derechos humanos y bienes jurídicos,* Cizur Menor, 2021, p. 17 y ss.

[11] La Directiva 2014/65/UE del Parlamento Europeo y del Consejo de Europa, de 15 de mayo de 2014, define en su artículo 4, n. 1, las negociaciones algorítmicas, como siendo: "la negociación de instrumentos financieros en la que un algoritmo informático determina automáticamente los distintos parámetros de las órdenes (si la orden va a ejecutarse o no, el momento, el precio, la cantidad, cómo va a gestionarse después de su presentación), con limitada o nula intervención humana. Esta definición no incluye los sistemas que solo se proponen dirigir las órdenes a uno o varios centros de negociación, o procesar las órdenes sin que ello implique determinar ningún parámetro de negociación, o confirmar las órdenes o el tratamiento post-negociación de las transacciones ejecutadas;". PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA: *Directiva 2014/65/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014: relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE*.

[12] Sobre estas estrategias: CAVALI, M. C.: *Manipulação do mercado de capitais: fundamentos e limites da repressão penal e administrativa,* São Paulo, 2018. Específicamente sobre estrategias ilícitas mediante el uso de algoritmos, ver: RODRIGUES, A. M.: "Os crimes de abuso de mercado e a "Escada Impossível" de Escher (o caso do Spoofing)", en *Julgar,* n. 45, 2021, p. 65 y ss.

[13] El período de latencia es el tiempo necesario para que un intermediario reciba un *feedback* sobre una orden introducida por él en el mercado. Es decir, el tiempo que transcurre entre la generación de una orden de compra o venta y su posterior ejecución, modificación o cancelación. Ver: ALMEIDA, M. S.: "Introdução à negociação de alta frequência", en *Cadernos de Valores Mobiliários*, n. 54, 2016, p. 26; RIORDAN, R., STORKENMAIER, A.: "Latency, Liquidity and Price Discovery", en *Journal of Financial Markets*, v. 15, n. 4, 2012, p. 417.

[14] JANUÁRIO, T. F. X.: "Inteligência artificial e manipulação do mercado de capitais: uma análise das negociações algorítmicas de alta frequência (high-frequency trading – HFT) à luz do ordenamento jurídico brasileiro", en *Revista Brasileira de Ciências Criminais,* ano 29, n. 186, 2021, p. 135.

[15] Ver en detalle en: JANUÁRIO, T. F. X.: "Inteligência artificial e manipulação do mercado de capitais: uma análise das negociações algorítmicas de alta frequência (high-frequency trading – HFT) à luz do ordenamento jurídico brasileiro", en *Revista Brasileira de Ciências Criminais,* ano 29, n. 186, 2021, p. 135 y ss.; COSTA, I. S.: *High Frequency Trading em câmera lenta: compreender para regular,* São Paulo, 2020; LESHIK, E., CRALLE, J.: *An Introduction to Algorithmic Trading: Basic to Advanced Strategies*, Chichester, 2011, p. 17 y ss.; BROGAARD, J., HENDERSHOTT, T., RIORDAN, R.: "High-Frequency Trading and Price Discovery", en *The Review of Financial Studies*, v. 27, n. 8, 2014, p. 2268; CAIVANO, V. et al.: "Il trading ad alta frequenza: caratteristiche, effetti, questioni di policy", en *CONSOB Discussion Papers*, n. 5, 2012, p. 17 y ss.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

En el ámbito de la salud, por su parte, los avances en el campo de la IA generan expectativas optimistas para los próximos años, en cuanto a aplicaciones de asistencia en diagnósticos, tratamiento y seguimiento de pacientes, cirugías robóticas, medicina personalizada e incluso en la prevención del suicidio a través del monitoreo de redes sociales[16] .

También son destacables las aplicaciones de esta tecnología en el ámbito del transporte. Aunque no todos los llamados "vehículos autónomos" están equipados con IA (teniendo diferentes niveles de autonomía[17]), existen grandes expectativas de avances progresivos en el sector. Una mayor capacidad que la inteligencia humana para procesar informaciones y tomar decisiones en un tiempo cada vez más reducido, sumada a que estos sistemas no suelen presentar los errores típicamente humanos en el tráfico (por ejemplo, imprudencia, exceso de velocidad y conducción tras consumo de alcohol), genera pronósticos optimistas respecto a la reducción del número de accidentes y muertes para el futuro[18] .

Finalmente, también es importante mencionar la aplicación cada vez más significativa de la IA en el sistema de justicia. A modo de ejemplo, en lo que respecta a la persecución penal, observamos el uso de estos sistemas en las áreas de inteligencia y supervisión[19] , investigaciones (públicas[20] y privadas[21]), toma de decisiones judiciales[22] y ejecución penal[23] .

---

[16] Ver en detalle en: JANUÁRIO, T. F. X.: "Inteligência artificial e responsabilidade penal no setor da medicina", *Lex Medicinae: Revista Portuguesa de Direito da Saúde*, ano 17, n. 34, 2020, p. 37 y ss.; JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 131 y ss.; PEREIRA, A. G. D.: "O médico-robô e os desafios para o direito da saúde: entre o algoritmo e a empatia", *Gazeta de Matemática*, ano LXXX, n. 189, 2019, p. 30 y ss.; PEREIRA, A. G. D.: "Inteligência artificial, saúde e direito: considerações jurídicas em torno da medicina de conforto e da medicina transparente", *Julgar*, n. 45, 2021, p. 235s.; MACHADO, L. S.: "Médico robô: responsabilidade civil por danos praticados por atos autônomos de sistemas informáticos dotados de inteligência artificial", en *Lex Medicinae: Revista Portuguesa de Direito da Saúde*, ano 16, n. 31-32, 2019, p. 101 y ss.

[17] De acuerdo con la clasificación presentada por la *National Highway Traffic Safety Administration – NHTSA* y desarrollada por la *Society of Automotive Engineers – SAE*, los niveles de automatización de los vehículos van desde 0 (sin autonomía) hasta 5 (autonomía total). En los niveles intermedios tenemos vehículos controlados por el conductor humano, con algunas herramientas de asistencia autónoma (nivel 1); los que tienen funciones autónomas (como el frenado y la aceleración) pero que dependen del ser humano para controlar el entorno externo en todo momento (nivel 2) –es el caso de los conocidos vehículos Tesla–; aquellos en los que el conductor no necesita monitorear el ambiente externo en todo momento, pero debe estar listo para tomar el control del vehículo cuando se le solicite (nivel 3) – este es el caso de los vehículos Uber, que están en fase de prueba; y aquellos que, en determinadas condiciones normales, son capaces de realizar de forma autónoma todas las funciones del vehículo (nivel 4). Ver en detalle en: UNITED STATES DEPARTMENT OF TRANSPORTATION, NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION – NHTSA: *Automated Vehicles for Safety.* <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>. Accedido en 31 de octubre de 2022.

[18] Sobre los potenciales y riesgos de los vehículos autónomos, ver: JANUÁRIO, T. X.: "Veículos autónomos e imputação de responsabilidades criminais por acidentes", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* Coimbra, 2020, p. 95 y ss; GLEß, S., SILVERMAN, E., WEIGEND, T. "If robots cause harm, who is to blame? Self-driving cars and criminal liability", en *New Criminal Law Review*, v. 19, n. 3, 2016, p. 412 y ss.; ESTELLITA, H., LEITE, A.: "Veículos Autônomos e Direito Penal: uma introdução", en ESTELLITA, H., LEITE, A. (orgs.), *Veículos autônomos e direito penal*, São Paulo, 2019, p. 15y ss.; HILGENDORF, E.: "Sistemas autônomos, inteligência artificial e robótica: uma orientação a partir da perspectiva jurídico-penal", en HILGENDORF, E., GLEIZER, O. (orgs.), *Digitalização e direito*, São Paulo, 2020, p. 43 y ss.; TEIXEIRA, R.: "Meritíssima, a culpa não é minha! Imputação de responsabilidade penal por danos provocados por veículos autónomos", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 65 y ss.

[19] Como ejemplo, podemos mencionar la denominada *PredPol*, que es una estrategia policial dirigida a la prevención del delito. Con el uso de algoritmos y la integración de datos obtenidos a través de otras tecnologías (como

Observamos que debido a algunas de sus potencialidades (como la capacidad de procesar una inmensa cantidad de datos, en tiempo muy reducido y muchas veces con mayor precisión que la humana), la IA tiende a impactar positivamente varios sectores de actividad, como los mencionados anteriormente de forma no exhaustiva. Sin embargo, también es importante

---

cámaras de vigilancia y temperatura corporal, publicaciones en internet y análisis estadístico de eventos pasados) con informaciones como los horarios de apertura de comercios y el flujo de personas, se busca determinar en qué lugares es más probable la ocurrencia de delitos (*hotspots*) y dirigir contingentes policiales más grandes al lugar, creando así una especie de mapa de delitos futuros. Ver: BARONA VILAR, S.: *Algoritmización del Derecho y de la Justicia: de la Inteligencia Artificial a la Smart Justice,*Valencia, 2021, p. 445 y ss. Ver también: QUATTROCOLO, S.: *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion,*Cham, 2020, p. 39. Además, también existe un gran potencial de aplicación de la IA en el modelo global de prevención y detección del blanqueo de capitales. Dado que las UIFs reciben una inmensa cantidad de datos, que son imposible revisar manualmente, es esencial emplear mecanismos de automatización para identificar patrones de actividad sospechosa. Ver: AGAPITO, L. S., MIRANDA, M. A., JANUÁRIO, T. F. X.: "On the Potentialities and Limitations of Autonomous Systems in Money Laundering Control", en RIDP, v. 92, n. 1, 2021, p. 90. Ver también: RODRIGUES, A. M.: "Compliance inteligente e prevenção e luta contra o branqueamento", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 207 y ss.

[20] Entre los muchos ejemplos de IA en investigaciones criminales, podemos mencionar el sistema VERIPOL, destinado a identificar posibles denuncias falsas, y el uso de la ICSE – DB (*International Child Sexual Exploitation Image Database*) por la Interpol en la lucha contra la explotación sexual infantil. Además, aun en este ámbito, existe el uso de *chatbots* que imitan a personas reales para identificar posibles depredadores sexuales en foros virtuales. Ver en detalle: "In Europe, Interpol manages the International Child Sexual Exploitation Image Database (ICSE DB) to fight child sexual abuse. The database can facilitate the identification of victims and perpetrators through an analysis of, for instance, furniture and other mundane items in the background of abusive images—e.g., it matches carpets, curtains, furniture,

and room accessories—or identifiable background noise in the video. Chatbots acting as real people are another advancement in the fight against grooming and webcam 'sex tourism'. […] The Sweetie avatar [from the NGO "Terre des Hommes"], posing as a ten-year-old Filipino girl, was used to identify offenders in chatrooms and online forums and operated by an agent of the organisation, whose goal was to gather information on individuals who contacted Sweetie and solicited webcam sex. Moreover, Terre des Hommes started engineering an AI system capable of depicting and acting as Sweetie without human intervention in order to not only identify persistent perpetrators but also to deter first-time offenders". ZAVRŠNIK, A.: "Criminal justice, artificial intelligence systems, and human rights", en *ERA Forum,* n. 20, 2020, p. 570. Respecto a VERIPOL: BARONA VILAR, S.: *Algoritmización del Derecho y de la Justicia: de la Inteligencia Artificial a la Smart Justice,* Valencia, 2021, p. 458.

[21] Como detallaremos más adelante, en el ámbito privado, los potenciales de la IA se han utilizado no solo en el monitoreo y supervisión diaria de empleados y colaboradores, sino también en investigaciones internas, procedimientos de *due diligence* y gestión de riesgos, siendo, por tanto, una herramienta importante en los programas de cumplimiento. Ver: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 363 y ss.; RODRIGUES, A. M.: "The Last Cocktail - Economic and Financial Crime, Corporate Criminal Responsibility, Compliance and Artificial Intelligence", en ANTUNES, M. J., SOUSA, S. A. (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Coimbra, 2021, p. 119 y ss.; BURCHARD, C.: "Das »Strafrecht« der Prädiktionsgesellschaft: …oder wie »smarte« Algorithmen die Strafrechtspflege verändern (könnten)", en *Forschung Frankfurt: das Wissenschaftsmagazin: Recht und Gesetz*, n. 1, 2020, p. 27 y ss.

[22] En este ámbito, son paradigmáticas algunas herramientas autónomas de evaluación de riesgos, de las cuales COMPAS y HART son los ejemplos más conocidos. En general, se sirven de factores personales del imputado para evaluar los riesgos de reincidencia y, en consecuencia, la eventual adecuación de medidas cautelares, penas concretas o progresión de regímenes. Ver: MIRÓ LLINARES, F.: "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", en *Revista de Derecho Penal y Criminología,* 3. época, n. 20, 2018, p. 108 y ss.

[23] En las llamadas *smart prisons,* la IA se emplea en el diseño y administración de la prisión, así como en la supervisión del día a día de los detenidos (detectando, por ejemplo, conductas ilícitas, actos violentos y posibles fugas). Ver: BARONA VILAR, S.: *Algoritmización del Derecho y de la Justicia: de la Inteligencia Artificial a la Smart Justice,* Valencia, 2021, p. 683 y ss.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

señalar que, a pesar de la alta tecnología utilizada en ellos, estos sistemas tienen algunas limitaciones e imponen algunos desafíos[24] que debe enfrentar el derecho[25] .

En primer lugar, debemos apuntar que la IA y los algoritmos que utiliza se consideran opacos. En otras palabras, tal es su complejidad técnica que es muy difícil para el ser humano comprender sus procedimientos internos, las razones que subyacen en determinadas tomas de decisiones e incluso los datos que se utilizan como *input* y su relación con un determinado *output*. En otras palabras, aunque tengamos acceso a una decisión concreta, entender el "cómo" y el "por qué" es muy complicado[26] .

---

[24] En un sentido similar, Valls Prieto señala: "Los avances tecnológicos suponen retos para la sociedad y eso conlleva al mismo tiempo nuevos desafíos para el ordenamiento jurídico. Integrar jurídicamente un avance tecnológico supone un beneficio económico para la sociedad, ya que implica un desarrollo industrial y de servicios, y al mismo tiempo una garantía de la modernización y actualización de los clásicos Derechos Fundamentales en los que se basa una sociedad, especialmente en una Democracia garante de las libertades de los ciudadanos". VALLS PRIETO, J.: *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial,* Madrid, 2017, p. 39.

[25] De hecho, como bien apunta de Hoyos Sancho, la mayoría de los posibles usos de los sistemas de IA en el sistema de justicia penal están catalogados como "sistemas de alto riesgo" por la Propuesta de Reglamento del Parlamento Europeo y del Consejo, presentada en abril de 2021. Así lo demuestra el Anexo III, especialmente en sus apartados 6 y 8, que prevén: "6.Asuntos relacionados con la aplicación de la ley: a)sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para llevar a cabo evaluaciones de riesgos individuales de personas físicas con el objetivo de determinar el riesgo de que cometan infracciones penales o reincidan en su comisión, así como el riesgo para las potenciales víctimas de delitos; b)sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley como polígrafos y herramientas similares, o para detectar el estado emocional de una persona física; c)sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para detectar ultrafalsificaciones a las que hace referencia el artículo 52, apartado 3; d)sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para la evaluación de la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de infracciones penales; e)sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para predecir la frecuencia o reiteración de una infracción penal real o potencial con base en la elaboración de perfiles de personas físicas, de conformidad con lo dispuesto en el artículo 3, apartado 4, de la Directiva (UE) 2016/680, o en la evaluación de rasgos y características de la personalidad o conductas delictivas pasadas de personas físicas o grupos; f)sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para la elaboración de perfiles de personas físicas, de conformidad con lo dispuesto en el artículo 3, apartado 4, de la Directiva (UE) 2016/680, durante la detección, la investigación o el enjuiciamiento de infracciones penales; g)sistemas de IA destinados a utilizarse para llevar a cabo análisis sobre infracciones penales en relación con personas físicas que permitan a las autoridades encargadas de la aplicación de la ley examinar grandes conjuntos de datos complejos vinculados y no vinculados, disponibles en diferentes fuentes o formatos, para detectar modelos desconocidos o descubrir relaciones ocultas en los datos. […] 8.Administración de justicia y procesos democráticos: a)sistemas de IA destinados a ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la aplicación de la ley a un conjunto concreto de hechos". Ver en detalle en: COMISIÓN EUROPEA: *Propuesta de Reglamento del Parlamento Europeo y del Consejo: por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión: {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}*. Para un estudio detallado de este documento y sus disposiciones, ver también: DE HOYOS SANCHO, M.: "El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea", en *Revista General de Derecho Procesal*, n. 55, 2021, p. 14 y ss.

