IUS ET SCIENTIA

Vol. 9 • Nº 2 ▪ 2023

ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA

IUS ET SCIENTIA

2023 • Vol. 9 • Nº 2 • ISSN 2444-8478

https://editorial.us.es/es/revistas/ius-et-scientia

https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

EQUIPO EDITORIAL

IUS ET SCIENTIA

2023 • Vol. 9 • Nº 1 • ISSN 2444-8478

https://editorial.us.es/es/revistas/ius-et-scientia

https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

IUS ET SCIENTIA. Vol. 9, Nº 2, diciembre (2023)

Edita: Editorial de la Universidad de Sevilla.

https://editorial.us.es/es/revistas/ius-et-scientia

https://institucional.us.es/iusetscientia/index.php/ies/index

Financiación: Revista financiada por la Universidad de Sevilla dentro de las ayudas del VII PPIT-US

Periodicidad Bianual (Junio, diciembre)

ISSN: 2444-8478

DOI: https://dx.doi.org/10.12795/IETSCIENTIA.2023.i02

Maquetación: Referencias Cruzadas - referencias.maquetacion@gmail.com

IUS ET SCIENTIA
2022 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

Índice

Comentarios

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 4-6
ISSN 2444-8478 •

Reseña de libros

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 4-6
ISSN 2444-8478 •

6

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

CARTA DE LOS EDITORES

EDITORS´ LETTER

Daniel García San José
Fernando Llano Alonso
César Villegas Delgado

El derecho a la intimidad en la sociedad de la vigilancia

En el año 2006 la Universidad de Edimburgo publicó un informe titulado: *The Surveillance Society*, firmado por Kirstie Ball y David Murakami Wood. Cuando ambos autores acuñaron el término "sociedad de la vigilancia" se referían a un modelo de sociedad organizado y estructurada por los gobiernos de los Estados, grandes compañías y organizaciones internacionales a través de la vigilancia tecnológica. Con las técnicas de videovigilancia se registran una ingente cantidad de datos e información sobre nuestros movimientos y actividades.

La necesidad de encontrar un fino equilibrio entre el derecho a la intimidad y los sistemas de alto riesgo de IA, como las técnicas de reconocimiento biométrico y de videovigilancia, fue, precisamente, uno de los grandes escollos que hubo que sortearse, con audacia y determinación, por parte de los negociadores del Parlamento Europeo y del Consejo, para llegar a un acuerdo sobre la Ley de Inteligencia Artificial, el 8 de diciembre de 2023.

Como señala Carissa Véliz en un libro publicado recientemente: *The Ethics of Privacy and Surveillance* (OUP, 2024), para que la vigilancia sea moralmente aceptable, es decir, para que pueda considerarse legítima dentro de un Estado de Derecho, deben observarse en el uso de las técnicas de vigilancia a la ciudadanía los principios de necesidad y proporcionalidad. En este sentido, sostiene esta autora, "siempre que se implanta la vigilancia (incluso cuando está justificada), surgen de ella sucesivas oleadas de deberes, porque se están incumpliendo los deberes de proteger el derecho a la intimidad. Estos nuevos deberes incluyen informar a los objetivos de la vigilancia (a menos que una investigación penal requiera el secreto temporal), mantener los datos seguros, eliminar los datos sensibles lo antes posible y minimizar los posibles daños de la vigilancia".

El presente número de nuestra revista, 2/2023, está dedicado al estudio de los riesgos y peligros que pueden de los excesos en el uso de la seguridad y la vigilancia en la sociedad de las nuevas tecnologías, y muy en particular, en el impacto que éstos puedan causar en los derechos y libertades de los ciudadanos.

El apartado de doctrina cuenta con nueve artículos en el que se abordan temas tan variados como la aplicación de la IA en la cooperación judicial penal internacional (Leticia Fontestad

Portalés); la captación de imágenes en lugares públicos sin autorización judicial (Manuel Díaz Martínez); un estudio criminológico sobre la inseguridad en las áreas rurales a partir del uso de herramientas TIC (Jordi García Ortiz et al.); la regulación del mercado de los criptoactivos en el reglamento MiCa (María de los Ángeles Pérez Marín); ¿el derecho o el deber? de los ciudadanos de relacionarse por medios electrónicos con las Administraciones Públicas, a la luz de los arts. 14 y 68 de la LPACAP (María Luisa Domínguez Barragán); el análisis de la Directiva Europea y el Reglamento que contiene las Órdenes europeas de Producción y Conservación de pruebas electrónicas (Carmen Cuadrado Salinas); la tecnología Blockchain y sus implicaciones procesales en materia probatoria (Andrea Martín Meneses); el uso de la IA generativa en la investigación de la ciberdelincuencia de género (Irene González Pulido) y, por último, el análisis de la gestión del riesgo transnacional digital por parte de la Unión Europea (Juan Ignacio Leo-Castela).

La sección de comentarios se compone de tres artículos de temática miscelánea relacionada con la revolución tecnológica 4.0: en el primer estudio, Madaoui Nadjia, analiza el rol de la IA en la lucha contra el ciber-terrorismo; en el segundo trabajo, del que son autores Diego Borbón et al., se lleva a cabo un estudio crítico sobre la Ley Modelo sobre Neuroderechos promulgada por el Parlamento Latinoamericano y Caribeño (Parlatino); finalmente, José Antonio Breceda Pérez et al., examinan los múltiples riesgos y desafíos que entrañan para el derecho garantizar la dignidad humana frente al uso abusivo de la ciencia y la tecnología.

El presente número de *Ius et Scientia* 2/2023 se cierra con dos recensiones a dos libros recientes de F. Bueno de Mata y M. J. Pérez Estrada realizadas, respectivamente, por Celia Carrasco Pérez y Francisco Javier Fernández Galarreta.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 7-8
ISSN 2444-8478 •

ARTÍCULOS

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

Consideraciones acerca de la aplicación de la IA en la cooperación judicial penal internacional*

CONSIDERATIONS ON THE APPLICATION OF THE IA IN INTERNATIONAL JUDICIAL COOPERATION IN CRIMINAL MATTERS

Leticia Fontestad Portalés
Catedrática (A) Derecho Procesal
Universidad de Málaga
Consejera Académica GUERRERO ABOGADOS
lfp@uma.es 0000-0001-5382-7990

Recibido: 3 de noviembre de 2023 | Aceptado: 6 de diciembre de 2023

RESUMEN

El estudio acerca del impacto de los sistemas de inteligencia artificial en el ámbito de la Administración de Justicia no es, en absoluto, una cuestión novedosa. Como tampoco lo es hablar hoy en día de la digitalización de la cooperación judicial penal internacional. Es por ello por lo que, partiendo de la consolidación del uso de las nuevas tecnologías para el intercambio de información entre las autoridades judiciales y policiales en relación con investigaciones penales transfronterizas, nos adentramos en la incidencia de las nuevas soluciones de inteligencia artificial en este ámbito de la cooperación entre Estados.

PALABRAS CLAVE

Cooperación judicial penal internacional
Inteligencia artificial
Digitalización de la justicia

ABSTRACT

The study of the impact of artificial intelligence systems in the field of the administration of justice is by no means a new issue. Nor is talking about the digitisation of international judicial cooperation in criminal matters. This is why, based on the consolidation of the use of new technologies for the exchange of information between judicial and police authorities in relation to cross-border criminal investigations, we will examine the impact of new artificial intelligence solutions in this area of cooperation between States.

KEYWORDS

International judicial cooperation in criminal matters
Intelligence systems
Digitisation of justice

* Este trabajo de investigación es resultado del Proyecto de investigación "Algoritmización de la Justicia Penal" – convocatoria 2022 – Modalidad B – IDP – Observatorio de Derecho Público de la Universitat de Barcelona, siendo Investigador Principal el Dr. VALLESPÍN PÉREZ; así como de los Proyectos estratégicos "Transición Digital de la Justicia" orientado a la transición ecológica y a la transición digital del Plan Estatal de investigación científica, técnica y de innovación 2021-2023, en el marco del Plan de Recuperación, Transformación y Resiliencia,

I. Introducción

Son muchas las reflexiones, críticas y estudios que a lo largo de los últimos años han realizado los expertos en torno a los beneficios y los inconvenientes del uso de las nuevas tecnologías y, concretamente, del uso de sistemas basados en la Inteligencia Artificial en el ámbito de la Administración de Justicia. Nos encontramos, por tanto, ante una cuestión que, sin ser ni mucho menos novedosa, genera y continuará generando polémica a lo largo de los próximos tiempos.

Las razones por las que el uso de sistemas de inteligencia artificial provoca rechazo desde un punto de vista jurídico, entre otras razones, como de todos es sabido, por la ausencia de una regulación normativa suficiente que garantice la protección de los Derechos humanos[1] y los Derechos Fundamentales[2] de los ciudadanos (Guerrero Palomares 2021: 151-186). En nuestro caso, además, la principal preocupación como procesalistas entre otras muchas cuestiones, es la protección de los derechos fundamentales en el ámbito procesal, esto es, el derecho fundamental a la tutela judicial efectiva que reconoce nuestra Constitución en el artículo 24. Derecho a la tutela judicial efectiva, por otra parte, que, como afirma MARTIN DIZ, desde hace casi una década "... evoluciona hacia una nueva versión, más integradora, del mismo: el derecho a la tutela efectiva de la Justicia" (Martín Diz 2014:161-176)[3].

La preocupación acerca de una normativa que regule el uso de la inteligencia artificial, en adelante IA, no es, lógicamente, exclusiva de nuestro país, ni de cada uno de los países desde un punto de vista nacional, esto es, individual, sino que a la vista de la evolución de este tipo de sistemas inteligentes en una sociedad moderna que se caracteriza, como todos sabemos, por la globalización y, en lo que a nosotros nos interesa, por la criminalidad transfronteriza, no cabe duda alguna, que se trata de una cuestión necesitada de regulación normativa en un contexto global.

El uso de sistemas de IA en el ámbito judicial y, concretamente, en el ámbito de la cooperación judicial penal, ha dejado de ser ciencia ficción hace años por lo que,

Ministerio de Ciencia e Innovación, financiado por la Unión Europea: Next Generation UE, con REF. RED 2021-130078B-100, siendo los IPs, la Dra. CALAZA LÓPEZ y el Dr. JOSÉ CARLOS MUINELO COBO y "Marco jurídico para la competencia dinámica en mercados digitales y para la innovación a través de Inteligencia Artificial" (REF. PID2021-122536OB-I00 MCIN/AEI/10.13039/501100011033. "NextGenerationEU"/PRTR), siendo el IP. el Dr. OLMEDO PERALTA.

1. *Vid*. Declaración Universal de los Derechos Humanos adoptada por la Asamblea General de las Naciones Unidas, París, 10 de diciembre de 1948. Resolución 217 A (III). Disponible en https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf (último acceso, 10.09.2023).

2. *Vid*. Título I de la Constitución Española, en adelante CE, rubricado *De los derechos y deberes fundamentales,* en cuya Sección 1º relativa a los derechos fundamentales y libertados públicas, se protegen, entre otros, y sin ánimo de exhaustividad, el derecho a la intimidad, a la inviolabilidad del domicilio, a la protección de datos, al secreto comunicaciones personales, etc. Específicamente, el artículo 18. 4 CE garantiza la limitación normativa en el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

3. Sobre el derecho a la tutela judicial efectiva desde una perspectiva clásica, De la Oliva Santos 1980; Díez-Picazo 1987: 41-49; Cordon Moreno 2004: 213-244. En relación con la futura Ley orgánica de Derecho de Defensa, resulta de interés Calaza López y De Prada Rodríguez 2023.

qué duda cabe que, en este momento más que nunca, resulta patente la necesidad de marcos regulatorios que garanticen que estas tecnologías emergentes beneficiarán a la humanidad en su conjunto. Así, como primer instrumento normativo mundial sobre la materia, desde la UNESCO, el 23 de noviembre de 2021, se aprobó la Recomendación sobre la ética de la inteligencia artificial[4].

Que evoquemos en este momento la ausencia de regulación normativa que garantice tanto a nivel individual –en cada Estado– como europeo o internacional, no implica el desconocimiento de las diferentes normativas que a lo largo de estos años han visto la luz en un intento de garantizar un uso ético y responsable de la IA tanto en los sistemas judiciales de cada Estado como en lo que se refiere a sus relaciones con otros países, esto es, en relación con la cooperación judicial internacional. Así, baste recordar la Carta Europea sobre el Uso Ético de la Inteligencia Artificial en los Sistemas Judiciales y su Entorno[5] y, con una finalidad armonizadora, la 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 Europea cuyos objetivos, entre otros, persiguen garantizar la seguridad jurídica para facilitar la inversión e innovación en IA, así como mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA[6]. Sin olvidarnos, por supuesto, del Libro Blanco de la UE sobre IA del año 2020[7] (De Hoyos Sancho 2020:9-44) y de la Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital, también del año 2020[8].

En España, debemos resaltar la más reciente Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación[9] que introduce la primera regulación positiva

4. Disponible en https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa (último acceso, 10.09.2023).

5. Adoptada por el CEPEJ en Estrasburgo, 3–4 de diciembre de 2018 (CEPEJ (2018) 14). Disponible en https://protecciondata.es/wp-content/uploads/2021/12/Carta-Etica-Europea-sobre-el-uso-de-la-Inteligencia-Artificial-en-los-sistemas-judiciales-y-su-entorno.pdf (último acceso, 10.09.2023). *Vid*. anteriormente, en el ámbito de la Unión Europea, el Reglamento general de protección de datos (Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DOUE L 119 de 4 de mayo de 2016).

6. Bruselas, 21 de abril de 2021 (COM (2021) 206 final). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206 (último acceso, 10.09.2023). Sobre la propuesta de Ley de inteligencia artificial, *Vid*. Informe del Parlamento Europeo de junio de 2023, disponible en https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (último acceso, 29.10.2023).

7. Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza (Bruselas, 19 de febrero de 2020. COM (2020) 65 final). Disponible en https://op.europa.eu/es/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1 (último acceso, 10.09.2023).

8. Bruselas, 21 de octubre de 2020 (disponible en https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/es/pdf, último acceso, 30.10.2023).

9. BOE núm. 167, de 13 de julio de 2022.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

de la inteligencia artificial en España[10] y, cómo no, la Carta de Derechos Digitales, con la que se pretende situar a España "a la vanguardia internacional en la protección de derechos de la ciudadanía"[11].

Unos días antes de iniciar este trabajo de investigación, como consecuencia de la Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes, así como en cumplimiento de lo previsto en el Plan de Recuperación, Transformación, y Resiliencia[12], se ha aprobado el Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial[13] adscrita al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Sin embargo, "La inteligencia artificial no está siendo desarrollada por los Gobiernos, sino sobre todo por las empresas privadas. Si finalmente esa tecnología, en esas condiciones, se acaba por introducir, como se espera, en el sector de los tribunales, existe el riesgo de que las instituciones democráticas pierdan, al menos en parte, el control sobre la jurisdicción en beneficio de alguna o algunas de esas empresas" (Nieva Fenoll, 2023:1).

Especial relevancia, en el contexto de este trabajo, presenta, como veremos a continuación, la Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales[14].

Dado que no somos expertos en cuestiones tecnológicas y, por ello, no nos atreveremos a explorar, ni siquiera de forma somera, el funcionamiento en sí de estos sistemas de inteligencia artificial, partiremos de la definición que sobre sistemas de IA

10. El Artículo 23 que regula la Inteligencia Artificial y mecanismos de toma de decisión automatizados establece que:
    1. En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales (LA LEY 16317/2021) y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.
    2. Las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos.
    3. Las administraciones públicas y las empresas promoverán el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido. Sobre el uso ético de la inteligencia artificial en el ámbito jurisdiccional.
    4. Se promoverá un sello de calidad de los algoritmos".
11. Disponible en https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (último acceso, 10.09.2023).
12. Disponible en https://planderecuperacion.gob.es/ (último acceso, 10.09.2023).
13. BOE núm. 210, de 2 de septiembre de 2023.
14. P9_TA (2021) 0405. Disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.pdf (último acceso, 10.09.2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

ofrece la propuesta de Ley de inteligencia artificial de la Unión Europea, según la cual, se entiende por Sistema de inteligencia artificial (sistema de IA) aquel "software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa"[15].

II. La investigación penal y la inteligencia artificial en el ámbito de la cooperación judicial penal internacional

Qué duda cabe que la armonización normativa sobre el uso de los sistemas de IA en el ámbito judicial deriva en una mayor eficacia de la cooperación policial y judicial transfronteriza (De Hoyos Sancho 2021). De ahí la relevancia de la mencionada propuesta de Reglamento del Parlamento europeo y del Consejo para establecer reglas armonizadas en materia de Inteligencia Artificial y, especialmente, en lo que a nosotros nos interesa, con relación al régimen relativo al uso de los sistemas de IA en la función tanto policial como jurisdiccional (Bujosa Vadell 2022a: 43-73).

La Unión Europea, tras las últimas enmiendas en el Parlamento, introduce un nuevo artículo 4 bis, que regula los *Principios generales aplicables a todos los sistemas de IA*[16]*:*

a) Intervención y vigilancia humanas»: los sistemas de IA se desarrollarán y utilizarán como una herramienta al servicio de las personas, que respete la dignidad humana y la autonomía personal, y que funcione de manera que pueda ser controlada y vigilada adecuadamente por seres humanos.
b) Solidez y seguridad técnicas»: los sistemas de IA se desarrollarán y utilizarán de manera que se minimicen los daños imprevistos e inesperados, así como para que sean sólidos en caso de problemas imprevistos y resistentes a los intentos de modificar el uso o el rendimiento del sistema de IA para permitir una utilización ilícita por parte de terceros malintencionados.
c) Privacidad y gobernanza de datos»: los sistemas de IA se desarrollarán y utilizarán de conformidad con las normas vigentes en materia de privacidad y protección de datos, y tratarán datos que cumplan normas estrictas en términos de calidad e integridad.
d) Transparencia»: los sistemas de IA se desarrollarán y utilizarán facilitando una trazabilidad y explicabilidad adecuadas, haciendo que las personas sean conscientes de que se comunican o interactúan con un sistema de IA, informando debidamente

15. *Vid*. artículo 3, 1) de la propuesta de Ley de inteligencia artificial. Sobre la necesidad de regular una definición de IA, el Comité Económico y Social Europeo, en año 2017, en el "Dictamen sobre la inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital)", declaraba, en la segunda conclusión, que no existía una definición concreta y aceptada de la inteligencia artificial. *Cfr*. Dictamen del Comité Económico y Social Europeo sobre la «Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad» (DOUE C 288 de 31 de agosto de 2017). Sobre la IA desde una perspectiva jurídica, Dolz Lago 2022.

16. Disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.html (último acceso, 12.10.2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

a los usuarios sobre las capacidades y limitaciones de dicho sistema de IA e informando a las personas afectadas de sus derechos.

e) Diversidad, no discriminación y equidad»: los sistemas de IA se desarrollarán y utilizarán incluyendo a diversos agentes y promoviendo la igualdad de acceso, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los efectos discriminatorios y los sesgos injustos prohibidos por el Derecho nacional o de la Unión.

f) Bienestar social y medioambiental»: los sistemas de IA se desarrollarán y utilizarán de manera sostenible y respetuosa con el medio ambiente, así como en beneficio de todos los seres humanos, al tiempo que se supervisan y evalúan los efectos a largo plazo en las personas, la sociedad y la democracia".

Asimismo, para los sistemas de IA de alto riesgo, los proveedores o implementadores, se prevé la aplicación y cumplimiento de los citados principios generales atendiendo a los requisitos establecidos en los artículos 8 a 15 del presente Reglamento junto a las obligaciones pertinentes a las que hace referencia el capítulo 3 del título III del mismo.

Igualmente, para los supuestos de los modelos fundacionales, los proveedores o implementadores de los sistemas de IA tendrán que aplicar y cumplir los mencionados principios generales en función de los requisitos a los que hace referencia los artículos 28 a 28 ter del mismo Reglamento.

Según el artículo 4 bis apartado 2, *in fine*, del Reglamento "Para todos los sistemas de IA, la aplicación de los principios a los que se hace referencia en el apartado 1 puede conseguirse, según proceda, a través de las disposiciones del artículo 28 o el artículo 52 o de la aplicación de las normas armonizadas, especificaciones técnicas y códigos de conducta a los que hace referencia el artículo 69, sin crear nuevas obligaciones en virtud del presente Reglamento".

En este sentido, la doctrina –sin ser contrarios al uso de los sistemas de inteligencia artificial en el ámbito judicial y, concretamente, en el de la cooperación judicial penal internacional– son unánimes al afirmar que, en todo caso, el uso de la IA debe respetar las siguientes premisas a las que, expresamente, alude y analiza DE HOYOS SANCHO (De Hoyo Sancho 2020: 32-39):

- Regulación normativa previa que determine el ámbito de aplicación y los procedimientos para el uso de estos sistemas IA. En lo que a nosotros concierne, en relación con el uso de herramientas de IA como apoyo a la función policial y jurisdiccional.
- Armonización normativa sobre el uso de algoritmos por las autoridades jurisdiccionales en el ámbito de la Unión Europea.
- Se debe llevar a cabo un control previo de la legalidad o admisibilidad del concreto algoritmo y del tratamiento de los datos que procesa el sistema IA. Supervisión de su aplicación y funcionamiento.
- Control humano —del juez— en la adopción de la decisión final —resolución jurisdiccional en sentido estricto—.
- Transparencia e imparcialidad de los sistemas IA, sin sesgos ni discriminaciones.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

2.1. De la digitalización al uso de la IA en la investigación penal: instrumentos de cooperación judicial internacional

Como afirmaba ya hace unos años la profesora CALAZA LÓPEZ, España se encuentra a la vanguardia europea en cuanto al uso de los nuevos métodos tecnológicos en el proceso penal (Calaza López 2021: 171-1; Dalia 2022: 251-275), sin embargo, y aunque todos somos conocedores del incremento en el uso de las nuevas tecnologías en apoyo a la investigación judicial y penal en el proceso penal (Lara López 2022: 277-307), así como en los diferentes instrumentos de cooperación judicial internacional, nos encontramos en un momento de tránsito desde la digitalización de la Justicia a la, en palabras de BARONA VILAR, "Justicia orientada al dato" (Barona Vilar 2023)[17].

Efectivamente, poca sorpresa causa ya la celebración de un juicio a través de la videoconferencia o el uso de otros muchos recursos digitales para el desarrollo de los procesos judiciales tanto nacionales como de carácter transfronterizo.[18]. Igualmente, en la actualidad, estos mismos recursos digitales están presente en la mayoría de los instrumentos de cooperación judicial entre los Estados[19] (Fontestad Portalés 2022a: 239-268; Jiménez López 2021:187-224. Así, para el intercambio de datos y material probatorio, en el ámbito de la Unión Europea, se utiliza el sistema e-Codex[20] que, como instrumento de comunicación de la justicia electrónica mediante el intercambio de datos en línea, se ha convertido en la piedra angular digital de la cooperación judicial de la UE. Sistema informatizado para el intercambio electrónico transfronterizo de datos que servía, incluso antes de la aprobación del Reglamento de la Unión Europea que lo regula, como soporte para el sistema digital de intercambio de pruebas electrónicas, así como para los intercambios en relación con las órdenes europeas de investigación y la asistencia judicial mutua en el ámbito de la cooperación judicial en materia penal[21].

Igualmente, en el ámbito iberoamericano de los países miembros de IberRed[22], se conforman nuevos sistemas electrónicos de transmisión con vistas, además, a su implantación

17. Sobre el "Big Data Judicial" se puede consultar la obra de Bueno de Mata 2020 y sobre la justicia digital y la eficiencia judicial, Suárez Xavier 2023a: 161-182.

18. Sobre el proceso de digitalización en la cooperación judicial penal en el ámbito de la Unión Europea se puede consultar Fontestad Portalés 2022b: 29-56; Bueno Jiménez 2022: 57-68. Resulta de especial interés la lectura de la obra Martín Ríos 2022: 391-406.

19. Sobre SITEL y otros sistemas en el ámbito de las comunicaciones interceptadas al amparo de la orden europea de investigación, *Vid*. López Gil 2021.

20. *E-Justice Communication via Online Data Exchange*, regulado en el Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a un sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal (sistema e-CODEX), y por el que se modifica el Reglamento (UE) 2018/1726 (DOUE L 150 de 1.6.2022).

21. Sobre el uso de métodos tecnológicos en el ámbito de la cooperación judicial en materia penal, *Vid*. Bujosa Vadell 2022b: 69-97; Bueno De Mata 2021a: 19-48; Perlingeiro y Faza 2022: 99-122; Flórez Álvarez 2021: 83-108 y Pérez Tortosa 2022: 231-248. También resulta de interés la obra de Vallespin Pérez 2023:13-22.

22. La propia institución iberoamericana de Cooperación Jurídica afirma que "La Red Iberoamericana de Cooperación Jurídica Internacional, IberRed, es una estructura formada por Autoridades Centrales

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

desde un punto de vista internacional, como es la Plataforma Iber@ para la transmisión de solicitudes de cooperación jurídica internacional entre Autoridades Centrales[23] (Fontestad Portalés 2021: 109-150).

Se trata ahora, por tanto, de dar un paso más dedicando la inteligencia artificial a lograr una mayor eficacia en materia de cooperación judicial penal internacional, no ya usando plataformas electrónicas para la comunicación, notificación e, incluso, intercambio de material probatorio, sino para determinar mediante sistemas de inteligencia artificial, por ejemplo, cómputos temporales; redactar o, incluso, traducir documentos legales de forma automática por voz, remisión de Órdenes Europeas Detención o de protección, etc.

Obviamente, y aun cuando todavía no haya entrado en vigor, no podemos dejar de lado y, al menos, mencionar la clasificación que de los sistemas de inteligencia artificial prevé, con carácter general, la citada propuesta de Ley de inteligencia artificial en función, como todos sabemos, del riesgo, atendiendo a aquellos que denomina de riesgo inaceptable[24], alto riesgo[25], riesgo limitado y riesgo mínimo o nulo. Sin olvidar, la referencia expresa a la inteligencia artificial generativa[26].

---

y por puntos de contacto procedentes de los Ministerios de Justicia, Fiscalías y Ministerios Públicos, y Poderes Judiciales de los 22 países que componen la Comunidad Iberoamericana de Naciones, así como por el Tribunal Supremo de Puerto Rico. Está orientada a la optimización de los instrumentos de asistencia judicial civil y penal, y al reforzamiento de los lazos de cooperación entre nuestros países. Constituye, así, un paso fundamental en la conformación de un Espacio Judicial Iberoamericano, entendido como un escenario específico donde la actividad de cooperación jurídica sea objeto de mecanismos reforzados, dinámicas e instrumentos de simplificación y agilización en la consecución de una tutela judicial efectiva" (Disponible en https://www.iberred.org/ (último acceso, 10.09.2023).

23. La Plataforma Iber@ se aprueba en el Tratado de Medellín, en la XXI Asamblea Plenaria de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB). A su vez, COMBIJ fue creada en 1992, por el Tratado de Madrid, para el estudio y promoción de formas de cooperación jurídica entre los Estados miembros y consiste en una organización internacional de carácter intergubernamental de la que forman parte los Ministerios de Justicia e instituciones homólogas de los 22 países de la Comunidad Iberoamericana. Para más información sobre esta organización internacional se puede consultar https://comjib.org/comjib/ (último acceso, 10.10.2023).

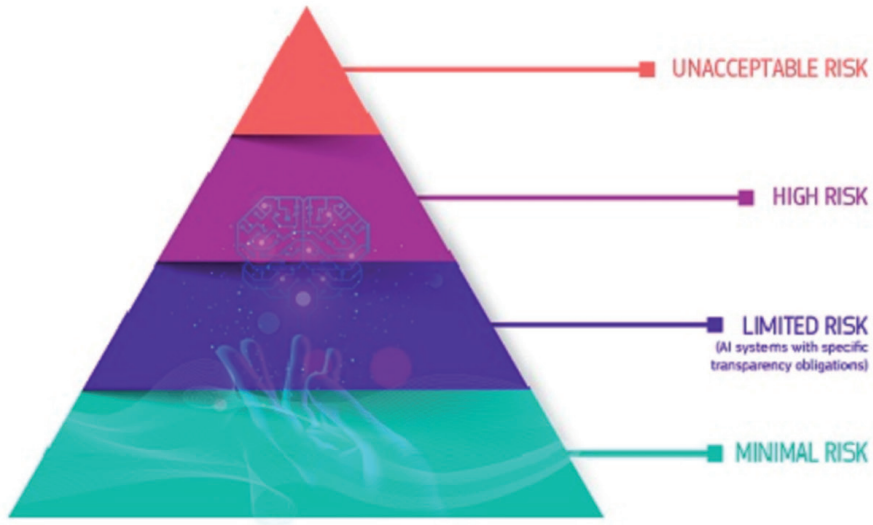
24. Los Considerando número 10 y 14 de la propuesta de Ley de inteligencia artificial afirman, respectivamente, que "Con vistas a que la Unión permanezca fiel a sus valores fundamentales, los sistemas de IA destinados a utilizarse para prácticas consideradas inaceptables por el presente Reglamento también deben considerarse inaceptables fuera de la Unión debido a su efecto especialmente perjudicial para los derechos fundamentales consagrados en la Carta. Procede, por tanto, prohibir a los proveedores residentes en la Unión que exporten tales sistemas de IA a terceros países".

Asimismo, "…es necesario prohibir determinadas prácticas de inteligencia artificial inaceptables, definir los requisitos que deben cumplir los sistemas de IA de alto riesgo y las obligaciones aplicables a los operadores pertinentes, e imponer obligaciones de transparencia a determinados sistemas de IA". *Vid*. Título II de la citada propuesta de Ley de Inteligencia artificial que, en su único artículo 5, determina las prácticas de inteligencia artificial que se considerarán prohibidas.

25. En el Considerando número 27 de la propuesta de Ley de inteligencia artificial se determina que "La calificación «de alto riesgo» debe limitarse a aquellos sistemas de IA que tengan consecuencias perjudiciales importantes para la salud, la seguridad y los derechos fundamentales de las personas de la Unión, y dicha limitación reduce al mínimo cualquier posible restricción del comercio internacional, si la hubiera. Habida cuenta del rápido ritmo del desarrollo tecnológico, así como de los posibles cambios en el uso de los sistemas de IA, la lista de ámbitos y casos de uso de alto riesgo que figura en el anexo III debe someterse, no obstante, a una revisión permanente mediante el ejercicio de evaluaciones periódicas". No

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

Gráfico 1.



El marco regulador define cuatro niveles de riesgo en la IA:

- Riesgo inaceptable
- Alto riesgo
- Riesgo limitado
- Riesgo mínimo o nulo

Fuente: Comisión Europea

obstante, a su vez, debemos advertir que la propia propuesta de Ley establece cuáles son las reglas para la clasificación de los sistemas de inteligencia artificial de alto riesgo en el Capítulo I del Título III, concretamente en el artículo 6, según el cual, "Un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación, con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b):

a. el sistema de IA está destinado a ser utilizado como componente de seguridad de uno de los productos contemplados en la legislación de armonización de la Unión que se indica en el anexo II, o es en sí mismo uno de dichos productos;
b. conforme a la legislación de armonización de la Unión que se indica en el anexo II, el producto del que el sistema de IA es componente de seguridad, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio.

2. Además de los sistemas de IA de alto riesgo mencionados en el apartado 1, también se considerarán de alto riesgo los sistemas de IA que figuran en el anexo III".

26. *Vid*. Artículo 28 ter, apartado 4, dedicado a las obligaciones del proveedor de un modelo fundacional, según el cual, "Los proveedores de modelos fundacionales utilizados en sistemas de IA destinados específicamente a generar, con distintos niveles de autonomía, contenidos como texto, imágenes, audio o vídeo complejos («IA generativa») y los proveedores que especialicen un modelo fundacional en un sistema de IA generativo, además: a) cumplirán las obligaciones de transparencia establecidas en el artículo 52, apartado 1; b) formarán y, en su caso, diseñarán y desarrollarán el modelo fundacional de manera que se garanticen salvaguardias adecuadas contra la generación de contenidos que infrinjan el Derecho de la Unión, en consonancia con el estado de la técnica generalmente reconocido y sin perjuicio de los derechos fundamentales, incluida la libertad de expresión; c) sin perjuicio de la legislación de la Unión, nacional o de la Unión sobre derechos de autor, documentarán y pondrán a disposición del público un resumen suficientemente detallado del uso de los datos de formación protegidos por la legislación sobre derechos de autor".

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

2.2. Soluciones de inteligencia artificial en el ámbito de la cooperación judicial penal internacional

Las soluciones de IA en el ámbito de la cooperación judicial penal internacional podríamos sintetizarlas, por poner un ejemplo, atendiendo a su finalidad, en cuyo caso, encontramos, por un lado, sistemas de IA para la "automatización de determinadas medidas transnacionales". Este sería el caso de DIGALAW-X[27], que se puede usar para la redacción/traducción automática por voz de una orden europea de detención; y, por otro lado, sistemas de IA con funciones asistenciales en la investigación y enjuiciamiento de la delincuencia organizada transfronteriza, por ejemplo.

Sin ánimo de llevar a cabo una enumeración taxativa ni un estudio detallado, entre los sistemas de inteligencia artificial de aplicación en el ámbito de la cooperación judicial penal internacional podemos destacar aquellos sistemas de identificación biométrica[28] a través de los cuales se puede identificar de forma unívoca a una persona basándose en algún rasgo físico que se considere único de cada persona[29], por ejemplo, el ADN,

27. Sobre DigaLaw–X como herramienta de reconocimiento vocal "Inteligente" o sistema de traducción automática, *Vid*. https://www.digalawx.com/ (último acceso, 10.09.2023).

28. *Cloudwalk*, por ejemplo, es una plataforma de coordinación hombre-máquina que proporciona a los usuarios servicios de IA personalizados, multisectoriales y multiescena. Para más información acerca de *Cloudwalk* se puede consultar https://www.cloudwalk.com/en/ (último acceso, 29.10.2023).

29. El Reglamento general de protección de datos, en su Considerando 53, determina que "…únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física" y, en consecuencia, en su artículo 4, establece que debe entenderse por datos biométricos aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Asimismo, el artículo 9.1 del citado Reglamento, hace referencia a los datos biométricos cuando prohíbe el tratamiento de categorías especiales de datos personales, aunque en el apartado 4 del mismo precepto admite la posibilidad de que los Estados miembros puedan mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. *Vid*. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DOUE núm. 119, de 4 de mayo de 2016). *Vide*. También la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo la ley española de transposición (DOUE L 119 de 4 de mayo de 2016), así como la ley española de transposición, Ley Orgánica 7/2021, de 26 de mayo de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (BOE núm. 126, de 27 de mayo de 2021). Sobre la citada Directiva 2016/680, *Vid*. Colomer Hernández 2021: 737-782; Fiodorova 2021:709-736; Pillado González, E 2021: 783-820. En relación con la Ley 7/2021, *Vid*. Por todos, Esparza Leibar 2022: 181-210. Sobre la protección de datos en relación con los instrumentos de digitalización en el ámbito de la cooperación judicial penal internacional, así como en relación con el uso de sistemas de IA, *Vid*. Bueno De Mata 2021b; Sánchez Barrios 2022: 123-140 y Suárez Xavier 2023b: 65-72.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

la huella dactilar o, incluso, el iris de los ojos[30]. En el ámbito de la cooperación judicial penal internacional, EUROPOL[31], para reforzar la seguridad de las fronteras, ha puesto en marcha la iniciativa HOTSPOT, basada en el uso de los datos biométricos (huellas dactilares e imágenes faciales, fundamentalmente) con el objetivo de detener a los terroristas que intentan huir de la acción de la justicia atravesando fronteras[32].

Especialmente útiles para las investigaciones penales son los sistemas de inteligencia artificial que permiten elaborar mapas criminales con identificación de los denominados *hotspots*, esto es, puntos geográficos en los que existe un elevado índice de delincuencia[33]. En esta línea, como instrumento de vigilancia predictiva, podemos hacer referencia a *PredPol*[34] como herramienta basada en inteligencia artificial que se utiliza, desde hace unos años, en Estados Unidos[35]. Asimismo, en relación con instrumentos

30. Sobre la posible vulneración del derecho a la protección de datos personales que, como de todos es sabido, ha sido reconocido en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea como un derecho independiente del derecho a la vida privada y familiar, así como para un exhaustivo estudio sobre el tratamiento de los datos personales en un proceso penal, *Vid*. Colomer Hernández 2023: 39-74. Igualmente, se puede consultar Martin Diz 2021: 969-1006; Villar Fuentes 2019: 399-441 y Marcos González 2021: 225-260.

31. *Vid*. Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DOUE L 135 de 24 de mayo de 2016).

32. Más información sobre la iniciativa HOTSPOT, así como de las diferentes operaciones que en este sentido ha venido desarrollando Europol desde 2019 a 2022, se pueden consultar en https://www.interpol.int/es/Delitos/Terrorismo/Proyectos-de-lucha-contra-el-terrorismo/HOTSPOT (último acceso, 29.10.2023).

33. Sobre la aplicación de la inteligencia artificial al proceso penal en general, *Vid*. Hernández Giménez 2019: 792-843 y, en particular, sobre las nuevas tecnologías para la elaboración de mapas criminales: 816-817. En relación con la Justicia predictiva aplicada al proceso judicial en materia probatoria, *Vid*. Martin Diz 2022: 134-154 y Llorente Sánchez-Arjona 2022: 91-124. Sobre los riesgos que generan los sistemas de policía predictivas en el ámbito del terrorismo, *Vid*. Suárez Xavier 2022.

34. Más información acerca del funcionamiento de *Predpol* se puede encontrar en su portal web: https://www.predpol.com/ (último acceso, 30.10.2023). En España, el primer programa español de crimen predictivo ha sido desarrollado por la empresa EuroCop Security Systems junto al Ayuntamiento y la Policía Local de Castellón, en colaboración con la Universidad Jaume I de Castellón. Se trata de un sistema para la Predicción y Prevención del Delito, denominado *EuroCop Pred-Crime*, que consiste en sistema integrado de tratamiento de datos masivos vinculados a delitos y faltas; se basa en un modelo espacio-temporal e información geográfica de mapas de calor que usa modelos y algoritmos matemáticos para la predicción y prevención de los delitos. Para más información, se puede visitar su página web, https://www.eurocop.com/sistemas-de-eurocop/analisis-y-prediccion-del-delito/ (último acceso, 30.10.2023). Otras herramientas de inteligencia artificial en el ámbito de la investigación penal, ya sean herramientas predictivas al servicio de la policía o herramientas de "evaluación de riesgo" al servicio de la autoridad judicial, serían –sin ánimo de exhaustividad– STEVIE; Pronóstico policial del lugar del crimen (PDLC) o, el más conocido y a la par controvertido, COMPAS, cuya guía práctica podemos encontrar en https://www.equivant.com/wp-content/uploads/Practitioners-Guide-to-COMPAS-Core-040419.pdf (último acceso, 30.10.2023). Sobre el uso de COMPAS en el proceso penal y sus riesgos, se puede consultar, entre otros, Roa Avella y Sanabria-Moyano 2022: 275-310. Especialmente de interés resulta la lectura de Suárez Xavier 2021y Suárez Xavier 2023c

35. Como ponía de relieve hace unos años HERNÁNDEZ GIMÉNEZ, la problemática fundamental de este tipo de herramientas tecnológicas aplicadas a la construcción de mapas criminales, es que

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

para la evaluación y predicción delictiva en España, podemos destacar VeriPol[36], para detectar denuncias falsas, así como el Sistema de Seguimiento Integral en los casos de Violencia de Género de la Secretaría de Estado de Seguridad del Ministerio del Interior[37], esto es, el Sistema VioGén[38].

Lógicamente, muchas de estas soluciones de IA a disposición tanto de las autoridades policiales como judiciales inciden, sin duda alguna, en las relaciones de cooperación judicial entre los Estados. Pensemos, por ejemplo, en instrumentos de cooperación judicial penal internacional como la orden europea de detención y entrega o en la extradición. Cuando las autoridades judiciales de ejecución tengan que decidir sobre una solicitud de detención y entrega a otro Estado miembro o, igualmente, en el caso de que en el proceso de la extradición el Estado requerido tenga que decidir sobre la extradición de la persona requerida a un tercer Estado, en ambos casos, dichas autoridades deberán analizar si el uso de herramientas de inteligencia artificial en el Estado solicitante, o requirente, en su caso, pone en riesgo el derecho fundamental a un juicio justo como consecuencia de la falta de transparencia en cuanto a la forma en la que opera la inteligencia artificial.

Son múltiples las implicaciones de la inteligencia artificial en las herramientas de cooperación judicial penal internacional, razón por la que la citada Resolución del Parlamento Europeo sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales reconociendo, no obstante, la contribución positiva de determinados tipos de aplicaciones de inteligencia artificial a la labor de las autoridades policiales y judiciales en la Unión Europea, "… considera que podrían estudiarse otros varios usos posibles de la IA para actuaciones de las

puede provocar "la estigmatización de determinadas zonas por tener estas un alto porcentaje de delincuencia, lo cual podría desembocar en prejuicios hacia los habitantes de esas zonas y consideramos que no se puede permitir que sea la propia policía la que contribuya a la discriminación de determinados grupos sociales". *Cfr*. Hernández Giménez 2019: 817.

36. Tal y como se recoge en el Portal web de la Policía Nacional, en octubre de 2018 se implementó VeriPol en todas las comisarías de España esta aplicación informática para la detección de las denuncias falsas interpuestas en casos de robos con violencia e intimidación o tirones (información disponible en https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=4433&idiomaActual=es. Último acceso, 30.10.2023).

37. Un análisis sobre otras herramientas de inteligencia artificial a disposición de los Cuerpos y Fuerzas de Seguridad del Estado se puede encontrar en Martin Ríos 2022.

38. El Sistema VioGén se puso en funcionamiento el 26 de julio del 2007, en cumplimiento de lo establecido en la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, con los objetivos de agrupar a las diferentes instituciones públicas con competencias en materia de violencia de género, así como para, entre otras funciones, llevar a cabo una predicción del riesgo y, en función del nivel de riesgo, realizar un seguimiento y dar protección a las víctimas en todo el territorio nacional. Del mismo modo, con el sistema VioGén, se pretende realizar una labor preventiva mediante la emisión de avisos, alertas y alarmas, a través del "Subsistema de Notificaciones Automatizadas", en el caso de que se detecte alguna incidencia o acontecimiento que pueda suponer un peligro para la integridad de la víctima. Información disponible en https://www.interior.gob.es/opencms/ca/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen/ (último acceso, 30.10.2023). En relación con el sistema VioGén, *Vid*. Por todos, Montesinos García 2021: 19-55; Borges Blázquez 2021; Magro Servet 2022: 397-415 y Llorente Sánchez-Arjona 2022: 371-396.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

autoridades policiales y judiciales teniendo en cuenta en el proceso los cinco principios de la Carta Ética sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno adoptados por la CEPEJ, y prestando especial atención a los «usos que han de estudiarse con la cautela más extrema», identificados por la CEPEJ"…[39].

Asimismo, la citada Recomendación afirma que todas las soluciones de IA para las autoridades policiales y judiciales "deben respetar plenamente los principios de dignidad humana, no discriminación, libertad de circulación, presunción de inocencia y derecho de defensa, incluido el derecho a guardar silencio, libertad de expresión e información, libertad de reunión y asociación, igualdad ante la ley, igualdad de armas y el derecho a una tutela judicial efectiva y a un juicio justo, de conformidad con la Carta y con el Convenio Europeo de Derechos Humanos; destaca que debe prohibirse todo uso de aplicaciones de la IA que sea incompatible con los derechos fundamentales"[40].

No cabe duda de que cualquier sistema judicial, con o sin el uso de sistemas de inteligencia artificial, debe garantizar y respetar los mencionados derechos y ello incluye, lógicamente, a las relaciones de cooperación judicial entre los Estados. Ningún instrumento de cooperación judicial penal internacional puede ser incompatible con los derechos fundamentales, ya sea con el derecho a un juicio justo, como acabamos de ver, o con el derecho a la protección de datos en atención a la cantidad de datos personales que a través de los sistemas de inteligencia artificial se pueden recopilar de forma automatizada y la posible transmisión de esos datos entre autoridades policiales y judiciales sin el requerido consentimiento de la persona afectada.

No obstante, a pesar de nuestra preocupación, como la de cualquier jurista, y casi me atrevería a decir, la de cualquier persona, acerca de las consecuencias del uso judicial –y policial– de la inteligencia artificial dada la incertidumbre que genera, en este ámbito, entre otras, la posible vulneración de los derechos fundamentales, nos planteamos si, en determinadas ocasiones, no estamos siendo más desconfiados y más exigentes con los sistemas judiciales de IA que con el juez-humano que, indudablemente, en el ejercicio de la función jurisdiccional, juzgando y haciendo ejecutar lo juzgado, también toma sus decisiones sesgado por sus principios, sus creencias y sus propios criterios. Es por ello que queremos por fin a este trabajo, a modo de reflexión, con la polémica afirmación de JAUME-PALASÍ acerca de que el derecho es un algoritmo que se aplica desde mucho antes de que existiera la informática de tal modo que cuando un juez juzga y condena en un juicio penal, también lo hace sesgado por sus propias convicciones, opiniones y aproximaciones a las diferentes teorías jurídicas[41].

39. *Vid*. Punto 4 de la Resolución del Parlamento Europeo sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales.

40. *Vid*. Punto 4 de la Resolución del Parlamento Europeo sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales.

41. *Cfr*. PASCUAL GARCÍA, A. (2020). "Inteligencia artificial y Justicia: ¿condenados a entenderse?", (disponible en https://www.unir.net/derecho/revista/inteligencia-artificial-justicia/, último acceso, 31.10.2023). En este sentido, *Vid*. BONET NAVARRO, J. (2023). "El juicio y el prejuicio por la máquina", *Revista General de Derecho Procesal*, núm. 60.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

Bibliografía

BARONA VILAR, S. (2023). "Resumen de Ecosistema digital de Justicia eficiente (De la Justicia digital orientada al documento a la Justicia orientada al dato)", *Actualidad civil*, núm. 5.

BONET NAVARRO, J. (2023), "El juicio y el prejuicio por la máquina", *Revista General de Derecho Procesal*, núm. 60.

BORGES BLÁZQUEZ, R. (2021). "Inteligencia artificial y perspectiva de género: programar, investigar y juzgar con filtro morado", *Revista General de Derecho Procesal*, núm. 55.

BUENO DE MATA, F. (2021a). "Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen", en L. Fontestad Portalés, (dir.) y M. N. Jiménez López (coord.), *La transformación digital de la cooperación jurídica penal internacional*, Ed. Aranzadi.

BUENO DE MATA, F. (2021b) "Protección de datos, investigación de infracciones penales e inteligencia artificial: novedades y desafíos a nivel nacional y europeo en la era postcovid", *La ley penal: revista de derecho penal, procesal y penitenciario*, núm. 150.

BUENO DE MATA, F. (2020). "Macrodatos, inteligencia artificial y proceso: luces y sombras", *Revista General de Derecho Procesal*, 51.

BUENO JIMÉNEZ, M. (2022). "Los Planes Estratégicos como herramientas básicas para la transformación digital del futuro (y del presente)", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Fontestad Portalés, L. (dir.); Jiménez López, M. N. (coord.), Ed. Aranzadi.

BUJOSA VADELL, L. (2022a). "Ética e inteligencia artificial: una mirada desde el proceso jurisdiccional", en *El impacto de las tecnologías disruptivas en el derecho procesal,* Ed. Aranzadi.

BUJOSA VADELL, L. (2022b). "Cooperación judicial para la obtención y transmisión de pruebas electrónicas", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Fontestad Portalés, L. (dir.); Jiménez López, M. N. (coord.), Ed. Aranzadi.

CALAZA LÓPEZ, S., y DE PRADA RODRIGUEZ, M. (2023). "Acción y Defensa en clave digital: «Dos caras de una misma moneda» y un «brindis al sol» en la inminente Ley de Derecho de Defensa", *Actualidad Civil*, num. 4.

CALAZA LÓPEZ, S. (2021). "La investigación tecnológica en el proceso penal español a la vanguardia europea", en *Estudios procesales sobre el espacio europeo de justicia penal,* J. A. Posada Pérez y M. Llorente Sánchez-Arjona (dirs.), Ed. Aranzadi.

COLOMER HERNÁNDEZ, I., (2023). "Limitaciones en el uso de la información y los datos personales en un proceso penal digital", en *El proceso penal ante una nueva realidad tecnológica europea*, Pillado González, E. y Freitas, P.M. (dirs.), Ed. Aranzadi.

COLOMER HERNÁNDEZ, I. (2021). "Control y límites en el uso de los datos personales penales en la investigación y represión de delitos a la luz de la Directiva 2016/680", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M.A. (dir.), Ed. Tirant lo Blanch.

CORDON MORENO, F. (2004). "El derecho a obtener la tutela judicial efectiva", *Manuales de formación continuada*, núm. 22 (Ejemplar dedicado a: Derechos procesales fundamentales).

DALIA, G. (2022). "El uso de la I.A. en el marco del proceso penal entre las exigencias de eficacia y las valoraciones judiciales", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Fontestad Portalés, L. (dir.); Jiménez López, M. N. (coord.), Ed. Aranzadi.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

DE LA OLIVA SANTOS, A. (1980). *Sobre el derecho a la tutela jurisdiccional: la persona ante la administración de justicia: derechos básicos,* J.M. Bosch Editor.

DÍEZ-PICAZO, L. (1987). "Notas sobre el derecho a la tutela judicial efectiva", *Poder Judicial*, núm. 5.

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

DE HOYOS SANCHO, M. (2020). "El Libro Blanco Sobre Inteligencia Artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo"", *Revista Española de Derecho Europeo*, núm. 76.

DOLZ LAGO, M.J. (2022). "Una aproximación jurídica a la Inteligencia Artificial", *Diario La Ley*, núm. 10096.

ESPARZA LEIBAR, I. (2022). "Derecho fundamental a la protección de datos de carácter personal en el ámbito jurisdiccional e inteligencia artificial. En especial la LO 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales", en *Inteligencia artificial legal y administración de justicia*, Calaza López, S. y Llorente Sánchez-Arjona, M. (dirs.), Ed. Aranzadi.

FIODOROVA, A. (2021). "Directiva 2016/680: hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M.A. (dir.), Ed. Tirant lo Blanch.

FONTESTAD PORTALÉS, L. (2022a). "Evolución y avances en materia de cooperación judicial internacional a través de las transmisiones electrónicas", en *Digitalización de la justicia: prevención, investigación y enjuiciamiento*, J. C. Muinelo Cobo (coord.); Llorente Sánchez-Arjona, M. y Calaza López, S. (dirs.), Ed. Aranzadi.

FONTESTAD PORTALÉS, L. (2022b). "La digitalización de la cooperación judicial penal en la Unión Europea", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Fontestad Portalés, L. (dir.), Jiménez López, M. N. (coord.), Ed. Aranzadi.

FONTESTAD PORTALÉS, L. (2021). "La digitalización de la cooperación jurídica internacional: la plataforma IBER@", en *La transformación digital de la cooperación jurídica penal internacional*, Fontestad Portalés, L. (dir.); Jiménez López, M. N. (coord.), Editorial Aranzadi.

FLÓREZ ÁLVAREZ, L. A. (2021). "Reflexiones sobre la innovación del ámbito probatorio en el modelo europeo de cooperación judicial en materia penal", en *La transformación digital de la cooperación jurídica penal internaciónal*, Fontestad Portalés, L. (dir.); Jiménez López, M.N., (coord.), Ed. Aranzadi.

GUERRERO PALOMARES, S. (2021). "La protección del derecho a la intimidad en el marco de la investigación tecnológica en el proceso penal", en *La transformación digital de la cooperación jurídica penal internacional,* Fontestad Portalés, L. (dir.); Jiménez López, M.N., (coord.), Ed. Aranzadi.

HERNÁNDEZ GIMÉNEZ, M. (2019). "Inteligencia artificial y derecho penal", *Actualidad Jurídica Iberoamericana*, núm. 10 bis.

JIMÉNEZ LÓPEZ, M. N. (2021). "Las medidas de investigación tecnológicas en la orden europea de investigación", en *La transformación digital de la cooperación jurídica penal internacional*, Fontestad Portalés, L. (dir.); Jiménez López, M. N. (coord.), Editorial Aranzadi.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

LARA LÓPEZ, A. M. (2022). "La captación y grabación de las comunicaciones orales mediante dispositivos electrónicos como medida de investigación tecnológica en el proceso penal", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Fontestad Portalés, L. (dir.), Jiménez López, M. N. (coord.), Ed. Aranzadi.

LLORENTE SÁNCHEZ-ARJONA, M. (2022). "Hacia una justicia penal predictiva", *Cuadernos de política criminal*, núm. 136.

LÓPEZ GIL, M. (2021). "La autenticidad de las comunicaciones interceptadas al amparo de la orden europea de investigación. SITEL versus otros sistemas", *Revista General de Derecho Procesal*, núm. 55.

MARCOS GONZÁLEZ, M. (2021). "Cesión de datos personales generados en las comunicaciones electrónicas y cooperación penal internacional", en *La transformación digital de la cooperación jurídica penal internacional*, Fontestad Portalés, L. (dir.); Jiménez López, M. N. (coord.), Editorial Aranzadi.

MARTIN DIZ, F. (2022). "Justicia predictiva: inteligencia artificial y algoritmos aplicados al proceso judicial en materia probatoria", en *El impacto de las tecnologías disruptivas en el derecho procesal,* Ed. Aranzadi.

MARTIN DIZ, F. (2021). "Inteligencia artificial y derecho procesal: luces, sombras y cábalas en clave de derechos fundamentales", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M.A. (dir.), Ed. Tirant lo Blanch.

MARTÍN DIZ, F. (2014). "Del derecho a la tutela judicial efectiva hacia el derecho a una tutela efectiva de la justicia", *Revista europea de derechos fundamentales*, núm. 23 (Ejemplar dedicado a: Tutela judicial efectiva en el siglo XXI: un análisis interdisciplinar).

MARTIN RÍOS, P. (2022). "Empleo de big data y de inteligencia artificial en el ciberpatrullaje de la tiranía del algoritmo y otras zonas oscuras", en IDP: *revista de Internet, derecho y política = revista d'Internet, dret i política*, núm. 36.

MARTÍN RÍOS, P. (2022). "Relevancia de las nuevas tecnologías en la práctica de actos de comunicación judicial transfronterizos en materia civil o mercantil", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Fontestad Portalés, L. (dir.), Editoiral Aranzadi.

MONTESINOS GARCÍA, A. (2021). "Los algoritmos que valoran el riesgo de reincidencia: En especial, el sistema Viogen", *Revista de derecho y proceso penal,* núm. 64.

NIEVA FENOLL, J. (2023). "Perder el control digital: ¿hacia una distopía judicial?", *Actualidad civil*, núm. 4.

PASCUAL GARCÍA, A. (2020). "Inteligencia artificial y Justicia: ¿condenados a entenderse?", (disponible en https://www.unir.net/derecho/revista/inteligencia-artificial-justicia/).

PÉREZ GIL, J. (2019). "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal", en *Justicia: ¿garantías versus eficiencia?*, Jiménez Conde, F. y Bellido Penadés, R. (dirs.), Ed. Tirant lo Blanch.

PÉREZ TORTOSA, F. (2022). "La propuesta de implantación de las órdenes europeas de entrega y conservación de pruebas electrónicas como instrumentos complementarios a la orden europea de investigación", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Fontestad Portalés, L. (dir.); Jiménez López, M. N. (coord.), Ed. Aranzadi.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

PERLINGEIRO, R. y FAZA, G. (2022). "Cooperación judicial internacional sobre pruebas en el derecho brasileño", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Fontestad Portalés, L. (dir.); Jiménez López, M. N. (coord.), Ed. Aranzadi.

PILLADO GONZÁLEZ, E. (2021). "Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M.A. (dir.), Ed. Tirant lo Blanch.

ROA AVELLA, M.P., y SANABRIA-MOYANO, J.E. (2022). "Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos", *Revista Brasileña de Derecho Procesal Penal*, v.8, núm. 1.

SUÁREZ XAVIER, P.R. (2023a). "Justicia digital, gobernanza y eficiencia procesal: algunos apuntes", en *Justicia en red para la Paz,* Calaza López, S. y Fontestad Portalés, L. (dirs.), Ed. Dykinson.

SUÁREZ XAVIER, P. R. (2023b) *Informe sobre aspectos bioéticos, legales y procesales del derecho a la identidad y el uso de procedimientos de reconocimiento facial por las fuerzas y cuerpos de seguridad,* Ed. Colex.

SUÁREZ XAVIER, P.R. (2023c). *Justicia predictiva: construyendo la justicia del siglo XXI*, Ed. Aranzadi.

SUÁREZ XAVIER, P.R. (2021). *Reconocimiento facial y policía predictiva: entre la seguridad y garantías procesales*, Ed. Colex.

SUÁREZ XAVIER, P. R. (2022). "Policía predictiva en el combate al terrorismo: ¿seguridad sin garantías fundamentales?", en *Justicia proceso y tutela judicial efectiva en la sociedad postpandemia*, Fontestad Portalés, L. y Jiménez López, M.N. (dirs.), Ed. Aranzadi.

VALLESPIN PÉREZ, D. (2023). "Robotización" de la valoración de la prueba en el proceso civil español", en *Inteligencia artificial y proceso: eficiencia vs. Garantías,* Vallespín Pérez, D. (dir.), Ed. Juruá.

VILLAR FUENTES, I. (2019). "Datos personales al servicio de la investigación y detección de infracciones penales", *Revista General de Derecho Procesal,* núm. 48.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 10-26
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2023.i02.01

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

La captación de imágenes en lugares públicos sin autorización judicial. La expectativa razonable de encontrarse al resguardo de la observación ajena como criterio clave

THE CAPTURE OF IMAGES IN PUBLIC PLACES WITHOUT JUDICIAL AUTHORIZATION. THE REASONABLE EXPECTATION OF BEING SHIELDED FROM THE OBSERVATION OF OTHERS AS A KEY CRITERION

Manuel Díaz Martínez
UNED
mdmartinez@der.uned.es 0000-0002-8710-3488

Recibido: 14 de junio de 2023 | Aceptado: 6 de diciembre de 2023

RESUMEN

Con el fin de dotar de la necesaria cobertura legal a determinadas medidas de investigación tecnológica absolutamente indispensables para hacer frente a una fenomenología criminal de nuevo cuño y, en definitiva, garantizar las exigencias derivadas de seguridad jurídica en el ámbito de los derechos fundamentales, la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica define las modalidades de investigación tecnológica y delimita los presupuestos, constitucionales y legales, que legitiman su adopción.

Una de las medidas que contempla es la captación de imágenes de la persona investigada en lugares o espacios públicos, que posee como singularidad respecto de las restantes la posibilidad de que sea acordada por la Policía Judicial sin necesidad de autorización judicial.

El presente estudio se centra en la determinación de lo que haya de entenderse por espacio o lugar público como premisa legitimadora de la medida, para lo cual se analiza la reciente sentencia del Tribunal Constitucional 92/2023, de 11 de septiembre, que determina que el garaje de una comunidad de propietarios no tiene tal consideración, por tratarse de un espacio que pertenece al ámbito de la intimidad protegida por el artículo 18.1 de la Constitución Española.

PALABRAS CLAVE

Investigación criminal
Nuevas tecnologías
Dispositivos técnicos de captación de la imagen
Derecho fundamental a la intimidad
Garaje

ABSTRACT

In order to provide the necessary legal coverage for certain technological investigation measures that are absolutely essential to deal with a new criminal phenomenology and, in short, to guarantee the requirements for legal security in the field of fundamental rights, Organic Law 13/2015, amending the Criminal Procedural Act, defines the modalities of technological investigation and sets out the constitutional and legal requirements that legitimize their adoption.

One such measures is the capture of images of the person under investigation in public places or spaces, which presents as unique in relation to all others the possibility of being ordered by the Judicial Police without the need for judicial authorization. The present study focuses on determining what is to be understood by public space or place as a legitimizing factor of the measure, for which the recent STC 92/2033, of September 11, is analyzed, which determines that the garage of a community of owners does not have such consideration, as it is a space that belongs to the area of the privacy protected by article 18.1of the Spanish Constitution.

KEYWORDS

Criminal Investigations
New technologies
Technical devices for image capture
Fundamental right to privacy
Garage

I. Introducción

Como consecuencia del progreso de la ciencia en el ámbito de las telecomunicaciones, casi todas las infracciones penales tienen hoy un soporte tecnológico. En este contexto, la utilización por la Policía de las modernas tecnologías constituye una herramienta de trabajo imprescindible para obtener las evidencias digitales del delito y contrarrestar los sofisticados medios de que se sirven los grupos criminales organizados, así como el carácter internacional de su actividad. La Policía debe disponer de los medios necesarios y adecuados toda vez que la eficacia de la actividad judicial probatoria se fundamenta, en última instancia, en la eficacia de la actuación policial previa.

Ello no obstante, la investigación criminal derivada del uso de estas tecnologías plantea nuevos desafíos que exigen una respuesta del legislador. Uno de ellos consiste en la necesidad de buscar un adecuado equilibrio entre la garantía de la seguridad pública y la protección de la privacidad del investigado. No puede desconocerse la intensa injerencia estatal en la esfera privada de los ciudadanos que muchas de estas medidas de investigación tecnológica conllevan. Ya en su sentencia 110/1984, de 26 de noviembre, el Tribunal Constitucional se refería al reconocimiento global de un derecho a la intimidad o a la vida privada que englobe las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida.

A lo expuesto hay que añadir la complejidad que supone la investigación de estos delitos por el reto técnico que implica el manejo de las nuevas tecnologías y que ha exigido la creación de unidades muy especializadas de investigación dentro de la Policía Judicial. Se trata de un campo sujeto a la innovación y evolución casi permanente que aporta la ciencia.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

Parece claro que la garantía del derecho a la esfera privada es uno de los grandes desafíos de los ordenamientos jurídicos en la actualidad y, por ende, también de nuestro proceso penal.

El compromiso con las libertades y la protección de los derechos de las personas en el ámbito de las sociedades democráticas, voluntariamente sometidas al imperio de la Ley, exige que el diseño y la redacción de los cuerpos normativos encargados de la regulación del ejercicio de esos derechos, y su defensa frente a las injerencias y ataques que puedan derivar de un uso incontrolado e inadecuado de las referidas medidas de investigación tecnológica, se lleve a cabo con escrupuloso respeto a las garantías del Estado de Derecho y de forma armonizada con los países de nuestro entorno.

Ahora bien, el derecho a la intimidad personal no es absoluto y, por tanto, no concede a su titular un poder omnímodo de exclusión, pues, como cualquier derecho fundamental, puede ceder ante otros derechos y bienes constitucionalmente relevantes, entre los que se encuentra el interés público en la persecución y castigo del delito, que se erige en un bien digno de protección constitucional, a través del cual se defienden otros como lo son la paz social y la seguridad ciudadana, bienes igualmente reconocidos en los artículos 10.1 y 104.1 de la Constitución Española (CE, en lo sucesivo) (SSTC 127/2000, de 12 de mayo; 292/2000, de 30 de noviembre y 14/2003, de 28 de enero)[1].

De lo anterior se desprende que el legislador ha de habilitar las potestades o instrumentos jurídicos que sean adecuados para que, dentro del respeto debido a los derechos, principios y valores constitucionales, las Fuerzas y Cuerpos de Seguridad del Estado cumplan con su función de averiguación del delito que legalmente les corresponde. Es decir, ha de existir expresa habilitación legal para que la Policía pueda practicar la injerencia en los derechos a la intimidad o a la propia imagen de una persona, en el marco de una investigación dirigida al esclarecimiento de la autoría, causas y circunstancias de un delito.

Sin embargo, nuestro Código Procesal Penal, durante mucho tiempo, ha estado huérfano de regulación con respecto a los actos de investigación nacidos con la aparición de las nuevas tecnologías, lo que ha ocasionado no pocos problemas procesales.

La situación se agravaba si se repara en que, lejos de colmar dicha laguna legal, el silencio del legislador era paralelo a una práctica en la que la dudosa validez de diligencias de investigación restrictivas de derechos fundamentales (por inexistentes, por no estar

1. En tal sentido, conviene recordar que la jurisprudencia constitucional ha reconocido que reviste la naturaleza de fin constitucionalmente legítimo que puede permitir la injerencia en el derecho a la intimidad "el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal (SSTC 25/2005, de 14 de febrero; 206/2007, de 34 de septiembre y 173/2011, de 7 de noviembre). Por eso mismo también ha precisado este Tribunal que "reviste relevancia e interés público la información sobre los resultados positivos o negativos que alcanzan en sus investigaciones las fuerzas y cuerpos de seguridad, especialmente si los delitos cometidos entrañan una cierta gravedad o han causado un impacto considerable en la opinión pública, extendiéndose aquella relevancia o interés a cuantos datos o hechos novedosos puedan ir descubriéndose por las más diversas vías, en el curso de las investigaciones dirigidas al esclarecimiento de su autoría, causas y circunstancias del hechos delictivo (SSTC 14/2003 y 173/2011).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

contempladas legalmente) era sorteada, tal y como señala MARCHENA (Marchena Gómez y González-Cuéllar Serrano, 2015, 336), mediante la aplicación analógica del régimen jurídico previsto en el artículo 579 de la Ley de Enjuiciamiento Criminal (LECRIM, en lo sucesivo) para la intervención de las comunicaciones. Sucedía entonces que la insuficiencia de este precepto no era obstáculo para obtener de él la máxima elasticidad.

El Tribunal Constitucional, en su sentencia 145/2014, de 22 de septiembre, afirmó el carácter inaplazable de una regulación que abordase las intromisiones en la privacidad del investigado en un proceso penal[2]. El intento de subsanación de la falta de regulación de determinadas medidas de investigación, acudiendo a la integración analógica, desbordaba los límites de lo constitucionalmente aceptable.

La Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica trata de paliar esta situación de insuficiencia normativa.

El presente trabajo aborda la medida de investigación tecnológica consistente en la utilización de dispositivos técnicos de captación de imágenes en lugares o espacios públicos (artículo 588 quinquies de la LECRIM), delimitando el alcance de lo que haya de entenderse por lugar o espacio público, para lo cual se analizará la reciente sentencia del Tribunal Constitucional 92/2023, de 11 de septiembre.

II. Regulación Legal

La citada Ley Orgánica 13/2015, de 5 de octubre, incorporó en el Título VIII ("*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*"), del Libro II ("*Del sumario*"), distintos Capítulos destinados a la regulación de las nuevas medidas de investigación tecnológica.

El Capítulo IV establece las disposiciones comunes a todas estas medidas de investigación tecnológica, como antecedente inmediato a la regulación, en los Capítulos siguientes, de todas y cada una de estas medidas: la interceptación de las comunicaciones telefónicas y telemáticas (Capítulo V), la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (Capítulo VI), la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y localización (Capítulo VII),

2. En dicha resolución judicial nuestro Alto Tribunal tuvo ocasión de pronunciarse acerca de la legitimidad de la utilización de un micrófono oculto que captó las conversaciones que tuvieron lugar en un calabozo entre los distintos detenidos en el siguiente sentido: a) Declaró la ilegalidad de la prueba consistente en la grabación de las comunicaciones desarrolladas en el calabozo al carecer de la suficiente cobertura normativa; b) Proclamó la insuficiencia del art. 579 LECRIM para abarcar en su ámbito este tipo de diligencias y c) Estimó que había sido vulnerado el derecho que reconoce el art. 18.3 CE a la inviolabilidad de las comunicaciones. De manera rotunda se afirma que "*no estamos ante un defecto por insuficiencia de Ley, ante un juicio sobre la calidad de la Ley, sino que se debate el efecto asociado a una ausencia total y completa de Ley. Y es que el art. 579.3 LECRIM se refiere de maneta incontrovertida a intervenciones telefónica, no a escuchas de otra naturaleza, ni particularmente a las que se desarrollan en calabozos policiales u entre personas sujetas a los poderes coercitivos del Estado por su detención*".

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

el registro de dispositivos de almacenamiento masivo de información (Capítulo IX) y las medidas de aseguramiento (Capítulo X).

Centraremos nuestra atención en la concreta medida de investigación consistente en la captación de imágenes en lugares o espacios públicos, si bien, para una adecuada delimitación del tema objeto de estudio, resulta preciso la diferenciación entre la captación de imágenes cuando dicha medida de investigación complementa a la de captación y grabación de comunicaciones orales o tiene lugar en espacios privados, de la captación de imágenes en espacios públicos.

La medida de investigación tecnológica consistente en la captación y grabación de comunicaciones orales aparece regulada en el Capítulo VI, artículos 588 quater a) - e) LECRIM (Díaz Martínez, 2018, 85 y ss.), el primero de cuyos preceptos autoriza, previa resolución judicial, la colocación y utilización[3] de dispositivos electrónicos que permitan la captación y grabación[4] de comunicaciones orales directas mantenidas por el investigado[5] en la vía pública u otro espacio abierto, en su domicilio o cualesquiera otros lugares cerrados, siempre y cuando se trate de comunicaciones que puedan tener lugar en uno varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación (Díaz Martínez, 2023, 165 y ss.).

Si resultara necesaria la entrada en el domicilio u otros espacios equiparables a efectos de protección constitucional, la resolución autorizante deberá incluir en su motivación las razones de la procedencia del acceso a tales lugares.

Asimismo, la escucha y grabación de comunicaciones puede complementarse con la obtención de imágenes, si expresamente lo autoriza la resolución judicial correspondiente (artículo 588 quinquies a. 3 LECRIM).

Se han planteado dudas acerca de si el Juez puede autorizar la captación y grabación, en lugares cerrados, únicamente de imágenes sin sonido.

En principio, el precepto contempla la captación y grabación de imágenes como complemento del sonido, por lo que no cabría la grabación únicamente de imágenes.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

3. Tal y como señala el precepto, el Juez podrá autorizar tanto la utilización del dispositivo como la colocación. Esta precisión es importante, ya que la colocación de los dispositivos electrónicos podrá necesitar, en algunos casos, de autorización judicial, al invadir espacios de privacidad no accesibles para la Policía sin dicha autorización.

4. Se distingue también entre la captación y grabación, con lo que se hace referencia tanto a la escucha simultánea de las conversaciones mientras están teniendo lugar, como a su conservación en un soporte adecuado, supuesto este último que supone un mayor grado de intromisión en la intimidad del investigado.

5. Las únicas conversaciones susceptibles de captación y grabación a través de esta medida serán las que mantenga el investigado con cualquier persona, aunque sea ajena a la investigación ("recogida de arrastre"). Sin embargo, no será posible, de modo análogo a lo que autoriza el art. 588 ter c para la interceptación de las comunicaciones, captar o grabar conversaciones de un tercero del que se sirva el sujeto investigado para transmitir o recibir información o que colabore con el investigado o que se beneficie de su actividad. En estos casos, o se convierte a este tercero en investigado, justificando en la resolución judicial que autorice la medida las sospechas que pudieran existir sobre él, o no se podrán captar o grabar sus comunicaciones orales directas.

Sin embargo, una interpretación lógica del precepto debe conducir a permitir que se autorice la captación y grabación únicamente de imágenes sin sonido: por una parte, existe previsión legal que permite la grabación de imágenes y, por otro, la exclusión del sonido supone una intromisión menor en los derechos de investigado, lo que puede responder, en algún supuesto, a la aplicación de los principios de necesidad y proporcionalidad al caso concreto.

Además, la propia LECRIM prevé expresamente la posibilidad de que el Juez autorice la captación de imágenes a propósito de la regulación de la figura del agente encubierto en el artículo 282 bis 7 (Gómez de Liaño Fonseca-Herrero, 2018, 217 y ss.), lo que vendría a reforzar la posición que aquí se sostiene.

En definitiva, al amparo de lo dispuesto en el artículo 588 quáter a LECRIM, el órgano judicial puede autorizar medidas de muy distinta índole y alcance en el particular espacio de exclusión de cualquier ciudadano, a saber: a) La captación y grabación de las comunicaciones orales en la vía pública o en otro espacio abierto o cerrado; b) La captación y grabación de las conversaciones orales en el propio domicilio (Marchena Gómez y González-Cuéllar Serrano, 2015, 338)[6]; y c) la obtención y grabación de imágenes en las mismas circunstancias en las que se desarrollan esas conversaciones de interés.

Por su parte, el Capítulo VII, titulado "*Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización*", regula en el artículo 588 quinquies a) LECRIM, bajo la rúbrica "*Captación de imágenes en lugares o espacios públicos*", una forma de seguimiento del investigado con empleo de cualquier medio técnico de obtención y grabación de imágenes, con la posibilidad de extender el objeto de la diligencia a personas distintas del investigado bajo determinadas condiciones (Gómez Soler, 2018, 123 y 124).

A diferencia de lo que sucede cuando la captación de comunicaciones orales vaya acompañada de la obtención de imágenes o cuando, como hemos defendido, se autorice de forma independiente la obtención de imágenes en espacios privados, supuestos ambos en los que se requiere la preceptiva autorización judicial, cuando se trata de la captación de imágenes en lugares o espacios públicos el legislador no ha sujetado la adopción de la medida a reserva de autorización judicial, sino que atribuye a la Policía judicial, directamente, la competencia para llevar a cabo esta diligencia de investigación.

Ningún derecho fundamental vulnera el agente que percibe con sus ojos lo que está al alcance de cualquiera. Ya en la década de los 90 la jurisprudencia estimaba que, si una persona se expone públicamente a los demás ubicándose en un espacio de acceso general o no restringido, no cabe apreciar ninguna injerencia añadida por el hecho de que un tercero que visualiza a esa persona en ese espacio abierto al público proceda a

6. Hay que entender que la habilitación judicial para el acceso domiciliario solo se admite respecto del que constituye el inmueble o inmuebles en los que desarrolla su vida el investigado: no sería legítima la instalación de esos artefactos en el domicilio de un tercero no investigado pero que se sirviera, por una u otra razón, de punto de encuentro de interés para la investigación.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

la grabación de sus imágenes (Etxebarria Guridi, 2021, 348). La grabación no sería sino la constatación de lo que el ojo humano visualiza (STS 1171/1994, de 6 de abril).

Así, pues, cuando de lo que se trata es únicamente de la captación de imágenes en lugares o espacios públicos, sin la simultánea grabación de las conversaciones mantenidas en tales espacios, no se requiere de resolución judicial, autorizándose a la Policía judicial a la obtención y grabación por cualquier medio técnico de imágenes de la persona investigada, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.

Conviene precisar que, tanto la captación de grabaciones orales acompañada de imágenes, cuanto la mera captación de imágenes, tienen por objeto la utilización de dispositivos electrónicos de captación y grabación de sonido y/o de la imagen en el marco de una investigación criminal de determinados delitos, quedando fuera de esta regulación los supuestos previstos en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, que, tal y como dispone su art. 1.1, tiene, esencialmente, una finalidad preventiva, así como la colocación de cámaras de videovigilancia por particulares, que deberá ajustarse a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En tales casos, la incorporación al proceso de archivos de imagen o sonido captados entrará dentro de las facultades y obligaciones de la Policía Judicial que regula el artículo 282 LECRIM, siendo la prueba así aportada perfectamente valorable por el Tribunal (STS nº 134/2017, de 2 de marzo).

En resumen, el artículo 588 quinquies a) LECRIM otorga cobertura legal para que la Policía Judicial, sin necesidad de autorización judicial, pueda obtener y grabar por cualquier medio técnico imágenes de la persona investigada, siempre y cuando: a) se encuentre en un lugar o espacio público y b) su alcance se limite a las facultades investigadoras de la Policía judicial que se desarrollen con el fin de preparar el juicio, averiguar y hacer constar la perpetración de los delitos y la culpabilidad de los delincuentes (artículo 299 LECRIM).

En tales casos, la Policía Judicial tendrá la responsabilidad, con carácter previo a aportar la imagen o el video digitalizado al proceso, de custodiar la prueba y realizar una tarea de aseguramiento, para lo cual parece razonable la aportación de una firma electrónica avanzada o un sellado de tiempo que haga que la imagen digital captada que, finalmente, constituye un archivo electrónico, no pueda ser modificada ni manipulaba en lo referente a su contenido y sus propiedades (Bueno de Mata, 2019, 137).

Corresponderá posteriormente al Juez Instructor, en el momento de decidir la incorporación de las imágenes captadas al proceso, normalmente después de ponerse fin a la medida, controlar que se cumplen los principios de especialidad, idoneidad, excepcionalidad, necesidad e idoneidad de la medida.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

III. Lugares o espacios públicos como presupuesto legitimador para la captación de imágenes sin autorización judicial

El artículo 588 quinquies a) LECRIM no exige autorización judicial para la captación de imágenes por parte de la Policía judicial a los indicados fines porque, tal y como precisa la Circular 4/2019, de 6 de marzo, de la Fiscalía General del Estado, tal exigencia no deriva del texto constitucional, reservándose para modalidades más invasivas.

Para que la Policía judicial pueda obtener y grabar imágenes de la persona investigada es preciso que esta se encuentre en un lugar o espacio público. Por tal ha de entenderse aquel que, con independencia de la titularidad dominical, puede ser usado o disfrutado por toda clase de persona.

En tal sentido, la referida Circular 4/2019, con cita de doctrina constitucional[7], señala que cuando el apartado primero del artículo 588 quinquies a) LECRIM alude a lugares o espacios públicos ha de entenderse que se refiere a aquellos en los que el investigado no puede ejercer su derecho a la intimidad, donde no puede reservarse al conocimiento de los demás lo que está sucediendo, al no disponer de ningún derecho de exclusión sobre ese lugar.

Se contrapone así ese concepto al de lugares privados, que serán aquellos en los que el individuo pueda limitar el acceso a terceros, ejerciendo de ese modo ámbitos de privacidad excluidos al conocimiento ajeno.

Aunque pudiera parece que la cuestión no presenta aristas, la determinación de lo que haya de entenderse por lugares o espacios públicos no está exenta de problemas.

Tal y como señala MAGRO SERVET (Magro Servet, 2023, 4), la cuestión clave es aquí interpretativa, ya que, si se comete el error de entender que es espacio o lugar público lo que no lo es, la actuación policial sin autorización judicial instalando estos dispositivos de grabación en un lugar que ellos consideran que es público corre el riesgo de que luego se considere que no lo es y venga, de ahí, la consideración de prueba ilícita. Y ello, con la consecuencia posterior de que el objeto u objetos encontrados en esa investigación por la captación de esas imágenes se tendrá por no válido y se declarará prueba ilícita con las consecuencias que de ellos se deriven en cuanto a la apreciación de la conexión de antijuridicidad con otras pruebas que tampoco podrán ser tenidas en cuenta.

La jurisprudencia del Tribunal Supremo ha considerado innecesaria la autorización judicial para incorporar al proceso imágenes obtenidas por las cámaras de seguridad de establecimientos comerciales abiertos al público (STS 124/2014, de 3 de febrero), instaladas en una nave industrial próxima a la vía pública (STS 129/2014, de 26 de febrero), o cuando se trata de imágenes grabadas en el domicilio por los propios moradores (STS 67/2014, de 28 de enero), zonas comunes o distribuidores de servicios higiénicos de un parque público, Sin embargo, los aseos públicos se consideran, como domicilio particular de las personas, espacios de privacidad opacos, estando vedada la captación de imágenes en los mismos fines de investigación criminal (STS de 5 de mayo de 1997).

7. SSTC 134/1999, de 15 de julio; 144/1999, de 22 de julio y 236/2007, de 7 de noviembre.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

Sin embargo, el máximo intérprete de las garantías constitucionales no se había pronunciado acerca de los lugares en los que la Policía judicial, sin previa autorización judicial, puede instalar válidamente dispositivos de captación y grabación de imágenes en el marco de una investigación de un delito, lo que sí ha realizado en la sentencia 92/2023, de 11 de septiembre, en la que se analiza si un garaje de una comunidad de vecinos es lugar o espacio público y, por tanto, los agentes de la Policía podían obtener y grabar imágenes del investigado al amparo del artículo 588 quinquies a) LECRIM, o es privado y, en consecuencia, hacía falta la preceptiva orden judicial.

En dicha resolución judicial, se afirma rotundamente que la habilitación legal que permite a la Policía Judicial la grabación de imágenes en el marco de una investigación criminal sin autorización legal se circunscribe a los lugares o espacios públicos, noción ésta que tiene un sentido inequívoco, referido a ámbitos espaciales de uso por todo el público, sin restricciones.

IV. Sentencia del Tribunal Constitucional 92/2023, SEC. 1ª, DE 11 DE SEPTIEMBRE DE 2023

4.1. Supuesto de hecho

El demandante de amparo impugna la sentencia del Juzgado de lo Penal Núm. 4 de Barcelona que le condenó como autor de un delito de tráfico de drogas, así como la sentencia dictada en apelación por la Audiencia Provincial de dicha capital, que vino a confirmar esa sentencia, alegando, entre otras, la vulneración del derecho a la intimidad y a la propia imagen (artículo 18.1 CE), en relación con el principio de legalidad penal (artículo 25.1 CE), porque la investigación que ha conducido a su condena tendría su origen en la instalación de cámaras de grabación de imágenes por la Guardia Urbana de Barcelona en el garaje de una comunidad de vecinos, sin autorización judicial ni permiso de la comunidad o comunicación a la autoridad competente.

En su fundamentación la sentencia dictada por el Juez de lo Penal descarta que se haya producido la alegada vulneración del derecho a la intimidad personal de los acusados por el hecho de que la Guardia Urbana de Barcelona instalase dispositivos de grabación de imágenes en el garaje comunitario en el que se hallaba estacionado el vehículo en el que encontraron 44 kilos de hachís cuando se procedía a su registro. Se afirma que los garajes no tienen la consideración de domicilio constitucionalmente protegido, porque las grabaciones videográficas obtenidas en dichos espacios no requieren de autorización judicial y tienen validez como prueba de cargo para desvirtuar la presunción de inocencia.

Por su parte, la Audiencia Provincial de Barcelona niega expresamente la vulneración del derecho a la intimidad alegada por el recurrente, considerando que la captación policial de imágenes en el garaje sin autorización judicial resulta amparada por lo dispuesto en el artículo 588 quinquies a) de la LECRIM, al carecer el garaje de la protección que el artículo 18.2 de la CE dispensa a los domicilios, por tratarse un espacio cerrado de titularidad privada pero público en cuanto a su uso, aunque de acceso restringido.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

Por tanto, entiende que el artículo 588 quinquies a) de la LECRIM habilita a la Policía judicial en el marco de una investigación criminal, sin necesidad de autorización judicial, para instalar videocámaras y grabar imágenes en cualquier espacio, aunque sea cerrado y de titularidad privada, siempre que no merezca la calificación de domicilio a efectos constitucionales.