[26] Ver: BURRELL, J.: "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms", en *Big Data & Society,* v. 3, n. 1, 2016, p. 1; PRICE II, W. N.: "Artificial Intelligence in Health Care: Applications and Legal Issues", en *U of Michigan Public Law Research Paper,* n. 599, 2017, p. 2; WIMMER, M.: "Inteligência Artificial, Algoritmos e o Direito: Um Panorama dos Principais Desafios", em LIMA, A. P. C., HISSA, C. B., SALDANHA, P. M. (eds), *Direito Digital: Debates Contemporâneos,* São Paulo, 2019; RODRIGUES, A. M.: "Inteligência Artificial no Direito Penal – A Justiça Preditiva entre a Americanização e a Europeização", en RODRIGUES, A. M. (coord.), *A Inteligência Artificial no Direito*

Esta opacidad también genera dudas sobre la legalidad y credibilidad de los datos utilizados como *input*. Como señala Miró Llinares, a diferencia del pasado, en el que el intercambio de datos dependía de una conducta mínimamente consciente y activa de las personas, en la actualidad se comparten de forma masiva, generando justificables temores de vulneración desproporcionada de la privacidad e intimidad de las personas[27] .

Además, la calidad de los datos utilizados para el entrenamiento del algoritmo puede ser baja. Esto puede ocurrir por una mala clasificación realizada por el programador responsable; por su recolección en un período de tiempo muy restringido; o por el simple hecho de que los datos recolectados no son representativos. En cualquiera de estos casos, la invalidez o imprecisión de los datos tiende a incrementar los riesgos de errores y de *outputs* de baja calidad[28] .

A lo anterior se suma la *imprevisibilidad* de los *outputs* logrados por los sistemas de IA. Con esto queremos decir que, en función de su capacidad para "aprender" de sus actuaciones pasadas y adaptar de forma autónoma sus propios algoritmos, los resultados obtenidos por la IA son a menudo impredecibles incluso para sus propios programadores[29] .

Por sus particularidades y limitaciones mencionadas anteriormente, sumadas al hecho de que no son infalibles y pueden causar daños a bienes jurídicos tutelados penalmente, los sistemas de IA crean algunos nuevos desafíos en materia de responsabilidad penal.

Penal, Coimbra, 2020, p. 25; DE HOYOS SANCHO, M.: "El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea", en *Revista General de Derecho Procesal*, n. 55, 2021, p. 4. Además, Nieva Fenoll señala que: "Ya es difícil acceder a su contenido técnicamente hablando, pero es que, si además ni siquiera se puede conocer dicho contenido por razones de propiedad intelectual, el derecho de defensa simplemente deja de existir". Ver: NIEVA FENOLL, J.: *Inteligencia artificial y proceso judicial,* Madrid, 2018, p. 143.

[27] MIRÓ LLINARES, F.: "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", en *Revista de Derecho Penal y Criminología,* 3. época, n. 20, 2018, p. 114 y ss.

[28] Para más detalles y con múltiples notas ver: MIRÓ LLINARES, F.: "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", en *Revista de Derecho Penal y Criminología,* 3. época, n. 20, 2018, p. 122 y ss. En la misma línea, de Hoyos Sancho señala que el uso de datos erróneos, insuficientes o sesgados, introducidos en el sistema sin corrección previa, sumado a la falta de transparencia en cuanto a la configuración y funcionamiento de los algoritmos utilizados en el sistema, genera importantes riesgos a los derechos fundamentales, como la protección de datos, la privacidad, la no discriminación, el *fair trial* y el *due process.* Ver: DE HOYOS SANCHO, M., "El Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo", en *Revista Española de Derecho Europeo,* n. 76, 2020, p. 16 y ss. Para un análisis detallado sobre el tema de la seguridad y calidad de los datos: MULHOLLAND, C., FRAJHOF, I. Z.: "Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning", en FRAZÃO, A., MULHOLLAND, C. (eds.), *Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade,*São Paulo, 2019; YAPO, A.. WEISS, J.: "Ethical Implications of Bias in Machine Learning", en *Proceedings of the 51st Hawaii International Conference on System Sciences,* 2018, p. 5366; PEIXOTO, F. H., SILVA, R. Z. M.: *Inteligência artificial e direito,* Curitiba, 2019, p. 34-35; JANUÁRIO, T. F. X. "Considerações preambulares acerca das reverberações da inteligência artificial no direito penal", en COMÉRIO, M. S., JUNQUILHO, T. A. (orgs.), *Direito e tecnologia: um debate multidisciplinar,* Rio de Janeiro, 2021 ; MIRANDA, M. A., JANUÁRIO, T. F. X.: "Novas tecnologias e justiça criminal: a tutela de direitos humanos e fundamentais no âmbito do direito penal e processual penal", en MOREIRA, V. et al (eds.), *Temas de Direitos Humanos do VI CIDH Coimbra 2021,* Campinas, 2021, p. 286 y ss.

[29] En este sentido, como explica Susana Aires de Sousa, una de las especificidades de los sistemas autónomos radica precisamente en su capacidad de llegar a respuestas sin interferencias humanas, basándose exclusivamente en informaciones y experiencias adquiridas por el sistema. Con esto, se pueden lograr resultados que ni siquiera fueron imaginados por el programador y tomar decisiones que incluso pueden ser ilegales. SOUSA, S. A.: ""Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal*, Coimbra, 2020, p. 64.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

La doctrina identifica y clasifica cuatro grupos de posibles delitos relacionados con la IA: I) delitos cometidos intencionalmente por personas físicas o jurídicas, con uso deliberado de la IA; II) delitos negligentes causados por fallas en la cadena productiva y/o uso de la IA; III) ilícitos provocados por la propia IA, sin intervención humana; IV) ilícitos cometidos por seres humanos, instrumentalizados por la IA[30] .

Si bien no podemos ignorar las eventuales dificultades encontradas en otros casos, es, a nuestro juicio, en los grupos (II), (III) y (IV) que se encuentran las mayores dificultades en la imputación de responsabilidades criminales individuales por los crímenes en cuestión.

Para visualizar mejor el problema, pensemos en los siguientes casos hipotéticos: i) en el empleo de la IA en el sector médico, si un diagnóstico erróneo presentado por un sistema de asistencia, o un error cometido por un robot inteligente en el contexto de una cirugía, resulta en lesiones, o incluso en la muerte de un paciente, ¿quién sería considerado penalmente responsable por estas conductas?; ii) en el contexto del mercado de capitales, si un operador hace uso de un sistema algorítmico que, al interpretar las condiciones del mercado y ejecutar órdenes de compra y venta, incurre en la práctica de *spoofing* o *layering*, ¿a quién se consideraría autor de estas conductas, con arreglo al art. 284.3 del CPEsp?[31] ; iii) finalmente, si un vehículo autónomo dotado con un sistema de IA, en un determinado evento y por causas desconocidas, realiza una maniobra que provoca un accidente y lesiona o mata a terceros o incluso a sus ocupantes, ¿quién sería, para efectos jurídico-penales el responsable de esta conducta? ¿El fabricante? ¿El programador? ¿El usuario? ¿El robot en sí?

La imputación de responsabilidades penales en casos relacionados con la IA se ve obstaculizada inicialmente por la propia complejidad del sector. En el desarrollo, fabricación, programación y uso de estas tecnologías, existe la intervención de innumerables personas físicas y jurídicas, que dividen sus atribuciones de forma no siempre regular y transparente. Si a esto le sumamos la opacidad de estos sistemas, llegaremos a la conclusión de que es muy difícil (y en algunos casos, imposible) precisar el nexo de causalidad entre una determinada conducta (la escrita de una línea de código, por ejemplo) y el daño o peligro de daño[32] .

Además, al depender del caso concreto y del tipo penal a la luz del cual se analice, entendemos que ni siquiera será posible sostener que haya un autor humano que haya

---

[30] PAGALLO, U., QUATTROCOLO, S.: "The Impact of AI on Criminal Law and its Twofold Procedures", en BARFIELD, W., PAGALLO, U. (eds.), *Research Handbook on the law of artificial intelligence,* Cheltenham, 2018, p. 404.

[31] "Artículo 284. 1. Se impondrá la pena de prisión de seis meses a seis años, multa de dos a cinco años, o del tanto al triplo del beneficio obtenido o favorecido, o de los perjuicios evitados, si la cantidad resultante fuese más elevada, e inhabilitación especial para intervenir en el mercado financiero como actor, agente o mediador o informador por tiempo de dos a cinco años, a los que: […]3.º Realizaren transacciones, transmitieren señales falsas o engañosas, o dieren órdenes de operación susceptibles de proporcionar indicios falsos o engañosos sobre la oferta, la demanda o el precio de un instrumento financiero, un contrato de contado sobre materias primas relacionado o índices de referencia, o se aseguraren, utilizando la misma información, por sí o en concierto con otros, una posición dominante en el mercado de dichos instrumentos o contratos con la finalidad de fijar sus precios en niveles anormales o artificiales, siempre que concurra alguna de las siguientes circunstancias: a) que como consecuencia de su conducta obtuvieran, para sí o para tercero, un beneficio superior a doscientos cincuenta mil euros o causara un perjuicio de idéntica cantidad; b) que el importe de los fondos empleados fuera superior a dos millones de euros; c) que se causara un grave impacto en la integridad del mercado." ESPAÑA. *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*.

[32] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 159. Acerca de la intervención de inúmeras personas jurídicas en varios momentos durante la programación, uso y supervisión del algoritmo, ver: DIAMANTIS, M. E.: "Algorithmic Harms as Corporate Misconduct", en ANTUNES, M. J., SOUSA, S. A. (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility,* Coimbra, 2022, p. 149.

realizado el hecho. A nuestro juicio, *autor*, en su nivel más básico (el *lógico-gramatical*), es quien practica la conducta correspondiente al sentido de la conducta descrita en el tipo penal, que debe identificarse, en el caso concreto, a partir de la interpretación del verbo típico[33] . Dicho esto, cuando no hay un uso intencional de la IA por una persona, para la comisión del ilícito, y ello tampoco es resultado de una falla en la cadena de producción y uso del sistema, sino que es resultado de su propia capacidad de aprendizaje autónomo, no vamos a tener, al depender del caso concreto y del tipo penal, una actuación humana en la realización del sentido de la acción descrita por el tipo[34] .

Aunque no sea así, es decir, si es posible identificar una conducta humana causadora del daño o peligro de daño, la *imprevisibilidad* de los *outputs* del algoritmo seguirá imponiendo dificultades en la imputación penal, ya que, en estos casos, el programador, el fabricante y, menos aún, el usuario directo de la tecnología, no siempre podrán prever el desempeño de la IA. Dado que el juicio de previsibilidad es fundamental para la tipicidad de determinadas conductas[35] , entendemos que la tipicidad del comportamiento de los actores humanos debe rechazarse cuando el resultado ilícito de la IA es totalmente impredecible[36] .

Debido a estas dificultades, hay parte de la doctrina que comienza a analizar[37] (y en algunos casos, a apoyar[38]) la imputación penal de los propios sistemas de IA. No entendemos, sin embargo, que ésta sea la solución más adecuada, no necesariamente por las indispensables adaptaciones dogmáticas que requeriría, sino principalmente porque impondría adecuadas revisiones sobre los propios fundamentos y finalidades de la pena y del derecho penal, que, tal

---

[33] Como puede verse, partimos de la *teoría de la acción significativa*, que se abstrae de la búsqueda de un "superconcepto" de acción y, en consecuencia, también de la búsqueda de un concepto general de autor, que siempre dependerá del tipo delictivo y su interpretación. Ver: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Concurso de agentes na perspectiva da teoria da ação significativa: um diálogo entre o sistema espanhol e o Projeto de Novo Código Penal Brasileiro", en *Revista Brasileira de Ciências Criminais*, ano 29, n. 178, 2021, p. 225 y ss.; MARTÍNEZ-BUJÁN PÉREZ, C.: *La autoría en derecho penal: un estudio a la luz de la concepción significativa (y del Código penal español)*, Valencia, 2019; VIVES ANTÓN, T. S.: *Fundamentos del sistema penal*, 2. ed., Valencia, 2011, p. 726; MARTÍNEZ-BUJÁN PÉREZ, C.: *Derecho penal económico y de la empresa – Parte general*, 5. ed. adaptada a la L.O. 1/2015, Valencia, 2016, p. 489-490.

[34] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 159.

[35] FRISCH, W.: *Comportamiento típico e imputación del resultado*, Madrid, 2004, p. 119-120. En un sentido similar, argumentando que la total imprevisibilidad del resultado tiene el poder de excluir la imputación objetiva: ROXIN, C.: *Derecho Penal: parte general: tomo I: fundamentos. La estructura de la teoria del delito*, Madrid, 2008, p. 1000-1001; DIAS, J. F.: *Direito Penal: parte geral: tomo I: questões fundamentais: a doutrina geral do crime*, São Paulo, 2007, p. 901.

[36] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 162; JANUÁRIO, T. F. X.: "Inteligência artificial e manipulação do mercado de capitais: uma análise das negociações algorítmicas de alta frequência (high-frequency trading – HFT) à luz do ordenamento jurídico brasileiro", en *Revista Brasileira de Ciências Criminais,* ano 29, n. 186, 2021, p. 160 y ss.

[37] Para una síntesis de algunos argumentos a favor y en contra, ver: GLEß, S., SILVERMAN, E., WEIGEND, T. "If robots cause harm, who is to blame? Self-driving cars and criminal liability", en *New Criminal Law Review*, v. 19, n. 3, 2016; GLEß, S., WEIGEND, T.: "Intelligente Agenten und das Strafrecht", en *Zeitschrift für die gesamte Strafrechtswissenschaft*, v. 126, n. 3, 2014.

[38] Por todos, ver: HALLEVY, G.: *Liability for Crimes Involving Artificial Intelligence Systems*, Heidelberg, 2015; HALLEVY, G.: *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, 2019; HALLEVY, G.: "The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control", en *Akron Intellectual Property Journal*, v. 4, n. 2, 2010, p. 171 y ss.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

y como se conciben actualmente, no parecen cumplirse con un eventual castigo a un sistema concreto de IA[39] .

Por estas razones, sin abandonar las discusiones sobre la responsabilidad penal individual en estos casos, que sin duda deben jugar un papel importante en este ámbito, creemos que la responsabilidad penal de las personas jurídicas debe ser objeto de especial atención en el contexto de los delitos cometidos con la intervención de la IA. Este será el objeto de nuestra atención en el siguiente tópico.

3. LAS EMPRESAS EN LA CADENA DE PRODUCCIÓN TECNOLÓGICA: RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL CONTEXTO DE LA INTELIGENCIA ARTIFICIAL

Los fundamentos político-criminales que subyacen a la responsabilidad penal de las personas jurídicas (RPPJ) ya han sido expuestos sucintamente a lo largo del texto[40] . El protagonismo asumido por estas entidades en las más variadas ramas de actividad, sumado a los riesgos delictivos que potencia el entorno empresarial y la complejidad de su enfrentamiento por la vía penal, en particular en lo que se refiere a la identificación y responsabilidad de los autores individuales de un determinado hecho típico, nos llevó a una realidad en la que son pocos los países que aún se resisten a la adopción de la RPPJ. Aún existen vivas discusiones, sin embargo, acerca de los sistemas concretos de imputación de responsabilidad penal a estos sujetos, que terminan reflejándose en modelos disonantes entre los ordenamientos jurídicos.

Es notorio que los primeros modelos de RPPJ, propuestos aún en una fase de progresivo abandono del dogma *societas delinquere non potest*, pueden agruparse en un género comúnmente conocido como de *heterorresponsabilidad de las personas jurídicas*. Como característica común de estos modelos, de los cuales Brasil[41] es todavía uno de sus restantes adoptantes, tenemos una especie de "transferencia" de la responsabilidad penal de un individuo particular a la entidad colectiva, cuando se cumplen ciertos requisitos. En la base de estas propuestas estaría el entendimiento de que la persona jurídica sería incapaz de existir, actuar y expresar una voluntad independiente de los individuos que la componen, por lo que su responsabilidad autónoma sería inadecuada[42] .

---

[39] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 148.