No estando conforme con la anterior sentencia dictada en apelación, se interpuso recuso de casación, que fue inadmitido mediante providencia por la Sala Segunda del Tribunal Supremo, por carencia de interés casacional.

4.2. La intimidad como derecho fundamental afectado

Tal y como se ha indicado, el recurrente alega, entre otros, la vulneración del derecho a la intimidad y a la propia imagen, como si del mismo derecho se tratase, porque entiende que en la investigación que ha conducido en último término a su condena por un delito de tráfico de drogas ha sido determinante la instalación de cámaras de grabación de imágenes por la Guardia Urbana de Barcelona en el garaje de una comunidad de vecinos, sin autorización judicial ni permiso de la comunidad o comunicación a la autoridad competente.

En atención a ello, el Tribunal Constitucional delimita, con carácter previo a entrar en el fondo del asunto, cuál de esos derechos fundamentales garantizados por el artículo 18.1 de la CE es el afectado, recordando que, conforme a reiterada doctrina constitucional, los derechos al honor, a la intimidad personal y a la propia imagen, a pesar de su estrecha relación entre sí, en tanto que derechos de la personalidad, derivados de la dignidad humana (artículo 10.1 CE) y dirigidos a la protección del patrimonio moral de las personas, tienen, no obstante, un contenido propio y específico cada uno de ellos.

Se trata, en palabras del propio Tribunal, de derechos autónomos, de modo que, al tener cada uno de ellos propia sustantividad, la apreciación de la vulneración de uno no conlleva necesariamente la vulneración de los demás.

Pues, bien, atendiendo al relato de hechos probados en las sentencias que se impugnan en amparo, entiende que, en el presente caso, el derecho fundamental afectado por la actuación concreta de los agentes de la Guardia Urbana de Barcelona es el derecho a la intimidad personal, en relación con el cual efectúa las siguientes precisiones:

— **Primera**: El derecho a la intimidad personal implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana[8].

8. SSTC 207/1996, de 16 de diciembre; 186/2000, de 10 de julio; 196/2004, de 15 de noviembre; 207/2007, de 24 de septiembre y 159/2009, de 29 de junio.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

— **Segunda**: El derecho a la intimidad atribuye a su titular el poder de reservarse un espacio resguardado de la curiosidad ajena, de una publicidad no querida[9], y, en consecuencia, el poder jurídico de imponer a terceros, sean particulares o poderes públicos, el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido[10], a fin de asegurar un ámbito privativo para el desarrollo de la propia personalidad ajeno a las injerencias externas.
— **Tercera**: La intimidad protegida por el artículo 18.1 de la CE no se reduce necesariamente a la que se desarrolla en un ámbito doméstico o privado[11].
— **Cuarta**: Resulta relevante, como criterio que debe tenerse en cuenta para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegida frente a intromisiones ilegítimas, el de las **expectativas razonables que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observancia o del escrutinio de los demás**[12].
— **Quinta:** Lo que el artículo 18.1 de la CE garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido es ese espacio.

4.3. El garaje de una comunidad de propietarios pertenece al ámbito de la intimidad protegida por el artículo 18.1 de la CE

Admitido que el derecho fundamental afectado es el derecho a la intimidad y matizado que no es un derecho absoluto y, por tanto, no confiere a su titular una facultad omnímoda de exclusión, pues, como cualquier derecho fundamental, puede ceder ante otros derechos y bienes especialmente relevantes, entre los que se encuentra, en lo que aquí nos interesa, el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal, siempre y cuando exista una expresa habilitación legal para que la Policía judicial pueda practicar la injerencia en el derecho a la intimidad, nuestro garante de la Constitución analiza si

9. SSTC 231/1988, de 2 de diciembre; 127/2003, de 30 de junio; 89/2006, de 27 de marzo; 236/2007, de 7 de noviembre; 60/2010, de7 de octubre y 93/2013, de 23 de abril.
10. SSTC 14/2003, de 28 de enero; 196/2004, de 15 de noviembre; 206/2007, de 24 de septiembre; 70/2009, de 23 de marzo; 173/2011, de 7 de noviembre.
11. SSTC 12/2012, de 30 de enero; 18/2015, de 16 de febrero y 25/2019, de 25 de febrero.
12. Así, por ejemplo, cuando se encuentra en un paraje inaccesible o en un lugar solitario debido a la hora del día, puede conducirse con plena espontaneidad en la confianza fundada de la ausencia de observadores. Por el contrario, no pueden abrigarse expectativas razonables al respecto cuando de forma intencional, o al menos consciente, se participa en actividades que por las circunstancias que las rodena, claramente pueden ser objeto de registro o de información pública (SSTEDH de 25 de septiembre de 2001, P.G. y J.H: c. Reino Unido, &57, y de 28 de enero de 2003, Peck c. Reino Unido, & 58).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

el artículo 588 quinquies a) de la LECRIM dota de la adecuada cobertura legal para la concreta actuación policial controvertida sin autorización judicial.

Previamente a entrar en el fondo del asunto, considera el Tribunal Constitucional que la Audiencia Provincial de Barcelona ha realizado una interpretación extensiva de la cláusula "lugar o espacio público" contenida en el apartado primero del artículo 588 quinquies a) de la LECRIM, en el sentido de considerar que también incluye todos aquellos lugares o espacios que, aun no siendo en puridad espacios públicos, no constituyen domicilio de conformidad con lo dispuesto en el artículo 18.2 de la CE.

Tal razonamiento, se señala por nuestro Alto Tribunal, no puede ser compartido, porque supone una interpretación extensiva del precepto legal que no se cohonesta con las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y libertades públicas.

Efectuada esta importante precisión, afirma rotundamente que, **la previsión legal que permite a la Policía judicial la grabación de imágenes en el marco de una investigación criminal sin autorización judicial se circunscribe** a los lugares o espacios públicos, noción esta que tiene un sentido inequívoco, referido **a ámbitos espaciales de uso por todo el público, sin restricciones**.

En atención a ello, "es notorio que, conforme al referido criterio de expectativa razonable de privacidad, el garaje de una comunidad de vecinos pertenece al ámbito de la intimidad protegida por el artículo 18.1 de la CE, pues se trata de un lugar cerrado que es, además, una propiedad privada de acceso restringido (a los titulares de las plazas de aparcamiento y a terceros a los que aquellos permitan la entrada) y por tanto es patente que se trata de un lugar en el que el recurrente tenía una expectativa razonable de no ser escuchado u observado subrepticiamente por terceras personas".

Por todo lo anterior, la captación policial de imágenes en el interior del garaje privado en el que se hallaba estacionado el automóvil en el que finalmente fue incautada la droga carecía de habilitación legal, por lo que vulneró el derecho del recurrente a la intimidad personal (artículo 18.1 CE), deviniendo nula la prueba de cargo obtenida por ese medio.

4.4. Voto particular

Frente a la opinión de la mayoría, se formula voto particular por uno de los Magistrados afirmando que, conforme al criterio de la expectativa razonable de encontrarse al resguardo de la curiosidad ajena, no es posible albergar semejante confianza cuando la actividad se desarrolla en el interior de un garaje de una comunidad de vecinos y por tanto se encuentra expuesta a la mirada de cualquier persona con acceso al referido garaje.

No puede afirmarse que un garaje comunitario se encuentre amparado por el derecho a la intimidad, salvo que se desnaturalice el contenido de este derecho y se transforme el derecho a la intimidad personal y familiar en una suerte de inexistente derecho a la intimidad vecinal o comunitaria ontológicamente contraria a la propia esencia del concepto de intimidad, por encontrarse desvinculada de la esfera de la personalidad y de la dignidad del individuo con la que entronca los derechos del artículo 18.1 de la CE.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

El garaje comunitario, se afirma, no puede ser un espacio ajeno al escrutinio o la mirada ajena, ni un espacio donde los recurrentes –en el desarrollo de su actividad delictiva– pudieran albergar una expectativa razonable de privacidad, por más que confiaran en no ser sorprendidos por ningún vecino –o por la policía– mientras realizaban las operaciones de carga y descarga de los bultos en el vehículo aparcado en una de sus plazas. No debe confundirse la expectativa a no ser sorprendidos en la actividad delictiva, con el ámbito tuitivo que proyecta el derecho a la intimidad.

Reflexiones personales

1. La Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica define las modalidades de investigación tecnológica y delimita los presupuestos, constitucionales y legales, que legitiman su adopción, dotando de la necesaria cobertura legal a determinadas medidas de investigación tecnológica absolutamente necesarias para hacer frente a una fenomenología criminal de nuevo cuño y, en definitiva, garantizar las exigencias derivadas de seguridad jurídica en el ámbito de los derechos fundamentales.
2. Dicho texto legal se hacía absolutamente necesario no sólo con la finalidad de actualizar el régimen jurídico de las diligencias de investigación a las exigencias de las nuevas tecnologías de la información y del entorno digital propio de la sociedad del S.XXI, sino también, y muy especialmente, para colmar la manifiesta insuficiencia de la regulación legal existente en esta materia, que afectada directamente al principio esencial de reserva de Ley en toda injerencia en el ámbito de los derechos fundamentales.
3. Por su afección en los derechos fundamentales contenidos en el artículo 18 de las CE, las medidas de investigación tecnológica requieren de la preceptiva autorización judicial dictada con sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida, a los que alude el artículo 588 bis a) LECRIM como principios rectores, recogiendo consagrada doctrina jurisprudencial de nuestro máximo intérprete de las garantías constitucionales.
4. Como única excepción a dicha regla general, se contempla la posibilidad de que la Policía Judicial obtenga y grabe por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, sin necesidad de autorización judicial, cuando ello sea necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos (artículo 588 quinquies a) de la LECRIM).
5. Nuestro Tribunal Constitucional no se había pronunciado acerca de los lugares en los que la Policía Judicial, sin previa autorización del Juez instructor, puede instalar válidamente dispositivos de captación y grabación de imágenes en el

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

marco de la investigación de un delito. Por primera vez lo hace en la STC 92/2023, de 11 de septiembre de 2023, que aborda como cuestión nuclear la captación de imágenes en el interior de un garaje privado llevada a cabo por la Policía Judicial sin autorización judicial, apreciando que concurre en el mismo una especial trascendencia constitucional, porque plantea un problema o afecta a una faceta de un derecho fundamental sobre el que no hay doctrina de este Tribunal.

6. Con independencia de que la cuestión esencial que aborda la citada resolución judicial sea la de dilucidar si el garaje de una comunidad de vecinos tiene o no la consideración de lugar o espacio público, en ella se efectúan una serie de precisiones básica en orden a la delimitación de lo que haya de entenderse por dicho concepto (lugar o espacio público) como presupuesto legitimador de la captación de imágenes sin autorización judicial.
7. Admitido que, en el caso sometido a consideración, el derecho fundamental afectado por la actuación controvertida es el derecho fundamental a la intimidad personal, nuestro Alto Tribunal efectúa, a mi entender, tres precisiones esenciales sobre lo que implica dicho derecho fundamental, a saber: a) El derecho a la intimidad personal implica la existencia de una ámbito propio y reservado frente a la acción y el conocimiento de los demás, sean particulares o poderes públicos, indispensable para mantener una calidad mínima de vida humana; b) La intimidad protegida por el artículo 18.1 de la CE no se reduce indefectiblemente a la que se desarrolla en un ámbito doméstico o privado; c) El criterio clave para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente a intromisiones ilegítimas es el de las expectativas razonables que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observancia o del escrutinio ajeno.
8. La habilitación legal que permite a la Policía Judicial la grabación de imágenes en el marco de una investigación criminal sin autorización judicial se circunscribe a los lugares o espacios públicos, noción esta que tiene un sentido inequívoco, referido a ámbitos espaciales de uso por todo el público, sin restricciones.
9. En atención a todo lo anterior, el garaje de una comunidad de vecinos pertenece al ámbito de la intimidad protegida por el artículo 18.1 de la CE; pues se trata de un lugar cerrado que es, además, una propiedad privada de acceso restringido y, por tanto, es patente que se trata de un lugar en el que la persona tiene una expectativa de no ser escuchado u observado subrepticiamente por terceras personas.

Bibliografía

BUENO DE MATA, F., Las diligencias de investigación penal en la cuarta revolución industrial, Aranzadi, 2019.

DÍAZ MARTÍNEZ, M., "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", en *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas* (directores: Díaz Martínez, M., López-Barajas Perea, I.), Tirant lo Blanch, 2018

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

DÍAZ MARTÍNEZ, M., "La existencia de encuentros concretos del investigado como factor de legitimación en la captación y grabación de comunicaciones orles e imágenes: Un presupuesto de difícil concreción», en *Revista Científica del Centro Universitario de la Guardia Civil, Revista Lógo*s, Número especial, febrero 2023.

ETXEBARRIA GURIDI. J.F., "Videovigilancia y su eficacia en el proceso penal", en *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, (Coord. Pérez Gil., J.), La Ley, 2021,

GÓMEZ DE LIAÑO FONSECA-HERRERO, M., "El uso de dispositivos electrónicos de captación de comunicaciones en operaciones de infiltración policial", en *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas* (directores: Díaz Martínez, M., López-Barajas Perea, I.), Tirant lo Blanch, 2018

GÓMEZ SOLER, E., "La utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. Cuando la práctica forense no puede esperar", en *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas* (directores: Díaz Martínez, M., López-Barajas Perea, I.), Tirant lo Blanch, 2018

MAGRO SERVET, V., "Afectación del derecho a la intimidad personal por la captación de imágenes en el interior de un garaje privado sin autorización judicial. (Análisis de la STC 92/2023 de 11 Se. 2023", en Diario La Ley, Núm. 1038.

MARCHENA GÓMEZ, M., GONZÁLEZ-CUÉLLAR SERRANO, N., La reforma de la Ley de Enjuiciamiento Criminal en 2015, Editorial Castillo de Luna, 2015.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 27-41
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.02

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

Estudio criminológico sobre la inseguridad en las áreas rurales a partir del uso de herramientas TIC

CRIMINOLOGICAL STUDY ON INSECURITY IN RURAL AREAS BASED ON THE USE OF ICT TOOLS

Jordi Ortiz García
Universidad de Extremadura
jortiz@unex.es 0000-0003-3672-9808
Ricardo Rodrigues Antúnez
Graduado en Derecho y Criminología
rrodriguesantunez@gmail.com 0009-0009-3849-6439

Recibido: 10 de noviembre de 2023 | Aceptado: 5 de diciembre de 2023

RESUMEN

La percepción de inseguridad y el miedo al delito han sido sobradamente analizados en la literatura criminológica nacional e internacional. Desafortunadamente, los estudios realizados se han centrado principalmente en las ciudades y sus barrios. Esta investigación tiene como finalidad conocer la inseguridad y el miedo que existe en las áreas rurales de nuestro país. Para ello, hemos llevado a cabo un estudio de victimización en la localidad de Cilleros, un municipio al noroeste de la provincia de Cáceres en la Comunidad Autónoma de Extremadura de 1.617 habitantes. Para este estudio se ha empleado una metodología geoestadística, y cuyos resultados muestran mayoritariamente que las personas se sienten seguras, pero arrojan también un número relevante de ilícitos acaecidos conforme al tamaño de la población o la necesidad de una mayor presencia policial en este municipio.

PALABRAS CLAVE

Medio Rural
Inseguridad
SIG
Criminalidad y Policía

ABSTRACT

The perception of insecurity and fear of crime has been extensively analyzed in the national and international criminological literature. Unfortunately, the studies carried out have mainly focused on cities and their neighbourhoods. This research aims to understand the insecurity and fear that exists in rural areas of our country. To this end, we have carried out a victimization study in the town of Cilleros, a municipality in the northwest of the province of Cáceres in the Autonomous Community of Extremadura with a population of 1,617 inhabitants. A geostatistical methodology was used for this study, the results of which mainly show that people feel safe, but also show a significant number of crimes that have occurred in accordance with the size of the population or the need for a greater police presence in this municipality.

KEYWORDS

Rural Environment
Insecurity
GIS
Crime and Police

I. Introducción

La inmensa mayoría de los estudios criminológicos realizados en nuestro país han tenido un importante sesgo urbano. Sí revisamos la literatura criminológica de estos últimos años, las investigaciones han tenido como marco espacial las áreas urbanas o áreas de alta concentración de personas como los barrios, siendo fácilmente localizable en estos textos expresiones como: *la delincuencia en las ciudades* o *la prevención de las ciudades*, palabras utilizadas para explicar habitualmente la delincuencia de nuestro país (San Juan y Vozmediano, 2021). Una metodología que ha obviado las áreas rurales y las personas que residen en ellas, y que presentan nuevos modelos de políticas locales de seguridad y estrategias enfocadas principalmente al contexto urbano (Fepsu, ONU-Habitat o La percepción importa)[1]. Una criminología en España, que está dejando a un lado a más de 5.000.000 de personas y más de un 80 por ciento de municipios en España (INE, 2022).

Una invisibilidad, como apuntan algunas investigaciones, que puede deberse a la idea que las áreas rurales son zonas seguras y con una baja tasa de criminalidad (Ceccato, 2016; Ortiz, 2022). Esta idealización choca con la opinión de algunas investigadoras, que apuntan a la necesidad de llevar a cabo estudios en zonas rurales, debido a que el delito no es únicamente un problema urbano, la naturaleza del medio rural influye en la delincuencia, existe una mercantilización de la seguridad o es necesaria una interseccionalidad de género de la seguridad en el contexto rural (Ceccato y Abraham, 2022; Soriano, 2022).

A día de hoy, el medio rural ofrece una postal con pueblos armoniosos y solidarios. Una imagen reforzada por medios de comunicación, operadores políticos y sociales frente a la vida hacinada y desorganizada de las ciudades (Vozmediano y San Juan, 2010). Una fotografía que ha provocado una mercantilización del turismo en muchas zonas del país, que está generando una gentrificación rural parecida a las grandes ciudades en determinados periodos del año, lo que pudiera provocar nuevas oportunidades delictivas que desde la criminología deberían analizarse.

Por todo ello, este trabajo tiene como objetivo principal profundizar en los problemas de seguridad en el medio rural, un estudio que puede ser punto de partida para futuras investigaciones. Este trabajo de investigación analiza la percepción de inseguridad y la gestión de la seguridad en áreas rurales[2].

1. El Foro Europeo para la Seguridad Urbana (FEPSU) fue creada en 1987. Los objetivos de esta red europea son: la promoción de políticas públicas de prevención y seguridad o un espacio de debate e intercambio de buenas prácticas en la red. Ver: https://fepsu.es. En el año 1995 Naciones Unidas creó el programa de ciudades seguras. Se trata de programas que tienen como objetivo prevenir y responder a determinados hechos delictivos contra mujeres y niñas en espacios públicos de diferentes entornos. En último lugar, el Departamento de Interior de la Generalitat de Catalunya elaboró una guía denominada *La percepción importa*, que tiene como objetivo analizar y responder a estallidos de la percepción de inseguridad. Ver: https://interior.gencat.cat/web/.content/home/010_el_departament/publicacions/seguretat/Toolkit/booklet_Digital_ES_no_20210611.pdf

2. Este estudio se ha desarrollado dentro de un proyecto de la Universidad de Extremadura denominado "La necesaria reforma de las administraciones públicas y del modelo territorial español ante el reto demográfico en Extremadura". Un proyecto que tiene como objetivo analizar la eficacia

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Para ello, hemos realizado una investigación en una pequeña localidad de 1.617 habitantes en el noroeste de la Comunidad Autonoma de Extremadura, cercano a Portugal. Una localidad fronteriza que está sufriendo los graves problemas de despoblación y supresión de servicios públicos, como es el municipio de Cilleros.

Para este trabajo hemos utilizado una metodología cuantitativa, con la elaboración de una encuesta de victimización y un estudio geoestadístico mediante un análisis de redes a través de sistemas de información geográfica (en adelante, SIG), a partir de los datos obtenidos en las entrevistas realizadas a efectivos de las fuerzas y cuerpos de seguridad durante el último trimestre del 2022.

Seguidamente, presentaremos algunos conceptos teóricos y la metodología empleada en esta investigación.

II. Marco Teórico

Desde hace años, la literatura criminológica tiene como objeto de estudio la percepción de la ciudadanía a los problemas delincuenciales más allá de su sustantividad, centrándose en la dimensión subjetiva de la seguridad, y concretamente, en la reacción de la población a ser víctima de un hecho delictivo, observándose que el miedo o temor a ser victimizado no está relacionado directamente con la tasa de criminalidad o el riesgo real a sufrir un delito.

Los estudios sobre percepción de inseguridad y el miedo al delito han sido en la investigación criminológica fundamentales para conocer las consecuencias de ser víctima de un hecho delictivo (Huesca, 2021). Y eso, a pesar de la falta de acuerdo científico y académico sobre la definición de estos dos fenómenos. Aun así, lo que sí parece cierto, es que el miedo tiene unas consecuencias negativas para la vida de las personas, económicas, sociales o políticas.

Estas investigaciones se han centrado principalmente en áreas urbanas, por lo que podríamos estar hablando de estudios insuficientes o incompletos, ya que se ha dejado de lado las áreas rurales. Lo que indicaría que estos resultados y sus conclusiones no puedan aplicarse a lugares con características tan distintas a las realizadas hasta ahora. Quizás, la falta de datos delincuenciales por parte de las administraciones y operadores políticos han hecho imposible realizarlas, tal vez la idealización del medio rural como áreas tranquilas, seguras, pacíficas, poco conflictivas y perfectas para la convivencia

real del marco institucional en sus políticas públicas frente al reto demográfico a la luz de su tamaño y adecuación territorial, haciendo hincapié en nivel local (problemática del inframunicipalismo y de las competencias impropias) o estudiar las capacidades de las administraciones públicas encargadas de hacer frente al reto demográfico para identificar sus necesidades concretas de reforma, tanto en su estructura y diseño como en su marco competencial. Análisis desde el prisma jurídico de los niveles competenciales en los que pueda introducirse la "perspectiva territorial". A tales fines, realización de encuestas y entrevistas a los actores implicados en la estrategia frente al reto demográfico, especialmente a los representantes públicos y funcionarios de la región previamente identificados en aquel marco.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

familiar, que choca frontalmente con los problemas de las áreas metropolitanas, han hecho de estos lugares espacios poco interesantes para la Criminología.

Pero lo cierto es, que investigaciones en el ámbito internacional si recogen e identifican los problemas delincuenciales del medio rural y la necesidad de analizar estos espacios desde un punto de vista criminológico. Algunos estudios llevados a cabo en Australia, Nueva Zelanda o países nórdicos muestran la importancia de analizar los problemas delincuenciales del medio rural, el papel esencial de las fuerzas y cuerpos de seguridad en la prevención de la delincuencia, como es la lucha contra la violencia de género, o la importancia del control informal en las áreas rurales (Donnermeyer y DeKeseredy, 2014). En definitiva, motivos suficientes para el estudio de estas áreas.

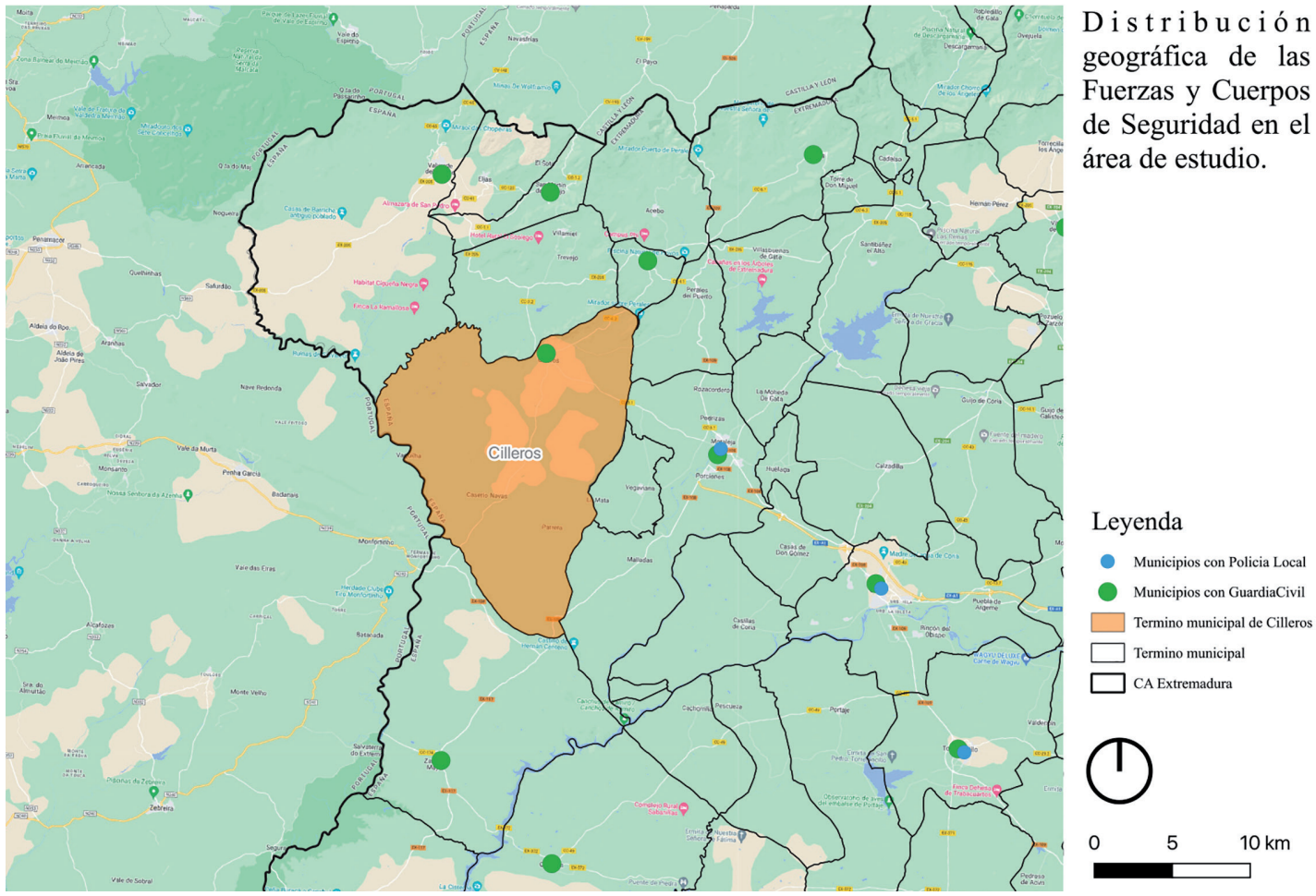
Desafortunadamente, esta atención no parece verse dentro de nuestras fronteras, y sólo de manera tangencial podemos encontrar referencia al medio rural desde la Criminología en España (Redondo y Garrido, 2023).

III. La seguridad en la localidad de Cilleros

La seguridad ha sido un componente esencial para el desarrollo de nuestras ciudades. A día de hoy, nadie puede entender un lugar en el que no existan medios o políticas que nos permitan sentirnos más seguros. Disponer de instituciones como la Policía, que garantizan el libre ejercicio de nuestros derechos fundamentales y el control y mantenimiento del orden público (art.104 C.E.), resulta esencial para la ciudadanía. Desgraciadamente, la seguridad pública y objetiva en el medio rural se ha desarrollado de manera muy distinta a las áreas urbanas. El cierre de cuarteles, el descenso de efectivos o la no obligatoriedad de servicios policiales en municipios de menos de 5.000 habitantes provoca desequilibrios entre ambas zonas. Así, la localidad de Cilleros no cuenta con un servicio policial propio (Policia Local), siendo la localidad de Moraleja la población más próxima con este servicio policial. Sin embargo, sí cuenta con desde hace más de 100 años con Guardia Civil. Una institución que se ha hecho esencial en esta localidad próxima a Portugal. Una zona que históricamente se caracterizado por el contrabando y otras conductas delictivas específicas de las áreas rurales, como los delitos contra la flora, fauna o robos (Alonso de la Torre, 2021). Hoy, el cuartel de la Guardia Civil se situa en el centro del municipio, dentro de un núcleo operativo que a su vez forma parte de una Compañía, en este caso, de la Compañía de Coria (Cáceres). El cuartel cuenta con un total de 8 efectivos, pero se eliminó la presencia y vigilancia permanente (24 horas), lo que provoca que en horario nocturno o fin de semana no tengan servicios policiales, salvo que existan algún espectáculo o actividad recreativa que necesite de la presencia de un servicio policial extraordinario**,** como se observa en el siguiente mapa:

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Mapa 1. Distribución geográfica de las fuerzas y cuerpos de seguridad en la localidad de Cilleros y Comarca Sierra de Gata (Provincia de Cáceres).



Nota: Elaboración propia a partir de los datos obtenidos de Junta de Extremadura y 112.

Desafortunamente, no contamos con datos oficiales sobre los hechos delictivos que se han producido en esta zona[3]. Sin embargo, desde el propio cuartel de la Guardia Civil de Cilleros afirman que durante el año 2022 se realizaron entre 500 y 600 intervenciones, un dato significativo en una localidad entorno a los 1.500 habitantes. Además, según datos del Centro de Atención de Urgencias y Emergencias 1.1.2. de la Junta de Extremadura se recibieron total de 11 llamadas clasificadas como Seguridad Pública en la localidad de Cilleros en el 2021, como puede verse en la Tabla 1.

Estos datos que podrían parecer poco significativos, salvo por el hecho que la población tiene que recurrir al 1.1.2. de Extremadura por cuestiones relacionadas con seguridad ciudadana, teniendo un servicio policial en el municipio, como es la Guardia Civil. Además, si analizamos el número de llamadas en toda la Comarca de Gata, zona en la que se encuentra esta localidad, fue durante el mismo periodo de 157 llamadas clasificadas como Seguridad Pública[4].

3. Cabe recordar que las instituciones y administraciones de nuestro país sólo publican datos de criminalidad por provincias o Comunidades Autónomas, obviando aquellos municipios de menos de 20.000 habitantes.

4. Las Localidades que se encuentran dentro de la Comarca de Gata son: Acedo, Cadalso, Cilleros, Descargarmaría, Eljas, Gata, Hernán-Pérez, Hoyos, La Moheda de Gata, Perales del Puerto, Robledillo

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Tabla 1. Número de incidentes clasificados como Seguridad Pública en Cilleros[5].

Localidad	Delitos contra la Seguridad Colectiva	Delitos contra la propiedad	Delitos contra las personas	Seguridad Pública (Otros)
Cilleros	2	4	3	2

Nota: Elaboración propia a partir de los datos obtenidos del 112

En cuanto a los servicios policiales, hemos indicado que la Guardia Civil de Cilleros depende de la Compañía de Coria. La Compañía de Coria está formada por 3 Núcleos Operativos, los cuales abarcan los siguientes pueblos: *Núcleo Operativo 1*: Valverde del Fresno, Eljas, San Martín de Trevejo, Villamiel, Trevejo, Hoyos, Acebo, Cadalso, Torre de Don Miguel, Villasbuenas de Gata, Santibáñez el Alto, Gata y Perales del Puerto; *Núcleo Operativo 2*: Cilleros, Moraleja, Vegaviana, Zarza la Mayor, Huélaga, Calzadilla y La Moheda de Gata, objeto de nuestra investigación, y que aparece en el siguiente mapa temático con un color más intenso. Por último, el Núcleo operativo 3: Coria (color amarillo)[6], Portaje, Ceclavín, Aceúche, Torrejoncillo, Cachorrilla, Pescueza, Cañaveral, Holguera y Casas de Don Gómez, como se puede ver en el Mapa 2.

Por lo que el sistema empleado en la gestión de la seguridad en esta área es la siguiente: Una patrulla operativa en cada núcleo por turno de trabajo, es decir, mínimo habrá tres patrullas rondando durante los turnos de mañana, tarde y noche. El patrullaje se realiza en función de las necesidades del servicio, por lo que ninguna patrulla permanece operativa en una localidad todo el tiempo del turno, sino que se desplazan aleatoriamente de un municipio a otro, mientras que lo harán de manera obligatoria con ocurrencia de hechos delictivos, festejos populares, ocio o vigilancia de incendios, entre otros. Al tener que trasladarse a otras localidades, cuando fuere necesario, se utiliza en la práctica, el aviso a la patrulla de otro núcleo, para que acudan a realizar tareas de vigilancia y disuasión al pueblo del que es originaria la patrulla que proporciona el aviso.

En ocasiones, puede incrementarse el número de patrullas por núcleo, llegando a haber tres por cada uno, aunque solamente se produce este fenómeno por motivos señalados o en caso de urgencia o necesidad.

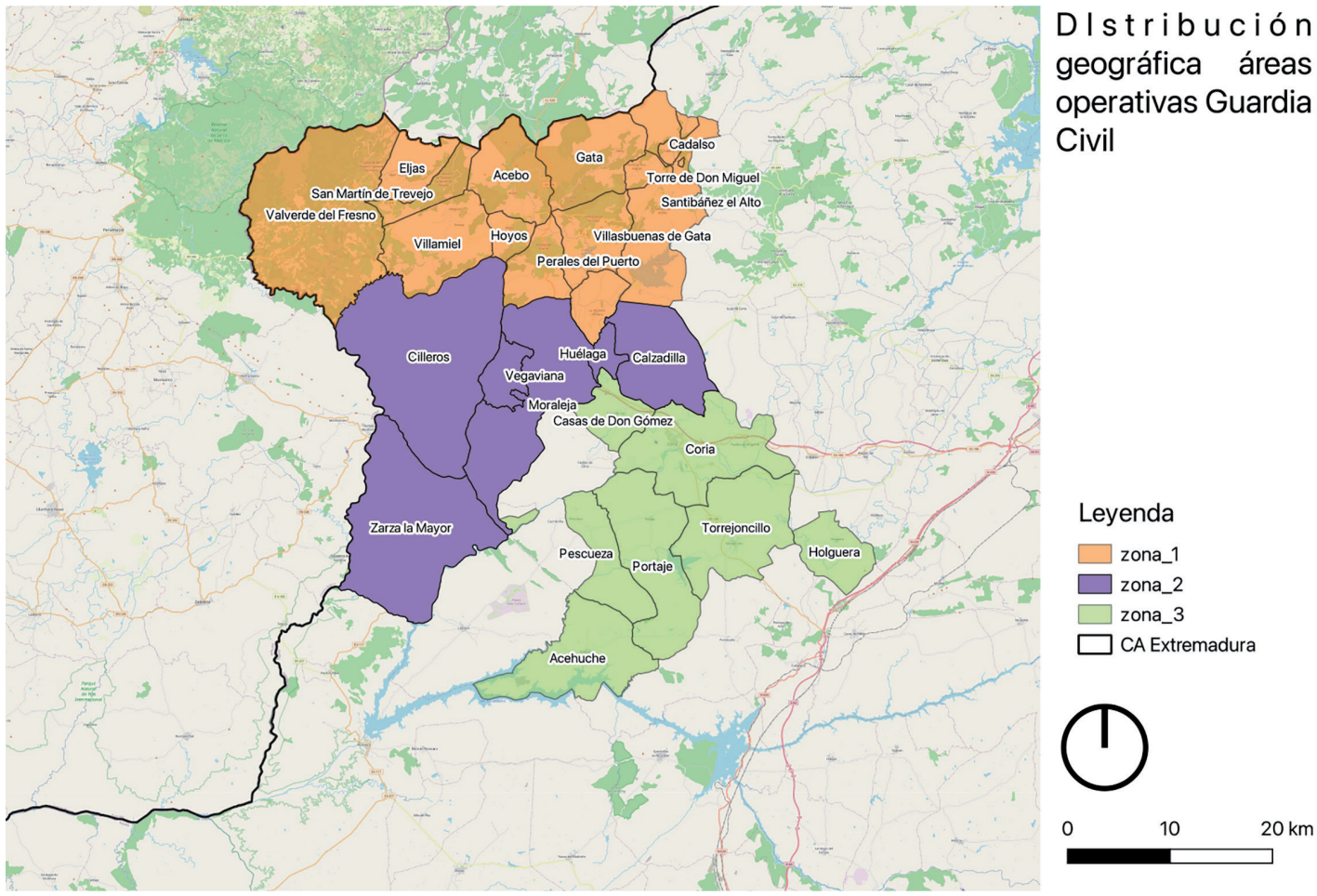
de Gata, San Martín de Trevejo, Santibañez el Alto, Torre de Don Miguel, Torrecilla de los Ángeles, Trevejo, Valverde del Fresno, Vegaviana, Villabuenas de Gata, Villamiel y Villanueva de la Sierra.

5. El Centro de Atención de Urgencias y Emergencias de la Junta de Extremadura clasifica las incidencias como Seguridad Pública en seis bloques: Seguridad Pública contra la seguridad colectiva (alteración del orden público, consumo. Salud Pública, Riñas y Altercados, Amenazas, Objetos sospechosos, etc.); Seguridad Pública contra las personas (Malos tratos, delitos sexuales, incidentes con menores, amenazas, secuestros, etc.); Seguridad Pública contra la propiedad (Robo, Timo, Daños a la propiedad, etc.) Delitos contra el medio ambiente (Caza y pesca, vertidos, otros…); Incidentes relacionados con el tráfico y Otros (pérdida de objetos, alarmas, convivencia o incidentes inmigración).

6. La localidad de Coria cuenta con el puesto más importante de la zona estudiada. Y por lo tanto, el único que permanece abierto las 24 horas del día.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Mapa 2. Distribución geográfica de los Núcleos Operativos de la Compañía de Coria.



Nota: Elaboración propia a partir de los datos obtenidos de Junta de Extremadura y 112.

Además, los servicios policiales cuentan con nuevas herramientas telemáticas para la prevención y actuación policial como *AlertCops o VioGen*. La herramienta AlertCops es un sistema gratuito que tiene como objetivo mejorar el acceso de la ciudadanía a los servicios públicos de seguridad ciudadana (Policia Nacional y Guardia Civil)[7]. Sobre esta cuestión, trataremos posteriormente en nuestras conclusiones.

En definitiva, estos datos no sólo demostrarían la necesidad de estudiar estas áreas, sino el importante esfuerzo humano, que los efectivos policiales deben realizar día tras día en las áreas rurales de la región extremeña y las consecuencias que esto tiene entre la población de las áreas rurales.

IV. Metodología

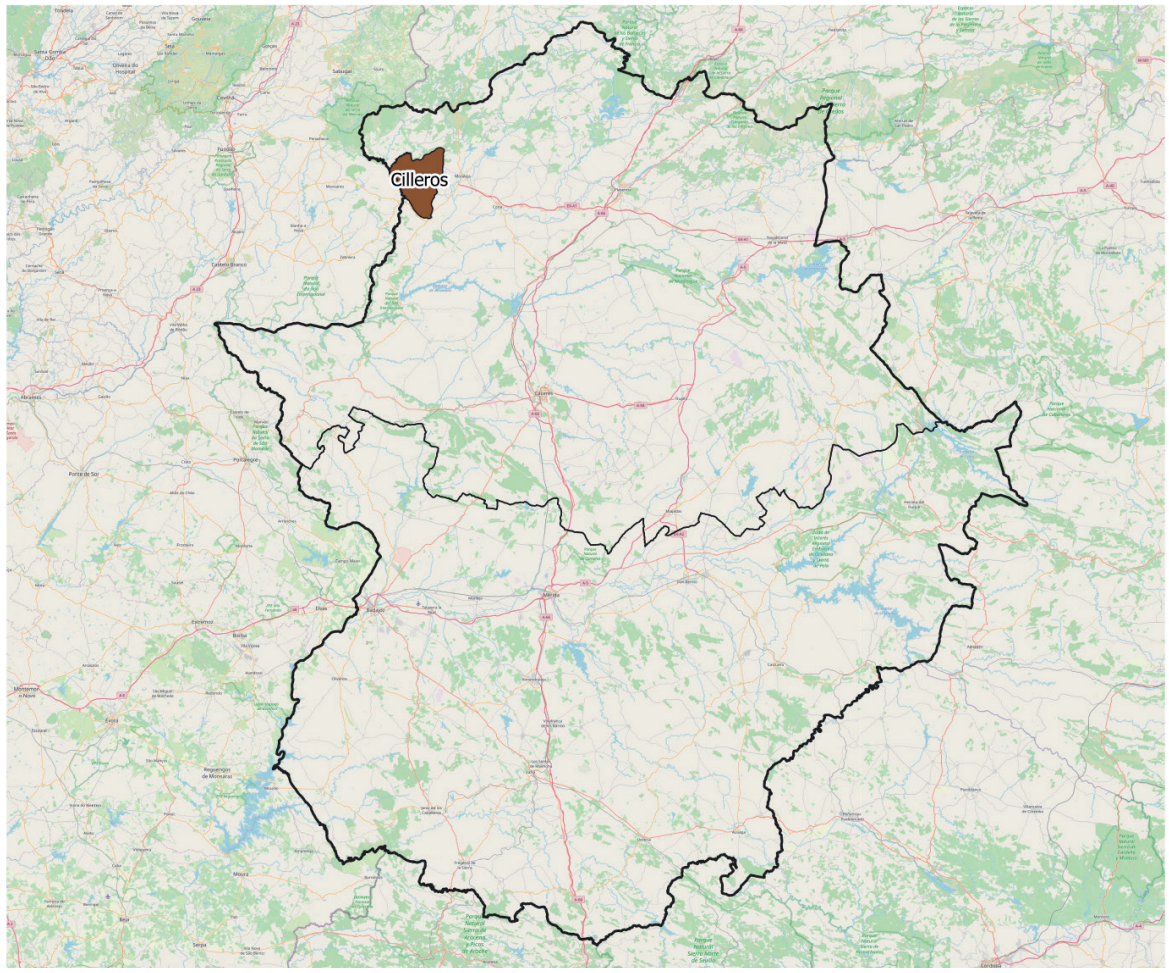
Después de corroborar la falta de investigaciones criminológicas en el medio rural de nuestro país. El objetivo principal de esta investigación es conocer la percepción de inseguridad y miedo al delito que existe en las áreas rurales españolas a partir de un micro-estudio llevado a cabo en la localidad de Cilleros, un municipio situado al

7. Se trata de un aplicación desarrollada por el Ministerio del Interior, que permite avisar a las fuerzas y cuerpos de seguridad de cualquier delito y conocer la ubicación de la víctima, ver: https://alertcops.ses.mir.es/publico/alertcops/ [última consulta 1 de agosto de 2023].