[40] Para un análisis detallado de las razones político-criminales generalmente invocadas para justificar la responsabilidad penal de las personas jurídicas, ver: GONZÁLEZ CUSSAC, J. L.: "El plano político criminal en la responsabilidad penal de las personas jurídicas", en MATALLÍN EVANGELIO, Á. (dir.), *Compliance y prevención de delitos de corrupción,* Valencia, 2018; GONZÁLEZ CUSSAC, J. L.: *Responsabilidad penal de las personas jurídicas y programas de cumplimiento,* Valencia, 2020, p. 25-46; CARBONELL MATEU, J. C.: "Responsabilidad penal de las personas jurídicas: reflexiones en torno a su dogmática y al sistema de la reforma de 2010", en *Cuadernos de política criminal,* segunda época, n. 101, 2010, p. 7-12; BUSATO, P. C.: "Razões político-criminais para a responsabilização penal de pessoas jurídicas", en BUSATO, P. (org.), *Responsabilidade penal de pessoas jurídicas: seminario Brasil – Alemanha,* Florianópolis, 2018; NETTO, A. V. S.: *Responsabilidade penal da pessoa jurídica,* 2. ed., São Paulo, 2020. Críticamente a los argumentos comúnmente invocados: DÍEZ, RIPOLLÉS, J. L.: "La responsabilidad penal de las personas jurídicas. Regulación española", en *InDret,* n. 1, 2012, p. 2-5.

[41] Para un análisis crítico, ver: JANUÁRIO, T. F. X.: "El modelo brasileño de responsabilidad penal para entidades jurídicas: un comentario de la Ley 9.605/98 y el nuevo Código Penal", en DEMETRIO CRESPO, E. et al (eds.), *Problemas y retos actuales del derecho penal económico,* Cuenca, 2020.

Un buen ejemplo de ese pensamiento es la denominada *alter ego theory*, desarrollada en el ámbito del derecho civil inglés por la *House of Lords*, en el caso *Tesco Supermarkets Ltd. v. Nattrass, de 1971*. Según esta, la empresa sería como un cuerpo humano, cuya mente serían los directores y administradores y los miembros serían los empleados. El estado mental de la empresa, por tanto, sería el de su dirección[43] .

Esta propuesta es claramente adoptada por el Código Penal Portugués (CPPt) en una de sus previsiones de RPPJ, a saber, el Artículo 11.º, n. 2, "a", ya que, si bien no se requiere la acumulación de responsabilidad de la persona física a los efectos de hacer responsable a la persona jurídica, sí existe una identificación de ésta con las personas que ocupan en ella un cargo de dirección y actúan en su nombre o por su cuenta, en su interés directo o indirecto[44] .

Otro ejemplo muy difundido de los modelos de *heterorresponsabilidad* es el denominado *modelo vicarial*. Como analiza críticamente Adán Nieto Martín, se trata de una propuesta que exige tres condiciones: i) la comisión de una infracción por parte de un agente de la empresa; ii) en el ejercicio de las funciones que le han sido atribuidas o por cuenta de la empresa; y iii) la intención de obtener un beneficio o ventaja para la empresa, que es una de las principales diferencias con la teoría de la identificación[45] . Inês Godinho también destaca la posibilidad, en esta última propuesta, de que la persona jurídica también sea responsable por los actos de los empleados subordinados, no dependiendo su responsabilidad penal de la actuación de una persona con poder de dirección[46] .

En cualquiera de sus modalidades, sin embargo, los modelos de *heterorresponsabilidad* fueron prontamente criticados por la doctrina. En primer lugar, porque como todavía dependientes de la identificación de una conducta individual de un determinado agente para que la persona jurídica sea responsabilizada, estas propuestas acaban por no resolver la cuestión antes mencionada de la irresponsabilidad organizada, problema que la RPPJ pretendía precisamente resolver[47] .

---

[42] Críticamente a esta posición: JANUÁRIO, T. F. X.: "Da (ir)relevância dos programas de compliance no modelo brasileiro de responsabilidade penal das pessoas jurídicas: considerações críticas ao projeto de novo Código Penal", en *Revista Direito e Liberdade*, v. 21, n. 2, 2019, p. 331.

[43] UNITED KINGDOM HOUSE OF LORDS: *Tesco Supermarkets Ltd. v. Nattrass,* 1971. Para un análisis detallado, ver también: TORRÃO, F.: *Societas delinquere potest?: da responsabilidade individual e colectiva nos "crimes de empresa",* Coimbra, 2010, p. 67.

[44] "Artigo 11.º Responsabilidade das pessoas singulares e colectivas [...] 2 - As pessoas coletivas e entidades equiparadas, com exceção do Estado, de pessoas coletivas no exercício de prerrogativas de poder público e de organizações de direito internacional público, são responsáveis pelos crimes previstos nos artigos 144.º-B, 150.º, 152.º-A, 152.º-B, 156.º, 159.º e 160.º, nos artigos 163.º a 166.º sendo a vítima menor, e nos artigos 168.º, 169.º, 171.º a 177.º, 203.º a 206.º, 209.º a 223.º, 225.º, 226.º, 231.º, 232.º, 240.º, 256.º, 258.º, 262.º a 283.º, 285.º, 299.º, 335.º, 348.º, 353.º, 359.º, 363.º, 367.º, 368.º-A e 372.º a 377.º, quando cometidos: a) Em seu nome ou por sua conta e no seu interesse direto ou indireto por pessoas que nelas ocupem uma posição de liderança; ou [...] 4 - Entende-se que ocupam uma posição de liderança os órgãos e representantes da pessoa coletiva e quem nela tiver autoridade para exercer o controlo da sua atividade, incluindo os membros não executivos do órgão de administração e os membros do órgão de fiscalização." PORTUGAL: *DL n.º 48/95, de 15 de março: Código Penal de 1982 versão consolidada posterior a 1995*. Para un análisis crítico, ver: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Responsabilidade penal da pessoa coletiva e princípio da culpabilidade: análise crítica do modelo português", en *Revista da Faculdade de Direito da UFRGS*, n. 39, 2018.

[45] NIETO MARTÍN, A.: *La responsabilidad penal de las personas jurídicas: un modelo legislativo,* Madrid, 2008, p. 89.

[46] GODINHO, I. F.: *A responsabilidade solidária das pessoas colectivas em direito penal económico*, Coimbra, 2007, p. 110-111.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

Además, tal transferencia de responsabilidades implica en una *responsabilidad por un hecho ajeno*, violando directamente el *principio de la culpabilidad*. En otras palabras, no hay un injusto empresarial per se, pero se toma prestado el de las personas físicas sin más cuestionamientos de cómo la persona jurídica habría colaborado efectivamente en el ilícito en cuestión[48] .

Por estas razones, se observa una progresiva tendencia (jurídica y doctrinal[49]) de migración a modelos de responsabilidad autónoma de las personas jurídicas, también conocidos como de *autorresponsabilidad*. Son varias las propuestas teóricas que se incluyen en este grupo, que tuvieron su arranque con los denominados modelos del *acto de conexión*. Aún muy próximas a los sistemas de *heteroresponsabilidad* (incluso en las críticas que se les pudieran dirigir[50]), estas propuestas exigían, para justificar el injusto empresarial, además de una acción consciente practicada por un representante válido de la empresa, que el hecho se hubiere dado en virtud de obligaciones funcionales de la persona jurídica o hubiere redundado en su enriquecimiento[51] . Así, como explica Tiedemann, además de los supuestos de responsabilidad directa de la empresa por los ilícitos cometidos por sus directores y demás personas con poder de dirección, las entidades colectivas tendrían un deber de vigilancia y control sobre sus demás miembros, por lo que deberían ser penalmente responsabilizadas por los ilícitos que se deriven del incumplimiento de estos deberes[52] .

Un ejemplo muy relevante de esta propuesta es la posibilidad prevista por el Art. 11.º, "2", "b", del CPPt, que admite la RPPJ por la conducta practicada por quienes, subordinados a personas con poder de dirección, actúan en nombre o por cuenta de la entidad colectiva, en su interés directo o indirecto, y comete el delito como consecuencia de la infracción de los deberes de vigilancia y control que incumbían a las personas con poder de dirección[53] .

Inmediatamente notamos la proximidad de esta propuesta teórica a los modelos de *heteroresponsabilidad*. Aunque tenga en cuenta una especie de *defecto de organización*, concretizado en la infracción de los deberes antes mencionada, el acto de conexión requerido es la violación de los deberes no de la empresa, sino de las personas individuales que ocupan

---

47 NETTO, A. V. S.: *Responsabilidade penal da pessoa jurídica,* 2. ed., São Paulo, 2020.

48 BUSATO, P. C.: "Responsabilidade penal das pessoas jurídicas no projeto (e no texto substitutivo) do novo código penal brasileiro", en LEITE, A. (org.), *Reforma penal: a crítica científica à parte geral do projeto de código penal (PLS 236/2012)*, São Paulo, 2015, p. 173. Ver también: JANUÁRIO, T. F. X.: "Dos limites do risco permitido para as pessoas jurídicas: uma análise do defeito de organização como um problema de imputação objetiva", en *Conpedi Law Review,* v. 4, n. 1, 2018, p. 6.

49 NETTO, A. V. S.: *Responsabilidade penal da pessoa jurídica,* 2. ed., São Paulo, 2020.

50 Para un análisis detallado de estas críticas, ver: NETTO, A. V. S.: *Responsabilidade penal da pessoa jurídica,* 2. ed., São Paulo, 2020.

51 BACIGALUPO, S.: *La responsabilidad penal de las personas jurídicas,* Barcelona, 1998, p. 379-399.

52 TIEDEMANN, K.: "La responsabilità da reato dell'ente in Europa: i modelli di riferimento per le legislazioni e le prospettive di armonizzazione", en *Rivista trimestrale di diritto penale dell'economia*, v. 25, n. 1-2, 2012, p. 4-5. Ver también: JANUÁRIO, T. F. X.: "Da (ir)relevância dos programas de compliance no modelo brasileiro de responsabilidade penal das pessoas jurídicas: considerações críticas ao projeto de novo Código Penal", en *Revista Direito e Liberdade*, v. 21, n. 2, 2019, p. 335.

53 "Artigo. 11.º [...] b) Por quem aja em seu nome ou por sua conta e no seu interesse direto ou indireto, sob a autoridade das pessoas referidas na alínea anterior, em virtude de uma violação dos deveres de vigilância ou controlo que lhes incumbem." PORTUGAL: *DL n.º 48/95, de 15 de março: Código Penal de 1982 versão consolidada posterior a 1995*.

un puesto de dirección y control en ella. Con ello, se produce una especie de fusión entre la responsabilidad directa de la persona colectiva y la *teoría del alter ego*, identificando el ente colectivo con las personas de su alta dirección[54] .

Ante estas y otras carencias, se desarrollaron algunas otras propuestas teóricas más audaces, no solo para delimitar mejor la idea de defecto organizacional, sino también para adecuarla a una teoría del delito de las personas jurídicas. Adán Nieto Martín, por ejemplo, trabaja con la idea de *déficit de organización permanente*, proponiendo que la culpabilidad de la persona jurídica sea imputada a partir de la comisión de un delito por cualquier persona que actúe en su nombre, cuando no exista la implementación de un código eficaz para la prevención y detección de este tipo de delitos. La adopción de este código, en cambio, eximiría de responsabilidad penal a la persona jurídica[55] .

Considerando que es necesaria la delimitación precisa entre la culpabilidad y el injusto empresarial - lo que conduciría a conceptos más fácilmente manejables y sistemáticamente correctos, favoreciendo la defensa de la persona jurídica ante los tribunales-, Gómez-Jara Díez también propone un modelo de autorresponsabilidad, que se basa en la organización y cultura de la persona jurídica de que se trate. El autor parte del supuesto de que algunas empresas alcanzan tal complejidad que pasan a presentar características propias de *autorreferencialidad, autoconducción* y *autodeterminación* [56] , transformándose en un sistema social (paralelo al ser humano, que es un sistema psíquico) garantizador de su propio ámbito organizativo[57] .

Partiendo de estas premisas y utilizando *equivalentes funcionales*, Gómez-Jara propone una *teoría del delito de las personas jurídicas*, elaborada sobre la base de un *injusto por defecto o falta de organización empresarial* y una *culpabilidad como reproche por no adoptar una cultura de cumplimiento normativo* [58] .

Sin extendernos demasiado en la interminable discusión acerca de los aspectos positivos y negativos de cada uno de los concretos modelos teóricos de responsabilidad penal de las personas jurídicas, creemos que el objeto del presente estudio, esto es, los delitos relacionados con la IA, presenta particularidades que enfatizan algunas de las ventajas dogmáticas y político-criminales de los sistemas de *autorresponsabilidad*.

Como ya hemos analizado, la complejidad de los sistemas de IA y de su cadena de producción impone severas dificultades a la identificación precisa del nexo causal entre una

---

[54] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 158; JANUÁRIO, T. F. X.: "Criminal liability for legal entities: a comparative study between Spain, Portugal and Brazil", en *POLAR – Portuguese Law Review*, v. 2, n. 2, 2018, p. 201.

[55] NIETO MARTÍN, A.: *La responsabilidad penal de las personas jurídicas: un modelo legislativo,* Madrid, 2008, p. 324-326.

[56] Para el autor, en las empresas complejas, las decisiones empresariales están conectadas con decisiones anteriores, llegando a ser independientes de sus integrantes concretos. Esto significa que, aunque haya cambios en las personas que las componen, se mantiene la identidad corporativa. Ver: GÓMEZ-JARA DÍEZ, C.: *Fundamentos modernos de la responsabilidad penal de las personas jurídicas: bases teóricas, regulación internacional y nueva legislación española*, Montevideo, 2010, p. 126-130.

[57] GÓMEZ-JARA DÍEZ, C.: "Fundamentos de la responsabilidad penal delas personas jurídicas", en BAJO FERNÁNDEZ, M., FEIJOO SÁNCHEZ, B., GÓMEZ-JARA DÍEZ, C., *Tratado de responsabilidad penal de las personas jurídicas: adaptada a la Ley 1/2015, de 30 de marzo por la que se modifica el Código Penal*, 2. Ed, Navarra, 2016, p. 102-104.

[58] Analizamos este modelo en detalle en: JANUÁRIO, T. F. X.: "Da teoria do delito para as pessoas jurídicas: análise a partir da teoria construtivista de "autorresponsabilidade" dos entes coletivos", en *Revista de Estudos Jurídicos UNESP*, ano 20, n. 32, 2016, p.161-191.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

acción u omisión y el daño en cuestión. Igualmente problemática será la individualización de una eventual autoría individual en estos casos, cuando existente. En consecuencia, no sólo la responsabilidad penal individual se puede obstaculizar en estas situaciones, sino también la de las personas jurídicas eventualmente involucradas, cuando el ordenamiento jurídico en cuestión hace depender la responsabilidad penal de estas personas de la identificación de una conducta individual. En otras palabras, los ya enfrentados *modelos de heterorresponsabilidad* resultan aún menos fructíferos cuando se trata de daños causados con la intervención de la IA[59] .

Además, hay que destacar la importancia que otorga la generalidad de los modelos de *autorresponsabilidad*, a la adecuada organización empresarial y a la cultura de cumplimiento normativo. Al analizar los posibles ilícitos cometidos con el uso de la IA, observamos que muchas veces nos podemos encontrar ante conductas realizadas en el seno de grandes entidades colectivas, y algunos casos pueden no ser aislados, sino derivados de las propias políticas internas de la organización empresarial. A esto se suma el hecho de que estamos ante un campo muy dependiente de los avances científicos y tecnológicos, marcado por el dinamismo y la incertidumbre en cuanto a sus avances y resultados[60] .

Por ello, sostenemos que el derecho penal debe asumir aquí un carácter secundario, reforzando ciertas normas primarias aprobadas sectorialmente, tales como códigos de ética y conducta, normas deontológicas profesionales, *leges artis* y estándares del sector y otras normas y reglas primarias de reducción del riesgo, que deben integrar el juicio de tipicidad del comportamiento del agente, ya sea persona natural o jurídica[61] .

Precisamente por la necesidad de definir e implementar estas normas primarias y sectoriales de reducción de riesgos, sumada al imperativo escrutinio y transparencia[62] en la producción, desarrollo y supervisión post-comercialización de esta tecnología[63] , que son muy relevantes en este ámbito los programas de cumplimiento[64] .

---

[59] Esta vinculación de la responsabilidad penal de la persona jurídica con la conducta de una persona física puede exigirse de forma más sencilla que una mención expresa a la "doble imputación". En el ordenamiento jurídico portugués, por ejemplo, si bien se declara expresamente la independencia entre la responsabilidad individual y la colectiva (Artículo 11.º, 7, CP), entendemos que será imperativo precisar la conducta humana y su autor, a fin de identificar los requisitos indispensables para la responsabilidad de la persona jurídica, tales como la actuación en nombre o por cuenta de la empresa, en su interés directo o indirecto y la propia posición de dirección que ocupa el agente (inciso a) y, adicionalmente, la violación de los deberes de vigilancia o control de quienes tenían autoridad sobre el agente (inciso b). Sin embargo, esta conducta humana, cuando existente, no siempre será identificable en el campo de la I.A. Ver con detalles: JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal*, volume II, Coimbra, 2022, p. 161.

[60] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 150.