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

noroeste de la provincia de Cáceres en la Comunidad Autónoma de Extremadura cercano a Portugal, y un término municipal de 208 km^2 con apenas 1.617 habitantes (INE, 2022). El municipio tiene unas características socioeconómicas singulares por su enclave geográfico en la región extremeña. La localidad se encuentra situada a 800 metros de altitud entre la espesura de sus montes (Flores, 2018), como puede verse en el siguiente mapa temático:

Mapa 3. Área de estudio: Municipio de Cilleros (Provincia de Cáceres).



Área de estudio: Localidad de Cilleros (Provincia de Cáceres).

Nota: Elaboración propia a partir del software Qgis (versión 3.30).

Junto al objetivo principal de esta investigación, hemos podido analizar otras cuestiones como: la percepción de inseguridad según algunas variables individuales de las personas encuestadas (sexo, edad, situación laboral o nivel educativo), sí han sido víctimas de un hecho delictivo, las posibles causas que provocan inseguridad en aquellas personas que afirman no sentirse seguras en la localidad, conocer la percepción de necesidad o no de aumentar la presencia policial en el municipio y conocer los problemas en la gestión de la seguridad provocado por la falta de servicios policiales en determinados horarios a partir de un análisis de redes con sistemas de información geográfica.

La consecución de dichos objetivos permitirá conocer el estado general en el que se encuentra la población cillerana respecto a esta cuestión, así como ofrecer una visión de la percepción de inseguridad y miedo al delito en zonas rurales, una mirada que permita mejorar las políticas y estrategias locales de seguridad en el medio rural.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Para llevar a cabo esta investigación se han realizado dos estudios. Por un lado, se ha realizado una encuesta a 316 personas que residen habitualmente en la localidad de Cilleros. La muestra recogida resulta representativa, con un nivel de confianza de un 95% y un 5% de margen de error. Las personas que han participado en esta investigación suponen aproximadamente un 19,5% del total de población mayor de edad.

El método utilizado ha sido mediante un cuestionario de elaboración propia, el cual ha podido cumplimentarse tanto de forma digital, a través de un formulario de Google Forms, como en formato papel. Durante el mes de noviembre de 2022 se repartieron un total de 100 copias de ésta entre los habitantes del municipio mayores de edad.

Además, se han obtenido datos de la Guardia Civil de la localidad respecto a la gestión de los servicios policiales de la localidad y su entorno. Tanto a nivel de actuación como de servicios.

La encuesta se administró durante el último trimestre de 2022 en la localidad de Cilleros. La participación se propuso directamente a las personas que teníamos acceso en los lugares públicos del municipio. Las personas que accedieron voluntariamente a participar, se les explico el objeto de la investigación, así como su anonimato y consentimiento informado. La duración aproximada de la encuesta fue de cinco minutos.

Una vez recogida la muestra, con el objeto de poder efectuar el posterior análisis estadístico, se ha diseñado y estructurado una base de datos, y una selección de campos, que constituyen un elemento esencial para la consecución de los objetivos marcados en este estudio: edad, sexo, profesión, ¿Ha sido víctima de un delito en los últimos 12 meses?, ¿Cómo se siente en Cilleros?, En el caso de sentirse inseguro/a ¿Cuál sería la causa? ¿Cree usted que es necesario aumentar la presencia policial en Cilleros?.

Posteriormente, se ha producido la medición de esta información, etapa fundamental, para disponer de datos fiables y exactos en los que fundamentar nuestra investigación y conclusiones. Los resultados de tablas y gráficos se han realizado con el programa estadístico SPSS versión 27[8].

Para la segunda fase de la investigación, hemos realizado una análisis geoestadístico a partir de la información obtenida sobre la gestión de los servicios policiales en la localidad de Cilleros por parte de la Guardia Civil. El objetivo ha sido comprobar el tiempo de respuesta de los servicios policiales en el área de estudio. Concretamente, sí la prestación del servicio de una patrulla sería adecuada a una situación de emergencia en la zona. Para ello, el software que hemos utilizado para este trabajo es Qgis (versión 3.30).

A continuación, vamos a mostrar los principales resultados de nuestra investigación.

8. La Universidad de Extremadura cuenta con una licencia del software SPSS para personal investigador, ver: https://www.unex.es/organizacion/servicios-universitarios/servicios/siue/funciones/gestion_corporativa/software

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

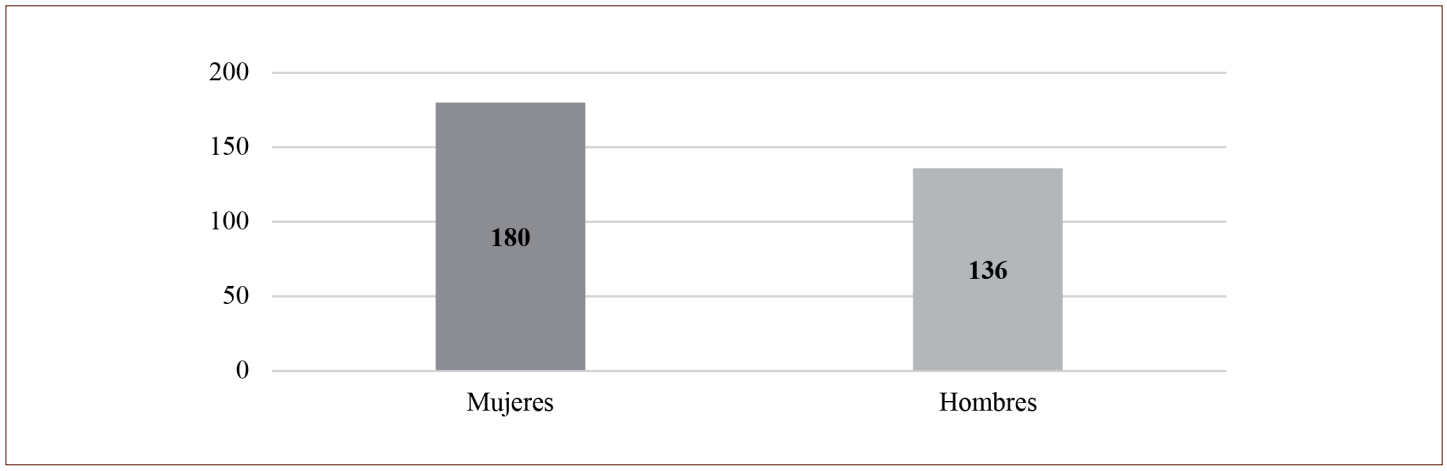
V. Resultados

Los resultados que exponemos a continuación deben ser analizados teniendo en cuenta las propias limitaciones que tiene cualquier investigación en el medio rural, como la falta de datos oficiales por parte de las distintas administraciones. Y a pesar, que los resultados de la investigación podrían ser más extensos, sólo abordaremos aquellas cuestiones más importantes, teniendo en cuenta las variables más significativas que recogen los estudios de Criminología respecto a la percepción de inseguridad o miedo al delito, como son: sexo, edad o situación laboral.

5.1. Resultados sobre percepción de inseguridad y medio al delito

La muestra de los resultados se ha dividido en cuatro bloques, los cuáles se corresponden al objeto principal de la investigación y otros objetivos secundarios del estudio. En el primer bloque, se analiza el perfil de las personas encuestadas. El segundo de los bloques analizará los resultados en cuanto haber sido víctima de un hecho delictivo en los últimos doce meses. En tercer lugar, se expondrán los resultados sobre las posibles causas de inseguridad de aquellas personas que manifestaron percepción de inseguridad. En último lugar, se analiza la necesidad de una mayor presencia policial en el municipio. Con respecto a las variables individuales de las personas encuestadas, el 56% son mujeres (n=180) frente al 43% que son hombres (Gráfico 1):

Gráfico 1. Personas encuestadas según el sexo.



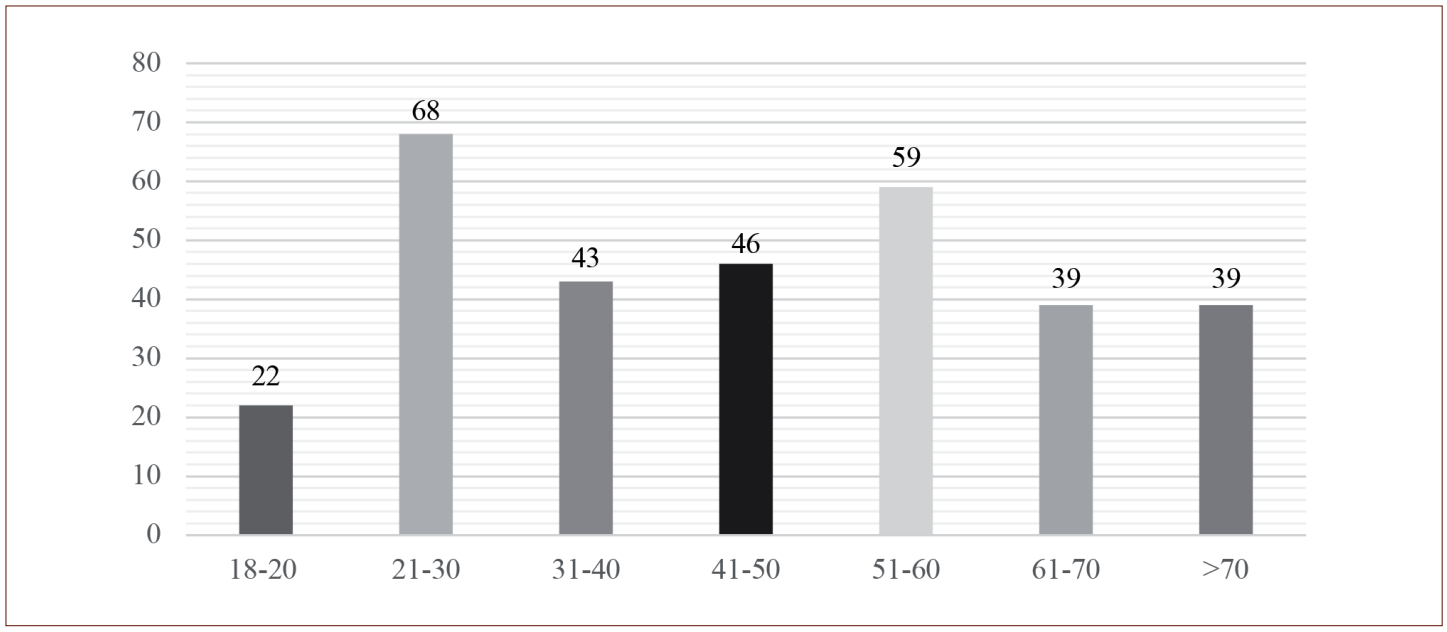
Nota: Elaboración propia a partir de los datos obtenidos en la encuesta.

En cuanto a la edad de las personas encuestadas, la distribución ha sido la siguiente: un 6’96 % son personas entre 18 y 20 años (ambos inclusive), un 21’51%, entre 21 y 30 años (ambos inclusive), un 13’6 %, entre 31 y 40 años (ambos inclusive), un 14’5 %, entre 41 y 50 años (ambos inclusive), un 18’6 por ciento, entre 51 y 60 años (ambos inclusive), un 12’3 por ciento, entre 61 y 70 años (ambos inclusive) y el resto de personas mayores

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

de 70 años, suponen también un 12’3 por ciento de las personas encuestadas, como se puede observar en el siguiente gráfico.

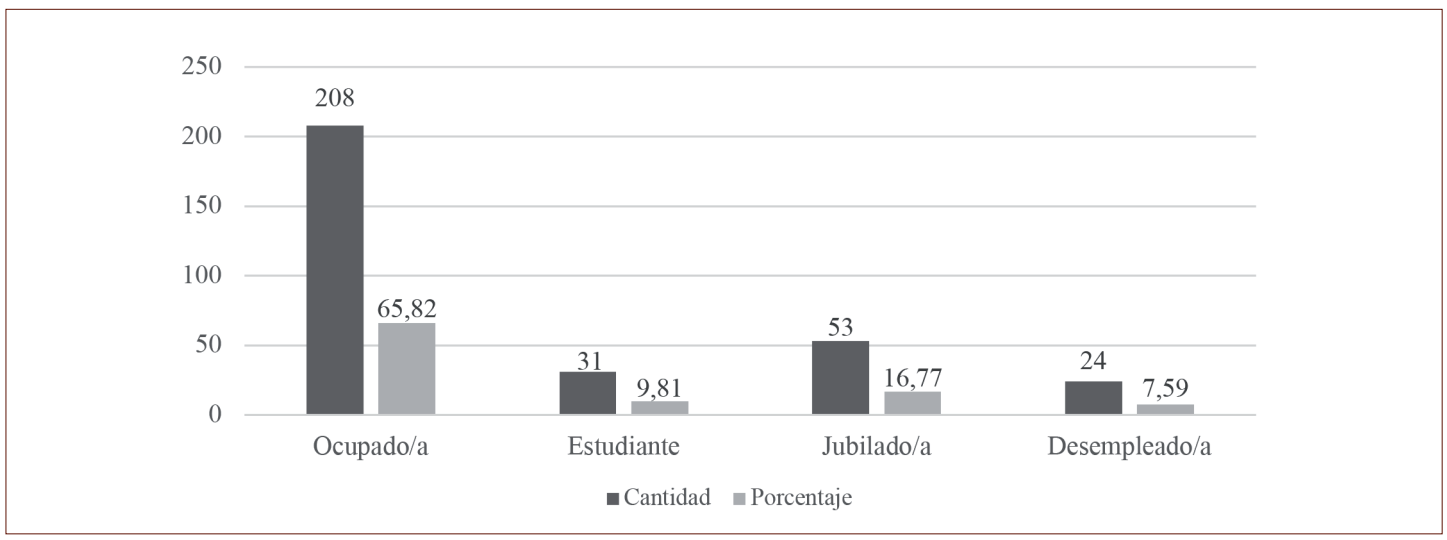
Gráfico 2. Personas encuestadas según su edad.



Nota: Elaboración propia a partir de los datos obtenidos en la encuesta.

En tercer lugar, respecto a una última característica personal de las personas encuestadas, situación laboral, ha sido muy heterogénea la respuesta, por lo que las hemos agrupado, al objeto de sistematizar la información. De este modo, de las 316 personas encuestadas, un 65’82 por ciento (n= 208) desempeña multitud de ramas laborales, lo que ha provocado dicha necesidad de agrupación en un grupo con denominador común; un 16’77 (n=53) percibe una pensión de jubilación; un 9’81 por ciento (n=31) se encuentran estudiando distintos niveles académicos; mientras que el 7’53 por ciento (n=24) se encuentra en situación de desempleo (véase, Gráfico 3):

Gráfico 3. Personas encuestadas según su situación laboral



Nota: Elaboración propia a partir de los datos obtenidos en la encuesta.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

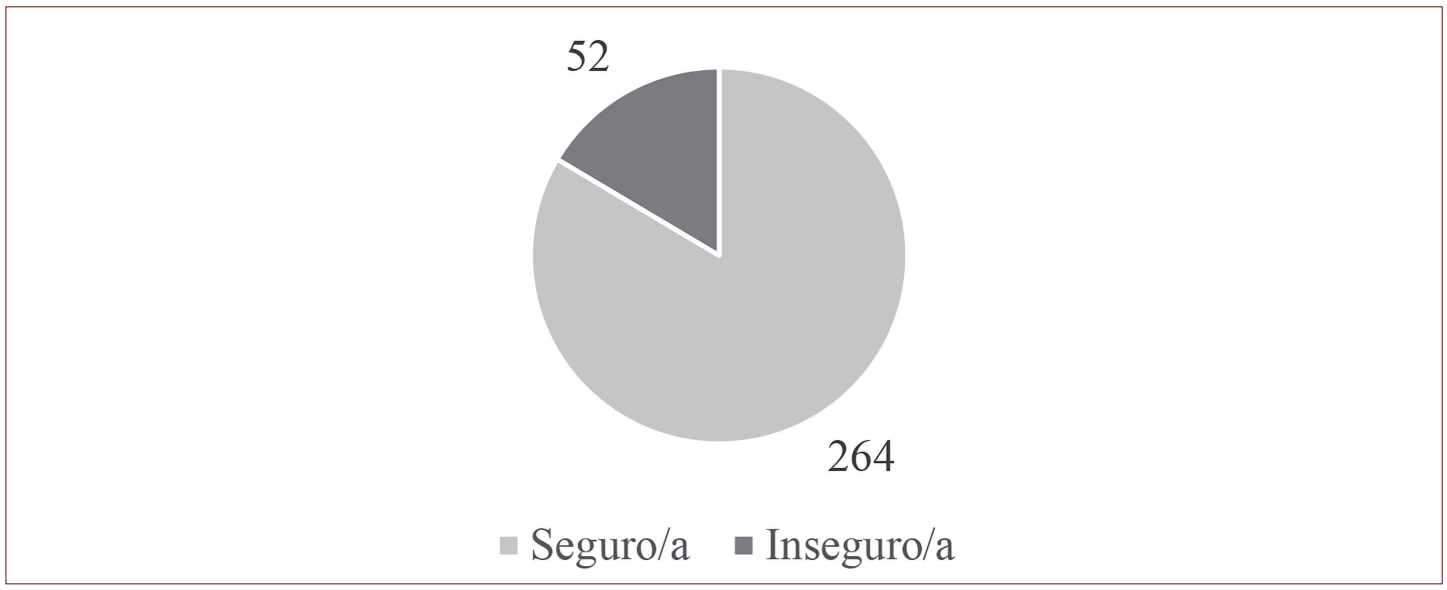
Respecto al segundo bloque, indicar que 21 personas afirman haber sido víctima de un hecho delictivo en los últimos doce meses, un dato significativo teniendo en cuenta el tamaño de la localidad y la muestra analizada para la investigación, lo que supone un 6,6 % de las personas encuestadas, como puede verse en el siguiente gráfico:

Gráfico 4. Personas encuestadas víctimas de un hecho delictivo en los últimos 12 meses

Nota: Elaboración propia a partir de los datos obtenidos en la encuesta.

El tercer bloque analiza la percepción de inseguridad de las personas encuestadas. Se trata del apartado más importante desde un punto criminológico. Los resultados indican que mayoritariamente las personas se sienten seguras en la localidad, un 83,5 por ciento del total (n=264), frente a un 16 por ciento (n=52) que se siente insegura, como se puede observar en el siguiente gráfico:

Gráfico 5. Percepción de inseguridad en la localidad de Cilleros.



Nota: Elaboración propia a partir de los datos obtenidos en la encuesta.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Sobre esta misma cuestión, existen personas que las investigaciones criminológicas han apuntado como más vulnerables a ser víctimas de un delito como son las mujeres y las personas mayores. Del total de personas que dicen sentirse inseguras, el 60 % (n= 31) son mujeres. Lo que supone un 17,2% del total de las 180 mujeres encuestadas (Gráfico 6). En el caso de las personas mayores, hemos seleccionado a aquellas con edad igual o superior a 60 años (n=87). El resultado muestra que un 20'6 % de este grupo se sienten inseguras, frente, al 79,4 % que sí se sienten seguras. Del grupo de personas que se sienten inseguras, un total de 8 personas tienen edades comprendidas entre los 60 y 70 años, lo que supone un 44'44 % del total de ciudadanos inseguros; mientras que 10 personas con edad superior a 70 años, traduciéndose en el 55'55 % del total de las 47 personas mayores entrevistadas (Gráfico 7):

Gráfico 6. Percepción de inseguridad entre las mujeres.

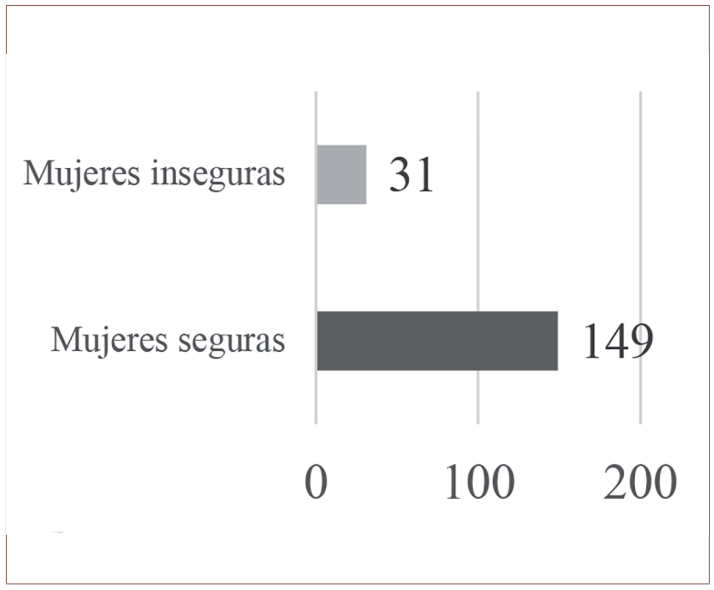
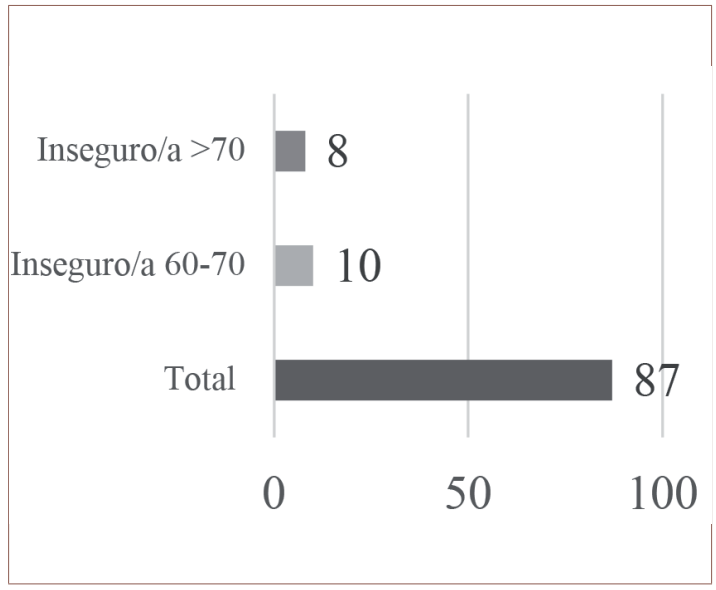


Gráfico 7. Percepción de inseguridad entre personas mayores.



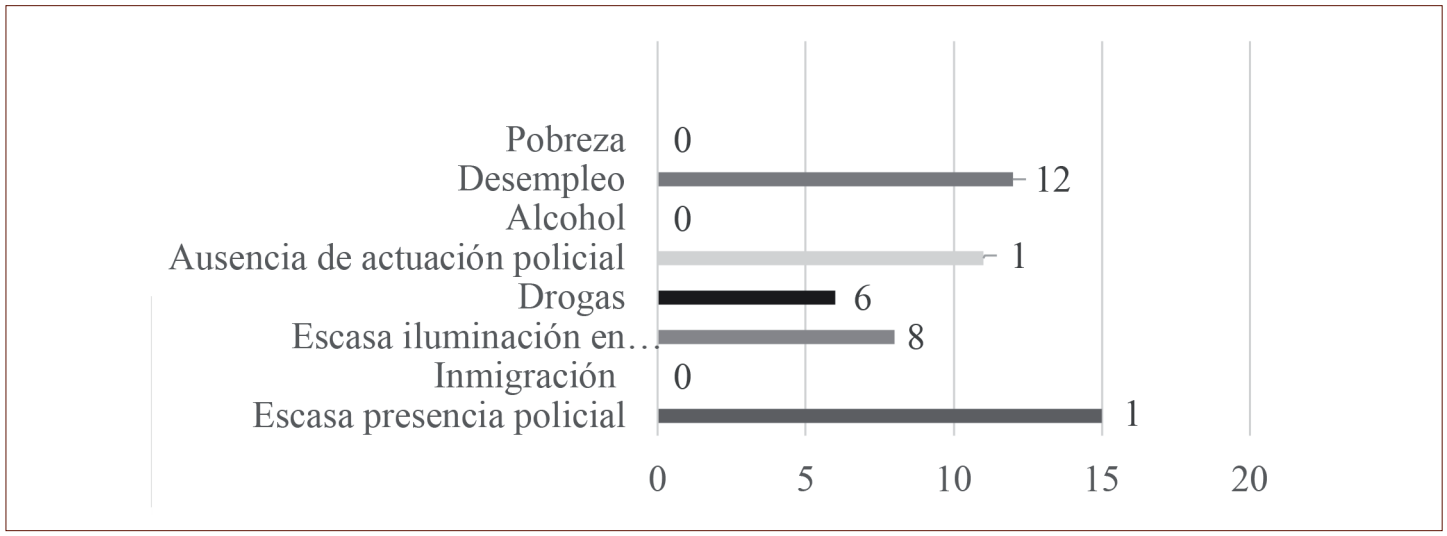
Nota: Elaboración propia a partir de los datos obtenidos en la encuesta.

Otro factor que incide en la percepción es la propia experiencia de victimización o de personas conocidas. En esta investigación, un 19 % de las personas que se sienten inseguras (10) han sido víctimas de un delito en los últimos doce meses. Sin duda, un factor determinante y relacionado con el miedo y la percepción de inseguridad.

Junto a la percepción de inseguridad, la investigación analiza las causas por las que las personas encuestadas se sienten inseguras. Un total de 52 personas respondieron a esta pregunta, de las que 15 (28'8 %) atribuyeron su inseguridad a la ausencia de actuación policial. La segunda de las causas más señalada como culpable de la inseguridad percibida es el desempleo, con un 23'07 por ciento. Por último, las causas menos señaladas han sido: la escasa iluminación existente en determinadas zonas con un 15'3 por ciento; y por otro lado, las drogas con un 11'53 por ciento, como se puede ver en el siguiente gráfico:

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

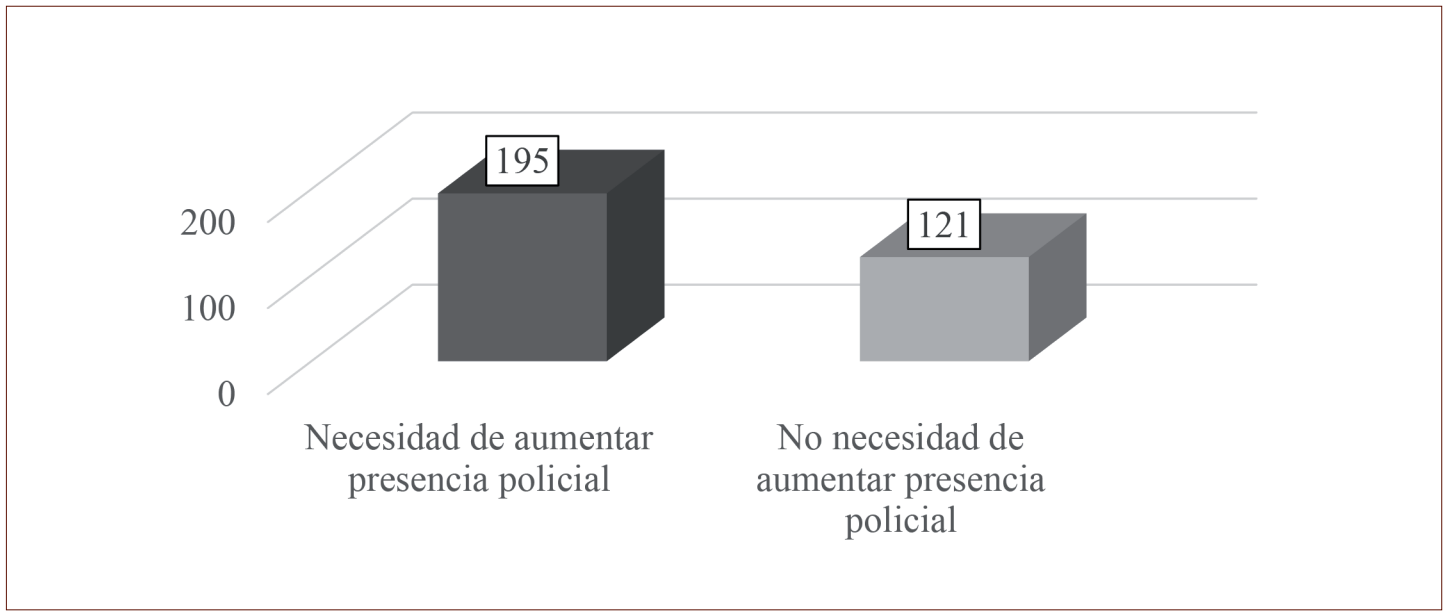
Gráfico 8. En caso de sentirse inseguro/a ¿Cuál sería la causa o el motivo?



Nota: Elaboración propia a partir de los datos obtenidos en la encuesta.

En último lugar, analizamos la respuesta de la población de Cilleros respecto a la presencia de servicios policiales en el municipio. Sin duda, la falta de servicios públicos en el medio rural está siendo fuente de un gran debate entre operadores políticos y sociales. Sin embargo, los servicios policiales en las áreas rurales no parecen estar en la agenda de los partidos políticos, centrando en resolver otros problemas como la sanidad, la educación o la economía de los municipios rurales. Y en este sentido, los resultados muestran que un total de 195 personas encuestadas confirmaron la necesidad de aumentar la presencia policial en la localidad, lo que supone un 61,7% frente al 38,3% que consideran que no es necesaria aumentar los servicios locales de Cilleros:

Gráfico 9. ¿Cree usted necesario aumentar la presencia policial en Cilleros?



Nota: Elaboración propia a partir de los datos obtenidos en la encuesta.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Sobre esta cuestión, las respuestas de mujeres y de personas mayores sobre la necesidad de aumentar la presencia policial en el municipio, se han obtenido los siguientes resultados:

En cuanto a las mujeres, los resultados obtenidos corroboran los extraídos sobre la percepción de inseguridad, pues en aquel caso se observaba que había mayor número de mujeres inseguras que hombres, por lo que cobra sentido que de las 180 mujeres encuestadas, 120 hayan afirmado que es necesario aumentar la presencia policial, lo que supone el 66'6 % de las que han participado, frente al 33'4 % que han manifestado la no necesidad de incrementar la presencia policial en la localidad.

Además, los datos recogidos sobre las personas mayores entorno a esta cuestión, muestra que el 20'6 % sienten inseguridad, por ende, en este caso de los 87 individuos considerados como personas mayores, al tener una edad superior a 60 años, 69 han respondido afirmativamente sobre la necesidad de aumentar la presencia de las FFCSE en la población, suponiendo 79,31 % del total de la muestra (n=87), frente al 20,69 % (n=18) que han manifestado que no es necesario aumentar la presencia policial.

5.2. Análisis geoestadístico de la seguridad en Cilleros

A partir de la información obtenida por parte de los efectivos de la Guardia Civil en la localidad de Cilleros, hemos querido analizar a partir del uso de sistemas de información geográfica, las consecuencias que tiene sobre la población, la situación actual que tiene el modelo policial actual para la protección de la seguridad en las áreas rurales.

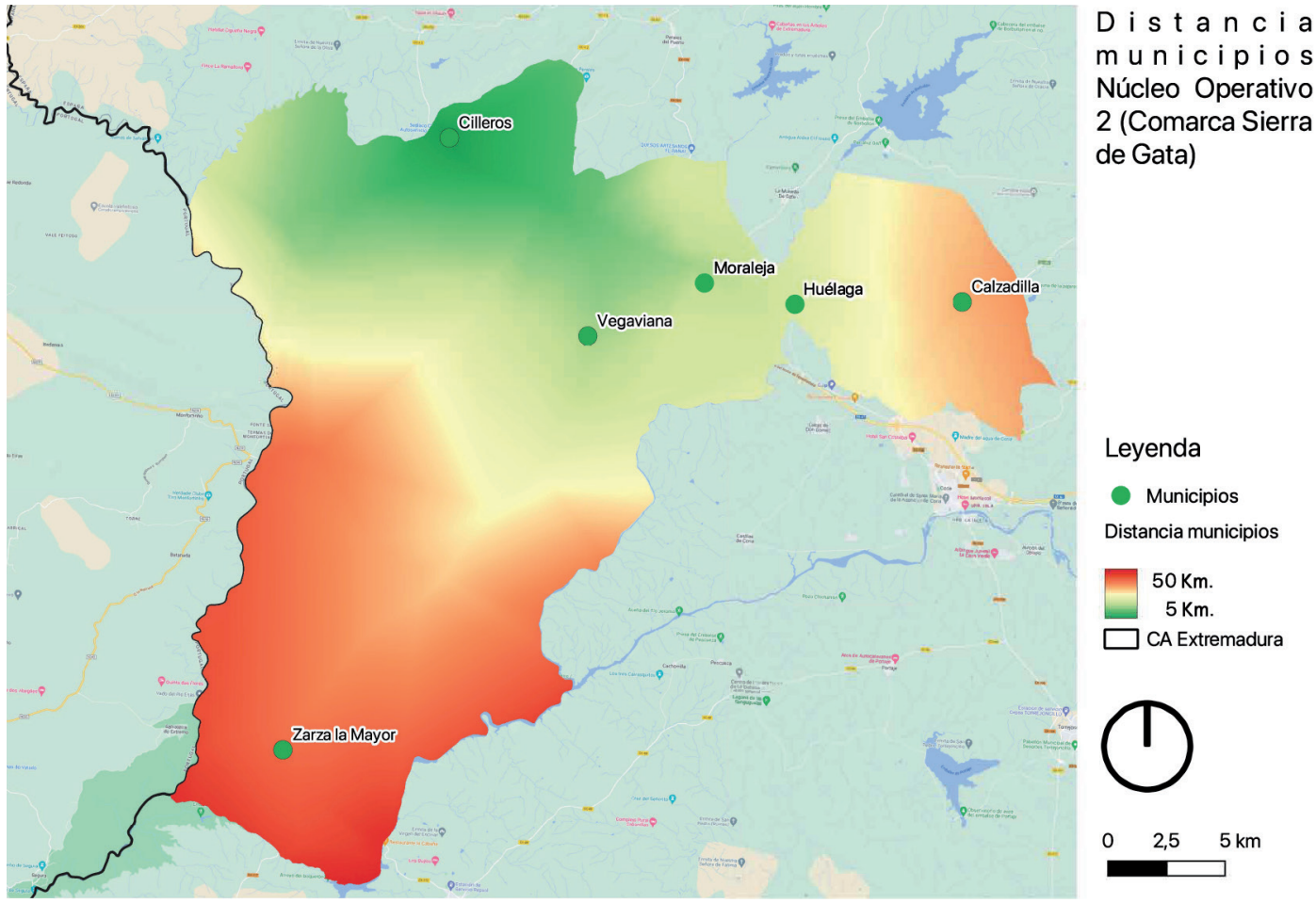
Como ya hemos indicado en el punto 2 de este trabajo, la seguridad en el área de estudio cuenta con un núcleo operativo dividido en 3 zonas. Y estos núcleos operativos tienen un vehículo patrulla en determinados horarios. La localidad objeto de estudio (Cilleros), se encuentra dentro del Núcleo Operativo 2. Esta zona la conforman las siguientes localidades: Vegaviana (845 ha.), Moraleja (6.685 hab.), Huélaga (210 hab.), Calzadilla (464 hab.) y Zarza la Mayor (1.192 hab.), es decir, que la población que reside dentro de este núcleo, incluido la localidad de Cilleros, es de aproximadamente 11.000 habitantes, un dato nada significativo, si tenemos en cuenta que es una patrulla la que presta servicio para toda la zona[9].

El siguiente mapa observamos un supuesto de actuación policial, en el caso que el vehículo patrulla se encuentre en el municipio de Cilleros, y tenga que desplazarse a otra localidad dentro de su núcleo operativo. El color rojo muestra que el coche patrulla tendría que recorrer hasta 50 kilómetros para llegar a la localidad de Zarza la Mayor, lo que supondría más de 30 minutos en llegar a esa localidad. El tiempo sería menor posible, pues no tenemos en cuenta si esa patrulla se encuentra en una actuación policial, lo que provocaría que el tiempo de reacción fuera superior.

9. La localidad de Moraleja cuenta con policia local. Sin embargo, de lunes a viernes el servicio no se presta las 24 horas del día.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Mapa 4. Distancia entre la localidad de Cilleros y resto de municipios del Núcleo Operativo 2 de la Guardia Civil.



Nota: Elaboración propia a partir del análisis con la herramienta QNEAT3.

En la siguiente tabla se puede observar la distancia en kilómetros y minutos que debe recorrer una vehículo policial estacionado en la localidad de Cilleros al resto de municipios que se encuentran dentro de su núcleo operativo:

Tabla 2. Distancia entre Cilleros y municipios del Núcleo Operativo 2

Municipios	Distancia (km)	Tiempo (min)
Cilleros - Vegaviana	13 Km.	14 min.
Cilleros - Moraleja	14 Km.	15 min.
Cilleros - Zarza la Mayor	35 Km.	32 min.
Cilleros - Calzadilla	31 Km.	28 min.
Cilleros - Huélaga	18 Km.	20 min.

Nota: Elaboración propia a partir del análisis de redes QNEAT3.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

VI. Discusión y conclusiones

Las áreas rurales han sido consideradas por la literatura criminológica lugares de bajo interés criminológico. Sin embargo, estos últimos años ha crecido el interés por parte de algunos países, por los problemas de criminalidad en el medio rural y las diferencias delincuenciales con las áreas urbanas (Hollis y Hankhouse, 2019:177-180). Así, cuestiones delincuenciales como la violencia de género, continúan siendo un elemento de preocupación destacado en estas áreas rurales (Soriano, 2022).

Es más, esta preocupación por parte de operadores políticos, sociales o científicos han llevado al desarrollo de acciones y estrategias para mejorar la calidad de vida de las personas que residen en ciudades o espacios con una mayor concentración de población. Unas políticas que se llevan a cabo con resultados similares a áreas menos pobladas, por lo que nos hemos preguntado: *¿Cuáles son los motivos que provocaría la falta de interés por la seguridad el medio rural?* En nuestra opinión, el motivo más importante puede ser la invisibilidad de estas áreas por la falta de datos de las administraciones o la idealización de estos lugares, como lugares seguros y baja tasa de criminalidad, una imagen dudosa, por la falta de estos datos.

Por lo tanto, la primera y más importante de las conclusiones de este trabajo, es subrayar la necesidad de abordar la problemática de la seguridad y el delito en el medio rural de nuestro país.

En líneas generales, los resultados de nuestro estudio muestran porcentajes muy parecidos a algunas investigaciones llevadas a cabo en nuestro país (Encuesta de Victimización, 2023)[10]. Estos estudios concluyen que la ciudadanía tiene una percepción de inseguridad moderada o alta en función del lugar en el que residen, un hecho que provoca un interés y preocupación por la seguridad de estos lugares por parte de la literatura criminológica, algo que no ocurre en el medio rural.

En segundo lugar, respecto al perfil de las personas que se sienten inseguras. Los resultados muestran datos similares a estudios en áreas urbanas respecto a las variables sexo y edad. Nuestros datos confirman que las mujeres se sienten más inseguras (Guillén, 2020), a pesar de que la última Encuesta de Seguridad Pública de Catalunya de 2022 concluye que las diferencias entre ambos sexos era cada vez menor y que los hombres son numéricamente hablando, víctimas de delitos más frecuente que las mujeres, como apunta Guillén (2023). En todo caso, como apuntan algunas autoras (Batlle y Vasilescu, 2022; Almécija,2022), la falta de investigaciones en género y los resultados obtenidos, nos invitan a seguir analizando la victimización de las mujeres en las zonas rurales de nuestro país. Tal vez, esta es una de las principales críticas que podemos hacer a la comunidad criminológica de nuestro país, la falta de estudios de género en el medio rural. Cómo reflexión, según datos de la Subdelegación del Gobierno de Cáceres en 2022, la provincia de Cáceres tenía un total de 493 órdenes de protección en el medio rural, un

10. Ver: https://ajuntament.barcelona.cat/seguretatiprevencio/sites/default/files/2023-08/Victimitzacio_BCN_Informe_2023.PDF

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

dato lo suficientemente importante, para analizar cuestiones relacionadas con la seguridad de las mujeres en las zonas rurales.

En cuanto a la edad, la franja de edad que se siente más insegura son las personas mayores de 60 años, con un 20% del total de personas mayores entrevistadas. Y dentro de este grupo, los mayores de 70 años, es el grupo que manifiesta una mayor inseguridad. Se tratan de unos datos que corroboran los resultados obtenidos en otras investigaciones, que muestran diferencias entre los dos grupos de edad dentro de este colectivo (Vauclair y Bratanova, 2017; Bogacka, 2020).

Respecto a los factores que tienen incidencia en la inseguridad, a diferencia de lo que sucede en las ciudades, algunas cuestiones son menos importantes o, directamente, no lo son, como puede ser la ansiedad, aislamiento o la diversidad cultural (San Juan, Vozmediano y Vergara, 2012; Guillén, 2018). En cambio, si se muestra un porcentaje muy significativo de percepción de inseguridad debido a factores económicos como el desempleo (Doran y Burgess, 2012). Otras de las causas importantes de la percepción de inseguridad es la falta de servicios policiales o de actuación policial, un motivo que pueden deberse a la falta de policia local o el cierre del cuartel en horario nocturno o fin de semana, situación que no ocurren en las ciudades o áreas más pobladas de nuestro país. En este sentido, no podemos olvidar que los servicios policiales en las zonas rurales realizan tareas, que van más allá de su función estrictamente policial. Los efectivos policiales en el medio rural son los responsables de trasladar al gobierno local problemas de índole urbanístico, social o administrativo, sobre todo, en municipios con escaso personal administrativo. Se trataría de un aspecto que va más allá de la incidencia que tiene la presencia policial o mayor patrullaje respecto al descenso de la criminalidad (Medina, 2011). No podemos obviar, que las continuas noticias de hechos delictivos también llegan a las áreas rurales a través de los medios de comunicación o las redes sociales, lo que puede ser visto por la población que reside en estos lugares como una amenaza real. Por lo tanto, la falta de efectivos policiales puede aumentar ese temor por parte de la población que reside en estas áreas rurales.

En cuanto al número de personas encuestadas víctimas de un delito en la localidad de Cilleros (6 %), son datos parecidos a las obtenidos en las numerosas encuestas realizadas en Catalunya (Murría, Sobrino y González, 2020). Este dato evidencia la necesidad de analizar desde la criminología y, sobre todo, desde los operadores políticos y sociales, las políticas locales de seguridad en estos lugares. Desgraciadamente, sí no se hacemos evaluaciones de las políticas locales de seguridad a nivel nacional o regional, no esperemos que se realicen en el medio rural.

Con respecto al análisis geoestadístico, el resultado muestra claramente los problemas que pueden darse en el medio rural por la falta de servicios policiales. La distancia que deben recorrer las patrullas para atender una emergencia puede significar un peligro real para las víctimas. Además, no podemos olvidar que el descenso de los servicios policiales en periodo vacacional puede ser aún más dañoso en áreas rurales que en las urbanas, lo que puede suponer un perjuicio aún más significativo que en otros periodos del año, con la problemática que supone un aumento de la población durante época de vacaciones (Ortiz y Rufo, 2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Finalmente, indicar que los programas electorales de los principales partidos políticos en las elecciones generales de 2023, con la excepción de VOX, presentan algunas medidas sobre políticas de seguridad en el medio rural[11]. Y de todos ellos, el partido político que parece abordar con más claridad la problemática en torno a la seguridad de las áreas rurales es SUMAR[12]. Una evidencia que muestra claramente la existencia de una problemática entorno a la seguridad de nuestras áreas rurales, que debe ser abordada y analizada por parte de los poderes públicos.

VII. Propuestas a futuro para políticas locales de seguridad y prevención en el medio rural

Para concluir, queremos ofrecer algunas propuestas a operadores políticos y personal investigador con vistas a evaluar o estudiar políticas locales de seguridad en el medio rural:

- Primero: La necesidad de evaluar las medidas aprobadas en las últimas leyes sobre reto demográfico, que incluyen en su articulado cuestiones relativas a la seguridad y prevención de la delincuencia[13].
- Segundo: Evaluar algunas de las estrategias implementadas por los gobiernos para mejorar la seguridad en las zonas rurales como AlertCops o VioGen[14].

11. En el caso de Extremadura, el acuerdo programático entre PP y VOX, sí menciona la seguridad en el medio rural. La medida número 60 recoge lo siguiente: "Exigiremos el orden público y la seguridad de los barrios y zonas rurales, ambos pilares prioritarios de este gobierno". En todo caso, deberían desarrollarse esas medidas.

12. El programa de Sumar recoge entre las páginas 127 a 130 las Políticas de Seguridad y Prevención. Concretamente, el punto 4 dice lo siguiente: Propondremos una comisión parlamentaria para reabrir el debate sobre el modelo policial español. Es preciso impulsar un nuevo modelo policial que delimite adecuadamente sus funciones sobre el principio de subsidiariedad frente a otros actores sociales e institucionales, que sirva para profundizar en su profesionalidad y su modernización y que acentúe su carácter de institución al servicio de la ciudadanía. El nuevo modelo ha de apostar por estructuras menos burocráticas, más horizontales y flexibles, con mayor capacidad para la colaboración con otras administraciones, más abierto a la participación ciudadana y con una mejor capacidad de planificación, gestión de la información y adaptación al cambio tecnológico. Este modelo tendrá. que reconocer las particulares necesidades y retos del ámbito rural y de la España vaciada. Esta comisión propondré las líneas maestras para la reforma de la Ley de Fuerzas y Cuerpos de Seguridad del Estado (FCSE) de 1986, a fin de diseñar un nuevo mapa de funciones actualizado a los retos de seguridad actuales, as. como nuevos mecanismos de coordinación y colaboración entre el nivel municipal, el autonómico y el central.

13. En el caso de nuestro país, distintos Ministerios han incorporado entre sus líneas de actuación el medio rural. A modo de ejemplo, encontramos cuestiones relativas al desarrollo rural en el Ministerio de Transición Ecológica y el Reto Demográfico, Ministerio de Política Territorial o el Ministerio de Agricultura, Pesca y Alimentación. Las Comunidades Autónomas han aprobado o están elaborando normas para fomentar o mejorar el medio rural. A modo de ejemplo, la Ley 2/2021, de 7 de mayo, de Medidas Económicas, Sociales y Tributarias frente a la Despoblación y para el Desarrollo del Medio en Castilla la Mancha.

14. A modo de ejemplo, en la provincia de Cáceres, de los 48 municipios que tienen policia local, sólo la localidad de Navalmoral de la Mata tienen acceso a VioGen. La localidad de Plasencia también

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

— Tercero: La necesidad de crear foros de debate tan importantes en materia de prevención y seguridad como FEPSU. Se trata de crear espacios de discusión para núcleos con menos densidad de población o el medio rural, como sucede en el Fórum Español para la Prevención y la Seguridad Urbana.
— Cuarto: Analizar el papel de la seguridad privada en el medio rural. Se trata de un servicio cada vez más demandado por los gobiernos locales de municipios rurales, es habitual encontrarnos servicios de seguridad privada para la gestión de espectáculos públicos o actividades recreativas, una labor que debería ser asumida por nuestras fuerzas y cuerpos de seguridad, cómo lo indica nuestra Constitución Española (art. 104 CE). Analizar el coste que supone a las administraciones locales de estos pequeños municipios el uso de estos servicios, por falta de servicios públicos, y que sean las distintas administraciones las que asuman esos gastos, suponen un importante ahorro para estos ayuntamientos, que día a día ven empobrecidos sus presupuestos por descenso de su población. Por ejemplo, las administraciones o instituciones como las Diputaciones Provinciales deberían crear partidas económicas específicas para los municipios rurales referentes a políticas locales de seguridad. Un presupuesto que permitiría asumir de forma eficiente estos servicios, sí el propio Estado no puede hacerlo, no sólo en formación como sucede actualmente.

En definitiva, entendemos que son numerosos los problemas criminológicos que podemos estudiar en las áreas rurales, esperemos que este trabajo sea un punto de partida significativo para futuras investigaciones en nuestro país.

Agradecimientos

Los autores quieren agradecer el trabajo diario de los efectivos policiales que desarrollan sus tareas en el medio rural, al Centro de Atención de Urgencias y Emergencias 1.1.2. de la Comunidad Autónoma de Extremadura por su apoyo en esta investigación y, especialmente, al Capitán de la UOPJ de la Comandancia de la Guardia Civil de Cáceres D. Marcelino Gil García, por su labor en la protección del medio rural durante toda su vida.

lo ha solicitado, pero dada la situación actual, creemos que el acceso a esta información por parte de las policías locales, más allá de la comisiones o las buenas prácticas y colaboración entre distintas fuerzas de seguridad, es fundamental en las áreas rurales, siendo los cuerpos policiales más próximos a la ciudadanía, en estas áreas, en muchas ocasiones.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

Bibliografía

AlertCops. https://alertcops.ses.mir.es/publico/alertcops/

ALMÉCIJA, A. (2022). La perspectiva de género. La gran ausente en la teoría de las ventanas rotas. En Guillén, F. y Brotat, R. (Coords.) *40 años de ventanas rotas. Luces y Sombras*. Bosch. Pp. 105 – 129.

BATLLE, A. y VASILESCU, C. (2022). La perspectiva de género en el estudio de las instituciones y el control del delito. En Medina J.J. (Coord.). *Instituciones de Control del Delito*. Dykinson.

BOGACKA, E. (2020). Safety of urban park users: The case of Poznan Poland. En Ceccato, V. y Nalla, M. (edts.) *Crime and fear in public places. Towards safe, inclusive and sustainable cities*. Oxon, New York. Routledge. pp. 108-124.

CECCATO, V. (2016). *Rural crime and community safety*, Routledge, London.

CECCATO, V. y Abraham, J. (2022). *Crime and safety in the rural*. Springer.

Constitución Española. https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

DORAN, B.J. y BURGESS, M.B. (2012). *Putting Fear of Crime on the Map. Investigating Perception of Crime Using Geographic Information Systems*. New York. Dordrecht, Heidelberg, London. Springer.

DONNERMEYER, J. y DEKESEREDY, W. (2014). *Rural Criminology*, Routledge, London.

Encuesta de Seguridad Pública de Catalunya (2020). https://interior.gencat.cat/es/el_departament/publicacions/seguretat/estudis-i-enquestes/enquesta_de_seguretat_publica_de_catalunya/index.html

Encuesta de Victimización de Barcelona (2023). https://ajuntament.barcelona.cat/seguretatiprevencio/es/documentacion/encuesta-de-victimizacion-de-barcelona

FEPSU. https://fepsu.es

FLORES, A. (2018). *Cilleros, Detalles de su Arquitectura Popular*. Ayuntamiento de Cilleros.

GUILLÉN, F. (2018). Detecting and tackling the different levels of subjective security. En Barabàs, A.T. (ed.) The dimensions of insecurity in urban areas. Research on the roots of unsafety and fear of crime in European cities. Budapest National Institute of Criminology, pp. 61-82.

GUILLÉN, F. (2020). La falacia de la seguridad objetiva y sus consecuencias. En *International e-Journal of Criminal Sciencies*, 4, 15.

GUILLÉN, F. (2023). Las ventanas rotas y la importancia de la percepción de seguridad. En Guillén, F. y Brotat, R. (Coords.) *40 años de ventanas rotas. Luces y Sombras*. Bosch. Pp.75 – 104.

HOLLIS, M.E. y Hankhouse, S. (2019). The growth of rural criminology: introduction to the especial issue. *Crime Prevention and Community Safety*, 21, pp. 177-180

HUESCA, A. M. (2021). La seguridad desde la perspectiva subjetiva: el miedo al delito" en Huesca González, A. M., Quicios García, M. P., y Grimaldo Santamaría, R., (eds.), Seguridad *y ciudadanía*, Madrid, Dykinson.

Instituto Nacional de Estadística (2023). https://www.ine.es/dyngs/INEbase/es/categoria.htm?c=Estadistica_P&cid=1254735572981

La percepción importa (2021). https://interior.gencat.cat/es/el_departament/publicacions/seguretat/projecte-europeu-toolkit-la-percepcio-importa/index.html

MEDINA, J. J. (2011). Políticas y estrategias de Prevención del delito y Seguridad ciudadana. Madrid – Montevideo – Buenos Aires, Edisofer, B y F.

MURRÍA, Sobrino y González, (2020). Las políticas locales de seguridad (y prevención). En Medina J.J. (Coord.). *Instituciones de Control del Delito*. Dykinson.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

ORTIZ, J. (2022). *Mito o Realidad. Un estudio criminológico de las áreas rurales de Extremadura*. Dykinson.

ORTIZ y RUFO, (2023). Seguridad y prevención del delito en las comunidades rurales de Extremadura: un estudio de caso desde la criminología, *Revista de estudios Jurídicos y Criminológicos*, nº 7, Universidad de Cádiz, p. 8, DOI: https://doi.org/10.25267/REJUCRIM.2023.i7.07.

Qgis (versión 3.30). https://www.qgis.org/es/site/

Redondo S. y Garrido, V. (2023). *Principios de Criminología*. Tirant lo Blanch. p. 208.

UN-Habitat. https://unhabitat.org/es/node/2973

SAN JUAN, C. VOZMEDIANO, L. y VERGARA, A. I. (2012). Self – protective behaviours against crime in urban settings: An empirical approach to vulnerability and victimization models, En *European Journal of Criminology*, 9, pp. 652-677.

SAN JUAN, C. y VOZMEDIANO, L. (2021). *Guía de prevención del delito. Seguridad, Diseño Urbano, Participación Ciudadana y Acción Policial*. Editorial Bosch.

Sistema VioGen. https://www.interior.gob.es/opencms/ca/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen/

SORIANO, S. (2022). La respuesta a la violencia de género en las zonas rurales. En Soriano S. (Coord.). *Los derechos de las mujeres en las zonas rurales: Un estudio de caso.* Thomson Reuters Aranzadi, pp. 281 – 311.

VAUCLAIR, C.M. y Bratanova, B. (2017). Income inequality and fear of crime across the European Region. En European Journal of Criminology. Vol. 14 (2). pp. 221-241.

VOZMEDIANO, L. y San Juan, C. (2010). Criminología Ambiental: ecología del delito y de la seguridad. UOC. pp.19-22.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 42-63
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.03

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

El reglamento MiCA: responsabilidad y sanción frente al incumplimiento de la regulación del mercado de criptoactivos

THE MICA REGULATION: LIABILITY AND SANCTION FOR NON-COMPLIANCE ON MARKET IN CRYPTO-ASSETS REGULATION

María Ángeles Pérez Marín*
Profesora Titular de Derecho Procesal
Universidad de Sevilla
mapmarin@us.es 0000-0003-2503-535X

Recibido: 10 de noviembre de 2023 | Aceptado: 06 de diciembre de 2023

RESUMEN

Los criptoactivos se han convertido en una vía de financiación dentro del mercado único y, aunque el uso de los mismos es todavía limitado, se espera un exponencial aumento de sus aplicaciones. Incorporan, además, debido a su naturaleza digital, una clara proyección transnacional que es connatural a su naturaleza, que exige la convergencia entre la Unión y otros ordenamientos, órganos y organismos internacionales para prevenir la falta de confianza de los inversores e impedir la inestabilidad que se deriva de las regulaciones hasta ahora existentes.

El Reglamento MiCA pretende regular los denominados activos no regulados, clasificándolos en función del riesgo que conlleven e instituye una infraestructura de negociación, que se basa en un régimen sancionador frente al cumplimiento de las obligaciones impuestos a los proveedores de servicios. Es necesario distinguir, no obstante, entre las funciones sancionadoras frente al incumplimiento y la tipificación penal de las conductas.

PALABRAS CLAVE

Criptoactivos
Mercado financiero digital
Delincuencia financiera
Responsabilidad penal

* Este trabajo ha sido realizado en el contexto de las Ayudas para la recualificación del sistema universitario español para 2021-2023 (Modalidad B. Ayudas para la recualificación del profesorado universitario funcionario), desarrollada en la Universidad de Coímbra.

Miembro del Proyecto I+D+i DER PID2021-124027NB-100 "El Derecho procesal civil y penal desde la perspectiva de la Unión Europea: la consolidación del espacio de libertad, seguridad y justicia", dirigido por la Profª Mar Jimeno Bulnes, Catedrática de Derecho Procesal de la Universidad de Burgos.

IP Grupo de Investigación SEJ-308, La Administración de justicia en España y en América.

ABSTRACT

Crypto-assets have become a means of financing within the single market and although their use is still limited, an exponential increase in their applications is expected. They also incorporate, due to their digital nature, a clear transnational projection that is connatural to their nature, which requires convergence between the Union and other international systems, bodies and organisations in order to prevent a lack of investor confidence and prevent the instability resulting from the regulations that have existed up to now The MiCA Regulation aims to regulate so-called unregulated assets, classifying them according to the risk they entail and instituting a trading infrastructure, which is based on a sanctioning regime for compliance with the obligations imposed on service providers. However, it is necessary to distinguish between the sanctioning functions for non-compliance and the criminalisation of conduct.

KEYWORDS

Cripto-assets
Digital financial market
Financial crime
Criminal liability

I. Encuadramiento del tema

La dificultad de prevenir y perseguir la delincuencia transfronteriza, así como la complejidad de los procedimientos de cooperación penal instaurados en la Unión Europea se tornan aún más arduas en el ámbito la delincuencia económico-financiera, pues, en este caso, no solo es preciso adoptar medidas dirigidas a impedir y a prevenir la comisión delictiva, sino a proteger las vías financieras que, como instrumentos del delito, son utilizadas con miras a blanquear los beneficios del delito o a financiar la delincuencia organizada, incluyendo el terrorismo.

Tengamos en cuenta, así, varias circunstancias que nos pueden ayudar a entender el problema que entraña lo que estamos refiriendo. Por ejemplo, los límites de aquello que podemos considerar delincuencia económico-financiera dibujan en la Unión un contorno extraordinariamente difuso, incorporando conductas que pueden incidir exclusivamente en intereses particulares o extenderse hasta alcanzar a los intereses públicos –nacionales, compartidos o exclusivos de la Unión–. Por otro lado, los intereses financieros de la Comunidad, en un primer momento, y de la Unión, hoy, han constituido y constituyen una preocupación connatural a la esencia de la Unión Europea que instituyó como objetivo de los Tratados la prevención y la protección de sus intereses financieros, dando lugar a una producción normativa incesante que, con el paso del tiempo, ha derivado en un paisaje legislativo ambiguo, a veces de difícil comprensión y altamente especializado en el que confluyen instrumentos jurídicos de distinta naturaleza –mercantil, penal y administrativa– a los que se debe encontrar su propia ubicación para que surtan la eficacia que se espera de ellos. A este paisaje sumemos que las decisiones marco y las directivas no son directamente aplicables, sino que lo son las normas nacionales de transposición, generando tal circunstancia un panorama normativo no siempre compatible con aquella idea de "protección sin fisuras" que se proclama para todos los ámbitos de la Unión, porque ello exige una armonización o equivalencia normativa que no siempre se logra.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

Esta irremediable necesidad de intentar legislar todos los aspectos relacionados con la delincuencia financiera con el afán de conseguir un espacio judicial blindando –que no se muestra como un objetivo fácilmente alcanzable–, no es sino huida hacia delante que tiene, básicamente, dos motivaciones: la primera, que la evolución del delito es más rápida que la evolución normativa de la Unión –sometida a criterios procedimentales rígidos y lentos, que hacen especialmente pesada y burocrática la discusión y la toma de decisiones–; la segunda, derivada de la anterior, que obliga a legislar a remolque de la realidad, porque los instrumentos jurídicos nacen, debido en parte a la lentitud de los procedimientos legislativos, con una eficacia limitada que, debido a su aprobación tardía, impiden hacer frente a una realidad que probablemente se haya transformado para contornar la legalidad. Así, la aprobación de una norma tras otra ha venido a provocar una concatenación de instrumentos jurídicos sobre una misma materia, que también es el reflejo de un cierto fracaso de las políticas implementadas, toda vez que, si se hubiese conseguido prevenir, perseguir y frenar el delito de forma eficaz, no sería hubiera sido necesario continuar buscando soluciones que aporten un mayor grado de efectividad. Esta situación de diversidad normativa, tanto en lo que hace a la cantidad como a la naturaleza de los aspectos regulados, y que traba la pretendida homogeneidad del tratamiento jurídico de las situaciones, debilitan al mercado único.

Por otro lado, la afirmación de un espacio económico común y sin fronteras interiores, pero al mismo tiempo sólido, no solo hace referencia a las características del sistema implementado a fin de facilitar las transacciones dentro del territorio de la Unión, sino que componen el concepto que se promociona hacia el exterior de cara a la captación de inversiones de terceros Estados que permitan fortalecer la posición de la Unión como uno de los bloques económicos del actual tablero geopolítico (Jarne Muñoz, 2018, 119-120). Podemos decir de una manera más coloquial que Europa "vende al exterior" su estabilidad, ya sea esta política o financiera, y que las inversiones externas constituyen un elemento esencial para su desarrollo y el de los Estados, si bien no debe perderse de vista que la ausencia de fronteras internas en este espacio financiero único provoca las mismas consecuencias que se advierten de la eliminación de las fronteras físicas entre Estados, y es que unas vías financieras aparentemente menos controladas permiten la circulación del delito que se comete a través del uso de estas.

A partir de este panorama inicial la Unión bifurcó su actividad legislativa para contener las operaciones o transacciones sospechosas que pudieran ser constitutivas de una infracción administrativa o de un delito de blanqueo de capitales o de financiación del terrorismo. El primer paso para evitar los comportamientos irregulares consistió en la implantación de criterios reguladores dirigidos a las entidades financieras para que estas incorporasen medidas de diligencia debida frente a los clientes, esto es, controles que permitiesen prever la finalidad ilícita o irregular de las operaciones pretendidas y, en su caso, obstaculizar la transacción. A pesar de la relevancia que cabe apreciar en esta función preventiva, esencial en la actualidad, y que se fue perfeccionando hasta convertir a las entidades financieras y a los profesionales vinculados a este sector en la primera frontera frente al delito (Pérez Marín, 2022, 297-301), tal decisión no terminó de mostrare suficiente, optándose entonces por acudir al Derecho penal en tanto que

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

instrumento que, en general, se presume más eficaz no solo como consecuencia de la imposición de la pena al comprobarse la comisión de la conducta ilícita, sino porque la amenaza que la sanción penal alberga la convierte en un elemento de prevención.

Así, la confluencia de normas penales y administrativa, con regulaciones cercanas al derecho privado, que prevén los arts. 310 y 325 TFUE, ha dado lugar a un sistema de prevención y represión de la delincuencia económico-financiera al que no solo se encuentran vinculados los órganos penales tradicionales, sino las entidades y los profesionales directamente ligados a la gestión financiera y a los procedimientos administrativos a partir de los cuales se pudiera deducir la comisión del delito o la intención delictiva (Pérez Marín, 2021)[1]. De este modo, el control de las vías financieras que pudieran ser usadas como instrumento de transacciones económicas sospechosas o de dudosa legalidad se separa, apuntando en dos direcciones: por un lado, evitar, como hemos dicho, la operación irregular o ilícita; por otro lado, garantizar que las entidades financieras adoptan las medidas necesarias para antever los comportamientos irregulares, de forma que una actividad negligente en la incorporación de las medidas de diligencia debida o en la aplicación de las mismas podría desembocar en la sanción –administrativa y/o penal– de la entidad responsable o de quienes hubieran facilitado, permitido o consentido, dentro de la misma, la operación ilícita a través de los medios operacionales ofrecidos por aquella.

Por último, en este escenario complejo, y como ejemplo de aquella evolución continuada del delito, en un periodo temporal relativamente corto han alcanzado especial relevancia ciertos productos virtuales que se utilizan como instrumentos alternativos de financiación: los criptoactivos, Estos no pueden ser confundidos con las monedas electrónicas de curso legal, que son implementadas a través de los correspondientes Bancos Centrales nacionales –esto es, organismos centralizados– y que, dicho de forma sencilla, constituyen la representación digital de la moneda física con la que se corresponde, teniendo, por lo tanto, el mismo valor fiduciario que esta[2] (Chiu, 2021, 243-246). Los criptoactivos no constituyen, así, dinero FIAT, aunque sean usados como medio de pago en determinadas transacciones, y al ser un producto creado por entidades privadas descentralizadas no les puede ser atribuido –o al menos no era factible hasta hace relativamente poco tiempo– un valor de referencia concreto y estable, siendo una de sus características, precisamente, la volatibilidad o la fluctuación de su valor al depender su cotización de las circunstancias económicas vigentes y de las propias oferta y demanda del producto.

Como contrapartida, las operaciones con criptomonedas son considerablemente sólidas. Incorporan, en el caso de los efectos t*okenizados*, un *smart contract*, resultando que la seguridad y la agilidad de estas transacciones son importadas de la *blockchain*

1. Véase el trabajo referenciado un análisis de las medidas que deben adoptar las entidades financieras y los profesionales ligados al sector para evitar el uso ilícito de las vías financieras.

2. En la actualidad, por ejemplo, está siendo objeto de análisis la implantación del euro virtual por parte del Banco Central Europeo. Una información más completa al respecto puede obtenerse en https://www.ecb.europa.eu/paym/digital_euro/html/index.es.html (último acceso 26 de octubre de 2023).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

que las sustenta y que exige, para alterar una anotación, la autorización mayoritaria de los componentes de la cadena. No puede, pues, un único nodo manipular los registros distribuidos ni el hash que se genera como clave criptográfica de la operación efectuada y que delata la autenticidad y la validez de la misma (Martín Ríos, 2020, 20). Pero tampoco podemos olvidar que la fluidez de las intervenciones con criptoactivos se justifica por una escasa regulación legal y, por consiguiente, por la inexistencia de requisitos que deban ser cumplidos para garantizar la validez para las partes de la operación realizada. Ello ha dado lugar al nacimiento de un mercado paralegal –paralelo a los mercados financieros físicos o digitales regulados– que no deja de tener una evidente trascendencia en el tráfico jurídico debido el empuje de la negociación con tales activos, pero que también ha provocado una especie de asociación automática de ideas que vinculaba a los criptoactivos con actividad delictiva, a pesar de que ni el origen ni la finalidad de su uso sean ilícitos por sí mismos. No podemos desconocer, sin embargo, que la protección que ofrece el anonimato o la privacidad de las operaciones ha puesto a este sector en el punto de mira de la delincuencia organizada[3] porque facilita la financiación de sus actividades sin el riesgo de que estas sean identificadas[4].

II. La necesaria transparencia de las transacciones

Aunque no fue la primera ocasión en la que el legislador europeo abordó la problemática de los criptoactivos[5], *la Directiva (UE) 2018/843 relativa a la prevención del uso*

3. Aunque el uso de criptomonedas va en aumento, el número total de transacciones es aún muy limitado si lo comparamos con la delincuencia financiera vinculada al dinero efectivo y otras transacciones, especialmente debido a la volatilidad de las criptodivisas. Sin embargo, el ámbito delictivo se ha ampliado y ya no queda circunscrito a la ciberdelincuencia, sino que se vincula a cualquier delito de naturaleza económico financiera, el fraude y el narcotráfico. Vid. Europol Spotlight *Cryptocurrencies: tracing the evolution of criminal finances*, 2022, https://www.azarplus.com/wp-content/uploads/2022/01/Europol-Spotlight-Cryptocurrencies-Tracing-the-evolution-of-criminal-finances.pdf (último acceso 17 de octubre de 2023).

4. Interpol ha creado un Centro contra la Delincuencia Financiero y la Corrupción que presta apoyo en las investigaciones transnacionales sobre la delincuencia facilitada por internet y que, con relación a los criptoactivos, está especializado en el rastreo de activos para interceptar los fondos ilícitos antes de su desaparición, en https://www.interpol.int/es/Delitos/Delincuencia-financiera/Papel-de-INTERPOL-en-la-lucha-contra-la-delincuencia-financiera (último acceso 23 de octubre de 2023).

5. La Directiva MIDFI (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, *Diario Oficial de la Unión Europea, L173*, de 12 de junio de 2014. http://data.europa.eu/eli/dir/2014/65/oj) incorpora en su regulación los *security tokens* o tokens de inversión, mientras que a los criptoactivos de dinero electrónico, o *payment tokens,* resultan de aplicación la Directiva 2009/110/CE del Parlamento Europea y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE, *Diario Oficial de la Unión Europea, L267*, de 10 de octubre de 2009. http://data.europa.eu/eli/dir/2009/110/oj), cuando puedan ser encuadrados en las condiciones especificadas en este instrumento.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

del sistema financiero para el blanqueo de capitales o la financiación del terrorismo[6] -5ª Directiva o 5AMLD por sus siglas en inglés– constituyó la ocasión en la que el foco se posaba, de un forma indubitada, en las divergencias que se apreciaban en las normas nacionales que, ante la falta de un instrumento normativo común, vinieron a ofrecer una regulación "territorialmente limitada" de los *tokens* o criptoactivos no regulados, esto es, los excluidos de las Directivas de 2009/110/UE (Directiva del dinero electrónico) y de 2014/65/UE (Directiva MIFID II por sus siglas en inglés). La Directiva de 2018 no nacía, sin embargo, como un elemento normativo autónomo, ni su objetivo principal era instaurar la regulación de tales criptoactivos, sino complementario y, en principio, dirigido a superar la falta de previsión de medidas específicas de diligencia debida para ciertas situaciones o la insuficiencia de las implementadas a través de la 4.ª Directiva –o 4AMLDpor sus siglas en inglés[7]- y que facilitaban transacciones que podían tener como objeto el blanqueo de capitales y/o la financiación del terrorismo y de la delincuencia organizada, usando las vías financieras legales.

Ya las directrices GAFI de 2015, prácticamente reiteradas en 2020[8], previnieron que los Estados no se encontraban en disposición de afrontar, con la regulación entonces vigente, los riesgos derivados del uso de determinados efectos financieros, apuntando directamente hacia el anonimato de los criptoactivos y a la dificultad de forzar la identificación real de las partes, protegidas por la privacidad de los protocolos subyacentes de la *blockchain*[9], debiéndose introducir organismos o mecanismos centralizados –que no existían– y a los que las autoridades competentes pudieran dirigirse para procurar información sobre las operaciones investigadas (Zaragoza Tejada, 2019, 10).

Nos encontrábamos, así, con que la imposibilidad de identificar a las partes intervinientes en este tipo de negociaciones tenía un doble motivo: por un lado, que no existía regulación que así lo exigiese; por otro, que la técnica de *blockchain* que le sirve de base dificulta la identificación, aunque no tanto la precisión del *iter* operacional que puede ser reconstruido a través de los diferentes nodos que conforman la cadena. Evidentemente, la imposibilidad de conocer quiénes están detrás del origen y del destino de la operación

6. Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, *Diario Oficial de la Unión Europea, L156*, de 19 de junio de 2018, http://data.europa.eu/eli/dir/2018/843/oj).

7. Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión, *Diario Oficial de la Unión Europea, L141*, de 5 de junio de 2015, http://data.europa.eu/eli/dir/2015/849/oj.

8. https://www.fatf-gafi.org/media/fatf/documents/Directrices-para-enfoque-basada-en-riesgo-Monedas-virtuales.pdf y https://www.cfatf-gafic.org/es/documentos/recursos-del-gafic/14971recomendaciones-del-gafi-2012-actualizadas-a-octubre-de-2020–1 (último acceso a ambos documentos 20 de octubre de 2023).

9. Vid. p. 13 Directrices GAFI 2015.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

obstruye la investigación penal y, por ello, en los considerandos 8 y 9 la Directiva (UE) 2018/843 el legislador insiste en el hecho de que la privacidad –anonimato– de los criptoactivos promueve un uso irregular de los mismos, en tanto que permite a los usuarios completar estas operaciones y proceder al cambio de moneda virtual por moneda FIAT sin levantar sospechas. En este escenario, el mercado único se convierte en un espacio altamente vulnerable que no puede evitar el uso ilícito de sus vías financieras y que, en el fondo, permite a las organizaciones delictivas transnacionales disfrutar de cierta impunidad para transferir fondos desde o hacia el sistema financiero de la Unión.

También el *Plan de acción en materia de tecnología financiera,* definido en el año 2018[10], puso de manifiesto que ni los Estados ni la Unión contaban con normas reguladoras suficientes para hacer frente al uso irregular de los medios alternativos de financiación no regulados y que, como consecuencia y por derivación, el espacio financiero se encontraba desprovisto de protección legal en este aspecto (Barrio Andrés, 2022). Se abordaba, además, una nueva perspectiva al reconocerse que el problema podía verse exponencialmente agravado no por la ausencia absoluta de previsión legal, toda vez que, en aquel momento, algunos ordenamientos habían ido incorporando de forma incipiente ciertas previsiones y ya la Unión se encontraba inmersa en una discusión sobre las estructuras de financiación de los criptoactivos no regulados, sino por la constatación de la falta de homogeneidad de las normas nacionales, siendo la armonización normativa una condición imprescindible a la que la Unión y los Estados debían aspirar (Kapsis, 2021, 97). No olvidemos que de cara al exterior la fortaleza del mercado financiero interno reside en que es precisamente "único", por lo que no podían tener cabida pormenores legislativos que vinieran a distinguir un ordenamiento de otro –un mercado de otro–, remarcando con ello las fisuras que en un espacio digital que podían ser optimizadas por las organizaciones delictivas para contornar la legalidad (Aben, 2022, 98).

En consonancia con lo anterior, en el *Plan de acción para una política global de la Unión en materia de prevención del blanqueo de capitales y de la financiación del terrorismo*[11], que adelantaba los criterios para afrontar los riesgos que supone la inestabilidad de un sistema financiero amenazado por la inseguridad que suscita su uso con fines ilícitos, se hacía especial hincapié en el riesgo de la proyección transnacional de las operaciones realizadas a través de las vías digitales que obliga a las entidades a atender a la evolución constante del mercado financiero digital.

Como resultado, las especialidades de los criptoactivos –ya fueran estos regulados o no regulados– no permitían aprovechar un sistema pensado para formas de financiación

10. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Banco Central Europeo, al Comité Económico y Social Europeo y al Comité Europeo de las Regiones - Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador, Bruselas, 8 de marzo de 2018, COM (2018) 109 final. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52018DC0109.

11. Comunicación de la Comisión sobre un Plan de acción para una política global de la Unión en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, Bruselas, 7 de mayo de 2020, COM (2020) 2800 final. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=PI_COM:C(2020)2800.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

tradicionales, porque los problemas surgidos a partir del uso de aquellos en muy poco o en nada se compadecían con las dificultades que habían ido emergiendo como consecuencia de la modernización del mercado financiero tradicional y que habían ido siendo progresivamente resueltas atendiendo a las necesidades de cada momento. La irrupción de un "modo disruptivo" de financiación que se contraponía a lo que se conocía hasta entonces, en lo que a sus características y condiciones de uso se refiere, y que prometía, cumpliéndolo, una mayor agilidad de las transacciones gracias a la inexistencia de requisitos legales, supuso una revolución para la que la Unión y los Estados no estaban preparados por mucho que, como ya adelantamos, todos fueran conscientes de la situación que se avecinaba.

Como el problema residía no tanto en las operaciones efectuadas a través de los criptoactivos, sino en las circunstancias aparejadas a esta –la imposibilidad de identificar a las partes, la dificultad de deducir la finalidad de las mismas (Pérez López, 2019, 91-94; Navarro Cardoso, 2019, 10-14) y la inexistencia de órganos centralizados que faciliten el acceso a los datos de la operación– la regulación recientemente aprobada se vuelca en el control de las condiciones que deben cumplir los criptoactivos, las entidades que los emite y los mercados en los que se opera con estos para garantizar la transparencia del sistema y la seguridad del mercado financiero en el que operan.

III. La infraestructura de mercado diseñada por el reglamento TRD para las operaciones con security tokens

Aunque en general se suele decir que los criptoactivos estaban desprovistos de regulación en la Unión Europea hasta la reciente aprobación del Reglamento MiCA, la realidad no es exactamente esa. Hemos viso que, desde su entrada en vigor, la Directiva MIFID II ha atendido a determinados criptoactivos –activos *tokenizados*– que sustentan un *smart contract* afianzado por la *blockchain*[12], siempre que, conforme a dicha Directiva, tales instrumentos tengan la consideración de activos financieros o *security tokens* y, por otro lado, la Directiva 2009/110/CE avanzó en la regulación del dinero electrónico, amparando sus previsiones a los criptoactivos que pudieran tener tal consideración. No obstante, aunque todos los criptoactivos estén basados en una técnica de registro descentralizado, no todos incorporan un contrato inteligente ni, por ejemplo, todos tienen la misma eficacia que la Directiva de 2009 atribuye al dinero electrónico, por lo que no es difícil concluir que no todos los criptoactivos son iguales. Como no puede afirmarse, pues, que estos, con independencia de su naturaleza y/o finalidad, sean siempre activos financieros y/o dinero electrónico, tales directivas carecían de una aplicabilidad genérica –no estaban referidas a todos los criptoactivos–, siendo imposible que una

12. Aunque normalmente –excepto en los ámbitos verdaderamente especializados– se usan de forma indistintas los términos criptoactivo y *token*, no son vocablos equivalentes. En concreto, los activos *tokenizados* regulados por esta Directiva llevan incorporado un *smart contract* y constituyen un tipo específico de criptoactivos.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

norma tuviera un ámbito material de aplicación tan amplio como para abarcar a cualquier criptoactivos de ahí que el legislador tuviera que hacer frente a la regulación de los mismos a través de distintos instrumentos jurídicos que han de atender a las diferencias existentes entre ellos.

Por su parte, los criptoactivos –o *security tokens*– comprendidos en la Directiva MIFID II constituyen, dicho de forma sencilla, la representación digital de un activo financiero tradicional, aunque también puede ser un activo nativo digital –considerando 3–. En cualquier caso, y en tanto que instrumentos o activos financieros les resultan de aplicación las normas que regulan tales elementos en el mercado sin tener en cuenta su condición digital[13]. No obstante, esta arquitectura legal se topaba con algunos problemas específicos vinculados a la natural digitalización de los criptoactivos y, de hecho, la dificultad de aplicar completamente los instrumentos jurídicos vigentes –planeados para un mercado tradicional o para formas o instrumentos de inversión tradicionales– a la negociación con estos nuevos activos demostraba que los presupuestos en los que el mercado tradicional se basaba no se correspondían de forma exacta con las características y exigencias de los activos *tokenizados*, e, incluso, se advertía con facilidad que los problemas que surgían con ocasión del negocio jurídico en el que estos eran utilizados diferían de los advertidos en la sistemática tradicional. Verdaderamente el mercado carecía de respuestas frente a las necesidades interpretativas y de aplicación de este tipo de activos y de su sistema subyacente, siendo ello considerado una fragilidad que debía

13. Reglamento (UE) 236/2012 del Parlamento Europeo y del Consejo, de 14 de marzo de 2012, sobre las ventas en corto y determinados aspectos de las permutas de cobertura por impago, *Diario Oficial de la Unión Europea, L86*, de 24 de marzo de 2012. http://data.europa.eu/eli/reg/2012/236/oj; Reglamento (UE) 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión, *Diario Oficial de la Unión Europea*, *L173*, de 12 de junio de 2014. http://data.europa.eu/eli/reg/2014/596/oj; Reglamento (UE) 909/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre la mejora de la liquidación de valores en la Unión Europea y los depositarios centrales de valores y por el que se modifica la Directiva 98/26/CE y 2014/65/UE y el Reglamento (UE) 236/2012, *Diario Oficial de la Unión Europea, L257*, de 28 de agosto de 2014. http://data.europa.eu/eli/reg/2014/909/2022-06-22 (versión consolidada); Reglamento (UE) 2017/1129 del Parlamento Europeo y del Consejo, de 14 de junio de 2017, sobre el folleto que debe publicarse en caso de oferta pública o admisión a cotización de valores en un mercado regulado y por el que se deroga la Directiva 2003/71/CE, *Diario Oficial de la Unión Europea, L168*, de 30 de junio de 2017. http://data.europa.eu/eli/reg/2017/1129/oj; Directiva 98/26/CE del Parlamento Europeo y del Consejo de 19 de mayo de 1998, sobre la firmeza de la liquidación en los sistemas de pagos y de liquidación de valores, *Diario Oficial de la Unión Europea, L166*, de 11 de junio de 1998. https://www.boe.es/doue/1998/166/L00045-00050.pdf (versión consolidada http://data.europa.eu/eli/dir/

2019/879/oj); Directiva 2013/50/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, por la que se modifican la Directiva 2004/109/CE del Parlamento Europeo y del Consejo sobre la armonización de los requisitos de transparencia relativos a la información sobre los emisores cuyos valores se admiten a negociación en un mercado regulado, la Directiva 2003/71/CE del Parlamento Europeo y del Consejo sobre el folleto que debe publicarse en caso de oferta pública o admisión a cotización de valores, y la Directiva 2007/14/CE de la Comisión por la que se establecen disposiciones de aplicación de determinadas prescripciones de la Directiva 2004/109/CE, *Diario Oficial de la Unión Europea, L 294*, de 6 de noviembre de 2013. http://data.europa.eu/eli/dir/2013/50/oj.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

ser superada. A pesar de todo, no puede dejar de reconocerse que existía un cuerpo de normas sustantivas que, aunque mejorables y, aun debiendo ser adaptadas, constituían la base reguladora de los negocios realizados con estos instrumentos.

Para dotar de una base de mercado a los activos regulados por la Directiva MIFID II, el *Reglamento relativo al establecimiento de un régimen piloto de infraestructuras de mercado basadas en la tecnología de registro descentralizado*[14] (Reglamento TRD) ponía en funcionamiento en el año 2022 un régimen de prueba –como su propia denominación indica un *régimen piloto*– con el que se pretende dotar al mercado de los *security tokens* de la base que específicamente requiere su negociación y que hasta ese momento no existía. No cabe olvidar que el mercado tradicional ofrecía para este sector una cobertura que no era pequeña –todos los instrumentos legales que regulaban el mercado financiero les resultaba prácticamente de aplicación–, pero al mismo tiempo limitada dadas las diferencias entre estos activos y los tradicionales, por lo que el mercado debía contar con una infraestructura legal adecuada que finalmente vendría a ser diseñada en este Reglamento. Ha de quedar claro que este únicamente resulta de aplicación a los *security tokens* o activos financieros de la Directica MIFID II, excluyendo cualquier otro tipo de criptoactivo que, basado en la misma tecnología de registro descentralizado, carezca de la consideración de "activo financiero" en la forma prevista por tal instrumento.