[61] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 150. Sobre el carácter secundario del derecho penal y la integración de normas concretas de conducta: FRISCH, W.: *Comportamiento típico e imputación del resultado*, Madrid, 2004, p. 128-129. Para más información sobre cómo estas normas primarias se integran en el injusto empresarial: JANUÁRIO, T. F. X.: "Dos limites do risco permitido para as pessoas jurídicas: uma análise do defeito de organização como um problema de imputação objetiva", en *Conpedi Law Review,* v. 4, n. 1, 2018, p. 15 y ss.

[62] Defendiendo una especie de solución colaborativa a través de normas consuetudinarias que establezcan unos requisitos mínimos de transparencia y de realización de testes, evitando así los constantes cambios legales que exigiría el desarrollo tecnológico: KAPLAN, A., HAENLEIN, M.: "Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence", en *Business Horizons,* v. 62, n. 1, 2019, p. 22.

Pueden definirse como instrumentos vinculados a la gobernanza corporativa, a través de los cuales las personas jurídicas buscan, desde el espacio de libertad otorgado por el Estado, autorregularse y autoinspeccionarse. Podemos decir que, entre sus fines inmediatos, se encuentran la promoción de una cultura de ética y cumplimiento normativo dentro de la organización empresarial, así como la prevención, investigación y eventual represión de prácticas ilícitas en la empresa. De forma mediata, buscan mantener la buena reputación de la

[63] PRICE II, W. N.: "Artificial Intelligence in Health Care: Applications and Legal Issues", en *U of Michigan Public Law Research Paper,* n. 599, 2017, p. 4.

[64] La Propuesta de Reglamento del Parlamento Europeo y del Consejo prevé, por ejemplo, la obligación de los proveedores de sistemas de IA de alto riesgo, de contar con sistemas de gestión de calidad. En ese sentido: "Artículo 17 Sistema de gestión de la calidad 1. Los proveedores de sistemas de IA de alto riesgo establecerán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema se documentará de manera sistemática y ordenada mediante políticas, procedimientos e instrucciones escritas e incluirá, al menos, los siguientes aspectos: a) una estrategia para el cumplimiento reglamentario, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y de los procedimientos de gestión de las modificaciones de los sistemas de IA de alto riesgo; b) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el diseño y el control y la verificación del diseño del sistema de IA de alto riesgo; c) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el desarrollo y el control y el aseguramiento de la calidad del sistema de IA de alto riesgo; d) los procedimientos de examen, prueba y validación que se llevarán a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, así como la frecuencia con que tendrán lugar; e) las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla los requisitos establecidos en el capítulo 2 del presente título; f) los sistemas y procedimientos de gestión de datos, lo que incluye su recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con ese fin; g) el sistema de gestión de riesgos que se menciona en el artículo 9; h) el establecimiento, la implantación y el mantenimiento de un sistema de seguimiento posterior a la comercialización con arreglo al artículo 61; i) los procedimientos asociados a la notificación de incidentes graves y defectos de funcionamiento con arreglo al artículo 62; j) la gestión de la comunicación con las autoridades nacionales competentes; las autoridades competentes, incluidas las sectoriales, que permiten acceder a datos o facilitan el acceso a ellos; los organismos notificados; otros operadores; los clientes, u otras partes interesadas; k) los sistemas y procedimientos destinados a llevar un registro de toda la documentación e información pertinente; l) la gestión de los recursos, incluida la seguridad de las medidas relacionadas con el suministro; m) un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado. 2. La inclusión de los aspectos mencionados en el apartado 1 será proporcional al tamaño de la organización del proveedor. 3. En el caso de los proveedores que sean entidades de crédito reguladas por la Directiva 2013/36/UE, se considerará que cumplen la obligación de establecer un sistema de gestión de la calidad cuando cumplan las normas relativas a los sistemas, procedimientos y mecanismos de gobernanza interna que figuran en el artículo 74 de dicha Directiva. En ese contexto, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40 del presente Reglamento". Además, el Artículo 19 establece que: "Artículo 19 Evaluación de la conformidad 1. Los proveedores de sistemas de IA de alto riesgo se asegurarán de que sus sistemas sean sometidos al procedimiento de evaluación de la conformidad oportuno, de conformidad con el artículo 43, antes de su introducción en el mercado o puesta en servicio. Cuando dicha evaluación de la conformidad demuestre que los sistemas de IA cumplen los requisitos establecidos en el capítulo 2 del presente título, sus proveedores elaborarán una declaración UE de conformidad con arreglo al artículo 48 y colocarán el marcado CE de conformidad con arreglo al artículo 49. 2. En el caso de los sistemas de IA de alto riesgo mencionados en el punto 5, letra b), del anexo III, introducidos en el mercado o puestos en servicio por proveedores que sean entidades de crédito reguladas por la Directiva 2013/36/UE, la evaluación de la conformidad se llevará a cabo como parte del procedimiento a que se refieren los artículos 97 a 101 de la mencionada Directiva". COMISIÓN EUROPEA: *Propuesta de Reglamento del Parlamento Europeo y del Consejo: por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión: {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}*.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

empresa, incrementar sus lucros y, sobre todo, proteger a la persona jurídica y a sus órganos de representación de posibles responsabilidades[65] .

Al analizar los posibles incentivos estatales para la autorregulación empresarial y, en consecuencia, la implementación de programas de cumplimiento, Marc Engelhart identifica 6 posibles niveles, clasificados de la siguiente manera: (1) *autorregulación pura*, sin mayores incentivos, siendo la adopción o no de estos programas una opción ética o empresarial por parte de la empresa; (2) el *apoyo estatal informal*, en el que el Estado se limita a promover cursos y capacitaciones sobre el tema y alentar a las asociaciones sectoriales a disciplinar las pautas necesarias para tal fin; (3) la *recompensa por el compliance*, observada cuando un determinado ordenamiento jurídico prevé mecanismos de recompensa (mitigación de penas o acuerdos procesales, por ejemplo) a las personas jurídicas que tengan un programa de cumplimiento efectivo; (4) las *sanciones por fallas o inexistencia de un programas de cumplimiento*; (5) la *exclusión de responsabilidad como consecuencia del compliance efectivo*, observada cuando se prevé la responsabilidad penal de las personas jurídicas y, por otro lado, que esta puede ser excluida cuando se ha implementado un programa de cumplimiento que cumple con ciertos requisitos; (6) una *obligación general* de todas las personas jurídicas que alcancen cierto nivel de complejidad, de adoptar programas de cumplimiento[66] .

En opinión del autor, dado que los incentivos de nivel 06 son prácticamente inexistentes (a excepción de las obligaciones sectoriales en ámbitos significativamente arriscados, como el de blanqueo de capitales[67]), los incentivos de nivel 05 serían la forma más eficiente de promover los programas de cumplimiento[68] . Dicho esto, y dada la importancia de los programas de cumplimiento en el campo de la producción y desarrollo de sistemas de IA, creemos que es imperativo no solo admitir legalmente la RPPJ por los delitos relacionados con esta área[69] , sino también la adopción de modelos de imputación que tengan en cuenta la correcta organización empresarial y la conducción de los negocios de acuerdo con una cultura de cumplimiento normativo[70] .

Aunque no existe unanimidad en la interpretación teórica que se ha de hacer del Artículo 31 bis del Código Penal, creemos que el ordenamiento jurídico español es un ejemplo paradigmático a mencionar respecto a la consideración de los programas de cumplimiento en el ámbito de la RPPJ[71] .

---

65 JANUÁRIO, T. F. X.: *Criminal compliance e corrupção desportiva: um estudo com base nos ordenamentos jurídicos do Brasil e de Portugal,* Rio de Janeiro, 2019, p. 85-86.

66 ENGELHART, M.: *The Nature and Basic Problems of Compliance Regimes*, Freiburg, 2018, p. 22-30. Ver también: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Dos níveis de exigibilidade dos procedimentos de investigação interna", en *Anais do IV Congresso de Pesquisas em Ciências Criminais, de 21 a 23 de outubro de 2020*, São Paulo, 2020, p. 221-223.

67 Sobre las obligaciones de *compliance* el contexto del blanqueo de capitales, ver: RODRIGUES, A. M.: *Direito penal económico: uma política criminal na era compliance,* 2.ed., Coimbra, 2020, p. 190 y ss.; CANESTRARO, A. C., JANUÁRIO, T. F. X., "Programas de compliance e branqueamento de capitais: implicações da lei nº 83/2017, de 31 de agosto, no regime jurídico de Portugal" en *Revista Científica do CPJM*, v. 1, n. 3, 2022.

68 ENGELHART, M.: *The Nature and Basic Problems of Compliance Regimes*, Freiburg, 2018, p. 22-30.

69 Mencionamos, de manera no exhaustiva, algunos de estos posibles delitos en el tópico 1, especialmente en las notas 30 y ss.

70 En sentido próximo: NIETO MARTÍN, A.: "Problemas fundamentales del cumplimiento normativo en el derecho penal", en KUHLEN, L., MONTIEL, J. P., DE URBINA GIMENO, I. O. (eds.), *Compliance y teoría del derecho penal,* Madrid, 2013, p. 21.

Luego de establecer las hipótesis y condiciones para la RPPJ[72] , el artículo establece que la PJ podrá quedar exenta de responsabilidad cuando adopte modelos de organización o gestión preventivos (*programas de cumplimiento*) que atiendan a ciertos requisitos y condiciones.

Para los casos en que la infracción haya sido cometida por representantes, administradores o directivos, el programa de cumplimiento deberá reunir las siguientes condiciones: i) *idoneidad temporal* ("con eficacia, antes de la comisión del delito"); ii) *idoneidad formal* ("delitos de la misma naturaleza"); iii) *idoneidad material* ("las medidas de vigilancia y control idóneas"); iii) *órgano con poderes autónomos de supervisión del funcionamiento y cumplimiento del programa*; iv) *que el delito se haya cometido eludiendo fraudulentamente los modelos de prevención;* v) *no omisión o insuficiencia del ejercicio de las funciones de supervisión, control y vigilancia* [73] .

A su vez, en los casos en que la infracción haya sido cometida por empleados subordinados, el programa de cumplimiento deberá cumplir las condiciones de idoneidad formal, material y temporal, para que la persona jurídica quede exenta de responsabilidad[74] .

El Artículo 31, bis, 5, establece los requisitos que deben cumplir estos modelos de organización y gestión para eximir de responsabilidad penal a la persona jurídica de la que se trate en cualquiera de los dos casos señalados. Son ellos: i) *mapa de riesgos* ("1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos"); ii) *documentación*; ("2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos"); iii) *recursos financieros* ("3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos"); iv) *deber de informar riesgos e incumplimientos* ("4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención"); v) *sistema disciplinario* ("5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo") vi) *verificación periódica* ("6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios")[75] .

---

[71] JANUÁRIO, T. F. X.: "O ônus da prova da existência e eficácia dos programas de compliance no âmbito do processo penal das pessoas jurídicas: um estudo com base no ordenamento jurídico espanhol", en *Revista Brasileira de Ciências Criminais,* ano 27, n. 160, 2019, p. 233.

[72] "Artículo 31 bis. 1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables: a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma. b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso." ESPAÑA: *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*.

[73] GONZÁLEZ CUSSAC, J. L.: *Responsabilidad penal de las personas jurídicas y programas de cumplimiento,* Valencia, 2020, p. 166-195.

[74] GONZÁLEZ CUSSAC, J. L.: *Responsabilidad penal de las personas jurídicas y programas de cumplimiento,* Valencia, 2020, p. 195.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

A pesar de las divergencias doctrinarias en torno al modelo español de RPPJ, es innegable que contempla la hipótesis de exención de responsabilidad y atenuación de la sanción[76] eventualmente impuesta a la entidad colectiva, por la adopción de programas de cumplimiento que cumplan con determinados requisitos y condiciones. Esta es una opción con potenciales impactos positivos en el campo de la IA.

Entre sus diversos mecanismos[77] , impuestos legalmente, por reglamentos, estándares del sector o adoptados espontáneamente por las personas jurídicas, se encuentran los procedimientos de gestión de riesgos, que son fundamentales para el área de bajo análisis. Al margen de las dificultades inherentes a la valoración de situaciones futuras en estos sectores complejos y nebulosos[78] , y considerando que en todos los ámbitos en los que hay acción humana pueden darse situaciones de riesgo que escapan al control, la identificación previa de estos casos permite una actuación dentro de los límites de lo legalmente tolerado y de lo socialmente necesario[79] , posibilitando, a partir de ahí, identificar estándares de actuación, definidos alternativa o acumulativamente por las propias personas jurídicas, en forma conjunta o individual, a través de *leges artis* sectoriales, normas administrativas o directivas abstractas que permitan la consideración de una "empresa media cuidadosa"[80] .

En el caso de la IA, la gestión de riesgos tiende a colaborar en el seguimiento de las investigaciones y descubrimientos científicos más recientes en la materia, así como de los consecuentes cambios legislativos y normativos relacionados con el caso, lo que permitirá una definición más concreta y adecuada de los parámetros de acción y, en consecuencia, los límites de permisibilidad del riesgo[81] .

---

75 ESPAÑA: *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal* ; GONZÁLEZ CUSSAC, J. L.: *Responsabilidad penal de las personas jurídicas y programas de cumplimiento,* Valencia, 2020, p. 221-237.

76 "Artículo 31 quater. 1. Sólo podrán considerarse circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades: […] ad) Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica." ESPAÑA: *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*.

77 Un análisis exhaustivo de los mismos desbordaría los límites del presente trabajo. Para más detalles, consultar: ENGELHART.: *Sanktionierung von Unternehmen und Compliance: eine Rechtsvergleichende Analyse des Straf- und Ordnungwidrigkeitenrechts in Deutschland und den USA,* 2. Ergänzte und erweiterte Auflage, Berlin, 2012; SIEBER, U.: "Compliance-Programme im Unternehmensstrafrecht: ein neues Konzept von Wirtschaftskriminalität", en SIEBER, U. et al (Hrsg.), *Strafrecht und Wirtschaftsstrafrecht – Dogmatik, Rechtsvergleich, Rechtstatsachen: Festschrift für Klaus Tiedemann zum 70. Geburtstag,* Köln, 2008, p. 458; NIETO MARTÍN, A. (dir.), *Manual de cumplimiento penal en la empresa,* Valencia, 2015; LEHMANN, E. E.: "Unternehmensorganisation und criminal Compliance", en ROTSCH, T. (Hrsg.), *Criminal Compliance: Handbuch,* Baden-Baden, 2015, p. 101-141; BOCK, D.: *Criminal compliance,* Baden-Baden, 2011, p. 585 y ss.

78 ROTSCH, T.: "Criminal compliance", en *InDret: revista para el análisis del derecho*, n. 1, 2012, p. 6.

79 BOCK, D.: *Criminal compliance,* Baden-Baden, 2011, p. 43.

80 LASCURAÍN, J, A,: "Compliance, debido control y unos refrescos", en ARROYO ZAPATERO, L., NIETO MARTÍN, A. (dir.), *El derecho penal económico en la era compliance,* Valencia, 2013, p. 125-126; JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 152.

81 JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 152. La importancia de la gestión de riesgos para el ámbito de la inteligencia artificial se observa en la Propuesta de Reglamento, que prevé: "Artículo 9 Sistema de gestión de riesgos 1. Se establecerá, implantará, documentará y mantendrá un sistema de gestión de riesgos asociado a los sistemas de IA de alto riesgo. 2. El sistema de gestión de riesgos consistirá en un proceso iterativo continuo que se llevará a

Estas normas de comportamiento deben estar incluidas en los códigos de ética y conducta, que son verdaderamente la "norma fundamental" de la persona jurídica y vinculan a sus empleados y órganos de representación[82] . Deben exponer expresamente los valores, políticas, ética y procedimientos de la empresa, con posibilidad de ser aprobados por organismos internacionales, grupos de interés y asociaciones sectoriales[83] .