A lo largo del Reglamento TRD, el legislador hace expresa referencia a los problemas que constituyen los principales obstáculos con los que se topa el mercado de los activos tokenizados y concreta los criterios o los procedimientos a fin de superar tales inconvenientes. Por un lado, había de afrontarse eficazmente los riesgos que se derivarían de la negociación y, por otro, era necesario fortalecer las garantías ofrecidas a los inversores y a los consumidores sobre la integridad del mercado, así como sostener una estabilidad financiera continuamente tocada por la evolución o la aparición de nuevos elementos financieros. Como consecuencia, la seguridad del mercado –y, en general, la del tráfico jurídico– quedaba vinculada a una regulación eficaz del mismo, siendo este, en definitiva, el objetivo que se marca el legislador con el Reglamento TRD. Así, con respecto a la creación de nuevas infraestructuras se detallan las formalidades legales que permiten otorgar las autorizaciones específicas para gestionar los diferentes soporte de negociación multilateral[15], y se exige la publicación de un libro blanco que contenga información relativa al negocio en cuestión y la descripción de las tecnologías utilizadas, introduciendo la noción de responsabilidad frente al riesgo soportado por el negocio, de tal manera que el solicitante [de la gestión del servicio] debe probar que "cuenta con

14. Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) n.º 600/2014 y (UE) n.º 909/2014 y la Directiva 2014/65/UE, *Diario Oficial de la Unión Europea, L151*, de 2 de junio de 2022, http://data.europa.eu/eli/reg/2022/858/oj.

15. SMN - sistema multilateral de negociación, basado en la TRD, art. 2.6 del Reglamento (UE) 2022/858– SL –sistema multilateral de negociación, basado en la TRD, art. 2.6 del Reglamento (UE) 2022/858– y SN –sistema de liquidación y negociación basado en la TRD, art. 2.8 del Reglamento (UE) 2022/858-.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

garantías prudenciales suficientes para satisfacer sus responsabilidades y compensar a sus clientes"[16].

Pero también cabe apreciar en este instrumento cómo el legislador establece los puentes para compatibilizar el régimen tradicional de cuenta de valores con la tokenización de los activos financieros, concretando las posibles exenciones a las que se pudieran acoger los sistemas basados en la técnica de registro descentralizado –considerando 30 y art. 5– y obligando a implementar condiciones diferentes a las del mercado tradicional sin afectar a la seguridad y sin dejar de ofrecer garantías a los inversores de tales servicios[17]. En este punto, volvemos a traer a colación que la tecnología subyacente de estos activos financieros se basa en la descentralización y que ello facilita la protección de la identidad de quienes intervienen, por lo que se debían fijar criterios de fiabilidad de los protocolos de los *smart contracts* incorporados a los activos. Como correlato de lo anterior, el considerando 5 del Reglamento anticipaba que la complejidad de este tipo de activos era doble, pues con independencia de las condiciones especiales de estos, la tecnología de registro descentralizada también debía afrontar los mismos riesgos que encontraban las tecnologías más convencionales, apuntando directamente el legislador hacia la necesidad de controlar la validez legal de los tokens, es decir, de los activos. Luego, el desarrollo del sistema implementado para la negociación con criptoactivos debía ser compatible, necesariamente, con la protección de los inversores y con la integridad el mercado, favoreciendo, como refiere el considerando 6, la instauración de "cadenas de responsabilidad [de las entidades emisoras y negociadora] frente a los clientes […] por toda pérdida debida a fallos operativos".

Por ello, cuando una entidad solicite autorización para gestionar un servicio multilateral basado en la técnica de registro descentralizado, también deberá incluir, para el caso de que se produzca un conflicto, medidas de mitigación que permitan asegurar la posición de los inversores, la integridad del mercado y la estabilidad financiera y detallar una relación de los mecanismos de tramitación de reclamaciones –art. 8.4 f)-. Por su parte, el apartado 6 del art. 7 advierte que "[l]os organismos rectores de infraestructuras del mercado basadas en la TRD establecerán disposiciones transparentes y adecuadas para garantizar la protección de los inversores […]", pudiendo las autoridades competentes revocar las autorizaciones otorgadas a las entidades para emitir y operar con tales activos cuando detecten un defecto en la tecnología utilizada o en los servicios prestados que pongan en riesgo la integridad del mercado o la estabilidad financiera.

Pero en otro orden de consideraciones, no podemos dejar de insistir en que, como el título indica, todas estas directrices no dejan de ser hoy un régimen piloto, esto es, en cierta manera un modelo experimental o un banco de pruebas provisional o temporal, por lo que se desenvuelve como una especie de laboratorio a través del cual se logra información para ordenar una futura infraestructura definitiva de mercado, superando las incompatibilidades observadas en la negociación desarrollada con activos financieros tokenizados a la luz de este Reglamento. De hecho, podemos leer

16. Vid. arts. 8, 9 y 10 del Reglamento (UE) 2022/858.
17. Vid. considerandos 3 y 4 del Reglamento (UE) 2022/858.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

en el considerando 5 que ante "la limitada experiencia en cuanto a la negociación de criptoactivos que tienen la consideración de instrumentos financieros […] sería prematuro realizar en este momento modificaciones significativas de la normativa de la Unión" para permitir el pleno despliegue de dichos criptoactivos y su tecnología subyacente, reconociendo que "la creación de una infraestructura del mercado financiero para los criptoactivos que tienen la consideración de instrumentos financieros se ve actualmente constreñida por requisitos imbricados en la normativa de la Unión en materia de servicios financieros que no son apropiados para los criptoactivos que tienen la consideración de instrumentos financieros ni al uso de la tecnología de registro descentralizado". Por ello, a más tardar el 24 de marzo de 2026, la AEVM deberá presentar a la Comisión un informe sobre el funcionamiento de las infraestructuras, pudiéndose prorrogar la validez del Reglamento tres años.

IV. El reglamento MiCA y la lucha contra la delincuencia financiera

4.1. Un análisis general de la norma

Cabe entender que tanto las Directivas 2015/849 y 2018/843, como el Dictamen elaborado sobre el *Plan de acción en materia de tecnología financiera*[18], constituyeron un paso decisivo para regularizar los criptoactivos "no regulados" por la Directiva MIFID II o por la Directiva de dinero electrónico.

En el año 2020 era publicada una Propuesta de Reglamento relativo a los mercados de criptoactivos "no regulados"[19], que no dejaba de ser una declaración de intenciones por parte de la Unión. Esta no estaba dispuesta a perder las oportunidades que ofrecía la evolución de un mercado financiero adaptado a las nuevas tecnologías y, especialmente, no podía dejar de beneficiarse de las ventajas de los nuevos instrumentos cuando las técnicas de registro descentralizado fuesen adaptadas de manera definitiva a los activos digitales de financiación, si bien no olvidaba la necesaria protección de inversores y consumidores (Maume, 2022, 110).

Pero tanto con respecto a los activos regulados, como respecto de los activos digitales no regulados, se apreciaban riesgos similares. Por ejemplo, como sabemos no era posible forzar la identificación de las partes sin la colaboración de estas debido a que la técnica de registro descentralizado viabiliza el anonimato de quienes intervienen

18. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Banco Central Europeo, al Comité Económico y Social Europeo y al Comité Europeo de las Regiones - Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador, Bruselas, 8 de marzo de 2018, COM (2018) 109 final. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52018DC0109.

19. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, Bruselas, 24 de septiembre de 2020, COM (2020) 593 final. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020PC0593.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

en estas transacciones, insistiéndose en otras circunstancias que debían ser tenidas en cuenta por contribuir al uso ilícito o irregular de los criptoactivos y que afectaban a la seguridad del mercado financiero, como ocurría con la falta de instrumentos jurídicos comunes –situación que abría la puerta a la impunidad de la delincuencia organizada que negociaba con criptoactivos–, que al amparo de las diferencias entre ordenamientos permitían esconder el blanqueo de capitales u otras operaciones delictivas (Patz y Wettlaufer, 2022, 255). Evidentemente, la falta de una regulación común y la existencia de normas reguladoras nacionales –diferentes– no determinaban necesariamente la ilicitud de estas operaciones, pero tampoco permitían asegurar la legalidad de las mismas.

Junto con este mismo trasfondo –garantizar la licitud y la transparencia de las transacciones con criptoactivos– el texto del Reglamento (UE) 2023/1114, recientemente aprobado[20] (Reglamento MiCA por sus siglas en inglés), se centra en inyectar un más elevado grado de seguridad al mercado financiero que constituye la infraestructura de negociación (Parrondo, 2023), contribuyendo a combatir el delito. Sin embargo no implanta medidas destinadas a sancionar penalmente el delito de blanqueo o de financiación del terrorismo que pudiera esconder la transacción de criptoactivos –al no ser un instrumento penal–, sino que establece medidas, obligaciones y deberes –medidas de diligencia debida– que necesariamente han de ser respetados por los operadores de activos digitales a fin de demostrar a los inversores que este es un mercado seguro, pues el blanqueo de capitales suele ser considerado como un delio indirecto en el contexto de la criminalidad que pudiera desenvolverse en el ámbito de los activos digitales (Huang, 2021, 132 y 133). Vemos, así, que la Unión avanza hacia la creación del entorno de negociación de los mismos, distinguiendo, como ya hizo con las Directivas AMLD, la regulación administrativa de la regulación penal. Este Reglamento instituye, por consiguiente, las infraestructuras administrativas y los requisitos para autorizar la prestación de servicios de criptoactivos y las condiciones de negociación que, al estar concretadas, dotan al sistema de un evidente grado de seguridad, permitiendo controlar la licitud de la actividad negociadora, pero no tiene como finalidad directa –aunque esté intrínsecamente ligada al espíritu de la norma– estipular criterios legales para el combate de este tipo de delincuencia financiera. Incorpora, por el contrario, un régimen sancionador (administrativo) frente al incumplimiento de los requisitos exigidos.

Así, los principios que rigen el nuevo mercado han de tener como objeto, tal y como indica el considerando 5, la seguridad de las empresas, de los inversores y del mercado ante la perspectiva de que, aun teniendo todavía un uso limitado, estos activos alcancen una gran proyección cuando estabilicen su precio y se conviertan en un instrumento de financiación estable no sujeto a las eventualidades de la oferta y la demanda. Por ello, y también para evitar desafíos que afecten al equilibrio financiero, el Reglamento

20. Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937, *Diario Oficial de la Unión Europea, L150*, de 9 de junio de 2023. http://data.europa.eu/eli/reg/2023/1114/oj.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

pretende superar la desconfianza de los consumidores, evitando que una actitud conservadora obstaculice el desarrollo del mercado e impida la expansión transfronteriza de las actividades desarrolladas por los proveedores de criptoactivos. A mayor abundamiento, se reconoce que este mercado es naturalmente transfronterizo, por lo que no es suficiente con regular las transacciones a nivel de la Unión, sino que se ha de potenciar la colaboración con organismos y organizaciones internacionales para mantener una convergencia globalizada –considerando 6–. Debemos entender, pues, que la regulación europea, siendo el medio a través del cual se concretan las condiciones del mercado de criptoactivos en el espacio financiero común, se encuadra en un contexto más ambicioso que procura la estabilidad financiera global para evitar riesgos de contagio que no solo perjudican a las transacciones, impidiendo un desenvolvimiento normal del mercado, sino que afecta, por ejemplo, a la seguridad que precisan percibir los inversores en el negocio jurídico que se disponen a realizar. De hecho, el riesgo de las operaciones reside, además de en el volumen del negocio, en la proyección transfronteriza de la operación, motivo por el cual los proveedores de servicios están obligados a cuidar la aplicación de medidas de diligencia debida.

Con este objeto se instituye un sistema de control dirigido a comprobar que los servicios se sujetan a las condiciones de legalidad previstas y se otorgan a las autoridades nacionales, a la Autoridad Bancaria Europea –en adelante ABE– y a la Autoridad Europea de Valores y Mercado –en adelante AEVM– facultades de control e inspección, entre las que, sin embargo, no se aprecia de forma nítida la naturaleza de las mismas, esto es si las medidas de inspección están dirigidas a realizar una mera comprobación o si, por el contrario, tienen finalidad sancionadora.

En cuanto a los activos virtuales, o criptoactivos definidos en el Reglamento MiCA, con la clasificación adoptada por la Unión se aparta de la ordenación tradicional de la AEVM sobre la materia. El nuevo instrumento prevé a grandes rasgos tres tipos de criptoactivos que están regulados de forma amplia por lo que abarcan diferentes opciones (Patz y Wettlaufer, 2022, 251-255), distinguiéndolos en función del riesgo que conlleve su negociación y a si pretenden estabilizar su valor con referencia al valor de otros activos (Chiu, 2021, 19-21), pues los activos de los que trata el Reglamento son, si utilizamos otra clasificación, los *stablecoins* cuya negociación se ha extendido de forma exponencial en los últimos años (Alvarado Herrera, 2022).

A nivel de esta norma se distinguen las fichas de dinero electrónico (ART, por sus siglas en inglés), que estabilizan su valoración en función del valor de una moneda de curso legal[21], las fichas referenciadas a activos (EMT, por sus siglas en inglés)[22], que acogen a la mayoría de los criptoactivos que no son fichas de dinero electrónico y que mantienen constante su valor gracias al valor o la cotización de un concreto bien o activo –por ejemplo el oro–, sobre un derecho o a la combinación de diferentes valores

21. Art. 3.1.7) del Reglamento (UE) 2023/1114.

22. Las fichas referenciadas concretan su valor en atención a una combinación de activos, mientras que el valor de las fichas de dinero electrónico se determina en tención a una única moneda de curso legal. Vid. art. 3.1.6) del Reglamento (UE) 2023/1114.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

que le sirven de referencia y, por último, un tercer grupo en el que se incluyen todos aquellos criptoactivos que no se compadecen con los requisitos de las dos tipologías anteriores y que serían, en parte, las que la AEVM denomina como *utility tokens* y que el Reglamento MiCA regula como fichas de consumo[23]. Estas, normalmente dan acceso a un determinado servicio ofrecido por el emisor del criptoactivo y no pueden ser usadas fuera del contexto o del entorno para cuyo desarrollo fueron creadas, aunque lo que verdaderamente identifica a este tipo de activos es que no incorporan un derecho de crédito frente al emisor ni es posible, en general, negociar con ellos fuera de su infraestructura de desarrollo específica. No obstante, también incluyen criptomonedas como *bitcoin*, *aethereum* y *litecoin*, en tanto que criptomonedas volátiles no referenciadas a activos (Gonçalves, da Costa Vale, 2023, 34 y 35).

Tengamos en cuenta, por último, que, a pesar de que pasen a ser "activos regulados" a partir de la entrada en vigor del Reglamento, las fichas referenciadas a activos tienen una naturaleza distinta a la de los activos financieros regulados en la Directiva MIFID II, por lo que esta y el conjunto de normas que disciplinan este mercado continúan sin serles de aplicación, conservándose dos regulaciones separadas e infraestructuras diferenciadas –por un lado el Reglamento TRD y por otro el Reglamento MiCA– que permitan desarrollar el negocio jurídico con garantías. Sin embargo, con las fichas de dinero electrónico no ocurre lo mismo en tanto que estas vienen a actuar como medio de pago y, por lo tanto, podrían ser encuadradas en las condiciones de la Directiva de dinero electrónico. Cuando ello acontezca, a estas fichas también les resultarán de aplicación las previsiones de los Títulos II y III de dicha Directiva, como refiere el Reglamento MiCA en su art. 48.2, alcanzándose un estatuto más completo al disfrutar estos activos de una doble naturaleza como *stablecoins* –fichas de dinero electrónico– y como dinero electrónico al mismo tiempo.

4.2. Las obligaciones de información y transparencia de los operadores de servicios de criptoactivos: la responsabilidad civil frente a la infracción

Para cada uno de los activos regulados el Reglamento introduce requisitos específicos que delimitan, en cada caso, las condiciones de la oferta pública o admisión a negociación de las fichas, pero, para todos en general, se impone a los oferentes, a los emisores, y a quienes soliciten la negociación de los mismos, la obligación de publicar un libro blanco, como ya se determinó en el Reglamento TRD para los *security tokens*, que incluya toda la información relativa al proveedor del servicio, las fichas, la oferta y la operación, así como una explicación de la tecnología subyacente, de los riesgos y una declaración de que el libro blanco no incurre en ninguna omisión que pudiera afectar a su contenido. Este debe contar, además, con un resumen claro a modo de introducción, que proporcionará información relevante de forma precisa, concisa y sin tecnicismos

23. Art. 3.1.9) del Reglamento (UE) 2023/1114.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

sobre la oferta pública de la ficha en cuestión[24]. Se trata, por lo tanto, de un deber general de información, transparencia y claridad que excluye, sin embargo, el deber de referir aquellos riesgos que difícilmente puedan materializarse, como adelantan los considerandos 24 y 27 y puede advertirse en los arts. 19 y ss.

De forma paralela, el legislador construye el régimen de responsabilidad civil de los operadores que incumplan este deber de información transparente. En este sentido, y en el caso de que la información recogida en el libro blanco no sea completa o se demuestre engañosa, tanto el emisor como los miembros del órgano de administración, dirección o supervisión serán responsables de las pérdidas sufridas por los titulares de las fichas cuando hubiera sido aquella información, errada o insuficiente, determinante para suscribir la operación[25], previendo el art. 37 un derecho permanente de devolución que mantienen los titulares de las fichas referenciadas frente a los proveedores para el caso de que estos no puedan cumplir las obligaciones que conllevan los planes de recuperación o de reembolso y que, previa decisión de la autoridad competente, serán ejecutados cuando el emisor no pueda –o se prevea que no pueda– cumplir con sus obligaciones, en los casos de insolvencia o en los casos de revocación de la autorización por el emisor[26].

Esta responsabilidad de naturaleza civil no es incompatible con el régimen de responsabilidad civil previsto en el ordenamiento nacional[27]. De esta manera, para los activos distintos de los referenciados a activos y a los activos de dinero electrónico, el art. 15 declara la nulidad de las cláusulas que excluyan la responsabilidad civil de los proveedores de servicios, recordando que el grado de responsabilidad determinado en el Reglamento es plenamente compatible con otras responsabilidades civiles precisadas en el Derecho nacional –art. 15.6–, recogiendo idéntica previsión para las fichas referenciadas a activos –art. 26.2– y para las fichas de dinero electrónico –art. 52.2-.

Complementando la obligación de información y transparencia, se requiere de los emisores de fichas referenciadas que, además de contar con una sistema de gobernanza sólido y con una estructura organizativa clara, establezcan pautas de responsabilidad bien definidas frente al incumplimiento del deber de información –considerando 51 y art. 34–, al tiempo que se les exige la constitución y el mantenimiento de una reserva de activos –art. 36– para garantizar la estabilidad de los mismos y que esta se corresponda con la naturaleza de los riesgos derivados de las operaciones. De forma paralela,

24. Exactamente las mismas disposiciones se recogen para los diferentes tipos de activos en los arts. 6, 19 y 51 del Reglamento, teniendo en cuenta las diferencias en el contenido del libro blanco, pues este debe adaptarse a las condiciones de cada activo.

25. Art. 26 del Reglamento (UE) 2023/1114.

26. Vid., así, arts. 56 y 47 del Reglamento (UE) 2023/1114. Ahora bien, corresponde a los inversores demostrar la infracción cometida por el emisor para que se deduzca la responsabilidad civil y estos no tienen responsabilidad por el uso erróneo que se haga de la información que se desprenda del resumen del libro blanco salvo cuando "a) sea engañoso, inexacto o incoherente con las demás partes del libro blanco de criptoactivos, o b) no proporcione, leído junto con las demás partes del libro blanco de criptoactivos, información relevante para ayudar a los potenciales titulares a tomar una decisión sobre la compra de la ficha referenciada a activos".

27. Art. 26.5 del Reglamento (UE) 2023/1114.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

el art. 52 aborda la responsabilidad de los emisores de fichas de dinero electrónico respecto de la información facilitada en el libro blanco sobre el criptoactivo, siendo el art. 14 la sede que recoge las obligaciones de los proveedores de servicio de activos distintos de las fichas referenciadas a activos y de las fichas de dinero electrónico, para las que también se prevé, a favor de los titulares minoristas, un derecho de desistimiento de la operación conforme a lo previsto en el art. 13.

4.3. El régimen sancionador frente al incumplimiento de las obligaciones

El Reglamento MiCA supone un importante avance que dota de estabilidad a los criptoactivos, pero no resuelve ciertas opacidades que inciden en la seguridad de las operaciones y del propio mercado y tal vez por ello obliga, por ejemplo, a los emisores de las fichas significativas de dinero electrónico a aceptar auditorías independientes cada seis meses[28] y, con relación a las fichas significativas referenciadas a activos, que sus emisores se sometan periódicamente a pruebas de resistencia de liquidez que abarquen todos los productos que ofertan en el caso de ser más de uno, como precisa el art. 45.4. Por otro lado, el régimen jurídico diseñado también incorpora un régimen sancionador por el incumplimiento de los deberes y obligaciones fijados, que permite a las autoridades competentes imponer las sanciones y medidas concretadas, básicamente en el art. 94, una vez tramitada la investigación. Por su parte, el art. 111 prevé la posibilidad de que los Estados miembros puedan tipificar las infracciones del Reglamento como conductas delictivas, entrándose así en el delicado límite que construyen los principios *nemo tenetur* y *non bis in idem*.

De este modo, el art. 94 determina las facultades genéricas de las autoridades competentes para desempeñar las funciones relacionadas con el control y la supervisión de las actuaciones de los proveedores de servicios con criptoactivos, mientras que el art. 111 concreta las sanciones administrativas, multas y "otras medidas administrativas" que, por otro lado, no dejan de ser sanciones en la mayoría de los casos.

Digamos que la regulación relativa a la supervisión y a la investigación como funciones atribuidas a las autoridades administrativas designadas para controlar el cumplimiento de los requisitos que dotan de seguridad a los criptoactivos, ofreciendo garantías a los inversores, a las operaciones y al mercado de negociación, resulta cuanto menos difusa y, en principio, difícil de entender. Parecen mezclarse funciones de inspección y control que asumen una finalidad sancionadora que excede de la mera comprobación de los requisitos exigidos para la situación que estuviera siendo investigada, adentrándose el procedimiento en un ámbito sancionador que es el que permite imponer las multas y las medidas administrativas dispuestas en el Reglamento. Además, la investigación iniciada puede finalizar con la derivación de la misma a la vía penal por entenderse que los hechos constatados constituyen un delito, asumiendo, por lo tanto, la jurisdicción penal carácter preferente.

28. Art. 58 del Reglamento (UE) 2023/1114.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

En esta cuestión entran en juego diferentes elementos a partir de los cuales deberíamos poder vislumbrar la verdadera naturaleza de las inspecciones desarrolladas, los límites de las facultades de inspección atribuidas y las consecuencias de las medidas acordadas tras la investigación. Así, además del principio *nemo tenetur*, que engloba el derecho a no declarar para evitar la autoincriminación y que se extiende hasta el ámbito administrativo para justificar el incumplimiento del deber de colaboración con la Administración cuando de esta pudiera derivarse una sanción (Picón Arranz, 2022, 379), deberán valorarse los efectos del principio *non bis in idem* aplicado a la dualidad sancionadora, administrativa y penal, que pudiera confluir como consecuencia de la tramitación del proceso penal a partir de la denuncia efectuada por la Administración, si esta ya hubiera acordado una sanción frente a la infracción comprobada.

En realidad, la función de control del cumplimiento de los requisitos exigidos a cada uno de los proveedores, y que podemos denominar como control preventivo o como actividad de comprobación, está desarrollada a lo largo del texto del Reglamento para cada servicio, y se va aplicando cada vez que se solicita una autorización por los proveedores o futuros proveedores. De hecho, en diferentes ocasiones se advierte la posibilidad de que los servicios no sean autorizados o de que, aun habiéndolos sido, la autorización inicial concedida sea revocada. Lógicamente, la denegación de la autorización o la revocación se producen por el hecho de que los proveedores de servicios concernidos no cumplan –o parezcan no cumplir– las condiciones requeridas por el Reglamento, lo cual implica, de suyo, que las autoridades competentes desarrollan una función continua de control respecto de las condiciones que permiten operar con criptoactivos.

Así, por ejemplo, el art. 63 dispone, conforme a su apartado 5, la facultad de denegar la autorización solicitada por un proveedor o por un futuro proveedor de servicios, enunciando las medidas de las que podrán hacer uso las autoridades a efectos de comprobar que los solicitantes cumplen los requisitos exigidos para ejercer las funciones que pretende desarrollar. De la misma forma, el art. 64 obliga a revocar una autorización concedida ante la constatación de que el proveedor ha dejado de cumplir las condiciones que justificaron la concesión del servicio, atribuyendo a la ABE la facultad de adoptar medidas para encontrar los elementos probatorios de la infracción presuntamente cometida, que es deducida o intuida, como consecuencia del primigenio ejercicio de supervisión de las solicitudes de los proveedores de servicio y del control del cumplimiento sostenido de los requisitos que justificaron las concesiones.

Con respecto a estas medidas de las que hablamos, dirigidas a comprobar la infracción y no meramente destinadas a controlar o comprobar el cumplimiento de requisitos, el considerando 106 y el art. 124 reconocen la facultad de la ABE para realizar inspecciones *in situ* con miras a la supervisión de fichas significativas. Además, las facultades asignadas a las autoridades en el art. 94[29] transmite que la práctica de las

29. Las medidas facultadas por dicho precepto son a) "acceder a cualquier documento y dato bajo cualquier forma, y obtener copia del mismo"; b) " solicitar o exigir información de cualquier persona, inclusive de aquellas que intervienen sucesivamente en la transmisión de órdenes o en la ejecución de las operaciones consideradas, así como de sus directivos, y en caso necesario citar e interrogar a

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

mismas tiene una clara finalidad sancionadora, toda vez que se trata de la ejecución de medidas acordadas de cara a encontrar información o pruebas, de las que aparentemente se tienen constancia, para justificar la sanción frente a la sanción presumida. Así, por ejemplo, acceder a los locales de personas físicas o jurídicas, a fin de proceder a la incautación de documentos y datos, bajo cualquier forma, "cuando haya una sospecha razonable de la existencia de documentos o datos relativos al objeto de la inspección o investigación que pudieran ser pertinentes para probar un caso de operación con información privilegiada o de manipulación de mercado", obtener copias de estos documentos o solicitar registros sobre tráfico de datos, entre otras medidas concretadas en el art. 94.3, requiere, como indica el propio texto, que se tenga la sospecha de la existencia de tales pruebas y de la supuesta infracción, pues, en caso contrario, estaríamos –valga el símil traído del Derecho penal– ante una investigación prospectiva que dotaría a la Administración de facultades de control exorbitantes respecto de los administrados, que no encuentra ningún tipo de justificación en un estado de derecho.

Al sobrepasar este tipo de investigaciones los límites de las actuaciones de mera comprobación para las cuales se estableció el deber de colaboración con la Administración que atañe a todos los administrados de forma ineludible (Gómez Tomillo, 2022, 6; Picón Arranz, 2022, 377), este quedaría excluido cuando las medidas de inspección derivaran –o pudieran derivar– en la incoación de un procedimiento sancionador o en la de un proceso penal, esto es, cuando lo tramitado fuera un procedimiento sancionador y no meramente de comprobación. Dado que las medidas de entrada en locales para proceder a su registro o para obtener material supuestamente existente, requeriría de la autorización de la persona afectada y en el procedimiento sancionador se prevé la negativa o la falta de colaboración, el art. 94 incorpora en su apartado 4 d) la obligación de solicitar la autorización de los órganos jurisdiccionalmente competentes –del orden contencioso administrativo– cuando el derecho nacional así lo requiera. En caso contrario, esto es, sin consentimiento del interesado y sin autorización del órgano jurisdiccional, tanto la entrada como el registro efectuado, por ejemplo, serían ilícitos, viciando también de nulidad el resultado obtenido.

Por otro lado, las autoridades administrativas no podrían continuar una investigación a sabiendas de que los hechos no constituyen una infracción administrativa,

una persona con el fin de obtener información"; c) "acceder a los locales de personas físicas y jurídicas a fin de proceder a la incautación de documentos y datos bajo cualquier forma cuando haya una sospecha razonable de la existencia de documentos o datos relativos al objeto de la inspección o investigación que pudieran ser pertinentes para probar un caso de operación con información privilegiada o de manipulación de mercado"; d) "remitir asuntos con fines de enjuiciamiento"; e) "solicitar, en la medida en que lo permita el Derecho nacional, los registros existentes sobre tráfico de datos que mantenga una empresa de telecomunicaciones cuando haya una sospecha razonable de que se haya cometido una infracción y cuando dichos registros puedan ser pertinentes para la investigación de una infracción de los artículos 88 a 91"; f) "solicitar la congelación o el embargo de activos, o ambos". Además, podrá prohibir el ejercicio temporal de una actividad profesional o adoptar medidas para informar adecuadamente al público de la situación y adoptar todas las medidas necesarias para garantizar que el público sea informado de la situación, así como para corregir la publicidad errónea o engañosa que haya sido advertida.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

sino una infracción penal, pues ello no solo pone de manifieste una clara falta de competencia, sino que exige la aplicación criterios más garantistas para proteger el derecho de defensa del afectado, que no siempre alcanzan la misma intensidad en el ámbito administrativo. De hecho, el art. 125.2, para las investigaciones relativas a fichas significativas, prevé que la autoridad judicial a la que se solicite la autorización la deniegue, precisamente por considerar que los hechos son claramente subsumibles en un tipo penal. Véase que el art. 124 prevé la misma condición de autorización judicial para el intercambio de información y para la práctica de las inspecciones *in situ* acordadas en el contexto de una investigación relativa a los servicios de fichas significativas, advirtiendo que aquella será denegada cuando lo que proceda sea una investigación de carácter penal.

Este criterio es el que debía prevalecer en cualquier situación, esto es, con independencia de la naturaleza –significativa o no– de la ficha o del criptoactivo vinculado al servicio inspeccionado; es más el art. 136 incorpora en su apartado 1 la obligación de designar un agente de investigación independiente, perteneciente a la ABE, ante la sospecha de que los hechos –relativos a las fichas significativas– son constitutivos de una de las infracciones administrativas de los anexos V[30] y VI[31] del Reglamento MiCA, no estando previsto nada parecido para las investigaciones relacionadas con los criptoactivos no significativos. Si bien es cierto que las primeras, por sus características –amplia base de clientes, una elevada capitalización bursátil o un gran número de operaciones– conllevan un mayor riesgo, la designación de un investigador independente refleja mayores garantías en un contexto que, como estamos viendo, entra decididamente en el ámbito sancionador, esto es, punitivo.

4.4. La sanción penal y la sanción administrativa: una dualidad punitiva

El art. 111 del Reglamento, que relaciona las sanciones administrativas que pueden ser impuestas frente a las infracciones referidas en el apartado 1 del mismo precepto[32], a

30. Lista de infracciones a que se refieren los títulos III y VI en relación con los emisores de fichas significativas referenciadas a activos.

31. Lista de infracciones de las disposiciones a que se refiere el título IV conjuntamente con el título III en relación con los emisores de fichas significativas de dinero electrónico.

32. Indica al respecto el art. 111 las "a) infracciones de los artículos 4 a 14 –activos distintos de fichas referenciadas a activos o fichas de dinero electrónico; b) infracciones de los artículos 16, 17, 19, 22, 23 y 25 –oferta pública y solicitud de admisión a negociación de fichas referenciadas a activos–, de los artículos 27 a 41 –obligaciones de los emisores de las ficas referenciadas a activos– y de los artículos 46 y 47 –planes de recuperación y reembolso para las fichas referenciadas a activos-;c) infracciones de los artículos 48 a 51 –requisitos que deben cumplir los emisores de fichas de dinero electrónico– y de los artículos 53, 54 y 55 –dedicados respectivamente a la comunicaciones publicitarias relativas a una oferta pública de una ficha de dinero electrónico, o a la admisión de dicha ficha de dinero electrónico a negociación, las condiciones de los fondos recibidos por los emisores de las fichas de dinero electrónico y los planes de recuperación y reembolso relativos a tales criptoactivos; d) infracciones de los artículos 59, 60 –autorización a los proveedores y prestación de servicios de criptoactivos– y 64 -revocación de la autorización como proveedor de servicios de criptoactivos– y de los artículos 65 a 83

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

través de una redacción poco clara prevé la posibilidad de que los Estados miembros tipifiquen penalmente las conductas que el Reglamento considera infracciones administrativas. Literalmente, el artículo comienza diciendo que "[s]in perjuicio de las sanciones penales, ni de las facultades de supervisión e investigación de las autoridades [administrativas] competentes enumeradas en el art. 94, los Estados miembros dispondrán, de conformidad con el Derecho nacional, que las autoridades competentes tengan la facultad de imponer sanciones administrativas y adoptar otras medidas administrativas adecuadas en relación, al menos" con dichas infracciones.

Si leemos atentamente el precepto podemos distinguir: a) que sin perjuicio de las facultades de investigación y de supervisión reconocidas en tal disposición, a las autoridades competentes, los Estados miembros, conforme al Derecho nacional, incorporarán las disposiciones necesarias para que aquellas puedan imponer las sanciones oportunas una vez desarrollada la investigación –toda vez que la investigación tendrá lugar en un Estado y conforme a la regulación de dicho ordenamiento–; y b) que los Estados deben actuar de esta forma, con independencia de las sanciones penales que pudieran ser impuesta, por estar previstas, respecto de estas mismas conductas o infracciones.

Por otro lado, cuando el texto dice que "[s]in perjuicio de las sanciones penales […] los Estados miembros *dispondrán*" que las autoridades administrativas tengan la facultad de imponer sanciones cuando constaten la comisión de las infracciones del Reglamento, en realidad parece obligar a los Estados –"los Estados dispondrán" y no "los Estados podrán disponer"- a reconocer a nivel nacional que las autoridades competentes [nacionales o europeas, según los casos] debían estar, en todo caso, en disposición de sancionar administrativamente los incumplimientos de las obligaciones dispuestas en el Reglamento. Ello ha tener lugar, no obstante, sin perjuicio de que el mismo ordenamiento nacional también hubiera previsto la tipificación penal de tales conductas y haya concretado, por lo tanto, las correspondientes sanciones penales. A mayor abundamiento, esta tipificación penal no puede impedir el ejercicio de las funciones enumeradas en el art. 94 y atribuidas a las autoridades administrativas competentes. Es decir, que lo que hace el legislador en el art. 111 es prever una doble tipificación –la administrativa y la penal–, de forma que la regulación administrativa no excluye la regulación penal -"[s]in perjuicio de las sanciones penales"- ni la penal excluye la administrativa –sin perjuicio "de las facultades de supervisión e investigación de las autoridades competentes enumeradas en el artículo 94"-. En este sistema doblemente sancionador –penal y administrativo– se debe marcar una clara línea divisoria entre ambos ámbitos que no queda definida en el Reglamento y que, por consiguiente, ha de ser fijada en función del principio *non bis idem* a fin de evitar una doble sanción de idéntica intensidad, esto es, punitiva.

En otro orden de cosas, y antes de continuar, recordemos que las disposiciones que deben recoger los Estados para permitir que las autoridades competentes puedan imponer

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

–en general sobre las obligaciones de los prestadores de servicios de criptoactivos–; e) infracciones de los artículos 88 a 92; f) la falta de cooperación o acatamiento de las investigaciones, inspecciones o requerimientos a que se refiere el artículo 94, apartado 3.

sanciones tras desarrollar la investigación correspondiente, son las normas de adaptación del ordenamiento nacional al Reglamento, que constituye norma directamente aplicable, y que no tienen la condición de normas de transposición, por lo que las disposiciones nacionales deberán asumir las infracciones y las sanciones tal y como son previstas por la Unión, esto es, sin posibilidad de adaptación.

Por su parte, el párrafo segundo del apartado 1 estipula que "[l]os Estados miembros podrán decidir no establecer normas relativas a las sanciones administrativas cuando las infracciones señaladas en el párrafo primero, letras a), b), c), d) o e)", que abarcan prácticamente la totalidad de las obligaciones relativas a los proveedores de servicios de las fichas referenciadas, incluyendo las relativas a las fichas significativas, cuando " ya estuvieran sujetas a sanciones penales en su Derecho nacional a más tardar el 30 de junio de 2024", debiendo los Estados, en tal caso, informar detalladamente a la Comisión, a la AEVM y a la ABE sobre las disposiciones penales en relación con tales infracciones.

A pesar de la contradicción que pudiera advertirse entre los dos párrafos –el primero indica que los Estados "dispondrán" las medidas que permitan a las autoridades nacionales sancionar, mientras que el segundo dice que los Estados miembros "podrán decidir no establecer normas relativas a las sanciones administrativas"-, parece claro que este segundo constituye la excepción frente a la regla general con la que principia el artículo –párrafo primero– y que obliga a disponer normas que incorporen las sanciones administrativas para que estas puedan ser efectivamente impuestas. Así, la excepción solo resulta aplicable cuando se advierta una condición ineludible, y es que las conductas previstas en el Reglamento estén penalmente sancionadas en el derecho nacional o que lo estén, a más tardar, el 30 de junio de 2024. Además, aquella comunicación detallada a la Comisión y a las autoridades europeas de las que habla el precepto parece tener como objeto comprobar que la sanción penal prevista en el ordenamiento nacional genere, como mínimo, el mismo efecto que las sanciones administrativas definidas en el Reglamento, ya que en caso contrario se estaría eludiendo la función sancionadora de las medidas y desprotegiendo el mercado. De este modo, el legislador intenta asegurar la eficacia de las disposiciones reglamentarias forzando su cumplimiento, ya sea bajo la amenaza de una sanción administrativa, ya bajo la amenaza de la sanción penal, pero con la condición de que ambas tengan una intensidad punitiva lo suficientemente disuasora.

Si un Estado no instituyera sanciones administrativas por haber incorporado sanciones penales, estaría resolviendo el problema que genera la doble imposición prohibida por el principio *non bis in idem* en cuanto que, al optarse exclusivamente por tipificar penalmente las conductas, despojándolas de cualquier trascendencia administrativa, solo podrá ser impuesta la sanción penal. Pero, por otro lado, la exclusión de la sanción administrativa es una decisión voluntaria de los Estados –"podrán decidir no establecer" – cuando opten por la sanción penal y esta tenga un efecto, como mínimo equivalente al atribuido a la sanción administrativa establecida. No podemos dejar de decir, asimismo, que tampoco resulta completamente acertado dejar a la decisión de los Estados el tipo de sanción que deba aplicarse en el ordenamiento interno, porque ello provocará que los mismos hechos merezcan un reproche administrativo o un reproche penal, cuando lo cierto es que la sanción penal implica una mayor intensidad

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

por su propia naturaleza. Sea como fuere, las sanciones administrativas del Reglamente son considerable incisivas, acercándose su espíritu al de una pena.

En el caso de concurrir ambos tipos de sanciones y unos mismos hechos puedan ser susceptibles de una sanción administrativa y de otra penal, comprobado que la situación debe ser efectivamente subsumida en el tipo penal, la autoridad administrativa deberá informar a las autoridades penales competentes, paralizar la investigación administrativa y no avanzar hacia el procedimiento administrativo sancionador debido a la preferencia de la jurisdicción penal. Nos topamos, en principio, con el muro que levanta el principio *non bis in idem* y que impide castigar doblemente.

Sin embargo, aquel límite opera cuando la sanción administrativa impuesta sea verdaderamente punitiva, esto es, cuando albergue un efecto o una finalidad similar o muy cercana a la que se desprende de una sanción penal, siendo entonces cuando el principio *non bis in idem* impide que la situación sea doblemente punida. Como consecuencia, determinada la sanción administrativa no podría incoarse o continuarse la investigación penal, por los mismos hechos, cuando aquella alcance, por su cuantía o extensión, casi la misma consideración que una pena. En caso contrario, y si la sanción administrativa no incorporara, por sus características, un reproche equivalente al penal, quedará margen para imponer una pena.

Por su parte, impuesta una pena normalmente no podría avanzarse hacia un procedimiento administrativo sancionador porque la Administración debe aceptar el relato jurídico de los hechos y circunstancias que resultaron probados, si bien cabría una sanción administrativa a pesar de la pena efectivamente impuesta, cuando los hechos que delimitan la infracción administrativa no se correspondiesen completamente con el tipo penal o cuando ambas sanciones se basen en motivaciones distintas.

V. Un avance de la futura regulación para la protección del sistema financiero

La regulación jurídica de los criptoactivos tiene entre sus objetos dotar de seguridad jurídica y transparencia a las transacciones efectuadas con aquellos, previniendo de este modo los delitos de naturaleza económico-financiera vinculados a tales operaciones. Sin embargo, la sanción penal a la que se refiere el art. 111 en su párrafo 1 no está referida a los delitos de naturaleza económico-financiera de blanqueo de capitales o de financiación del terrorismo que pudiera cometerse a través del mercado de criptoactivos, sino a las conductas que conforme al Reglamento constituyen una infracción administrativa y a la que los ordenamientos nacionales pueden dotar de naturaleza penal. El delito relativo al incumplimiento de las condiciones del Reglamento MiCA tiene, pues, como sujeto activo de la infracción –y sujeto pasivo del proceso penal correspondiente– a los proveedores de servicios y a quienes ocupen cargos de responsabilidad en los órganos de gestión de tales entidades.