---

cabo durante todo el ciclo de vida de un sistema de IA de alto riesgo, el cual requerirá actualizaciones sistemáticas periódicas. Constará de las siguientes etapas: a) la identificación y el análisis de los riesgos conocidos y previsibles vinculados a cada sistema de IA de alto riesgo; b) la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo en cuestión se utilice conforme a su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible; c) la evaluación de otros riesgos que podrían surgir a partir del análisis de los datos recogidos con el sistema de seguimiento posterior a la comercialización al que se refiere el artículo 61; d) la adopción de medidas oportunas de gestión de riesgos con arreglo a lo dispuesto en los apartados siguientes. 3. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), darán la debida consideración a los efectos y las posibles interacciones derivados de la aplicación combinada de los requisitos estipulados en el presente capítulo 2. Asimismo, tendrán en cuenta el estado actual de la técnica generalmente reconocido, que, entre otras fuentes, está reflejado en las normas armonizadas o las especificaciones comunes pertinentes. 4. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), considerarán aceptables los riesgos residuales asociados a cada peligro, así como el riesgo residual general de los sistemas de IA de alto riesgo, siempre que el sistema de IA de alto riesgo de que se trate se utilice conforme a su finalidad prevista o que se le dé un uso indebido razonablemente previsible. Se informará al usuario de dichos riesgos residuales. A la hora de determinar cuáles son las medidas de gestión de riesgos más adecuadas, se procurará: a) eliminar o reducir los riesgos en la medida en que sea posible mediante un diseño y un desarrollo adecuados; b) implantar, cuando proceda, unas medidas de mitigación y control apropiadas en relación con los riesgos que no puedan eliminarse; c) proporcionar la información oportuna conforme al artículo 13, en particular en relación con los riesgos mencionados en el apartado 2, letra b), del presente artículo y, cuando proceda, impartir formación a los usuarios. Cuando se eliminen o reduzcan los riesgos asociados a la utilización del sistema de IA de alto riesgo, se tendrán en la debida consideración los conocimientos técnicos, la experiencia, la educación y la formación que se espera que posea el usuario, así como el entorno en el que está previsto que se utilice el sistema. 5. Los sistemas de IA de alto riesgo serán sometidos a pruebas destinadas a determinar cuáles son las medidas de gestión de riesgos más adecuadas. Dichas pruebas comprobarán que los sistemas de IA de alto riesgo funcionan de un modo adecuado para su finalidad prevista y cumplen los requisitos establecidos en el presente capítulo. 6. Los procedimientos de prueba serán adecuados para alcanzar la finalidad prevista del sistema de IA y no excederán de lo necesario para ello. 7. Las pruebas de los sistemas de IA de alto riesgo se realizarán, según proceda, en cualquier momento del proceso de desarrollo y, en todo caso, antes de su introducción en el mercado o puesta en servicio. Los ensayos se realizarán a partir de parámetros y umbrales de probabilidades previamente definidos que sean adecuados para la finalidad prevista del sistema de IA de alto riesgo de que se trate. 8. Cuando se implante el sistema de gestión de riesgos descrito en los apartados 1 a 7, se prestará especial atención a la probabilidad de que menores accedan al sistema de IA de alto riesgo de que se trate o se vean afectados por él. 9. En el caso de las entidades de crédito reguladas por la Directiva 2013/36/UE, los aspectos descritos en los apartados 1 a 8 formarán parte de los procedimientos de gestión de riesgos que estas establezcan conforme al artículo 74 de dicha Directiva". COMISIÓN EUROPEA: *Propuesta de Reglamento del Parlamento Europeo y del Consejo: por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión: {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}*. Ver también: SUÁREZ XAVIER, P. R.: *Reconocimiento facial y policía predictiva: entre seguridad y garantías procesales,* A Coruña, 2022, p. 99 y ss.

[82] LASCURAÍN, J. A.: "Compliance, debido control y unos refrescos", en ARROYO ZAPATERO, L., NIETO MARTÍN, A. (dir.), *El derecho penal económico en la era compliance,* Valencia, 2013, p. 129.

[83] NAVAS MONDACA, I.: "Los códigos de conducta y el derecho penal económico" en: SILVA SÁNCHEZ, J. M (dir.), MONTANER FERNÁNDEZ, R. (coord.), *Criminalidad de empresa y compliance: prevención y reacciones corporativas,* Barcelona, 2013, p. 113-119. Un buen ejemplo es la Resolución 2015/2103(INL), que propone en anexo un código de conducta para ingenieros en robótica y comités de ética en investigación. Ver: PARLAMENTO EUROPEO: *Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL))*.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

Entendemos que las disposiciones de los códigos de ética y conducta deben ser interpretadas como normas pre-jurídicas[84] de cuidado, debiendo ser incluidas en la referida categoría de las "normas primarias de reducción de riesgos" y consideradas en la imputación de la tipicidad de la conducta[85] . Se observa que, mucho más que el Estado, las personas jurídicas y las entidades sectoriales están en mejores condiciones de identificar y gestionar los riesgos derivados de las nuevas tecnologías y determinar los procedimientos y normas de conducta aceptables en el caso[86] .

En definitiva, por tanto, se observa que, además de auxiliaren al Estado en la prevención, investigación y represión de posibles ilícitos y en la identificación y gestión de riesgos en el ámbito en que se insertan, los programas de cumplimiento y sus normas internas son importantes para delimitar el riesgo permitido en el juicio de tipicidad de la conducta. Esta posibilidad, aunque sigue perjudicada, de *lege data*, en países como Portugal, que insisten en hacer depender la responsabilidad de la persona jurídica de la identificación de la conducta de una persona física y en atribuir poca relevancia a los programas de cumplimiento[87] , está muy avanzada en España, cuyo ordenamiento jurídico ya contempla expresamente estos programas en la atribución de responsabilidades de la persona jurídica[88] .

En nuestra opinión, los modelos como tales tienen mayor potencial para enfrentar los casos aquí analizados, ya que, en la valoración del *defecto organizacional de la persona jurídica* - que no necesariamente corresponderá a un defecto en el algoritmo o sistema de IA – incluirá evaluaciones de las políticas y procedimientos de la persona jurídica con respecto al sistema de IA en cuestión, especialmente en cuanto al entrenamiento de los algoritmos, pruebas, supervisión, transparencia para los clientes y la sociedad, y mejoras continuas de la tecnología. De esta forma, se podrá verificar si la persona jurídica de que se trate se organizó de manera defectuosa, creando un riesgo por encima del permitido, que terminó concretizándose en un resultado de daño o de peligro[89] .

---

[84] Wolfgang Frisch propone una clasificación según la cual, además de la limitación de riesgos a través del derecho penal, existen conductas que están reguladas por normas (I) *"pre-jurídicas"* - programas de reducción de riesgos, *leges artis*, directivas éticos - ; (II) "*prejuridico-penal*" – Códigos de Tránsito Vehicular y Códigos de Ética Médica, por ejemplo; y (III) las cuales que no encuentran regulación en las normas de cuidado. Ver: FRISCH, W.: *Comportamiento típico e imputación del resultado,* Madrid, 2004, p. 106-156.

[85] Según Wolfgang Frisch, cuando el agente actúa conforme a la norma del cuidado y ésta puede considerarse, desde una perspectiva ex ante, suficiente y adecuada para reducir los riesgos concretamente afectados, la conducta no puede considerarse típica. FRISCH, W.:*Comportamiento típico e imputación del resultado*, Madrid, 2004, p. 126.

[86] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 154.

[87] En cuanto a la responsabilidad penal de las personas jurídicas, la relevancia de los programas de cumplimiento se limita a: i) en materia de imputación de la tipicidad, el Art. 11.º, "6", CPPt, establece que la responsabilidad quedará excluida cuando *"o agente tiver actuado contra ordens ou instruções expressas de quem de direito*"; ii) en las consecuencias jurídicas del delito, el Art. 90.º-A, "4", prevé la atenuación de la pena por la adopción e implementación, antes de la comisión del delito, de programas de cumplimiento adecuados para prevenir la comisión del delito o de delitos de la misma naturaleza; iii) el Art. 90.º-A, "5" prevé una posibilidad de sanción accesoria por no no-adopción del programa de cumplimiento; y iv) el Art. 90.º-A, "6" prevé una posibilidad de sustitución de la pena multa por una pena alternativa en razón de la adopción e implementación de programas de cumplimiento. PORTUGAL: *DL n.º 48/95, de 15 de março: Código Penal de 1982 versão consolidada posterior a 1995*.

[88] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 154 y ss.

4. LAS EMPRESAS COMO USUARIAS DE LA INTELIGENCIA ARTIFICIAL: ASPECTOS PROCESALES PENALES

Como ya hemos mencionado, no es solo cuando se insertan en el ámbito de la cadena productiva que las empresas asumen relevancia en el contexto de la IA. Son también, en un número cada vez más significativo, consumidoras de esta tecnología en sus procedimientos internos. En este tópico, analizaremos uno de los usos que, a nuestro juicio, tienen las consecuencias más significativas en el contexto del proceso penal, a saber, el uso de la IA en actividades de *compliance, due diligence* e investigaciones internas[90] .

Según Christoph Burchard, se acabó la época en la que solo los agentes estatales utilizaban sistemas predictivos para detectar y prevenir delitos de forma anticipada. De hecho, para el autor, el *digital criminal compliance* (DCC) puede ser considerado la "expresión del momento" cuando se trata del uso de medios digitales para la prevención en tiempo real de violaciones de conformidad[91] . Buscando la digitalización del *compliance* penal, el DCC se basa en el análisis inteligente de un gran conjunto de datos (*big data*), especialmente a través de la IA, con el fin de asegurar el cumplimiento de las leyes y evitar la comisión de ilícitos en el ámbito de las corporaciones[92] .

La principal razón para optar por digitalizar la estructura de cumplimiento radica en su eficiencia. Como explican Anabela Rodrigues y Susana Aires de Sousa, los sistemas informáticos más avanzados son capaces de predecir con mayor eficacia y eficiencia los actos y procesos productivos, así como prevenir y detectar situaciones que puedan ser perjudiciales para la empresa. Por lo tanto, se espera una mayor seguridad en el contexto empresarial[93] .

Burchard explica que, bajo el paradigma del cumplimiento tradicional (humano), existe un dilema innegable: a pesar de la necesidad de contener el crimen en el contexto empresarial, cuantas más medidas de cumplimiento, más paralizada tiende a estar la empresa. Además, debido a limitaciones y errores humanos, la estructura de *compliance* a menudo se ve obligada a operar de forma retrospectiva (*ex post*), a pesar de que los datos sobre posibles incumplimientos ya estaban disponibles *ex ante*. Por sus capacidades, el DCC se presenta con la promesa (no necesariamente cumplida) de ser una forma de cumplimiento más completa, objetiva, neutral y eficaz. Además, propone un giro en organización de *compliance*, ya que su capacidad de análisis de *big data* en tiempo real permitiría predecir gran parte de las infracciones, evitando que se cometan. E incluso si una parte de ellas no se detecta a priori, la capacidad de almacenamiento de datos de la IA beneficiaría la investigación *ex post* [94] .

---

[89] JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* volume II, Coimbra, 2022, p. 161.

[90] Ver con detalles: JANUÁRIO, T. F. X. "Corporate Internal Investigations 4.0: on the criminal procedural aspects of applying artificial intelligence in the reactive corporate compliance", en *Revista Brasileira de Direito Processual Penal*, v. 9, n. 2, 2023, p. 723 y ss.

[91] BURCHARD, C.: "Das »Strafrecht« der Prädiktionsgesellschaft: …oder wie »smarte« Algorithmen die Strafrechtspflege verändern (könnten)", en *Forschung Frankfurt: das Wissenschaftsmagazin: Recht und Gesetz*, n. 1, 2020, p. 28. Ver también: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 369.

[92] BURCHARD, C.: "Digital Criminal Compliance", en ENGELHART, M., KUDLICH, H., VOGEL, B. (Hrsg.), *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70. Geburtstag: Teilband II,* Berlin, 2021, p. 742.

[93] RODRIGUES, A. M., SOUSA, S. A.: "Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal,* vol. II, Coimbra, 2022, p. 13.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

Se observa, por tanto, que la concordancia práctica entre prevención penal y dinamismo empresarial tiende a verse muy favorecida.

Es importante mencionar que, aunque parezca futurista, muchas de las funcionalidades de la IA en el *compliance* ya están operativas. Desde funciones un poco más simples, como la digitalización de los propios instrumentos del programa[95] y el mapeo legal y regulatorio, hasta tareas mucho más complejas, como la gestión de riesgos[96] , la realización de procedimientos de *due diligence* [97] y el monitoreo autónomo en tiempo real. Esta última aplicación, a nuestro juicio, no sólo es la más paradigmática, sino también la que presenta mayores controversias.

Por un lado, es innegable que la supervisión de los trabajadores es inherente al ambiente de trabajo, estando incluida en las facultades del empleador, especialmente en la *función de fiscalización* incluida en su *potestad directiva* [98] . Sin embargo, las innovaciones tecnológicas, especialmente en términos de IA, han dado un nuevo aspecto a estas actividades. A través de la llamada *vigilancia predictiva de los empleados*, por ejemplo, se lleva a cabo un análisis de un conjunto de datos para determinar con alto grado de precisión, qué empleados tienen más probabilidades de practicar actos de incumplimiento normativo e ilícitos criminales[99] . Para ello, son analizados datos como los provenientes de archivos de audio y video de grabaciones ambientales y telefónicas, monitoreo de correos electrónicos y navegadores de internet,

---

[94] BURCHARD, C.: "Digital Criminal Compliance", en ENGELHART, M., KUDLICH, H., VOGEL, B. (Hrsg.), *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70. Geburtstag: Teilband II,* Berlin, 2021, p. 744-747.

[95] Pensemos, por ejemplo, en la digitalización de los canales de denuncia y orientación y de las estructuras de formación y evaluación de empleados. Sobre las ventajas y limitaciones de la IA en este ámbito, véase: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 370-371.

[96] La citada capacidad de tratamiento de una inmensidad de datos ayuda no solo a identificar los aspectos legales y reglamentarios aplicables al caso, sino también los principales riesgos a los que puede estar sujeta la persona jurídica de que se trate. A esto se suma la capacidad algorítmica de actualizarse de acuerdo a sus experiencias previas y con los últimos conocimientos científicos, actualizaciones legales y entendimientos jurisprudenciales, lo que sin duda aumentará la eficiencia del programa. CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 372. Sobre los procedimientos de gestión de riesgos, ver: PAMPEL, J., GLAGE, D.: "Unternehmensrisiken und Risikomanagement", en HAUSCHKA, C. E. (Hrsg.), *Corporate Compliance: Handbuch der Haftungsvermeidung im Unternehmen.,* München, 2007, p. 82 y ss.

[97] Dado que el objetivo principal de estos procedimientos es la recopilación de información sobre *third-parties*, empresas objetivo de fusiones y adquisiciones o cualquier otro agente con el que la empresa pretenda celebrar un acuerdo comercial, los datos procesados por los sistemas autónomos y de IA hace posible un análisis de la factibilidad y riesgos de estas operaciones. Cuanto mayor sea la capacidad de recopilar, procesar y categorizar datos, más informativo tenderá a ser el informe de *due diligence*. Ver con ejemplos: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 372. Sobre las dificultades relacionadas con los procedimientos de *due diligence* transnacional, ver: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Beyond Ecocide: Extraterritorial Obligations of Due Diligence as an Alternative to Address Transnational Environmental Damages?", en *RIDP*, v. 93, n. 1, 2022, p. 231 y ss.

[98] DELGADO, M. G.: *Curso de direito do trabalho*, 11. ed., São Paulo, 2012, p. 662; BARROS, A. M. *Curso de direito do trabalho*, 7. ed., São Paulo, 2011, p. 462; CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 373.

[99] BURCHARD, C.: "Digital Criminal Compliance", en ENGELHART, M., KUDLICH, H., VOGEL, B. (Hrsg.), *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70. Geburtstag: Teilband II,* Berlin, 2021, p. 747.

información sobre teclas efectivamente tecleadas en el ordenador, contenidos publicados en redes sociales e incluso expresiones faciales, calor corporal, gestos físicos y tonos de voz a los que se puede acceder a través de dispositivos incorporados en las mesas y sillas de los trabajadores[100] -[101] .

Teniendo en cuenta los riesgos y limitaciones de la IA ya analizados aquí - entre otros, la *opacidad*, la *imprevisibilidad* y el potencial *sesgo de los datos* -, el DCC tiende a convertirse en un problema con relevancia procesal penal desde el momento en que, en el ámbito de los procedimientos en los que esta tecnología es utilizada, es posible descubrir hechos penalmente relevantes que pueden llegar al conocimiento de las entidades estatales de persecución penal. Por ejemplo, si se realiza una investigación interna y la persona jurídica en cuestión decide denunciar los hechos ante la autoridad competente, los documentos (videos, audios, informes, transcripciones y otros) producidos en este ámbito privado y con la ayuda de IA pueden ser admitidos en el proceso penal? ¿Serán plenamente valorados como prueba a todos los efectos?

Es importante mencionar, inicialmente, la existencia de una *expectativa de privacidad* por parte de los empleados con respecto a sus herramientas de trabajo, como teléfonos móviles, correos electrónicos y ordenadores corporativos[102] . Esto se debe a que, aunque están destinadas al trabajo, estas herramientas también se utilizan para algunos fines personales, fuera del entorno laboral o no directamente relacionados con él. Sin embargo, dado que esta expectativa de privacidad no es absoluta, puede ser eliminada cuando se le da conocimiento previo y explícito al empleado[103] , que podrá haber inspección en sus instrumentos de trabajo y cuáles serán exactamente la informaciones que se podrán recolectar[104] .