Tenemos que percibir, por otro lado, que en el asunto pueden concurrir la infracción administrativa y/o penal que supone el incumplimiento de los deberes u obligaciones

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

que refiere el art. 111 en su apartado 1 y un delito de blanqueo o de financiación del terrorismo, por ejemplo, que hubiera podido ser dolosa o imprudentemente consentido por el proveedor. Con respecto a esta última situación habrá de contemplarse el caso en su totalidad para comprobar si, además de quienes tengan la consideración de proveedores, pudieran haber intervenido otras persona –en las diferentes formas previstas en el ordenamiento concernido– que pudieran tener la consideración de sujeto activo del delito cometido a través de los criptoactivos, pero no del delito que tipifica el incumplimiento de las obligaciones impuestas en el Reglamento al proveedor a la entidad proveedora del servicio. Cabrá, así, la posibilidad de un concurso de delitos y de una posible conexión delictiva que daría lugar, en su caso, a un proceso de objeto complejo.

Queremos exponer con este ejemplo, que el Reglamento MiCA solo regula las condiciones de negociación de los criptoactivos y que ello está directamente vinculado con la prevención del blanqueo de capitales y de financiación del terrorismo, pero que no constituye una norma que expresamente tenga como finalidad reprimir o castigar penalmente las conductas de naturaleza financiera o de terrorismo perpetradas a través de las operaciones que dispone. La regulación sustantiva de estos comportamientos encuentra su sede en la Directiva relativa a la lucha del blanqueo de capitales a través del derecho penal, en la Directiva de lucha contra el terrorismo y en los demás instrumentos aprobados para combatir la delincuencia financiera o que use sus vías para la perpetración de los hechos[33].

33. Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, cit.; Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo, *Diario Oficial de la Unión Europea, L88*, de 31 de marzo de 2017. http://data.europa.eu/eli/dir/2017/541/oj (en el art. 4 el legislador exige a los Estados la tipificación de cualquier forma de participación en la financiación de un grupo terrorista y dedica el art. 11 a la regulación del delito de financiación del terrorismo, relacionando las conductas que deben ser tipificadas como tal); Directiva (UE) 2017/1371 del Parlamento Europeo y del Consejo de 5 de julio de 2017, sobre la lucha contra el fraude que afecta a los intereses financieros de la Unión a través del Derecho penal, *Diario Oficial de la Unión Europea, L198*, de 28 de julio de 2017. http://data.europa.eu/eli/dir/2017/1371/oj; Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, cit.; Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal, *Diario Oficial de la Unión Europea, L284*, de 12 de noviembre de 2018. http://data.europa.eu/eli/dir/2018/1673/oj; Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo, *Diario Oficial de la Unión Europea, L186*, de 11 de julio de 2019. http://data.europa.eu/eli/dir/2019/1153/oj.

Podemos incluir el Reglamento (UE) 2017/1939 del Consejo de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de una Fiscalía Europea, *Diario Oficial de la Unión Europea, L28*, de 31 de octubre de 2017. http://data.europa.eu/eli/reg/2017/1939/oj; el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos, cit., y el Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

Actualmente está siendo objeto de discusión dos Propuestas de Reglamento y una de Directiva que pretende otorgar una nueva arquitectura al escenario de la prevención y de la represión del blanqueo de capitales y de financiación del terrorismo, y que parece que hará referencia, de forma específica, al delito cometido a través de estos activos, si bien tampoco se trata de instrumentos penales, sino de naturaleza administrativa y, por lo tanto, dirigidos a fortalecer las medidas de diligencia debida frente al uso ilícito de las vías financieras y del mercado –incluyendo el de criptoactivos-.

Dejando a un lado el Reglamento a través del que se creará la autoridad europea contra el blanque de capitales –AMLA por sus siglas en inglés[34]-, la Propuesta de Reglamento relativo a la prevención de la utilización del sistema financiero o la financiación del terrorismo[35] asume parte de la regulación que hoy contiene la 4AMLD –de la que ya hemos referido su escaso éxito–, mientras que la Propuesta de Directiva[36] (Propuesta de 6ª Directiva) restructura los aspectos de la 4AMLD no absorbidos por el Reglamento. Adviértase, además, cómo el legislador adopta la decisión de regular a través de Reglamento aquellos aspectos de la Directiva que no fueron transpuestos y aplicados de forma armonizada. Aprobado este Reglamento, los ordenamientos tendrán que adaptarse a sus disposiciones, desapareciendo, en parte, el problema de las diferencias normativas que se generan a partir de las normas de transposición de las directivas.

Este paquete legislativo forma parte del *Plan de Acción de la Comisión* de 2020, dirigido a definir una estructura normativa contra el blanqueo de capitales y de financiación del terrorismo más acorde con la situación actual, advirtiendo la Propuesta de Reglamento que su contenido procura la prevención eficaz del uso ilícito del sistema financiero, al tiempo que refunde las disposiciones del Reglamento (UE) 2015/847 para ampliar los requisitos de trazabilidad de las operaciones financieras a los criptoactivos. Considera igualmente necesario adoptar las modificaciones relativas a determinar la responsabilidad de los obligados y a la aplicación y control de las medidas de diligencia debida para proteger el mercado y las vías financieras, al haber sido incorporados los proveedores de criptoactivos al conjunto de entidades obligadas[37]. De hecho, el considerando

mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849, *Diario Oficial de la Unión Europea, L150*, de 9 de junio de 2023. http://data.europa.eu/eli/reg/2023/1113/oj.

34. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo y se modifican los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 y (UE) n.º 1095/2010, de 20 de julio de 2021, COM (2021) 421 final. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0421.

35. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la prevención de la utilización del sistema financiero o la financiación del terrorismo, de 20 de julio de 2021, COM (2021) 420 final. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0420.

36. Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y por la que se deroga la Directiva (UE) 2015/849, de 20 de julio de 2021, COM (2021) 423 final. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0423.

37. Comunicación de la Comisión sobre un Plan de acción para una política global de la Unión en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, cit., p. 9.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

9 indica que estos "y las plataformas de financiación participativa están expuestos al uso indebido de los nuevos canales para la circulación de dinero ilícito y se hallan bien situados para detectar estos movimientos y mitigar los riesgos".

Incide, por otro lado, el Reglamento en la necesidad de suprimir la privacidad de las operaciones con criptoactivos –problema que parece no quedar definitivamente resuelto con el Reglamento MiCA ni con las demás disposiciones normativas aplicables– porque lo contrario pone en duda el nivel de diligencia debida, permitiendo un uso irregular de las vías financieras –considerando 93–. De este modo, el art. 15.2 obligaría a adoptar medidas de prevención a los proveedores de servicios de criptoactivos cuando la operación sea compatible con una trasferencia ocasional de fondos o cuando aquella consista en una transferencia de criptoactivos superior a 1000 euros, prohibiendo, además, el art. 58 que las entidades de crédito, las entidades financieras y los proveedores de servicios mantengan cuentas anónimas, libretas de ahorro anónimas, cajas de seguridad anónimas o monederos de criptoactivos anónimos, "así como cualquier cuenta que permita la "anonimización" del titular de la cuenta del cliente".

Por su parte, la Propuesta de sexta Directiva, exige a los Estados con relación a los criptoactivos que, dada la vulnerabilidad de estos frente al blanqueo, los proveedores establecidos en su territorio –en formas distintas de una sucursal y cuya administración central esté situada en otro Estado – designen un punto de contacto central que actuará en nombre de la entidad que lo haya designado. Este podría actuar, como también se exigen para las entidades proveedoras nacionales de servicios de criptoactivos, a modo de aquella "autoridad centralizada", que no puede ser identificada en los activos digitales debido a que la técnica subyacente es la de registro descentralizado, y que permitiría facilitar información relativa a la identidad de quienes intervengan en las transacciones, así como sobre la trazabilidad de la misma –considerando 7 y art. 4.1-.

VI. A modo de conclusión: la regulación penal indirecta del reglamento MiCA

La infraestructura normativa creada por la Unión Europea para fortalecer las vías financieras y protegerlas frente al delito está siendo continuamente modificada y ampliada. La necesidad de hacer frente a los riesgos que conllevan las nuevas formas de financiación y los negocios vinculados a los activos digitales ha obligado a prever y regular situaciones impensables hace pocos años. Podemos decir, así, que los criptoactivos constituyen una de estas situaciones y que han pasado de ser una anécdota a precisar de una regulación exhaustiva que no puede ser clasificada con los criterios tradicionales.

Efectivamente, el Reglamento MiCA es difícilmente clasificable. Contiene normas de naturaleza administrativa, mercantil e, indirectamente, normas penales, aunque no sea posible calificarlo de esta forma. Así, sabemos que la regulación penal sustantiva se basa en Directivas y que es imposible –o que es prácticamente imposible– imponer regulación sustantiva a los Estados a través de reglamento.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

Como correlato de lo anterior, el Reglamento no contiene ninguna norma de naturaleza penal, pero fuerza a los Estados a legislar de tal forma que la infracción de las obligaciones impuestas a los proveedores de servicios de criptoactivos deben ser sancionadas, ya en la vía administrativa –asumiendo los Estados la intensidad de las sanciones fijadas, pues el Reglamento es de aplicación directa– ya en la vía penal, tal y como permite el art. 111, ya incorporando un doble sistema sancionador –administrativo y penal– respecto del que los Estados deben fijar la línea divisoria que evite la imposición de una doble medida punitiva prohibida por el principio *non bin in idem*.

La referencia final que incorpora el último párrafo del apartado 1 de este precepto, y que dispone para aquellos Estados que opten por sancionar penalmente las infracciones un deber de comunicación "a la Comisión, a la AEVM y a la ABE, en detalle, las disposiciones pertinentes de su Derecho penal", parece tener como finalidad que las autoridades europeas comprueben la intensidad de la sanción penal, para evitar la desprotección del mercado al amparo de una regulación sustantiva de esta naturaleza que disminuya el reproche que incorpora la sanción administrativa recogida en el Reglamento y que, por lo tanto, deshabilitando la protección del mercado de activos de activos digitales. Aunque esta opinión pueda ser discutible, de lo que no cabe duda es de que el legislador está procurando un espacio homogeneizado en el que la equivalencia de sanciones evite resquicios a través de los que la delincuencia pueda eludir la pena.

Evidentemente el texto de la norma no está imponiendo una regulación concreta, ni exige para las infracciones una tipificación sustantiva determinada ni establece sanciones penales específicas, si bien al exigir que la sanciones tengan intensidades similares y al tener el Reglamento efecto directo, obligando a los Estados a aceptar las sanciones especificadas sin posibilidad de adaptarlas a través de una norma de transposición, de forma indirecta reconduce la tipificación penal nacional a los requerimientos establecidos en el propio Reglamento. De este modo, el Reglamento MiCA entra en el ámbito penal para determinar la sanción punitiva, pues el legislador sabe que la homogeneidad sancionadora –o la equivalencia de sanciones– es prácticamente la única forma de evitar diferencias entre ordenamientos que debiliten al mercado de financiación de criptoactivos y que este se convierta en un ámbito de impunidad para la delincuencia.

Bibliografía

ABEN, J. (2022). "Regulación de las Fintech en la Unión Europea: tendencias y líneas difusas", *Revista CIDOB d'Afers Internacionals, 131*, 95-114. http://doi.org/10.24241/rcai.2022.131.2.95 (último acceso 17 de octubre de 2023)

ALVARADO HERRERA, L. (2022). "Los criptoactivos con función de pago: criptomonedas estables y sistemas de pago a la luz de la propuesta del reglamento relativo a los mercados de criptoactivos (MICA)" en M.J. BLANCO SÁNCHEZ y A. MADRID PARRA (Dirs.), *Derecho digital y nuevas tecnologías* (pp. 857-888). Ed. Thomsom-Reuters Aranzadi

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

BARRIO ANDRÉS, M. (2022). "La nueva regulación de los criptoactivos en España", *Diario La Ley, 10010*. https://diariolaley.laleynext.es/Content/Documento.aspx?params=H-4sIAAAAAAAEAMtMSbF1CTEAAmMTC0sTY7Wy1KLizPw8WyMDIyAyMFfLy09JDXFxti3NS-0lNy8xLTQEpyUyrdMlPDqksSLVNS8wpTlVLTcrPz0YxKR5mAgCzphe8YwAAAA==WKE (último acceso 1 de octubre de 2023)

CHIU, I. H-Y. (2021). *Regulating the Cripto Economy. Business transformation and financialisation,* Hart Publishing

GÓMEZ TOMILLO, M. (2022). "Los derechos a no declarar contra sí mismo, a no declararse culpable y a guardar silencio en procedimientos de inspección o supervisión administrativa previos a un procedimiento sancionador o penal", *Estudios penales y criminológicos, 42*, 1-31. https://doi.org/10.15304/epc.42.8069 (último acceso 1 de octubre de 2023)

GONÇALVES, DA COSTA VALE, M.L. (2023). *A tributação dos criptoativos em Portugal (Impostos sobre o rendimento)*, https://estudogeral.uc.pt/retrieve/263916/A%20tributac%CC%A7a%CC%83o%20dos%20Criptoativos_M%C2%AA%20Leonor%20Gonc%CC%A7alves.pdf (último acceso 27 de octubre de 2023)

JARNE MUÑOZ, P. (2018). "La Unión Europea ante el reto de las fintech. Algunas notas al Plan de acción en materia de tecnología financiera", *Revista de Estudios Europeos, 72,* 118-128. https://dialnet.unirioja.es/servlet/articulo?codigo=6862732 (último acceso 1 de octubre de 2023).

HUANG, S. (2021). "Cryptocurrencies and Crime" en A. LUI & N. RAYDER (Eds.), *FinTech, Artificial Intelligence and the Law: Regulation and crime Prevention* (pp. 125-143). Routledge, Taylor & Francis Group

KAPSIS, I. (2021). "Should we trade market stability for more financial inclusion? The case of crypto-assets regulation in EU", en A. LUI & N. RAYDER (Eds.), *FinTech, Artificial Intelligence and the Law: Regulation and crime Prevention,* Routledge (pp. 85-104). Taylor & Francis Group

MARTÍN RÍOS, P. (2020). "Problemas de admisibilidad de la prueba obtenida de dispositivos de almacenamiento digital", *Revista General de Derecho Procesal, 51*, 1-31. https://www-iustel-com.eu.1.proxy.openathens.net//v2//revistas/detalle_revista.asp?id=9 &numero=51 (último acceso 17 de octubre de 2023)

MAUME, P. (2022). "Consumer Protection", en Maume/Maute/Fromberger (Dirs.), *The law of crypto assets. A handbook* (pp. 109-120). Beck-Nomos-Hart Ed.

NAVARRO CARDOSO, F. (2019). "Criptomonedas, (en especial, bitcoin) y blanqueo de dinero", *Revista Electrónica de Ciencia Penal y Criminología, 21*(14), 1-45. http://criminet.ugr.es/recpc/21/recpc21-14.pdf (último acceso 16 de octubre de 2023)

PARRONDO, L. (2023). "El Reglamento de Mercados de Criptoactivos (MiCA)", *Técnica contable y financiera,* 67, 1-10. https://www.academia.edu/106860564/El_Reglamento_de_Mercados_en_Criptoactivos (último acceso 1 de octubre de 2017)

PATZ, A. y WETTLAUFER, I.M. (2022). "E-money Tokens, Ttablecoins and Token Payment Services" en Maume/Maute/Fromberger (Dirs.), *The law of crypto assets. A handbook* (pp. 242-268). Beck-Nomos-Hart Ed.

PÉREZ LÓPEZ, X. (2019). "Las criptomonedas: consideraciones generales y empleo de las criptomonedas con fines de blanqueo" en D. Fernández Bermejo (Dir.), *Blanqueo de capitales y TIC: marco jurídico nacional y europeo, modus operandi y criptomonedas. Ciberlaundry. Informe de situación* (pp. 71-147). Ed., Thomson Reuters-Aranzadi

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

PÉREZ MARÍN, M.A. (2022). "La función preventiva del sistema financiero en el espacio judicial europeo: ¿Medidas (Penales) de Prima Ratio? *Revista Internacional CONSINTER de Direito, 8* (14), 289-311. https://revistaconsinter.com/index.php/ojs/article/view/48/80 (último acceso 17 octubre de 2023)

PÉREZ MARÍN, M.A. (2021). "El control de las vías financieras frente a la delincuencia organizada en el espacio de libertad, seguridad y justicia: los avances hacia la persecución de nuevas amenazas" en F.J. Garrido Carrillo (Dir.), *Retos en la lucha contra la delincuencia organizada. Un estudio multidisciplinar: garantías, instrumentos y control de los beneficios económicos* (pp. 85-119). Ed. Aranzadi

PICÓN ARRANZ, A. (2022). "El derecho a la no autoincriminación en el procedimiento administrativo sancionador: un estudio a la luz de la jurisprudencia del TJUE". *Revista de Estudios Europeos, 79,* 367-388. https://doi.org/10.24197/ree.79.2022.367-388 (último acceso 1 de octubre de 2023)

ZARAGOZA TEJADA, J. I. (2019). "Criptoactivo y blanqueo de capitales. Problemas jurídico procesales", *Revista Aranzadi Doctrinal, 8.* https://www.thomsonreuters.es/es/tienda/revistas/revista-aranzadi-doctrinal.html (último acceso 17 de octubre de 2023)

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 64-92
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.04

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

¿Derecho o deber del ciudadano a relacionarse electrónicamente con las Administraciones Públicas? Análisis de las impugnaciones judiciales en aplicación de los artículos 14 y 68.4 de la LPACAP y del impacto del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

IS IT A CITIZEN'S RIGHT OR DUTY TO INTERACT ELECTRONICALLY WITH PUBLIC ADMINISTRATIONS? JURISPRUDENTIAL ANALYSIS OF ARTICLES 14 AND 68.4 OF THE LPACAP AND THE IMPACT OF ROYAL DECREE 203/2021, OF 30 MARCH, 2021, APPROVING THE REGULATION ON THE PERFORMANCE AND FUNCTIONING OF THE PUBLIC SECTOR BY ELECTRONIC MEDIA.

María Luisa Domínguez Barragán
Universidad de Sevilla
mdominguez16@us.es 0000-0003-4796-3624

Recibido: 20 de octubre de 2023 | Aceptado: 01 de diciembre de 2023.

RESUMEN

El presente trabajo tiene como objetivo el estudio jurisprudencial relativo al derecho u obligación del ciudadano a relacionarse, a través de medios electrónicos, con las Administraciones Públicas. Así, se lleva a cabo la profundización en las distintas resoluciones judiciales que, desde 2016, han interpretado los artículos 14 y 68 de la LPACAP y el impacto que, en esta materia ha tenido la norma de desarrollo.

PALABRAS CLAVE

Medios electrónicos
Administración pública
Sector público
Jurisprudencia

ABSTRACT

The objective of this paper is the jurisprudential study related to the right or obligation of the citizens to interact, through electronic media, with Public Administrations. Thus, an in-depth look is made at the different judicial resolutions that, since 2016, have interpreted articles 14 and 68 of the LPACAP and the impact that in this matter has had the implementing regulation.

KEYWORDS

Electronic media
Public Administration
Public sector
Jurisprudence

I. Introducción

Puede afirmarse que, en el año 2015, las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) y 40/2015, también de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP) revolucionaron la configuración del procedimiento administrativo español. Como se afirmaba por la doctrina, estas leyes serían, por tanto, no ya troncales, sino esenciales para el funcionamiento del actual Estado social y democrático de Derecho que, integrado en la Unión Europea (cuyo ordenamiento es, esencialmente, jurídico-público y, más concretamente, administrativo), adquiere progresivamente la coloración de Estado regulador y garante de la dación de bienes y la prestación de servicios que, aún entregados a la lógica del mercado, tienen dimensión pública (PAREJO ALFONSO, 2016, 38).

Como indica la Exposición de motivos de la LPACAP, mediante ambas normas se proponía una reforma del ordenamiento jurídico público articulada en dos ejes fundamentales: las relaciones "ad extra" y "ad intra" de las Administraciones Públicas. Por ese motivo, se impulsaban simultáneamente las dos normas que iban a convertirse en los pilares sobre los que se asienta el actual derecho administrativo español. En relación a la LPACAP, la citada Exposición de motivos indica:

> Esta Ley constituye el primero de estos dos ejes, al establecer una regulación completa y sistemática de las relaciones «ad extra» entre las Administraciones y los administrados, tanto en lo referente al ejercicio de la potestad de autotutela y en cuya virtud se dictan actos administrativos que inciden directamente en la esfera jurídica de los interesados, como en lo relativo al ejercicio de la potestad reglamentaria y la iniciativa legislativa. Queda así reunido en cuerpo legislativo único la regulación de las relaciones «ad extra» de las Administraciones con los ciudadanos como ley administrativa de referencia que se ha de complementar con todo lo previsto en la normativa presupuestaria respecto de las actuaciones de las Administraciones Públicas, destacando especialmente lo previsto en la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera; la Ley 47/2003, de 26 de noviembre, General Presupuestaria, y la Ley de Presupuestos Generales del Estado.

En ese contexto, la Administración no podía quedar al margen de la forma en que los ciudadanos y las personas jurídicas se interrelacionaban, en un espacio donde las tecnologías de la información y comunicación estaban ocupando un papel primordial (mucho más reforzado tras la pandemia de COVID-19), por lo que la introducción de medios electrónicos en el procedimiento administrativo se convirtió en una realidad de primer orden (DE ALBA BASTARRECHEA, 2017, 91). De hecho, el reconocimiento expreso del principio de eficacia administrativa en nuestra Constitución otorga la base jurídica suficiente para promover la necesidad de adecuación sinérgica de la Administración a los cambios que está experimentando el conjunto de la sociedad, además de dotar de perfecta cabida a los nuevos contenidos exigibles a la Administración del futuro (EXPÓSITO GÁZQUEZ, 2022, 48).

Así, en conexión con la posibilidad que tiene el ciudadano de relacionarse con la Administración Pública por medios electrónicos, nos recuerda también la Exposición de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

motivos de la LPACAP que esto no es ninguna novedad, ya que fue la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, la que les dio carta de naturaleza legal "al establecer el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas, así como la obligación de éstas de dotarse de los medios y sistemas necesarios para que ese derecho pudiera ejercerse". Además, la Exposición de motivos continúa en los siguientes términos:

> Sin embargo, en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos sino que debe constituir la actuación habitual de las Administraciones. Porque una Administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados. En efecto, la constancia de documentos y actuaciones en un archivo electrónico facilita el cumplimiento de las obligaciones de transparencia, pues permite ofrecer información puntual, ágil y actualizada a los interesados.

Con estos antecedentes[1], se establece el artículo 14[2] de la LPACAP como eje principal de articulación de dicha relación ciudadano-Administración Pública. Dicho artículo, titulado "Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas" establece una voluntariedad en dicha relación, pues en su apartado primero recoge que las personas físicas podrán elegir, en todo momento, si se comunican con las Administraciones

1. Para un análisis en mayor profundidad de los antecedentes de este artículo, puede verse SANCHEZ LAMELAS, 2023, 204 y ss.
2. Dicho artículo establece:
   1. Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento.
   2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:
      a. Las personas jurídicas.
      b. Las entidades sin personalidad jurídica.
      c. Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.
      d. Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.
      e. Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración.
   6. Reglamentariamente, las Administraciones podrán establecer la obligación de relacionarse con ellas a través de medios electrónicos para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no (salvo que estén obligadas a relacionarse a través de estos medios). Se incluye, además, la posibilidad del ciudadano de cambiar de medio cuando estime conveniente. En relación a la mencionada salvedad, en su apartado segundo dispone una lista de las personas que, en todo caso, están obligadas a utilizar los medios electrónicos como son las personas jurídicas[3]; las entidades sin personalidad jurídica; aquellos que ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional; aquellos que representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración y los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración. Asimismo, y como cláusula de cierre, en su último apartado establece que, reglamentariamente, las Administraciones podrán establecer la obligación de relacionarse con ellas a través de medios electrónicos para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios. Como es lógico, este último apartado también ha generado mucha controversia.

En relación al artículo 14, hemos de mencionar también el artículo 68 del mismo texto normativo y, en concreto, su apartado cuarto, ya que su conexión con el apartado segundo del mencionado artículo 14 es indudable. Dicho artículo 68.4 dispone que: "Si alguno de los sujetos a los que hace referencia el artículo 14.2 y 14.3 presenta su solicitud presencialmente, las Administraciones Públicas requerirán al interesado para que la subsane a través de su presentación electrónica. A estos efectos, se considerará como fecha de presentación de la solicitud aquella en la que haya sido realizada la subsanación".

Como puede pensarse, el desarrollo de estas relaciones telemáticas ha ido más allá. En 2021 entró en vigor el Real Decreto 203/2021, de 30 de marzo, por el que se aprobaba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos[4]. Como norma de desarrollo de la LPACAP, esta norma concreta algunos aspectos relativos al mencionado artículo 14, especialmente en sus artículos tercero y cuarto y en su disposición adicional primera, donde se establece la obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado[5]. Este Reglamento nos indica en su Exposición de motivos que:

3. En relación a las personas jurídicas, es de gran interés: GARCÍA LOPEZ, 2022.

4. En conexión con esta materia debe citarse, por su importancia, la aparición en el BOE el pasado 23 de octubre del Instrumento de ratificación del Convenio del Consejo de Europa sobre el acceso a los documentos públicos, hecho en Tromsø el 18 de junio de 2009.

5. La disposición adicional primera establece: "Las personas participantes en procesos selectivos convocados por la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes a la misma, deberán realizar la presentación de las solicitudes y documentación y, en su caso, la subsanación y los procedimientos de impugnación de las actuaciones de estos procesos selectivos a través de medios electrónicos".

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

> (…) La Ley 39/2015, de 1 de octubre, y la Ley 40/2015, de 1 de octubre, han dado respuesta a la demanda actual en el sentido de que la tramitación electrónica de los procedimientos debe constituir la actuación habitual de las Administraciones Públicas, y no solamente ser una forma especial de gestión de los mismos. En consecuencia, se prevé que las relaciones de las Administraciones entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes se realizará a través de medios electrónicos, y se establece la obligatoriedad de relacionarse electrónicamente con la Administración para las personas jurídicas, entes sin personalidad y, en algunos supuestos, para las personas físicas, y ello sin perjuicio de la posibilidad de extender esta obligación a otros colectivos, por vía reglamentaria.
>
> Con estos antecedentes, era necesario desarrollar y concretar las previsiones legales con el fin, entre otros aspectos, de facilitar a los agentes involucrados en el uso de medios tecnológicos su utilización efectiva, aclarando y precisando, al mismo tiempo, aquellas materias reguladas en estas leyes que permiten un margen de actuación reglamentaria".

Ciertamente, reforzar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica de todos los sectores. Al hilo del citado Reglamento, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, actualizándolo a los nuevos retos que se presentan en un mundo hiperconectado, expone en su Exposición de motivos lo siguiente:

> (…) El Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros…".

Dicho todo lo anterior, este trabajo tiene como objetivo realizar un análisis sobre la labor jurisdiccional relativa a la interpretación del citado artículo 14 LPACAP, pues como indica el Informe *Sociedad Digital en España 2023,* la digitalización es un fenómeno global imparable. En el pasado año 2022, casi dos tercios (66,3 %) de la población mundial era usuaria de internet, siendo este porcentaje de 3,7 puntos superior al de 2021 (62,6 %)[6]. De igual forma, se atenderá al estudio de los supuestos subsanados basados en el artículo 68 LPACAP y a las, aun escasas, resoluciones judiciales relativas a la aplicación, en ciertos casos controvertida, del Real Decreto 203/2021.

II. Visión judicial

2.1. Interpretaciones sobre la aplicación del artículo 14.1 LPACAP

Del estudio de la jurisprudencia relacionada se desprende que el apartado primero del artículo 14 es el que menos problemas interpretativos y de aplicación ha generado. Si

6. Vid. Informe "Sociedad Digital en España 2023" de la Fundación Telefónica, pág. 15.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

bien no hemos encontrado ninguna resolución del Tribunal Supremo que, concretamente, resuelva sobre el particular, sí que, en algún caso, los Tribunales Superiores de Justicia han tenido ocasión de pronunciarse. Veamos dos ejemplos: uno resuelto a favor del ciudadano y el otro, a favor de la Administración.

El Tribunal Superior de Justicia valenciano en su STSJ CV 6135/2022, de 31 de octubre[7], estima el recurso de apelación presentado por una Administración pública local al considerar que, en aplicación del artículo 14.1, el particular apelado podía elegir el modo de relacionarse con la Administración (vía electrónica/ordinaria en papel), habiendo elegido la vía electrónica que, en principio, era legal aunque se diera la circunstancia, como recoge la STSJ, que el Ayuntamiento de la Pobla del Duc no tenía preparada la vía electrónica ni estaba obligada a ello. Con estas premisas, la STSJ entiende que la Administración no tiene obligación de tener por presentado un recurso de reposición remitido al correo de una funcionaria, a lo que añade que el demandante, que además tiene la condición de letrado, puesto que remitió el correo con tiempo, debió cerciorarse de su presentación y no lo hizo. Por ello, considera la Sala que el Ayuntamiento no está obligado a reconocer como presentado el recurso de reposición objeto de la controversia. A nuestro juicio, la condición de letrado del particular no puede considerarse como un argumento más a favor de la poca efectividad de la Administración local, por lo que entendemos que se trataría de un problema probatorio que no respeta las premisas de lo que se ha considerado como "buena administración".

Los problemas de interoperabilidad son los que han llevado a los Tribunales Superiores de Justicia, en gran medida, a tener que pronunciarse sobre este apartado. En la STSJ M 10169/2023, de 18 de septiembre, el Tribunal Superior de Justicia de Madrid estima el recurso contencioso-administrativo interpuesto, condenando a la Administración y anulando la resolución administrativa porque entiende que, en aplicación del artículo 14.1 LPACAP, ésta tenía que haber vuelto al sistema ordinario de notificaciones y no optar por la utilización de los medios electrónicos. En un procedimiento de gestión tributaria, el administrado había presentado un escrito que estaba encabezado con la indicación de un domicilio a efectos de notificaciones, denunciando la incorrección de las practicadas con anterioridad, alegando el desconocimiento de la razón del sistema empleado de notificaciones electrónicas y recogiendo la no obligatoriedad del mismo en el caso del interesado en el procedimiento.

2.2. Respuesta judicial al tratamiento del artículo 14.2 LPACAP

El segundo apartado del artículo 14, al establecer la obligación que tienen algunos sujetos de utilizar los medios electrónicos en sus relaciones con las Administraciones Públicas, también ha sido objeto de interpretaciones judiciales, principalmente en lo

7. Téngase en cuenta que, para la cita de todas las resoluciones de este trabajo, se ha utilizado la base de datos del CENDOJ y para su identificación el código ROJ, es decir, el número de identificación de las mismas en el Repertorio Oficial de Jurisprudencia.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

relacionado con la eficacia de la actuación cuando no se ha cumplido dicho mandato. Este fue el caso, entre otros, de la STS 4549/2022, de 14 de diciembre, donde la Sala se manifiesta acerca de las consecuencias de que las notificaciones a una persona jurídica no se hagan por vía electrónica[8]. De hecho, la cuestión que generaba interés casacional en este caso era la interpretación de los artículos 14.2 y 41.1 de la LPACAP "a los efectos de determinar cuáles son las consecuencias que se derivan de una notificación efectuada a una persona jurídica en formato papel, y no a través de medios electrónicos". La sentencia desestima el recurso de casación planteado por la persona jurídica afectada, en base a la fundamentación recogida en su FJ V, donde expone:

> Ante todo, tiene razón la representación de la Junta de Galicia cuando señala que la notificación es un requisito de eficacia y no de validez del acto administrativo (artículo 39, apartados 1 y 2, de la Ley 39/2015). Por lo demás, es oportuno destacar que en el caso que examinamos la notificación de la resolución sancionadora no se tacha de defectuosa porque su contenido fuera incompleto, ni porque se omitiera en ella alguna indicación de las que la norma señala como necesarias, sino, únicamente, por haberse practicado la notificación en papel y no por medios electrónicos.
>
> En fin, es relevante señalar que en el expediente administrativo hay constancia de que en el mismo procedimiento hubo otras actuaciones administrativas anteriores que se notificaron a la recurrente en la misma vía que la resolución sancionadora a la que se refiere la controversia. En particular, la notificación de la propuesta de arbitraje que la Administración actuante dirigió a la recurrente fue entregada a la misma persona y en el mismo domicilio en el que posteriormente se practicaría la notificación de la resolución sancionadora. Y la propia entidad recurrente admite haber recibido aquella notificación de la propuesta de arbitraje, a la que formuló alegaciones, sin que la representación de Volkswagen formulase entonces objeción ni protesta alguna.

Visto estos antecedentes, la Sala entiende que la entidad jurídica recurrente había admitido, aunque fuera de forma implícita, que se le practicasen las notificaciones en papel. Dicho esto, la STS continúa en los siguientes términos:

> (…) Esta Sala no ignora los preceptos de los que resulta la procedencia de la notificación por medios electrónicos cuando se trata de personas jurídicas establecido (artículos 14.2.a) y 41.1 de la Ley 39/2015). Sin embargo, siendo así que, como ya hemos señalado, en actuaciones anteriores del mismo procedimiento administrativo la entidad Volkswagen había admitido que se practicasen las notificaciones en papel, y no habiendo duda de que la recurrente tuvo pleno conocimiento de la resolución sancionadora notificada por esa vía, no cabe tachar de inválida tal notificación por haberse practicado de ese modo. A tal efecto es obligado tener presente que, según el citado artículo 41.1 de la Ley 39/2015, "[...] Con independencia del medio utilizado, las notificaciones serán válidas siempre que permitan tener constancia de su envío o puesta a disposición, de la recepción o acceso por el interesado o su representante, de sus fechas

8. Hemos hecho especial referencia a la STS 4549/2022 pero, ciertamente, es un asunto resuelto en varias ocasiones, principalmente desde julio de 2022. Por ejemplo, en idéntico sentido, vid. SSTS 3139/2022, de 20 de julio, 4156/2022, de 18 de noviembre, 4155/2022 y 4332/2022, ambas de 21 de noviembre y 2646/2023, de 14 de junio. Esta doctrina se ha seguido por tribunales inferiores, vid. a título ilustrativo: SSAN 3675/2022, de 9 de diciembre y 1114/2023, de 8 de marzo o STSJ BAL 884/2023, de 13 de junio.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

> y horas, del contenido íntegro, y de la identidad fidedigna del remitente y destinatario de la misma. La acreditación de la notificación efectuada se incorporará al expediente."
>
> En definitiva, no cabe afirmar se haya causado indefensión a la recurrente. Por ello entendemos que el hecho de haberse llevado a cabo la notificación en papel constituye una irregularidad que carece de relevancia invalidante (artículo 48.2 de la Ley 39/2015)".

Como podemos comprobar, el Tribunal pondera la importancia en la aplicación de los artículos 14.2 y el relativo a las notificaciones, dando un valor superior a la realización efectiva de la notificación que a la aplicación *ad extra* del mencionado artículo 14.

En relación a este aspecto, hemos de citar el ATS 11631/2023, de 13 de septiembre donde la Sala de admisión ha considerado como asunto que presenta interés casacional objetivo un recurso de casación donde se enuncia, en primer lugar, la infracción del artículo 41.1 de la LPACAP, en relación con el artículo 14.2.a) y 43.3. La parte recurrente alega que no cabe admitir que el deber de resolver y notificar se entienda cumplido por un intento de notificación en papel, cuando la notificación se tenía que haber efectuado por medios electrónicos. Asimismo, justifica el interés casacional de esta cuestión invocando la presunción del artículo 88.3.a) LJCA, alegando que la jurisprudencia que aplica la Sala de instancia está prevista para una realidad jurídica distinta, pues analiza exclusivamente los efectos de los intentos de notificación, ya sea en papel o por medios electrónicos, cuando éste es el medio válido para llevar a cabo la notificación, considerando que la problemática suscitada no tiene una respuesta legal clara en la LPACAP, encontrándose ante un vacío legal de la norma. Como indica la Sala "para la sentencia recurrida, ese intento de notificación debe valorarse como intento de notificación legal a los efectos del artículo 58.4 Ley 30/1992, hoy 40.4 Ley 39/2015, mientras que para la recurrente dicho intento de notificación no puede tomarse en consideración a los citados efectos, pues no se trata de un intento de notificación efectuado en legal forma, ya que se le tenía que efectuado por medios electrónicos y, por consiguiente, la obligación de la Administración de notificar dentro del plazo máximo de duración del procedimiento se entenderá cumplida con la puesta a disposición de la notificación en la sede electrónica de la Administración u Organismo actuante o en la dirección electrónica habilitada única". Ante todo lo dicho, la Sala entiende que, aunque ya se ha pronunciado en varios supuestos relacionados con este aspecto[9], no justamente sobre lo alegado por la parte recurrente. Así, establece: (FJ II *in fine*):

9. En relación a dichos precedentes, el ATS establece en su FJ II lo siguiente: "(…) Pues bien, existen diferentes pronunciamientos de esta Sala sobre cuestiones relacionadas a la aquí planteada. Así, por ejemplo, sobre la regla contenida en los artículos 58.4 de la Ley 30/1992 y 40.4 de la Ley 39/2015 y el concreto efecto que los indicados preceptos legales atribuyen al intento de notificación debidamente acreditado (STS de 17 de noviembre de 2003 –recurso de casación en interés de ley 128/2002– y STS de 3 de diciembre de 2013 –recurso 557/2011-), sobre cuándo debe entenderse cumplida la obligación de notificar, a efectos del dies ad quem del plazo de 12 meses establecido por el artículo 42.4 de la Ley 38/2003 en las notificaciones por medios electrónicos (STS de 10 de noviembre de 2021 –RCA 4886/2020), y sobre cuáles son las consecuencias que se derivan de una notificación efectuada a una persona jurídica en formato papel, y no a través de medios electrónicos (STS de 20 de julio de 2022 –RCA 1662/2022)".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

> (…) Pero en dichos precedentes no se resolvía una cuestión idéntica a la planteada en el presente recurso, pues, y como alega la recurrente, o no trataban sobre si el medio idóneo para efectuar la notificación era en papel o por medios electrónicos, o, como ocurre en la última de las sentencias dictadas, no se trataba de valorar un "intento de notificación" a los efectos del artículo 40.4 Ley 39/2015, sino que trató de los efectos de una "notificación efectuada" a una persona jurídica en formato papel, y no a través de medios electrónicos, a efectos de la extemporaneidad de la interposición de un recurso de alzada. Y esta Sala considera que la cuestión planteada no carece manifiestamente de interés casacional, teniendo en cuenta, en relación con la presunción del artículo 88.3.a) LJCA, que hemos puntualizado que la ausencia de jurisprudencia no hace referencia a la inexistencia absoluta de pronunciamientos, pudiéndose incluir en este supuesto aquellos asuntos en los que sea necesario matizar, concretar, reforzar o, en su caso, corregir la jurisprudencia dictada en relación con nuevas realidades jurídicas. Además, la cuestión planteada trasciende del caso objeto del proceso, afectando a un gran número de situaciones, al afectar a los plazos de caducidad de los procedimientos administrativos, por lo que concurre también el supuesto del artículo 88.2.c) LJCA.

Tendremos que esperar la respuesta del TS en este asunto.

La forma y los requisitos exigidos a los sujetos recogidos en el apartado segundo del artículo 14 también han sido objeto de respuesta por parte del Tribunal Supremo. Este fue el caso de la STS 169/2022, de 26 de enero, donde se resolvió sobre si, al amparo del artículo 5. 2, 3 y 4 de la LPACAP, las personas jurídicas obligadas a relacionarse con la administración a través de medios electrónicos por imposición del artículo 14.2.a) y de cualquier otra norma sectorial (en este caso, se trataba del artículo 56 de la Ley 16/1987, de 30 de julio, de Ordenación de los Transportes Terrestres), podía acreditarse la representación de tales personas jurídicas a través de copia simple de la escritura pública de nombramiento de administrador único/consejero delegado u otro documento notarial similar que así lo acreditase y que se presentase en la sede electrónica de la administración actuante o, por el contrario, debía exigirse la presentación de específico poder notarial a fin de verificar esta representación y, además, si resultaba ineludible que el documento notarial se emitiese en soporte electrónico o que la copia de escritura aportada presencialmente fuese digitalizada. La STS se basa en una anterior (STS 3718/2021, de 28 de septiembre) para considerar, en su FJ IV, que:

> (…) El artículo 5 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en relación con el articulo 209 del Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital, debe interpretarse en el sentido de que el administrador único de una sociedad anónima ostenta la representación externa de la misma, por lo que puede actuar como representante de dicha entidad ante la Administración Pública sin necesidad de disponer de un poder específico para ello, dado que su representación la ostenta ex lege mientras esté vigente su nombramiento.

Debe mencionarse aquí que no nos encontramos solo ante las disposiciones de la LPACAP y su normativa de desarrollo, sino que estamos ante una proliferación de normas especiales que también inciden y desarrollan (a veces de forma muy compleja) esta

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

obligación de relación a través de medios electrónicos con la Administración (SANCHEZ LAMELAS 2023, 207).

2.3. Interpretación de la norma para el ámbito tributario: la STS 3295/2023, de 11 de julio

Como hemos adelantado, el último apartado del artículo 14 ha provocado no pocas reacciones. A diferencia de la realidad social en la que nos encontramos inmersos donde parece que todo ha de realizarse por medios electrónicos, si atendemos a las últimas resoluciones judiciales, se observa que los tribunales son cada vez más conscientes de que la relación por medios electrónicos con la administración es "todavía" un derecho y no, en todo caso, un deber de la ciudadanía.