---

[100] DEARDEN, L.: "The Telegraph Backtracks on Sensors Monitoring Whether Journalists are Sitting at Desks Amid Outrage", en *The Independent,* 2016, https://www.independent.co.uk/news/media/the-telegraph-backtrackson-sensors-monitoring-whether-journalists-are-sitting-at-desks-amidoutragea6807336.html accedido en 24 de Junio de 2021; MOORE, P. V.: *The Threat of Physical and Psychosocial Violence and Harassment in Digitalized Work*, Geneva, 2018, p. 26. Con ejemplos de sistemas ya operativos, ver: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 373.

[101] También citando que estas tecnologías ya están en pleno uso bajo la terminología de *eletronic performance monitoring,* Burchard cita como ejemplos, entre otros, el uso de datos GPS y la (en teoría, voluntaria) implantación de chips en los empleados - chipping. Ver: BURCHARD, C.: "Digital Criminal Compliance", en ENGELHART, M., KUDLICH, H., VOGEL, B. (Hrsg.), *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70. Geburtstag: Teilband II,* Berlin, 2021, p. 747.

[102] TEDH: *Case of Copland v. United Kingdom, 03/04/2007*.

[103] De hecho, al analizar el posible uso de sistemas de IA con fines procesales, Martín Diz defiende la necesidad de un "consentimiento informado del afectado cuando se emplean herramientas de inteligencia artificial en funciones automatizadas y decisorias que pueden dar lugar a efectos jurídicos o afectarle de manera significativa en el plano personal". Así: "Es, por tanto, condicionante absoluto para la utilización de inteligencia artificial en fines procesales (en sede judicial o en vía extrajudicial), el requerimiento de información previa con relación a su utilización, características y datos, así como el consentimiento de los afectados. Las partes en litigio, ya sea en sede procesal o extraprocesal, con independencia de la posición que ocupen o de los intereses que postulen, deberán ser informadas y posteriormente asentir expresamente frente al empleo de dicha inteligencia, o, visto de otra forma, podrán libremente rechazar su utilización". Ver: MARTÍN DIZ, F.: "La disrupción de la inteligencia artificial en el proceso judicial: avances y retrocesos", en RAMÍREZ CARVAJAL, D. M. (coord.), *Justicia Digital: una mirada internacional en época de crisis,* Medellín, 2020, p. 540-542.

[104] BRASIL.TRIBUNAL SUPERIOR DO TRABALHO: *RR - 61300-23.2000.5.10.0013*, Rel. Ministro João Oreste Dalazen, 1ª. Turma, DJ 10/06/2005; TEDH: *Case of Bărbulescu v. Romania,* 05/09/2007; PORTUGAL. SUPREMO TRIBUNAL DE JUSTIÇA: *Processo 07S043. N.º Convencional JSTJ000. N.º do Documento SJ200707050000434*, Rel. Mário Pereira,

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

Además, la exclusión de las expectativas de privacidad aún depende del cumplimiento de un "juicio de proporcionalidad" por parte del empleador. Es decir, deberá (i) haber informado previamente a su colaborador sobre las prohibiciones (parciales o totales) de utilizar el aparato para fines personales; (ii) haber informado de que se podrían adoptar medidas de control y vigilancia sobre él; y (iii) haber agotado otros medios menos invasivos a la privacidad del empleado[105] .

Con respecto específicamente a la IA, es interesante señalar que la Comisión Europea, a través de su Grupo Independiente de Expertos de Alto Nivel en Inteligencia Artificial, ha establecido algunos principios éticos a observar en el desarrollo, implementación y uso de esta tecnología, a saber: i) respeto de la autonomía humana; ii) prevención del daño; iii) equidad y iv) explicabilidad[106] . En cuanto a los objetivos de nuestro texto, debemos hacer breves comentarios sobre los dos últimos.

En cuanto a la *explicabilidad*, la Comisión propone la transparencia de los procesos, capacidades y finalidades de los sistemas de IA, así como, en la medida de lo posible, de las decisiones tomadas por los mismos, para garantizar su eventual refutación. Cuando no sea posible, pueden ser necesarias medidas alternativas, como la trazabilidad, la auditabilidad y la comunicación transparente sobre el sistema[107] .

Respecto a la *equidad*, además de su dimensión sustantiva - de garantizar una distribución justa y equitativa de los beneficios y costos de estas tecnologías, asegurando que las personas no sufran con sesgos injustos -, su dimensión procedimental pretende que los profesionales del área de IA respeten el principio de proporcionalidad entre los medios y los fines que se persiguen con esta tecnología, buscando el equilibrio entre los distintos intereses contrapuestos[108] .

Este último punto es extremadamente relevante cuando se trata del uso de la IA en el contexto empresarial. A nuestro juicio, la utilización en un proceso penal de los elementos de información obtenidos de una investigación interna dependerá no sólo del respeto a los derechos fundamentales del investigado también en este ámbito privado, sino también de una valoración de si los instrumentos efectivamente utilizados (entre ellos, herramientas de

---

05/07/2007. Ver con detalles: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 377.

[105] ESTRADA I CUADRAS, A., LLOBET ANGLÍ, M.: "Derechos de los trabajadores y deberes del empresario: conflicto en las investigaciones empresariales internas", en SILVA SANCHEZ, J. M., MONTANER FERNÁNDEZ, R.: *Criminalidad de empresa y compliance: prevención y reacciones corporativas*, Barcelona, 2013, p. 216-217.

[106] GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL CREADO POR LA COMISIÓN EUROPEA EN JUNIO DE 2018: *Directrices éticas para una IA fiable*.

[107] GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL CREADO POR LA COMISIÓN EUROPEA EN JUNIO DE 2018: *Directrices éticas para una IA fiable,* p. 16. La Propuesta de Reglamento del Parlamento Europeo y del Consejo también hace mención expresa a los niveles necesarios de transparencia de los sistemas de IA. En ese sentido, los artículos 13 y 52 en: COMISIÓN EUROPEA: *Propuesta de Reglamento del Parlamento Europeo y del Consejo: por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión: {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}*. Sobre la importancia de la transparencia en este contexto, ver también: NEIRA PENA, A. M.: "Inteligencia artificial y tutela cautelar. Especial referencia a la prisión provisional", en *Revista Brasileira de Direito Processual Penal*, vol. 7, n. 3, 2021, p. 1920 y ss.

[108] GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL CREADO POR LA COMISIÓN EUROPEA EN JUNIO DE 2018: *Directrices éticas para una IA fiable*, p. 15.

IA) y los datos concretamente tratados en el caso obedecían a los criterios de la legalidad, adecuación, necesidad y proporcionalidad en sentido estricto. Sólo tal análisis justificaría esta relativización de los derechos de los trabajadores[109] .

La *legalidad* y la *adecuación* no nos parece que planteen más problemas en lo que se refiere al uso de la IA en el DCC. No sólo es incuestionable que el uso de los medios tecnológicos aquí analizados tiene el poder de facilitar el logro de los objetivos fijados para los programas de cumplimiento, investigaciones internas y procedimientos de debida diligencia, sino que también se autoriza (y muchas veces se fomenta) la realización de estos procedimientos por las leyes laborales, societarias, administrativas e incluso penales[110] .

En cambio, pueden darse indagaciones un poco más contundentes en cuanto a la *necesidad* y *proporcionalidad en sentido estricto*. En el caso concreto, es necesario valorar si, entre los numerosos instrumentos igualmente eficaces que pueden adoptarse en el ámbito de estos procedimientos, el uso de un determinado sistema de IA sería el menos lesivo para los derechos de los involucrados, y si la intensidad de la restricción de los derechos en cuestión (a saber, la intimidad y los derechos conexos) está justificada por el poder de dirección y control del empleador, a la luz de la gravedad de lo que se pretende vigilar e investigar[111] .

Superadas, en su caso, las cuestiones de la expectativa de privacidad por parte de los empleados y la proporcionalidad de obtener estas informaciones por un determinado instrumento de IA, surge la importante cuestión sobre el intercambio de estos elementos de información para un determinado proceso penal. La relevancia de este tema queda atestiguada por el hecho de que, en el ámbito de estas investigaciones privadas, se recoge un amplio cuerpo de pruebas que pueden no sólo limitarse a eximir a la persona jurídica de sanciones administrativas o penales o incluso impedir el inicio de acciones penales contra ella, pero podrá indicar quiénes son los particulares responsables de los hechos específicamente investigados. Por lo tanto, la pretensión de llevar los resultados de estas investigaciones al proceso penal, ya sea presentándolos ante las autoridades estatales, o presentándolos directamente ante los tribunales como prueba de defensa de la persona jurídica, impone varios cuestionamientos, tales como: cómo garantizar la fiabilidad de los elementos de prueba recabados en el contexto de investigaciones internas? ¿Cómo compatibilizar estos procedimientos privados, sin contradictorio, con garantías procesales penales, como el derecho a la no autoincriminación, el contradictorio y la presunción de inocencia?[112]

Entendemos que, en principio, los elementos de información provenientes de los programas de cumplimiento son admisibles en proceso penal cuando los presente la persona

---

[109] CANESTRARO, A. C.: *As investigações internas no âmbito do criminal compliance e o direito dos trabalhadores: considerações sobre a possibilidade de investigar e a transferência de informações para o processo penal,* São Paulo, 2020; CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 382.

[110] CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia*, Porto Alegre, 2022, p. 382-383.

[111] Ver, con ejemplos, en: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia*, Porto Alegre, 2022, p. 382-383.

[112] JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1474-1475.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

jurídica en su propia defensa. Un entendimiento contrario, a nuestro juicio, atentaría contra el derecho de defensa y el derecho a la prueba del ente colectivo imputado, así como afectaría la funcionalidad misma de los programas de cumplimiento e investigaciones internas, sirviendo como factor desincentivador para la adopción de estos procedimientos[113] .

Más complicada es la cuestión de si estos elementos son igualmente admisibles cuando presentados por la Fiscalía, en perjuicio de otro Acusado (como un empleado), o incluso cuando presentados por la defensa de la corporación, en prejuicio de otro Acusado. Como se observa, en este último caso están en conflicto los derechos de defensa de ambos Acusados, además de las garantías al contradictorio y al debido proceso del sujeto afectado por la prueba[114] . Para estos casos, proponemos los siguientes supuestos:

I) los elementos de información provenientes de los programas de cumplimiento serán admisibles en el proceso penal cuando los presente el imputado, en ejercicio de su derecho de defensa, y podrán ser valorados plenamente a tal efecto, salvo los casos en los existan ilegalidades en la obtención (por ejemplo, tortura de un tercero)[115] .

II) estos elementos nunca pueden considerarse suficientes para sustentar una condena, ya sea que los presente la Fiscalía o uno de los Acusados contra otro. Entre la valoración plena y la inadmisión, entendemos que esta sería una solución intermedia, que atendería los intereses relacionados con la funcionalidad de los programas de cumplimiento, especialmente en la colaboración con el Estado en el esclarecimiento de la verdad, pero sin desconocer los derechos de los afectados al debido proceso y al contradictorio[116] .

Al desarrollar en detalle esta propuesta, Anna Carolina Canestraro explica que, una vez superada la expectativa de privacidad del trabajador y la proporcionalidad de la medida en el ámbito privado, el intercambio de estas informaciones para el proceso penal también debe someterse a un nuevo juicio de legalidad y proporcionalidad, que, por regla general, es positivo para compartir (con la excepción de los informes de entrevistas, que, en opinión de la autora, no pasan por el criterio de la necesidad, y los testigos deben ser interrogados nuevamente en el tribunal, con respecto a lo contradictorio). Sin embargo, precisamente por no haber sido producidas en contradictorio, la autora entiende que estos elementos no pueden, por sí solos, sustentar una convicción, siendo suficientes únicamente para formar la

[113] JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1483-1484. Para un análisis de las investigaciones internas como una especie del género "investigaciones defensivas", posición que apoyamos, ver: CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Investigação defensiva corporativa: um estudo do Provimento 188/2018 e de sua eventual aplicação para as investigações internas de pessoas jurídicas", en *Revista Brasileira de Direito Processual Penal*, v. 6, n. 1, 2020.

[114] JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1483-1484.

[115] JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1483-1484.

[116] JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1483-1484.

opinio delicti de la Fiscalía, en un régimen análogo a los derivados de los actos de investigación estatales[117] .

III) como resultado de las dos primeras premisas, entendemos que a pesar de la posibilidad de que la persona jurídica presente los resultados de sus investigaciones internas como prueba defensiva, éstos no pueden ser valorados a efectos de fundamentar, por sí mismos, la condena de otro Acusado. La solución a este impasse, a nuestro juicio, pasa por una de dos alternativas: a) considerar que, si bien las personas físicas y jurídicas gozan del derecho de defensa y de las garantías relacionadas con el mismo, estos derechos no necesariamente tendrían el mismo "peso" para ambas[118] . En otras palabras, si los derechos de las personas físicas y jurídicas están en conflicto, los primeros tendrían primacía, ya sea por la relativización que los segundos admiten en cuanto a la naturaleza de estos sujetos, o por la propia vinculación de algunos derechos procesales, no sólo con las garantías directamente relacionadas con el equilibrio procesal, sino también con la propia dignidad humana, que no puede extenderse a las personas jurídicas[119] . b) la segunda posibilidad, que a nuestro juicio sería más adecuada, sería el uso de la facultad prevista por algunos ordenamientos jurídicos (por ejemplo, CPP Portugués, Art. 30.º; CPP Brasileño, Art. 80) de separación de procesos, admitiendo el juicio separado de los Acusados, por razones de conveniencia procesal (como posibles riesgos graves para los intereses del Acusado)[120] .

Sin embargo, resuelta la cuestión de la admisibilidad de los elementos de información provenientes de los programas de cumplimiento, investigaciones internas y procedimientos de debida diligencia[121] , aún queda la atormentadora cuestión de la confiabilidad de estos documentos, tema que se torna aún más controvertido si consideramos la posible

---

[117] CANESTRARO, A. C.: *As investigações internas no âmbito do criminal compliance e o direito dos trabalhadores: considerações sobre a possibilidade de investigar e a transferência de informações para o processo penal,* São Paulo, 2020, p. 95 y ss.; CANESTRARO, A. C.: "Investigaciones internas en el marco de los programas de los programas de cumplimiento: un análisis de los límites de las investigaciones frente al derecho de los trabajadores y las garantías procesales penales", en DEMETRIO CRESPO, E. et al (eds.), *Problemas y retos actuales del derecho penal económico,* Cuenca, 2020, p. 54 y ss.; CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia,* Porto Alegre, 2022, p. 384.

[118] En ese sentido: ANTUNES, M. J.: "Privatização das investigações e compliance criminal", en *Revista Portuguesa de Ciência Criminal*, ano 28, n. 1, 2018, p. 126-127.

[119] Sobre esta distinción, especialmente en lo que se refiere al *nemo tenetur se detegere*, ver: NEIRA PENA, A. M.: *La instrucción de los procesos penales frente a las personas jurídicas*, Valencia, 2017, p. 235 y ss.

[120] JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1483-1484.

[121] Es claro que estas no son las únicas cuestiones procesales penales relevantes en materia de cumplimiento. Optamos por este corte solo porque, en nuestra opinión, los temas aquí presentados son los que presentan mayores particularidades al considerar la aplicación de la IA en este contexto. Para un análisis más amplio y otros temas particulares, ver: ANTUNES, M. J.: *Processo penal e pessoa coletiva arguida,* Coimbra, 2020; GIMENO BEVIÁ, J.: *Compliance y proceso penal: el proceso penal de las personas jurídicas: adaptada a las reformas del CP y LECRIM, circular FGE 1/2016 y jurisprudencia del TS*, Cizur Menor, 2016; NEIRA PENA, A. M.: *La instrucción de los procesos penales frente a las personas jurídicas*, Valencia, 2017; JANUÁRIO, T. F. X.: "O sigilo profissional no âmbito das pessoas jurídicas: um estudo da particular posição dos in-house lawyers e dos advogados de compliance e de investigações internas", en *Revista Brasileira de Ciências Criminais*, ano 27, n. 159, 2019.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

intervención de IA. En otras palabras, ¿estamos en condiciones de saber si los elementos recogidos en estos procedimientos privados, muchas veces desvinculados de las entidades estatales de investigación, serán los mismos que serán valorados en los tribunales? ¿Existen condiciones técnicas para dar fe de su integridad, identidad y autenticidad?[122]

En nuestra opinión, igual que tratándose de evidencias digitales[123] , es fundamental la documentación de la cadena de custodia de la prueba[124] , que, en el caso de investigaciones privadas, puede ser la única forma de asegurar la legitimidad y licitud de los elementos recabados, evitando que éstos puedan ser removidos del proceso por inadmisibilidad[125] . Una eventual quiebra de la cadena de custodia de la prueba, por tanto, puede representar grandes perjuicios para la persona jurídica que espera, de la promoción de un programa de cumplimiento efectivo, beneficios procesales y exenciones de responsabilidad.

De acuerdo con modelos y procedimientos propuestos por institutos internacionales de certificación, la doctrina afirma la total viabilidad de documentación de la cadena de custodia de evidencias digitales[126] , que puede (y debe) cumplirse también en un ámbito privado. Sin embargo, una pregunta compleja y que aún depende de mayores investigaciones es si estos procedimientos serían igualmente útiles para evidencias digitales relacionadas con la IA[127] . A nuestro juicio, la relación simbiótica entre cadena de custodia e inteligencia artificial es uno de los puntos más urgentes a investigar en los próximos años, en materia de proceso penal e IA.

5. CONCLUSIÓN

Como se puede observar, las ciencias jurídico-penales nuevamente se ven desafiadas por el progreso científico y tecnológico. Todavía no hemos alcanzado un mínimo consenso sobre

---

[122] JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1476. Figueroa Navarro habla en *mismidad de la prueba*, en: FIGUEROA NAVARRO, M. C.: "El aseguramiento de las pruebas y la cadena de custodia", en *La ley penal: revista de derecho penal, procesal y penitenciario*, v. 8, n. 84, 2011, p. 7.

[123] Sobre la cadena de custodia de evidencias digitales, ver: PRADO, G.: *A cadeia de custodia da prova no processo penal*, 2. ed., São Paulo, 2021; BADARÓ, G. H.: "Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia", *Boletim IBCCRIM*, ano 29, n. 343, 2021.

[124] Ver: ESPAÑA. TRIBUNAL SUPREMO. SALA DE LO PENAL: *STS 7710/2009*, Ponente: Juan Ramon Berdugo Gomez de la Torre, 03.12.2009.

[125] Existe gran controversia doctrinal acerca de si la quiebra de la cadena de custodia sería causa de ilicitud probatoria y, en consecuencia, de inadmisibilidad (o exclusión) de la misma o si procedería remitir ese análisis al momento de la valoración de la evidencia. Para un resumen de esta discusión y nuestra posición, ver: JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1491 y ss.

[126] Ver: RAMALHO, D. S.: *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra, 2017; CASEY, E.: "Foundations of digital forensics", en CASEY, E. (ed.). *Digital Evidence and Computer Crime: forensic science, computers and the internet*, 3. Ed, Waltham, MA, 2011; MENDES, C. H. C. F.: "Dado informático como prova penal confiável(?): apontamentos procedimentais sobre a cadeia de custódia digital", en *Revista Brasileira de Ciências Criminais*, v. 27, n. 161, 2019, p. 131 y ss. MARSHALL, A.: *Digital forensics: Digital Evidence in Digital Investigation*, West Sussex, 2008. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST: *Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology*, 2006.

[127] Sobre algunas de las dificultades probatorias el contexto de la IA, ver: FIDALGO, S.: "A utilização da inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo", en RODRIGUES, A. M. (coord.), *Inteligência artificial no direito penal*, Coimbra, 2020, p. 129 y ss.

diversos puntos de los sistemas de imputación de la responsabilidad penal de las personas jurídicas – cuyas divergencias no son exclusivas de España, pero sí motivo de discusiones en varios países - y ni siquiera hemos madurado los debates sobre los necesarios aspectos procesales que los circundan, y este campo ya se ve nuevamente "molesto" por el rápido desarrollo de los sistemas de IA.

El protagonismo de las empresas tanto en la producción de esta tecnología como en su uso plantea cuestionamientos de carácter sustantivo, especialmente sobre su responsabilidad penal por los posibles daños causados por estos sistemas y las dificultades dogmáticas a superar para ello, y de carácter procesal, como por ejemplo los fundamentos y límites del uso de la IA en el ámbito del DCC y, principalmente, de su intercambio para eventuales procesos penales.

Constatamos que las particularidades y limitaciones de la IA dificultan no solo la imputación de responsabilidades penales individuales, sino también la RPPJ en ordenamientos que aún la vinculan a una necesaria identificación de una conducta humana. Por tanto, los modelos de *autorresponsabilidad* tienden a responder mejor a estos casos, además de fomentar los programas de cumplimiento, que juegan un papel importante en este ámbito.

Aún con respecto a estos programas, es evidente que la IA tiene un enorme potencial para hacerlos más eficientes y eficaces. Sin embargo, su uso ciertamente no es ilimitado, especialmente si en su adopción se busca algún tipo de efecto penal. Los instrumentos específicos del programa de cumplimiento deben cumplir con los juicios de legalidad y proporcionalidad en su ejecución, así como sus frutos nuevamente deben ser objeto de estas ponderaciones, añadidas del análisis de la documentación de la cadena de custodia, a los efectos de la admisibilidad en el proceso penal. Todo ello sin perjuicio de los necesarios límites a su valoración, especialmente en lo que se refiere a la eventual condena de uno de los imputados.

Como vemos, el dinamismo de este sector y la insipiencia de sus implicaciones penales frustran y hacen pretencioso cualquier intento de ser exhaustivo en la materia, relegando rápidamente a la obsolescencia cualquier investigación que se aventure a ello. Sin embargo, esperamos que las líneas generales esbozadas en este trabajo sean capaces de resistir a los inminentes avanzos tecnológicos y ofrecer soluciones que sigan siendo útiles a los problemas que posiblemente surgirán en los próximos años.

Bibliografía

AGAPITO, L. S., MIRANDA, M. A., JANUÁRIO, T. F. X.: "On the Potentialities and Limitations of Autonomous Systems in Money Laundering Control", en *RIDP*, v. 92, n. 1, 2021.

ALMEIDA, M. S.: "Introdução à negociação de alta frequência", en *Cadernos de Valores Mobiliários*, n. 54, 2016.

ANTUNES, M. J.: "Privatização das investigações e compliance criminal", en *Revista Portuguesa de Ciência Criminal*, ano 28, n. 1, 2018.

ANTUNES, M. J.: *Processo penal e pessoa coletiva arguida*, Coimbra, 2020.

BACIGALUPO, S.: *La responsabilidad penal de las personas jurídicas*, Barcelona, 1998.

BADARÓ, G. H.: "Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia", *Boletim IBCCRIM*, ano 29, n. 343, 2021.

Estudios Penales y Criminológicos., 44(ext) (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.44.8902

BAJO FERNÁNDEZ, M.: "El derecho penal económico: un estudio de derecho positivo español", en *Anuario de derecho penal y ciencias penales*, v. 26, n. 1, 1973.

BARONA VILAR, S.: *Algoritmización del derecho y de la justicia: de la inteligencia artificial a la Smart Justice*, Valencia, 2021.

BARROS, A. M. *Curso de direito do trabalho*, 7. ed., São Paulo, 2011.

BOCK, D.: *Criminal compliance*, Baden-Baden, 2011.

BRASIL. TRIBUNAL SUPERIOR DO TRABALHO: *RR - 61300-23.2000.5.10.0013*, Rel. Ministro João Oreste Dalazen, 1ª. Turma, DJ 10/06/2005.

BROGAARD, J., HENDERSHOTT, T., RIORDAN, R.: "High-Frequency Trading and Price Discovery", en *The Review of Financial Studies*, v. 27, n. 8, 2014. https://doi.org/10.1093/rfs/hhu032.

BURCHARD, C.: "Das »Strafrecht« der Prädiktionsgesellschaft: …oder wie »smarte« Algorithmen die Strafrechtspflege verändern (könnten)", en *Forschung Frankfurt: das Wissenschaftsmagazin: Recht und Gesetz*, n. 1, 2020.

BURCHARD, C.: "Digital Criminal Compliance", en ENGELHART, M., KUDLICH, H., VOGEL, B. (Hrsg.), *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70. Geburtstag: Teilband II*, Berlin, 2021.

BURRELL, J.: "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms", en *Big Data & Society*, v. 3, n. 1, 2016. https://doi.org/10.1177/20539517156225.

BUSATO, P. C.: "Razões político-criminais para a responsabilização penal de pessoas jurídicas", en BUSATO, P. (org.), *Responsabilidade penal de pessoas jurídicas: seminario Brasil – Alemanha*, Florianópolis, 2018.

BUSATO, P. C.: "Responsabilidade penal das pessoas jurídicas no projeto (e no texto substitutivo) do novo código penal brasileiro", en LEITE, A. (org.), *Reforma penal: a crítica científica à parte geral do projeto de código penal (PLS 236/2012)*, São Paulo, 2015.

CAIVANO, V. et al.: "Il trading ad alta frequenza: caratteristiche, effetti, questioni di policy", en *CONSOB Discussion Papers*, n. 5, 2012. https://dx.doi.org/10.2139/ssrn.2191669.

CANESTRARO, A. C.: *As investigações internas no âmbito do criminal compliance e o direito dos trabalhadores: considerações sobre a possibilidade de investigar e a transferência de informações para o processo penal*, São Paulo, 2020.

CANESTRARO, A. C.: "Investigaciones internas en el marco de los programas de los programas de cumplimiento: un análisis de los límites de las investigaciones frente al derecho de los trabajadores y las garantías procesales penales", en DEMETRIO CRESPO, E. et al (eds.), *Problemas y retos actuales del derecho penal económico,* Cuenca, 2020. https://doi.org/10.18239/congresos_2020.24.05.

CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Beyond Ecocide: Extraterritorial Obligations of Due Diligence as an Alternative to Address Transnational Environmental Damages?", en *RIDP*, v. 93, n. 1, 2022.

CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Concurso de agentes na perspectiva da teoria da ação significativa: um diálogo entre o sistema espanhol e o Projeto de Novo Código Penal Brasileiro", en *Revista Brasileira de Ciências Criminais*, ano 29, n. 178, 2021.

CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Dos níveis de exigibilidade dos procedimentos de investigação interna", en *Anais do IV Congresso de Pesquisas em Ciências Criminais, de 21 a 23 de outubro de 2020*, São Paulo, 2020.

CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", en D'ÁVILA, F. R., AMARAL, M. E. A. (eds.), *Direito e Tecnologia*, Porto Alegre, 2022.

CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Investigação defensiva corporativa: um estudo do Provimento 188/2018 e de sua eventual aplicação para as investigações internas de pessoas jurídicas", en *Revista Brasileira de Direito Processual Penal*, v. 6, n. 1, 2020. https://doi.org/10.22197/rbdpp.v6i1.324.

CANESTRARO, A. C., JANUÁRIO, T. F. X., "Programas de compliance e branqueamento de capitais: implicações da lei nº 83/2017, de 31 de agosto, no regime jurídico de Portugal" en *Revista Científica do CPJM*, v. 1, n. 3, 2022. https://doi.org/10.55689/rcpjm.2022.03.005.

CANESTRARO, A. C., JANUÁRIO, T. F. X.: "Responsabilidade penal da pessoa coletiva e princípio da culpabilidade: análise crítica do modelo português", en *Revista da Faculdade de Direito da UFRGS*, n. 39, 2018. https://doi.org/10.22456/0104-6594.77092.

CANESTRARO, A. C., KASSADA, D. A., JANUÁRIO, T. F. X.: "Nemo tenetur se detegere e programas de compliance: o direito de não produzir prova contra si próprio em face da Lei n. 13.303/16", en SAAD-DINIZ, E., BRODT, L. A., TORRES, H. A. A., LOPES, L. S. (orgs.), *Direito penal econômico nas ciências criminais*, Belo Horizonte, 2019.

CARBONELL MATEU, J. C.: "Responsabilidad penal de las personas jurídicas: reflexiones en torno a su dogmática y al sistema de la reforma de 2010", en *Cuadernos de política criminal*, segunda época, n. 101, 2010.

CASEY, E.: "Foundations of digital forensics", en CASEY, E. (ed.). *Digital Evidence and Computer Crime: forensic science, computers and the internet*, 3. Ed, Waltham, MA, 2011.

CAVALI, M. C.: *Manipulação do mercado de capitais: fundamentos e limites da repressão penal e administrativa*, São Paulo, 2018.

COMISIÓN EUROPEA: *Propuesta de Reglamento del Parlamento Europeo y del Consejo: por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión: {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}*.

COSTA, I. S.: *High Frequency Trading em câmera lenta: compreender para regular*, São Paulo, 2020.

DE HOYOS SANCHO, M., "El Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo", en *Revista Española de Derecho Europeo*, n. 76, 2020. https://doi.org/10.37417/REDE/num76_2020_534.

DE HOYOS SANCHO, M.: "El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea", en *Revista General de Derecho Procesal*, n. 55, 2021.

DELGADO, M. G.: *Curso de direito do trabalho*, 11. ed., São Paulo, 2012.

DIAS, J. F.: *Direito Penal: parte geral: tomo I: questões fundamentais: a doutrina geral do crime*, São Paulo, 2007.

DIAMANTIS, M. E.: "Algorithmic Harms as Corporate Misconduct", en ANTUNES, M. J., SOUSA, S. A. (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Coimbra, 2022. https://doi.org/10.47907/livro2021_4c6.

DÍEZ, RIPOLLÉS, J. L.: "La responsabilidad penal de las personas jurídicas. Regulación española", en *InDret*, n. 1, 2012.

ENGELHART, M.: *Sanktionierung von Unternehmen und Compliance: eine Rechtsvergleichende Analyse des Straf- und Ordnungwidrigkeitenrechts in Deutschland und den USA*, 2. Ergänzte und erweiterte Auflage, Berlin, 2012.

ENGELHART, M.: *The Nature and Basic Problems of Compliance Regimes*, Freiburg, 2018. https://doi.org/10.30709/archis-2018-3.

ESPAÑA. *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.*

ESPAÑA. TRIBUNAL SUPREMO. SALA DE LO PENAL: *STS 7710/2009*, Ponente: Juan Ramon Berdugo Gomez de la Torre, 03.12.2009.

ESTELLITA, H., LEITE, A.: "Veículos Autônomos e Direito Penal: uma introdução", en ESTELLITA, H., LEITE, A. (orgs.), *Veículos autônomos e direito penal*, São Paulo, 2019.

ESTRADA I CUADRAS, A., LLOBET ANGLÍ, M.: "Derechos de los trabajadores y deberes del empresario: conflicto en las investigaciones empresariales internas", en SILVA SANCHEZ, J. M., MONTANER FERNÁNDEZ, R.: *Criminalidad de empresa y compliance: prevención y reacciones corporativas*, Barcelona, 2013.

FIDALGO, S.: "A utilização da inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo", en RODRIGUES, A. M. (coord.), *Inteligência artificial no direito penal*, Coimbra, 2020.

FIGUEROA NAVARRO, M. C.: "El aseguramiento de las pruebas y la cadena de custodia", en *La ley penal: revista de derecho penal, procesal y penitenciario*, v. 8, n. 84, 2011.

FRISCH, W.: *Comportamiento típico e imputación del resultado*, Madrid, 2004.

GIMENO BEVIÁ, J.: *Compliance y proceso penal: el proceso penal de las personas jurídicas: adaptada a las reformas del CP y LECRIM, circular FGE 1/2016 y jurisprudencia del TS*, Cizur Menor, 2016.

GLEß, S., SILVERMAN, E., WEIGEND, T. "If robots cause harm, who is to blame? Self-driving cars and criminal liability", en *New Criminal Law Review*, v. 19, n. 3, 2016. https://doi.org/10.1525/nclr.2016.19.3.412.

GLEß, S., WEIGEND, T.: "Intelligente Agenten und das Strafrecht", en *Zeitschrift für die gesamte Strafrechtswissenschaft*, v. 126, n. 3, 2014. https://doi.org/10.1515/zstw-2014-0024.

GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL CREADO POR LA COMISIÓN EUROPEA EN JUNIO DE 2018: *Directrices éticas para una IA fiable.*

HILGENDORF, E.: "Sistemas autônomos, inteligência artificial e robótica: uma orientação a partir da perspectiva jurídico-penal", en HILGENDORF, E., GLEIZER, O. (orgs.), *Digitalização e direito*, São Paulo, 2020.

GODINHO, I. F.: *A responsabilidade solidária das pessoas colectivas em direito penal econômico*, Coimbra, 2007.

GÓMEZ-JARA DÍEZ, C.: *A responsabilidade penal da pessoa jurídica: teoria do crime para pessoas jurídicas*, São Paulo, 2015.

GÓMEZ-JARA DÍEZ, C.: "Fundamentos de la responsabilidad penal delas personas jurídicas", en BAJO FERNÁNDEZ, M., FEIJOO SÁNCHEZ, B., GÓMEZ-JARA DÍEZ, C., *Tratado de responsabilidad penal de las personas jurídicas: adaptada a la Ley 1/2015, de 30 de marzo por la que se modifica el Código Penal*, 2. Ed, Navarra, 2016.

GÓMEZ-JARA DÍEZ, C.: *Fundamentos modernos de la responsabilidad penal de las personas jurídicas: bases teóricas, regulación internacional y nueva legislación española*, Montevideo, 2010.

GONZÁLEZ CUSSAC, J. L.: "El plano político criminal en la responsabilidad penal de las personas jurídicas", en MATALLÍN EVANGELIO, Á. (dir.), *Compliance y prevención de delitos de corrupción,* Valencia, 2018.

GONZÁLEZ CUSSAC, J. L.: *Responsabilidad penal de las personas jurídicas y programas de cumplimiento*, Valencia, 2020.

GRACIA MARTÍN, L.: "Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica", en *Revista Electrónica de Ciencia Penal y Criminología*, n. 18-05, 2016.

GRECO, L.: "Por que é ilegítimo e quase de todo inconstitucional punir pessoas jurídicas", en BUSATO, P. (org.), *Responsabilidade penal de pessoas jurídicas: seminario Brasil – Alemanha,* Florianópolis, 2018.

HALLEVY, G.: *Liability for Crimes Involving Artificial Intelligence Systems*, Heidelberg, 2015. https://doi.org/10.1007/978-3-319-10124-8.

HALLEVY, G.: *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, 2019. https://doi.org/10.2139/ssrn.3402527.

HALLEVY, G.: "The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control", en *Akron Intellectual Property Journal*, v. 4, n. 2, 2010.

JANUÁRIO, T. F. X.: "Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação", en *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, 2021. https://doi.org/10.22197/rbdpp.v7i2.453.

JANUÁRIO, T. F. X. "Considerações preambulares acerca das reverberações da inteligência artificial no direito penal", en COMÉRIO, M. S., JUNQUILHO, T. A. (orgs.), *Direito e tecnologia: um debate multidisciplinar*, Rio de Janeiro, 2021.

JANUÁRIO, T. F. X. "Corporate Internal Investigations 4.0: on the criminal procedural aspects of applying artificial intelligence in the reactive corporate compliance", en *Revista Brasileira de Direito Processual Penal*, v. 9, n. 2, 2023. https://doi.org/10.22197/rbdpp.v9i2.837.

JANUÁRIO, T. F. X.: *Criminal compliance e corrupção desportiva: um estudo com base nos ordenamentos jurídicos do Brasil e de Portugal*, Rio de Janeiro, 2019.

JANUÁRIO, T. F. X.: "Criminal liability for legal entities: a comparative study between Spain, Portugal and Brazil", en *POLAR – Portuguese Law Review*, v. 2, n. 2, 2018.

JANUÁRIO, T. F. X.: "Da (ir)relevância dos programas de compliance no modelo brasileiro de responsabilidade penal das pessoas jurídicas: considerações críticas ao projeto de novo Código Penal", en *Revista Direito e Liberdade*, v. 21, n. 2, 2019.

JANUÁRIO, T. F. X.: "Da teoria do delito para as pessoas jurídicas: análise a partir da teoria construtivista de "autorresponsabilidade" dos entes coletivos", en *Revista de Estudos Jurídicos UNESP*, ano 20, n. 32, 2016. https://doi.org/10.22171/rej.v20i32.2155.

JANUÁRIO, T. F. X.: "Dos limites do risco permitido para as pessoas jurídicas: uma análise do defeito de organização como um problema de imputação objetiva", en *Conpedi Law Review,* v. 4, n. 1, 2018. https://doi.org/10.26668/2448-3931_conpedilawreview/2018.v4i1.4514.

JANUÁRIO, T. F. X.: "El modelo brasileño de responsabilidad penal para entidades jurídicas: un comentario de la Ley 9.605/98 y el nuevo Código Penal", en DEMETRIO CRESPO, E. et al (eds.), *Problemas y retos actuales del derecho penal económico,* Cuenca, 2020. https://doi.org/10.18239/congresos_2020.24.01.

JANUÁRIO, T. F. X.: "Inteligência artificial e manipulação do mercado de capitais: uma análise das negociações algorítmicas de alta frequência (high-frequency trading – HFT) à luz do ordenamento jurídico brasileiro", en *Revista Brasileira de Ciências Criminais,* ano 29, n. 186, 2021.

JANUÁRIO, T. F. X.: "Inteligência artificial e direito penal da medicina", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal*, volume II, Coimbra, 2022.

JANUÁRIO, T. F. X.: "Inteligência artificial e responsabilidade penal no setor da medicina", *Lex Medicinae: Revista Portuguesa de Direito da Saúde*, ano 17, n. 34, 2020.

JANUÁRIO, T. F. X.: "O ônus da prova da existência e eficácia dos programas de compliance no âmbito do processo penal das pessoas jurídicas: um estudo com base no ordenamento jurídico espanhol", en *Revista Brasileira de Ciências Criminais*, ano 27, n. 160, 2019.

JANUÁRIO, T. F. X.: "O sigilo profissional no âmbito das pessoas jurídicas: um estudo da particular posição dos in-house lawyers e dos advogados de compliance e de investigações internas", en *Revista Brasileira de Ciências Criminais*, ano 27, n. 159, 2019.

JANUÁRIO, T. F. X.: "Vulnerabilidad e hiposuficiencia 4.0: la protección jurídico-penal de los consumidores en la era de la inteligencia artificial", en FONTESTAD PORTALÉS, L. (dir.), PÉREZ TORTOSA, F. (coord.), *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI*, A Coruña, en curso de publicación.

JANUÁRIO, T. X.: "Veículos autónomos e imputação de responsabilidades criminais por acidentes", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal*, Coimbra, 2020.

KAPLAN, A., HAENLEIN, M.: "Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence", en *Business Horizons*, v. 62, n. 1, 2019. https://doi.org/10.1016/j.bushor.2018.08.004.

LASCURAÍN, J. A.: "Compliance, debido control y unos refrescos", en ARROYO ZAPATERO, L., NIETO MARTÍN, A. (dir.), *El derecho penal económico en la era compliance*, Valencia, 2013.

LEHMANN, E. E.: "Unternehmensorganisation und criminal Compliance", en ROTSCH, T. (Hrsg.), *Criminal Compliance: Handbuch*, Baden-Baden, 2015.

LESHIK, E., CRALLE, J.: *An Introduction to Algorithmic Trading: Basic to Advanced Strategies*, Chichester, 2011. https://doi.org/10.1002/9781119206033.

MACHADO, L. S.: "Médico robô: responsabilidade civil por danos praticados por atos autônomos de sistemas informáticos dotados de inteligência artificial", en *Lex Medicinae: Revista Portuguesa de Direito da Saúde*, ano 16, n. 31-32, 2019.

MARSHALL, A.: *Digital forensics: Digital Evidence in Digital Investigation*, West Sussex, 2008.

MARTÍN DIZ, F.: "La disrupción de la inteligencia artificial en el proceso judicial: avances y retrocesos", en RAMÍREZ CARVAJAL, D. M. (coord.), *Justicia Digital: una mirada internacional en época de crisis*, Medellín, 2020.

MARTÍNEZ-BUJÁN PÉREZ, C.: *Derecho penal económico y de la empresa – Parte general*, 5. ed. adaptada a la L.O. 1/2015, Valencia, 2016.

MARTÍNEZ-BUJÁN PÉREZ, C.: *La autoría en derecho penal: un estudio a la luz de la concepción significativa (y del Código penal español)*, Valencia, 2019.

MAYOR, A.: *Gods and Robots: myths, machines and ancient dreams of technology*, Princeton, 2018.

MCCARTHY, J., MINSKY, M. L., ROCHESTER, N., SHANNON, C. E.: "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955", en *AI Magazine*, v. 27, n. 4, 2006. https://doi.org/10.1609/aimag.v27i4.1904.

MCCARTHY, J.: *What is Artificial Intelligence?*, Stanford, 2007.

MENDES, C. H. C. F.: "Dado informático como prova penal confiável(?): apontamentos procedimentais sobre a cadeia de custódia digital", en *Revista Brasileira de Ciências Criminais*, v. 27, n. 161, 2019.

MIRANDA, M. A., JANUÁRIO, T. F. X.: "Novas tecnologias e justiça criminal: a tutela de direitos humanos e fundamentais no âmbito do direito penal e processual penal", en MOREIRA, V. et al (eds.), *Temas de Direitos Humanos do VI CIDH Coimbra 2021*, Campinas, 2021.

MIRÓ LLINARES, F.: "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", en *Revista de Derecho Penal y Criminología*, 3. época, n. 20, 2018. https://doi.org/10.5944/rdpc.20.2018.26446.

MULHOLLAND, C., FRAJHOF, I. Z.: "Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning", en FRAZÃO, A., MULHOLLAND, C. (eds.), *Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade*, São Paulo, 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST: *Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology*, 2006.

NAVAS MONDACA, I.: "Los códigos de conducta y el derecho penal económico" en: SILVA SÁNCHEZ, J. M (dir.), MONTANER FERNÁNDEZ, R. (coord..), *Criminalidad de empresa y compliance: prevención y reacciones corporativas*, Barcelona, 2013.

NETTO, A. V. S.: *Responsabilidade penal da pessoa jurídica*, 2. ed., São Paulo, 2020.

NEIRA PENA, A. M.: "Inteligencia artificial y tutela cautelar. Especial referencia a la prisión provisional", en *Revista Brasileira de Direito Processual Penal*, vol. 7, n. 3, 2021. https://doi.org/10.22197/rbdpp.v7i3.618.

NEIRA PENA, A. M.: *La instrucción de los procesos penales frente a las personas jurídicas*, Valencia, 2017.

NIETO MARTÍN, A.: *La responsabilidad penal de las personas jurídicas: un modelo legislativo*, Madrid, 2008.

NIETO MARTÍN, A. (dir.), *Manual de cumplimiento penal en la empresa*, Valencia, 2015.

NIETO MARTÍN, A.: "Problemas fundamentales del cumplimiento normativo en el derecho penal", en KUHLEN, L., MONTIEL, J. P., DE URBINA GIMENO, I. O. (eds.), *Compliance y teoría del derecho penal*, Madrid, 2013.

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

PAGALLO, U., QUATTROCOLO, S.: "The Impact of AI on Criminal Law and its Twofold Procedures", en BARFIELD, W., PAGALLO, U. (eds.), *Research Handbook on the law of artificial intelligence*, Cheltenham, 2018. https://doi.org/10.4337/9781786439055.00026.

PAMPEL, J., GLAGE, D.: "Unternehmensrisiken und Risikomanagement", en HAUSCHKA, C. E. (Hrsg.), *Corporate Compliance: Handbuch der Haftungsvermeidung im Unternehmen*, München, 2007.

PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA: *Directiva 2014/65/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014: relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE.*

PEIXOTO, F. H., SILVA, R. Z. M., *Inteligência artificial e direito*, Curitiba, 2019.

PEREIRA, A. G. D.: "Inteligência artificial, saúde e direito: considerações jurídicas em torno da medicina de conforto e da medicina transparente", *Julgar*, n. 45, 2021.

PEREIRA, A. G. D.: "O médico-robô e os desafios para o direito da saúde: entre o algoritmo e a empatia", *Gazeta de Matemática*, ano LXXX, n. 189, 2019.

PORTUGAL: *DL n.º 48/95, de 15 de março: Código Penal de 1982 versão consolidada posterior a 1995*.

PORTUGAL. SUPREMO TRIBUNAL DE JUSTIÇA: *Processo 07S043. N.º Convencional JSTJ000. N.º do Documento SJ200707050000434*, Rel. Mário Pereira, 05/07/2007.

PRADO, G.: *A cadeia de custodia da prova no processo penal*, 2. ed., São Paulo, 2021.

PRICE II, W. N.: "Artificial Intelligence in Health Care: Applications and Legal Issues", en *U of Michigan Public Law Research Paper,* n. 599, 2017.

QUATTROCOLO, S.: *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion,* Cham, 2020. https://doi.org/10.1007/978-3-030-52470-8.

RAMALHO, D. S.: *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra, 2017.

RIORDAN, R., STORKENMAIER, A.: "Latency, Liquidity and Price Discovery", en *Journal of Financial Markets*, v. 15, n. 4, 2012. https://doi.org/10.1016/j.finmar.2012.05.003.

RODRIGUES, A. M.: "Compliance inteligente e prevenção e luta contra o branqueamento", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal*, volume II, Coimbra, 2022.

RODRIGUES, A. M.: *Direito penal económico: uma política criminal na era compliance*, 2.ed., Coimbra, 2020.

RODRIGUES, A. M.: "Inteligência Artificial no Direito Penal – A Justiça Preditiva entre a Americanização e a Europeização", en RODRIGUES, A. M. (coord.), *A Inteligência Artificial no Direito Penal*, Coimbra, 2020.

RODRIGUES, A. M.: "Os crimes de abuso de mercado e a "Escada Impossível" de Escher (o caso do Spoofing)", en *Julgar*, n. 45, 2021.

RODRIGUES, A. M.: "The Last Cocktail - Economic and Financial Crime, Corporate Criminal Responsibility, Compliance and Artificial Intelligence", en ANTUNES, M. J., SOUSA, S. A. (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Coimbra, 2021. https://doi.org/10.47907/livro2021_4c5.

RODRIGUES, A. M., SOUSA, S. A.: "Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal*, vol. II, Coimbra, 2022.

ROTSCH, T.: "Criminal compliance", en *InDret: revista para el análisis del derecho*, n. 1, 2012.

ROXIN, C.: *Derecho Penal: parte general: tomo I: fundamentos. La estructura de la teoria del delito*, Madrid, 2008.

SCHÜNEMANN, B.: "Cuestiones básicas de dogmática jurídico-penal y política criminal sobre la criminalidad empresarial", en *Anuario de derecho penal y ciencias penales*, v. 41, n. 2, 1988.

SHABBIR, J., ANWER, T.: "Artificial intelligence and its role in near future", en *Journal of Latex Class Files*, v. 14, n. 8, 2015. https://doi.org/10.48550/arXiv.1804.01396.

SIEBER, U.: "Compliance-Programme im Unternehmensstrafrecht: ein neues Konzept von Wirtschaftskriminalität", en SIEBER, U. et al (Hrsg.), *Strafrecht und Wirtschaftsstrafrecht – Dogmatik, Rechtsvergleich, Rechtstatsachen: Festschrift für Klaus Tiedemann zum 70. Geburtstag,* Köln, 2008.

SOUSA, S. A.: ""Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal*, Coimbra, 2020.

SOUSA, S. A., *Questões fundamentais de direito penal da empresa*, Coimbra, 2019.

SUÁREZ XAVIER, P. R.: *Reconocimiento facial y policía predictiva: entre seguridad y garantías procesales,* A Coruña, 2022.

TEDH: *Case of Bărbulescu v. Romania*, 05/09/2007.

TEDH: *Case of Copland v. United Kingdom*, 03/04/2007.

TEIXEIRA, R.: "Meritíssima, a culpa não é minha! Imputação de responsabilidade penal por danos provocados por veículos autónomos", en RODRIGUES, A. M. (coord.), *A inteligência artificial no direito penal*, volume II, Coimbra, 2022.

THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE: *A Definition of AI: Main Capabilities and Scientific Disciplines: Definition Developed for the Purpose of the Deliverables of the High-Level Expert Group*, Brussels, 2018.

TIEDEMANN, K.: "El concepto de derecho economico, de derecho penal economico y de delito económico" en *Revista Chilena de Derecho*, v. 10, n. 1, 1983.

TORRÃO, F.: *Societas delinquere potest?: da responsabilidade individual e colectiva nos "crimes de empresa",* Coimbra, 2010.

UNITED KINGDOM HOUSE OF LORDS: *Tesco Supermarkets Ltd. v. Nattrass*, 1971.

UNITED STATES DEPARTMENT OF TRANSPORTATION, NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION – NHTSA: *Automated Vehicles for Safety.* https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety. Accedido en 31 de octubre de 2022.

VALLS PRIETO, J.: *Inteligencia artificial, derechos humanos y bienes jurídicos*, Cizur Menor, 2021.

VALLS PRIETO, J.: *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*, Madrid, 2017.

VIVES ANTÓN, T. S.: *Fundamentos del sistema penal*, 2. ed., Valencia, 2011.

WIMMER, M.: "Inteligência Artificial, Algoritmos e o Direito: Um Panorama dos Principais Desafios", em LIMA, A. P. C., HISSA, C. B., SALDANHA, P. M. (eds), *Direito Digital: Debates Contemporâneos*, São Paulo, 2019.

YAPO, A.. WEISS, J.: "Ethical Implications of Bias in Machine Learning", en *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018. https://doi.org/10.24251/hicss.2018.668.

ZUÑIGA RODRÍGUEZ, L.: *Bases para un modelo de imputación de responsabilidad penal a las personas jurídicas*, Navarra, 2000.