Como ejemplo de lo afirmado, debemos citar que la Sala Tercera del Tribunal Supremo acaba de reconocer en su STS 3295/2023, de 11 de julio, como doctrina jurisprudencial que: "no es ajustada a Derecho la imposición a los obligados tributarios de relacionarse electrónicamente con la Administración, recogida en la Orden HAC/277/2019, de 4 de marzo, pues se establece de manera general para todos los obligados tributarios sin determinar los supuestos y condiciones que justifiquen, en atención a razones de capacidad económica, técnica, dedicación profesional u otros motivos, que se imponga tal obligación, que constituye una excepción al derecho de los ciudadanos a ejercer sus derechos y cumplir con sus obligaciones a través de técnicas y medios electrónicos, informáticos o telemáticos con las garantías y requisitos previstos en cada procedimiento, reconocido en el art. 96.2 LGT".

En relación a la interpretación del artículo 14 que realiza la Sala, es interesante el FJ VI, puesto que analiza si es de aplicación directa o no el tercer apartado, concluyendo que es una interpretación supletoria pero que no puede quedar desvirtuada por una norma de carácter inferior[10]. En términos de procedimiento administrativo común la cuestión

10. Es de gran interés el ejercicio de reflexión que realiza la Sala sobre el mandato contenido en el artículo 96.2 de la Ley 58/2003, de 17 de diciembre en aras de la coherencia del ordenamiento. Así, en su FJ VI continua: "(…) Es indudable que tanto por su posición sistemática como por su contenido, el art. 96.2 LGT expresa un auténtico principio general del ordenamiento jurídico tributario. Sistemáticamente está situado en la regulación de los principios generales de los procedimientos de aplicación de los tributos, concretamente en el Título III, y dentro de su Capítulo I, Principios Generales, en la Sección IV, que lleva por rúbrica "Tecnologías informáticas y telemáticas". Y en cuanto a su contenido, la mera lectura del art. 96.2 LGT evidencia que el legislador ha reconocido en el mismo el derecho de los ciudadanos, que no obligación, a utilizar los medios electrónicos, y el deber de la Administración de promover su utilización. En efecto, el apartado 1 del mismo art. 96 señala que la Administración tributaria "promoverá" la utilización de las técnicas y medios electrónicos, informáticos y telemáticos necesarios para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que la Constitución y las leyes establezcan. Pero el verbo "promover" significa, según el diccionario de la Real Academia de la Lengua Española, impulsar el desarrollo o la realización de algo, no a imponer el resultado. Por tanto la Administración puede realizar acciones que propicien y faciliten la consecución de determinado objetivo, en este caso la utilización de "técnicas y medios electrónicos, informáticos y medios telemáticos", pero no puede imponer su utilización obligatoria a los ciudadanos, en

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

es más compleja y se centra en determinar si la especialidad de las normas tributarias puede suponer un desplazamiento interpretativo de las normas de procedimiento administrativo común que determinar, en las personas físicas, un grado de voluntariedad

tanto que obligados tributarios, a los que, como reconoce el art. 96.2 LGT, se les reconoce el derecho a relacionarse con la Administración, y a hacerlo con las garantías necesarias a través de técnicas y medios electrónicos, informáticos o telemáticos, pero no la obligación de hacerlo, no desde luego como resultado de esta norma, cuyo significado como principio general de ordenamiento jurídico tributario resulta patente. Es en el contexto de este principio general que configura el derecho –que no el deber– de los obligados tributarios de relacionarse electrónicamente con la Administración tributaria, como ha de ser interpretado el art. 98.4 LGT, situado en el capítulo II (normas comunes sobre actuaciones y procedimientos tributarios) del mismo Título III, así como el art. 96.5 LIRPF. El art. 98.4 LGT habilita al Ministro de Hacienda, en el ámbito de las competencias del Estado, para determinar los "supuestos y condiciones", en que los obligados tributarios deberán presentar por medios telemáticos sus declaraciones, autoliquidaciones, comunicaciones, solicitudes y cualquier otro documento con trascendencia tributaria. (…) Pues bien, proclamado en el art. 96.2 LGT el derecho de los ciudadanos a relacionarse electrónicamente con la Administración, no cabe interpretar que la habilitación legal del art. 98.4 LGT, al igual que la contenida en el art. 96.5 LIRPF o en el art. 117 RGAT, permitan al Ministro de Hacienda establecer con carácter general una obligación allí donde el art. 96.2 LGT establece un derecho. Y eso es, cabalmente, lo que hace la Orden HAC/277/2019, impugnada, pues el sometimiento a la obligación de presentar telemáticamente la declaración se dirige a todo el potencial colectivo de obligados tributarios por un impuesto que, como es el caso del impuesto sobre la renta de las personas físicas, alcanza a la generalidad de las personas físicas que realicen el hecho imponible, sin distinguir ninguna condición personal que justifique que se imponga la obligación de declarar y liquidar por medios electrónicos. Por tanto, se impone una interpretación conjunta de los arts. 98.4 LGT y 96.5º LIRPF, en relación con el principio general del derecho de los obligados tributarios a relacionarse electrónica o telemáticamente con la Administración tributaria, que proclama el art. 96.2 LGT –en la misma línea del art. 14.2 LPAC–, y de esta interpretación conjunta resulta indispensable que la disposición reglamentaria recurrida hubiera establecido las características y condiciones de determinados colectivos de personas físicas que, como establece el art. 14.3 LPAC, "[...] por su capacidad económica, técnica, dedicación profesional u otros motivos [...]" deban relacionarse obligatoriamente por medios electrónicos con la Administración, delimitando así los supuestos y condiciones del alcance de esa obligación. Determinar los supuestos y condiciones no se refiere, como sostiene la Abogacía del Estado, al establecimiento de los diferentes modelos de declaración. Esa facultad la establece el art. 98.3 LGT y el art. 96.2 primer inciso de la LIRPF, pero a continuación, dentro de los diferentes modelos de declaración establecidos, o en su caso del único, la acción de determinarlos supuestos y condiciones de presentación por medios telemáticos o electrónicos de esos modelos, es algo sustancialmente diferente, que exige aislar los presupuestos bajo los que se impone la obligación de presentar electrónicamente el modelo de declaración, de aquellos en los que no es obligatoria tal forma de relación, aunque el ciudadano sigue teniendo derecho, si es posible, a hacerlo electrónicamente (art. 96.2 LGT) y la Administración debe promover las condiciones necesarias para satisfacer este derecho. En definitiva, determinar los supuestos y condiciones de presentación de las declaraciones por medios electrónicos o telemáticos no significa que la ley autorice a la norma reglamentaria a dejar sin efecto el derecho, que es lo que hace la Orden HAC/277/2019, sino que requiere identificar que características o circunstancias concurren en determinados obligados tributarios, que les diferencien del conjunto de los obligados tributarios –para los que relacionarse electrónicamente es un derecho– y que justifican la pertinencia de imponerles la obligación de relacionarse necesariamente de forma electrónica, en lugar del derecho, ejercitable o no, a hacerlo en esta forma. El art. 14.2 LPAC establece aquí una serie de criterios que, en ausencia de previsión específica de la ley tributaria, deben ser aplicados supletoriamente conforme al art. 7.2 LGT y el apartado 2 de la Disposición adicional primera de la Ley 39/2015, de 1 de octubre".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

en la relación electrónica que no debería obviarse en la normativa específica (PALOMAR OLMEDA, 2023). Así, la STS dispone que:

> "(…)Son dos las líneas discusivas que se plantean: por una parte, su aplicación supletoria en el sector tributario del ordenamiento jurídico; y, en segundo lugar, y concurrentemente con lo anterior, también se argumenta su aplicación como principio, en tanto que elemento "axial" de las relaciones Administración - ciudadano, que, en la tesis de la recurrente, debería informar la interpretación de los preceptos de la LGT que regulan la obligación de relacionarse electrónicamente con la Administración tributaria. Hemos de determinar, por tanto, si el art. 14 LPAC es de aplicación directa, o en su caso supletoria, y si concurren las circunstancias para su aplicación supletoria, además del valor que pueda tener como elemento interpretativo de las normas del ordenamiento jurídico tributario sobre la obligación de relacionarse electrónicamente con la Administración tributaria. (…) Dado que la imposición del uso obligado de los medios electrónicos se establece como excepción al reconocimiento del derecho de las personas a comunicarse con la Administración por medios electrónicos, reconocido en el propio art. 14 LPAC, es preciso satisfacer cumplidamente tanto los presupuestos que habilitan para tal imposición, como el rango necesario para la norma que imponga tal obligación".

2.4. La relación entre los artículos 14 y 68 de la LPACAP

Como hemos venido anunciando, el artículo 14.2 obliga a ciertas personas a relacionarse con las Administraciones Públicas a través de los medios electrónicos. Dentro de esta obligación, juega un papel importante el artículo 68.4, pues permite la subsanación si la solicitud realizada por dichas personas se ha realizado presencialmente. Como puede imaginarse, la interpretación de este artículo no ha sido pacífica, puesto que de su interpretación en un sentido o en otro pueden derivarse distintos efectos administrativos[11].

A nivel jurisprudencial, este fue el caso que se presentó ante la Sala Tercera y que fue resuelto por la STS 2747/2021, de 1 de julio. En esta STS, la Sala entendía que debía pronunciarse sobre el alcance aplicativo de dicho artículo 68.4, en relación con lo dispuesto en los artículo 14.2 y 112, a los efectos de dilucidar si, en los supuestos de interposición de recursos administrativos, en los casos en que el interesado proceda a subsanar el incumplimiento de dicha obligación, tras el requerimiento efectuado por la Administración, debe entenderse como fecha de presentación aquella en que se presentó el recurso personalmente ante el órgano administrativo o la fecha en que se produjo la subsanación. Como hemos mencionado, a nivel procedimental es una cuestión de suma importancia, pues permitiría, en la práctica, ampliar el plazo administrativo de interposición de un recurso. Así, se estableció como cuestión que presentaba interés casacional objetivo para la formación de jurisprudencia la aclaración de cuáles eran las consecuencias que se derivaban del requerimiento de subsanación que prevé el artículo 68.4 cuando no se había cumplido con la obligación de relación a través de medios electrónicos que

11. En relación a la dicotomía que presenta el mencionado artículo 68.4, vid, por ejemplo: RODRIGUEZ-ARANA MUÑOZ y ALVAREZ BARBEITO, 2022.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

impone el artículo 14.2 y, concretamente, si una vez subsanado el defecto y presentado el recurso por medios electrónicos, la subsanación era retroactiva o es la que fija el día en que ha de entenderse cumplimentado el trámite de que se trate. El artículo 68.4 es claro y así lo argumenta la Sala tercera en defensa de la coherencia de la LPACAP en su totalidad. Para resolver esta compleja cuestión (a nuestro juicio de forma correcta), la Sala considera que no puede realizarse una interpretación exorbitante del artículo 68.4 que de lugar a indefensión. En su FJ III dispone:

> "(…) esta Sala considera que, tal como argumentó el Tribunal de instancia, la decisión de la Consejera de Economía y Hacienda de la Junta de Castilla y León de inadmitir el recurso de alzada interpuesto por la Confederación de Organizaciones Empresariales de Castilla y León infringe el principio antiformalista y los principios de buena fe y confianza legítima que rigen en la tramitación de los procedimientos administrativos, en la medida que se sustenta en una aplicación exorbitante del artículo 68.4 de la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas que cause indefensión. En efecto, cabe partir como premisa para abordar esta cuestión del presupuesto de que el artículo 68.4 de la Ley 39/2015 regula un trámite procedimental de subsanación especifico respecto de las solicitudes que se hubieren presentado ante la Administración de forma presencial, que resulta estrictamente aplicable a los procedimientos iniciados a solicitud del interesado y no a los procedimientos iniciados de oficio por la Administración, ni a los procedimientos de revisión de los actos administrativos. Por ello, sostenemos que no resulta convincente la tesis argumental que desarrolla el Letrado de la Comunidad Autónoma de Castilla y León, que postula la aplicación generalizada de la previsión contenida en el artículo 68.4 de la Ley 39/2015, en aras de incentivar el cumplimiento de la obligación de relacionarse con la Administración por medios electrónicos contemplada en el articulo 14.2 del citado texto legal, por cuanto no hay –según se aduce–- diferenciación de objetos entre el procedimiento administrativo común y los procedimientos revisorios, pues no tiene en cuenta que el instituto procedimental de la subsanación no puede comportar para el interesado que cumple en tiempo y forma el requerimiento efectuado por la Administración unas consecuencias jurídicas lesivas del derecho a la protección jurídica, que constituye uno de los postulados nucleares de la configuración del Estado social y democrático de Derecho, en contravención del deber de buena administración".

En lo referente al juego entre los artículos 14 y 68 LPACAP es de gran relevancia, también, la STS 167/2022, de 27 de enero, donde se establecía como cuestión que presentaba interés casacional objetivo para la formación de jurisprudencia el siguiente asunto (FJ II):

> "(…) La Sección de Admisión entiende que tiene interés casacional objetivo para la formación de jurisprudencia la cuestión suscitada en la instancia, circunscrita a si, al amparo del artículo 5 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, resulta conforme al principio pro actione exigir a las personas jurídicas la presentación por medios electrónicos de poder notarial a fin de acreditar su representación. En detalle, si al amparo del artículo 5, apartados 2, 3 y 4, de la referida Ley 39/2015, de 1 de octubre, las personas jurídicas obligadas a relacionarse con la Administración a través de medios electrónicos por imposición del artículo 14.2.a) de la citada Ley y de cualquier otra norma sectorial (en este caso, artí-

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

culo 56 de la Ley 16/1987, de 30 de julio, de Ordenación de los Transportes Terrestres), puede acreditarse la representación de tales personas jurídicas a través de copia simple de la escritura pública de nombramiento de administrador único/consejero delegado u otro documento notarial similar que así la acredite y que se presente en la sede electrónica de la Administración actuante o, por el contrario, debe exigirse la presentación de específico poder notarial a fin de verificar esta representación y si resulta ineludible que el documento notarial se emita en soporte electrónico o que la copia de escritura aportada presencialmente sea digitalizada".

Para dar respuesta a esta cuestión y estimar el recurso de casación planteado, la Sala Tercera alude a varias sentencias anteriores y, en su FJ IV, expone:

> Así, con reiteración de la doctrina establecida en las SSTS de 28 de septiembre y 25 de octubre de 2021 dictadas en los RRCA 1379/2020 y 706/2020, el administrador único ostenta la representación externa de la sociedad, por lo que puede actuar como representante de dicha entidad ante la Administración Pública sin necesidad de disponer de un poder específico para ello, dado que su representación la ostenta ex lege mientras esté vigente su nombramiento. El administrador único que ha obtenido del organismo certificador competente un certificado de firma electrónica que le habilita para actuar telemáticamente en representación de una persona jurídica no necesita aportar, mientras esté vigente dicho certificado, un poder de representación de la sociedad con motivo de cada actuación concreta ante la Administración. Pues bien, a la vista de todo lo anterior, estimamos que la condición de D. Juan Carlos como representante de la sociedad recurrente estaba suficientemente acreditada, por lo que procede estimar el recurso de casación, anular la sentencia impugnada y, resolviendo la concreta controversia jurídica planteada en la instancia conforme a los anteriores razonamientos, debemos estimar el recurso contencioso administrativo y anular la resolución administrativa que tuvo a la parte recurrente por desistida del recurso de reposición por no acreditar la representación de la sociedad, ordenando la retroacción de las actuaciones para que la Administración resuelva el recurso de reposición presentado.

Con el análisis de estas resoluciones podemos observar como la Sala, a diferencia del resto de estratos sociales y basándose en el principio *pro actione,* en este punto aboga por simplificar los trámites en lo que a la Administración electrónica se refiere, facilitando, en la medida de lo posible, los trámites electrónicos tanto a las personas físicas como a las personas jurídicas. El actual marco jurídico ha de quedar bajo la buena Administración electrónica y bajo la imposición de un criterio de interpretación favorable para el administrado electrónicamente (COTINO HUESO, 2021,4).

III. Tratamiento de las disposiciones del Real Decreto 203/2021, de 30 de marzo, por los tribunales contencioso-administrativos

Por su poco tiempo de vigencia en nuestro ordenamiento, escasas son aun las resoluciones del Tribunal Supremo interpretativas de las disposiciones contenidas en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el reglamento de actuación

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

y funcionamiento del sector público por medios electrónicos. No obstante, llama la atención la STS 2286/2022, de 25 de mayo, puesto que resuelve la impugnación de los artículos 3 y 40 a 45[12] de dicho decreto, siguiendo los trámites del procedimiento ordinario[13]. Estamos de acuerdo con MARTINEZ GUTIERREZ (2021) cuando expresa que, en cuanto a la obligación y los sujetos que necesariamente deben actuar y tramitar electrónicamente con las Administraciones, el mencionado artículo tercero del Real Decreto no aporta grandes novedades, más allá de clarificar la necesidad de aprobación de norma reglamentaria para obligar a colectivos de personas físicas a la utilización de medios electrónicos. Es justo sobre este aspecto sobre el que se pronuncia la mencionada STS a la que aludiremos a continuación[14].

En relación al artículo 3[15], el objetivo era que se declarase la nulidad en lo referente a la frase contenida en el apartado 1 "para la realización de cualquier trámite de un proce-

12. No hacemos referencia en este trabajo a la argumentación y las consideraciones relativas a estos artículos por no estar relacionados de forma directa con el objeto de este análisis.

13. No debe olvidarse que, en virtud de lo dispuesto en el artículo 12 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Sala del Tribunal Supremo es la competente para conocer en primera instancia de la impugnación de este tipo de instrumentos jurídicos.

14. De hecho, este autor ya recogía que hubiera sido necesario que se desarrollara el alcance concreto de la obligación "perfilando la necesidad de que la norma reglamentaria que obligue determine con claridad en su memoria y en definitiva justifique las razones que aconsejan la obligación, ya que el artículo 14.3 de la Ley viene a emplear expresiones que son claramente conceptos jurídicos indeterminados. La adecuada motivación de la imposición de la obligación a los colectivos de personas físicas que vayan a ser obligados por norma reglamentaria debe ser objeto de motivación y justificación, ya que si no fuera así podría incurrirse en un supuesto de nulidad de la norma reglamentaria".

15. Dicho artículo tercero bajo el título "Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas" establece: "1. Estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los sujetos a los que se refiere el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

2. Las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas podrán ejercitar su derecho a relacionarse electrónicamente con la Administración Pública de que se trate al inicio del procedimiento y, a tal efecto, lo comunicarán al órgano competente para la tramitación del mismo de forma que este pueda tener constancia de dicha decisión. La voluntad de relacionarse electrónicamente o, en su caso, de dejar de hacerlo cuando ya se había optado anteriormente por ello, podrá realizarse en una fase posterior del procedimiento, si bien deberá comunicarse a dicho órgano de forma que quede constancia de la misma. En ambos casos, los efectos de la comunicación se producirán a partir del quinto día hábil siguiente a aquel en que el órgano competente para tramitar el procedimiento haya tenido constancia de la misma. 3. De acuerdo con lo previsto en el apartado 3 del artículo 14 de la Ley 39/2015, de 1 de octubre, la obligatoriedad de relacionarse electrónicamente podrá establecerse reglamentariamente por las Administraciones Públicas para determinados procedimientos y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios. A tal efecto, en el ámbito estatal la mencionada obligatoriedad de relacionarse por medios electrónicos con sus órganos, organismos y entidades de derecho público podrá ser establecida por real decreto acordado en Consejo de Ministros o por orden de la persona titular del Departamento competente respecto de los procedimientos de que se trate que afecten al ámbito competencial de uno o varios Ministerios cuya regulación no requiera de norma con rango de real decreto. Asimismo, se publicará en el Punto de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

dimiento administrativo", así como del apartado 2 de dicho precepto, en su totalidad, y del apartado 3, respecto de la frase "o por orden de la persona titular del Departamento competente respecto de los procedimientos de que se trate que afecten al ámbito competencial de uno o varios Ministerios cuya regulación no requiera de norma con rango de Real Decreto". Vayamos por partes.

En lo relativo al artículo 3.1 del Real Decreto, la parte actora consideraba que la alusión "para la realización de cualquier trámite de un procedimiento administrativo", no era conforme a la Constitución española, en cuanto conllevaba la exclusión formal y radical de otras posibilidades de comunicación con la Administración para determinados sujetos, profesionales y personas jurídicas, cualquiera que fuese la naturaleza material o jurídica del trámite implicado. Como indica la STS: "A su juicio, la solución normativa adoptada coloca al ciudadano que decide relacionarse con la Administración asistido de profesional en desigualdad de condiciones, negativa e injustificada, respecto al que actúa sin ese asesoramiento o asistencia, y, por ello, conculca el artículo 9.3 de la Constitución (interdicción de la arbitrariedad de los poderes públicos), el artículo 103.1 de la CE (principio de eficacia administrativa), en relación con el artículo 14 y el artículo 24 del texto constitucional". Si bien es cierto que determinar la obligatoriedad en la relación con la Administración de forma electrónica a unos sujetos sí y a otros no puede conculcar el principio de igualdad, la Sala razonadamente lo niega en base a los siguientes argumentos (FJ III):

> (…) Esta Sala sostiene que la pretensión anulatoria del citado inciso del artículo 3.1 del Reglamento carece de fundamento, porque, partiendo del hecho de que dicha disposición reglamentaria reproduce literalmente la regulación establecida en el artículo 14.2 de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que impone a determinados sujetos la obligación de relacionarse con la Administración por medios electrónicos, no estimamos que se produzca una desigualdad de trato, que resulte lesiva del principio de igualdad o del derecho de protección jurídica, y por ende del derecho de defensa, o que por falta de justificación racional sea arbitraria, en los términos que se propugna respecto de las personas físicas que comparecen por si mismas ante la Administración –que tienen reconocido el derecho a comunicarse con las administraciones públicas por medios telemáticos o no para el ejercicio de sus derechos y obligaciones, salvo que reglamentariamente, y en razón de determinadas circunstancias, se excluya la facultad de elección–, de aquellos que comparecen asistidos de un profesional, que, aunque asuma la representación, no le priva al interesado de la facultad de optar, según los términos del artículo 14.2 d) de la citada Ley procedimental.

De igual forma, continua considerando que no aprecia término de comparación válido que permita evidenciar que el titular de la potestad reglamentaria haya quebrantado el principio de igualdad, porque "si el interesado es asistido por letrado, sigue siendo el propio interesado el que tiene el derecho –si se trata de la persona física– de

Acceso General electrónico (PAGe) de la Administración General del Estado y en la sede electrónica o sede asociada que corresponda".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

optar por la forma en que desea relacionarse con la Administración, ya que solo, en el supuesto de que el profesional actúe como representante de un sujeto obligado se le considera obligado a relacionarse con la Administración Pública por medios electrónicos". Igualmente, la Sala señala que la frase impugnada tiene un ámbito de aplicación limitado, en cuanto se circunscribe a los sujetos del 14.2 LPACAP por lo que no afecta, en principio, con carácter prescriptivo, a las personas físicas. Avanzado en la argumentación continúa:

> (…) La interpretación de dicha disposición reglamentaria, que delimita, con carácter general, la extensión de la obligación de relacionarse con la Administración por medios electrónicos de los sujetos obligados respecto de la realización de «cualquier trámite», debe efectuarse en el marco de los principios y garantías procedimentales enunciados en el artículo 2 del referido reglamento, atendiendo a la naturaleza y circunstancias de cada procedimiento administrativo, a la luz del derecho al procedimiento debido y al deber de buena administración, con la finalidad de impedir que se cause indefensión al interesado. Por ello, cabe poner de relieve que la previsión legal del artículo 14.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, no veda que determinados actos procedimentales se sigan realizando de forma presencial tal como lo requiera la normativa específica reguladora del procedimiento, ni que para tales actos pueda ser asistido por Abogado u otro profesional, ya que no cabe eludir que dicho precepto se refiere a los actos de comunicación, cuya práctica no puede suponer una merma de los derechos que configuran el estatuto del interesado en el procedimiento administrativo en los términos del artículo 53 del citado texto legal[16].

Atendiendo al apartado segundo de dicho artículo tercero, la parte actora consideraba que ya que todas las personas físicas tenían reconocido el derecho a no tener que relacionarse electrónicamente con la Administración, no debían establecerse límites al ejercicio de un derecho imponiendo un anuncio previo al inicio del procedimiento ni a uno posterior para poder cambiar del medio elegido. De la misma manera, se cuestionaba la previsión de que los efectos del cambio de forma de comunicación se produjeran a partir del quinto día hábil en que la Administración tuviese constancia de la comunicación de la opción, por cuanto resultaba incompatible con las normas reguladoras establecidas en los artículos 14.1 y 31.2 LPACAP. En lo referente a este apartado, la Sala también entiende que es un motivo que ha de ser desestimado al no compartir la tesis de que se limita el ejercicio del derecho al imponer al interesado el deber jurídico

16. Además, la mencionada STS expone: "Cabe precisar al respecto que no entendemos que exista conexión, desde la perspectiva de aplicación de los derechos y principios constitucionales, entre el contenido de dicha previsión legal y los preceptos constitucionales invocados, que permita dudar de la validez constitucional de la de dicho precepto, pues no cabe inferir que de la concreta imposición a los sujetos obligados de relacionarse electrónicamente con la Administración Pública "para la realización de cualquier trámite" se derive la diferencia de trato por razón del sujeto entre personas físicas y personas jurídicas y profesionales, de carácter discriminatorio, sin perjuicio de que dicha previsión deba aplicarse, en todo caso, de conformidad con los principios constitucionales que rigen la Administración pública, entre los que cabe considerar los principios de objetividad, racionalidad y proporcionalidad".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

de realizar un anuncio previo ni de que deba necesariamente efectuarse al órgano competente para la tramitación del mismo, en la medida que considera que no se aducen argumentos sólidos, en términos de estricta legalidad, referidos a la vulneración de los artículos 14, 31.2 c) o 41 LPACAP. Con la previsión del artículo 3.2 se vuelve a recuperar el derecho a la intermodalidad tradicional/electrónica en la tramitación del procedimiento en la normativa (MARTÍNEZ GUTIERREZ, 2021).La Sala se fundamenta, a nuestro juicio de forma razonada, en los siguientes términos:

> (…) No obstante, cabe señalar que no apreciamos que dicha previsión reglamentaria contravenga el artículo 14 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que establece, en sede de la regulación del derecho de relacionarse electrónicamente con las Administraciones Públicas, que «el medio elegido por la persona para comunicarse con la Administración Pública podrá ser modificado por aquella en cualquier momento», puesto que la concreción del órgano administrativo al que debe efectuarse la comunicación no se revela contraria a dicha disposición legal, al derivarse de la interpretación sistemática de la propia ley efectuada conforme al principio de seguridad jurídica, ya que se vincula a comunicar la decisión al órgano competente para la tramitación del procedimiento. Tampoco consideramos que proceda declarar la nulidad del inciso de esta disposición reglamentaria, referida a que los efectos de la comunicación se producirán a partir del quinto día hábil siguiente a aquel en que el órgano competente para la tramitación del procedimiento haya tenido constancia de la misma», pues no entendemos que resulte incompatible con la regulación contenida en el artículo 14.1 de la Ley 39/2015, de 1 de octubre, del ya que, como aduce el Abogado del Estado en sus escritos de contestación a la demanda, se trata de supuestos de colaboración reglamentaria que tiene la finalidad de permitir incorporar los medios electrónicos a la actividad de la Administración de forma racional, fijando las reglas mínimas para garantizar la actuación eficaz de la Administración, debiendo tener en cuenta que la incorporación al sistema electrónico, o su abandono, requiere unas comprobaciones previas (firma electrónica, revisión de las notificaciones personales), que debe efectuar los funcionarios públicos encargados de la tramitación del procedimiento administrativo de forma ágil pero también segura.

Al aludir a la impugnación del apartado tercero del mencionado artículo 3 basada en que la Orden Ministerial para imponer la obligatoriedad de relacionarse con la Administración por medios electrónicos suponía una banalización de la habilitación reglamentaria que se mostraba contraria al artículo 128 (donde se exige la expresa y específica habilitación por la Ley formal para hacer posible la Orden Ministerial), la Sala también establece su desestimación. En este caso considera que la previsión reglamentaria está amparada en el artículo 14.3 al disponer éste que: "reglamentariamente, las Administraciones Públicas podrán establecer la obligación de relacionarse con ellos a través de medios electrónicos para determinados procedimientos y para cuestiones colectivas de personas física" y, teniendo en cuenta también que, conforme a lo establecido en el artículo 4.b) de la Ley 50/1997, de 27 de noviembre, del Gobierno está atribuido a los titulares de los Departamentos ministeriales ejercer la potestad reglamentaria en materias propias del Departamento. Además, realiza la siguiente observación:

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

> (…) Cabe, asimismo, señalar que no compartimos la tesis argumental que desarrolla la defensa letrada de la parte demandante, que mantiene que dicha disposición contradice abiertamente lo dispuesto en el artículo 128.4, penúltimo párrafo, de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que reserva al Gobierno el ejercicio de la potestad reglamentaria, en consonancia con el artículo 97 de la Constitución, puesto que no cabe eludir que dicha disposición reglamentaria se ajusta a los términos del artículo 14.3 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que contiene una habilitación especifica al Ministro –en los supuestos que no sea exigible la aprobación de un Real Decreto por el Gobierno– para establecer, respecto de determinados procedimientos y ciertos colectivos de personas físicas, la obligación de relacionarse con la Administración por medios electrónicos.

La aplicación de este Real Decreto no está siendo pacífica[17], sobre todo, en lo relativo a ese artículo tercero. Veamos otro ejemplo. En la STSJ de Galicia 5914/2023, de 14 de septiembre, se resuelve sobre el caso de la regularidad de los intentos de notificación efectuadas por correo y no a través de medios electrónicos. La parte actora planteaba en su demanda que los intentos de notificación del acuerdo de incoación cursados por correo no habían de entenderse como válidos porque había optado por la notificación electrónica, teniendo en cuenta que sí se había utilizado el medio electrónico para hacerle llegar la sanción, por lo que recurre aduciendo que se le había ocasionado efectiva indefensión durante la tramitación del expediente. El TSJ gallego desestima el recurso interpuesto y en relación a este aspecto concreto establece, en su FJ V, lo siguiente:

> (…) Con arreglo al Art. 14 de la Ley 39/2015 las personas físicas pueden optar por recibir electrónicamente las comunicaciones de la administración, pero con arreglo a dicho precepto la elección ha de surtir efectos a partir de su realización sin que puedan invalidar de los intentos de notificación cursados con anterioridad, pudiendo modificarse por los interesados en cualquier momento. Es más, el Art. 3 del Real Decreto 203/2001 de 30 de marzo, por el que se aprobó el Reglamento del Funcionamiento Electrónico de la Administración retarda los efectos de la opción hasta el quinto día hábil siguiente a la comunicación efectuada a la administración que sigue el expediente, al disponer: Artículo 3. Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas. 2. Las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas podrán ejercitar su derecho a relacionarse electrónicamente con la Administración Pública de que se trate al inicio del procedimiento y, a tal efecto, lo comunicarán al órgano competente para la tramitación del mismo de forma que este pueda tener constancia de dicha decisión. La voluntad de relacionarse electrónicamente o, en su caso, de dejar de hacerlo cuando ya se había optado anteriormente por ello, podrá realizarse en una fase posterior del procedimiento, si bien deberá comunicarse a dicho órgano de forma que quede constancia de la misma. En ambos casos, los efectos de la comunicación se producirán a partir del quinto día hábil siguiente a aquel en que el órgano competente para tramitar

17. Vid. STS 2187/2022, de 30 de mayo, donde la Sala estima parcialmente el recurso contencioso-administrativo interpuesto por la Generalitat de Cataluña contra el Real Decreto 203/2021, de 30 de marzo, y declara nula su disposición transitoria primera, con desestimación de las demás pretensiones.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

> el procedimiento haya tenido constancia de la misma. Por lo que este motivo del recurso ha de ser desestimado ya que la opción por la notificación electrónica se produjo con posterioridad al dictado de la resolución sancionadora y de forma simultánea a la interposición del recurso potestativo de reposición.

Como puede comprobarse, más que una aplicación exacerbada por la Administración de estas disposiciones relativas a la comunicación electrónica, a veces son los administrados los que esperan encontrar algunos resquicios legales para su beneficio a la hora de aplicar el juego de lo contenido en los artículos 14 LPACAP y 3 del Real Decreto 203/2021.

Siguiendo esta línea, por último, creemos interesante mencionar también la STSJ M 8618/2023, de 11 de julio, donde se declara la nulidad de algunas disposiciones de la Ordenanza 6/2022, de 26 de abril, de Licencias y Declaraciones Responsables Urbanísticas del Ayuntamiento de Madrid publicada en el boletín oficial de la Comunidad Autónoma de Madrid de 17 de mayo de 2022. Los recurrentes entendían que el Acuerdo recurrido era nulo al considerar que infringía los principios de seguridad jurídica, jerarquía normativa y los artículos 14 y 16 de la LPACAP. Estimaban que no se podía imponer "manu militari" la obligación de relacionarse con las Administraciones Públicas por medios electrónicos para todas las personas físicas, afirmando que no todas las personas físicas poseen capacidad y medios para relacionarse con la Administración de forma telemática: "No se pueden limitar las formas de relacionarse del administrado. No se le puede negar ni tan siquiera la presentación presencial. Hay una norma con rango de ley que lo permite y establece". La argumentación de la Administración pública afectada (que en este caso era el Ayuntamiento de Madrid) para negar la nulidad se basaba en entender que la previsión contenida en el mencionado artículo 14 no limita que dicho desarrollo deba ser efectuado por reglamento estatal a nivel nacional, según pretendía la demanda, ya que la referencia se hace a las Administraciones Públicas, dentro de las cuales se incluyen los Ayuntamientos en cuanto Entidades Locales. De igual forma, afirma que el artículo 3.3 del Real Decreto 203/2021, de 30 de marzo, también dispone, con una redacción similar al 14 que: "De acuerdo con lo previsto en el apartado 3 del artículo 14 de la Ley 39/2015, de 1 de octubre, la obligatoriedad de relacionarse electrónicamente podrá establecerse reglamentariamente por las Administraciones Públicas para determinados procedimientos y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios". Como vemos, la cuestión litigiosa se centraba en la consideración de forma más o menos amplia del concepto de Administración Pública en relación a la normativa de aplicación. En este punto, la parte demandada recalcaba lo siguiente (FJ IV):

> (…) es relevante indicar, en contra de lo que indica la parte recurrente, que el desarrollo por ordenanza local responde a la exigencia legal de desarrollo reglamentario en la medida en que resulta criterio jurisprudencial absolutamente consolidado que las ordenanzas locales son expresión del poder normativo local (ex artículo 4 Ley 7/1985 de 5 de abril, reguladora de las Bases de Régimen Local) y participan de la naturaleza jurídica de disposición administrativa de carácter general a todos los efectos.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

A juicio de la Sala los preceptos impugnados no imponían de forma directa obligación alguna a las personas físicas de relacionarse con la administración única y exclusivamente por medios electrónicos, sino estableciendo una obligación de presentar las solicitudes y demás documentos a través del Registro Electrónico General del Ayuntamiento de Madrid, de forma exclusiva y excluyente. Obviamente, tal disposición es contraria no a los preceptos señalados por la actora sino a lo establecido en el artículo 16 LPACAP, por el que se establece que cada Administración dispondrá de un Registro Electrónico General, en el que se hará el correspondiente asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, Organismo público o Entidad vinculado o dependiente a éstos. Asimismo, dicho artículo indica que también se podrán anotar en el mismo, la salida de los documentos oficiales dirigidos a otros órganos o particulares. Sin embargo, el mencionado apartado sólo establece la obligación de la administración de disponer de un registro general electrónico pero no impone a los interesados la obligación de presentar las solicitudes y demás documentos en dicho Registro. Así, como afirma la Sala, está claro que los artículos discutidos eliminan el derecho de presentar escritos y documentos en las oficinas de Correos, en la forma que reglamentariamente se establezca y en las representaciones diplomáticas u oficinas consulares de España en el extranjero. En el FJ VI *in fine* de la STSJ se recogen los motivos que sustentan la nulidad:

> (…)En consecuencia, la citada ley básica contempla la posibilidad de que el ciudadano comparezca de forma presencial ante la administración pública para presentar documentos circunstancia esta que elimina sin justificación alguna la Ordenanza 6/2022, de 26 de abril, de Licencias y Declaraciones Responsables Urbanísticas del Ayuntamiento de Madrid, y como quiera que la citada Ley de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas no prevé que puedan eliminarse la posibilidad representar los documentos escritos a través del correo administrativo es decir en las oficinas de correos y en las oficinas consulares y diplomáticas la previsión que contiene la citada ordenanza es nula de pleno derecho por ser contraria al principio de jerarquía normativa tal y como establece el artículo 47 apartado 2º de la de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas que indica que también serán nulas de pleno derecho las disposiciones administrativas que vulneren la Constitución, las leyes u otras disposiciones administrativas de rango superior.

IV. A modo de conclusión

Sin duda, el paso de la Administración Pública tradicional a la e-Administración ha sido el gran desafío del sector público en los últimos años. Las llamadas leyes siamesas (LPACAP y LRJSP) configuraron desde su aprobación un nuevo horizonte en el que la tramitación electrónica debía constituirse como la actuación habitual de las Administraciones Públicas en sus vertientes de gestión interna, de relación con los ciudadanos y entre sí (DEL POZO MARMOL y RODRIGUEZ CAMPOS, 2022, 154). En este aspecto, la labor de los tribunales contencioso-administrativos está consistiendo, en gran medida, en

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

adecuar las antiguas pautas procedimentales administrativas a una efectiva administración electrónica que responda a los estándares mínimos de eficacia, eficiencia y buen gobierno que la sociedad espera en pleno siglo XXI. Un ejemplo muy reciente de esta labor lo constituye la STS 4309/2023, de 26 de octubre que, en relación al expediente administrativo electrónico (base de la actuación de este orden jurisdiccional) ha recordado que "una transformación de documentos en formato papel a un formato digital no es simplemente proporcionar una imagen escaneada, sino que la imagen ha de poder identificarse para su eficaz y rápida consulta mediante el correspondiente índice conforme a las exigencias legales" exigiendo, por tanto, que los expedientes administrativos cumplan los parámetros necesarios para una consulta ordenada, rápida y eficiente[18].

Como hemos podido observar a lo largo de este trabajo, dicha labor jurisdiccional está siendo especialmente intensa a la hora de interpretar la relación diaria del ciudadano con sus Administraciones públicas de referencia a través de los medios electrónicos, afanándose por dejar claros algunos aspectos en los que el legislador ha optado por guardar silencio. Además, no deben olvidarse los problemas prácticos que este esfuerzo conlleva. Así, nos mostramos en total acuerdo con la afirmación de que la verdadera limitación o restricción de derechos que conlleva la obligatoriedad de la relación electrónica se manifiesta, en la práctica, en las dificultades reales que conlleva en no pocas ocasiones la cumplimentación de los formularios diseñados por las Administraciones o en los no menos infrecuentes problemas de interoperabilidad (SANZHEZ LAMELAS, 2023, 207).

La cuestión es, incluso, de relevancia constitucional. Lo que se recoge para los sujetos particulares en el artículo 14.1 es un derecho que se convierte en una obligación para los sujetos del apartado 14.2. Debido a ello, nos ha llamado mucho la atención la reciente STC 147/2022, de 29 de noviembre, donde el Tribunal Constitucional otorga el amparo a una persona jurídica que, teniendo la obligación de relacionarse electrónicamente con la Agencia Tributaria, no accedió a su buzón electrónico en plazo, teniéndose por efectuada la notificación de un requerimiento del que no tuvo conocimiento, considerando que ante "lo infructuoso de las comunicaciones practicadas por vía electrónica, la administración debería haber desplegado una conducta tendente a

18. Esta idea ya la encontramos también en otras SSTS. Como indica el FJ III de la mencionada STS 4309/2023 denominado "Una consideración previa sobre el expediente administrativo. Reiteración de lo dicho en las recientes SSTS de 3 de julio de 2023, recurso ordinario 419/2022 y de 2 de octubre de 2023 recurso ordinario 109/2022": "Este Tribunal en fecha reciente, SSTS de 3 de julio 2023 y 2 de octubre 2023, enjuiciando actos del Consejo General del Poder Judicial, recordó que se había pronunciado en varias ocasiones, unas referidas a la Administración Local y otras a la Administración General del Estado, sobre el expediente administrativo y el deficiente modo de presentación mediante el amontonamiento de hojas que se produce cuando se escanean documentos (entre otras SSTS 15 de marzo de 2021, 24 de junio de 2021, recurso casación 1559/2020, 14 de diciembre de 2021, recurso ordinario 112/2020, 6 de julio de 2022, recurso casación 6577/2020) aunque la Administración remitente lo denomine "expediente digital" o como, en el caso de autos, lo remita en un moderno "pen drive" con logotipo del suprimido Ministerio de Administraciones Públicas si bien el órgano remisor es el Ministerio de Política Territorial…".

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

lograr que las mismas llegaran al efectivo conocimiento de la interesada". Como vemos, levanta ese mandato del 14.2 LPACAP y lo hace en los siguientes términos (FJ V):

> (…) Debemos insistir, a riesgo de ser reiterativos, en el hecho de que la Agencia Tributaria supo que la interesada no tuvo conocimiento del requerimiento del que fue objeto por vía electrónica; y sin embargo, no empleó formas alternativas de comunicación, a fin de advertirla del procedimiento de comprobación limitada que había iniciado y de la documentación contable que recababa, de suerte que la liquidación provisional finalmente practicada no tuvo en cuenta la eventual incidencia de los datos que los libros y las facturas solicitados pudieran contener. Y al desconocer el objeto de las notificaciones que se remitieron a su dirección electrónica habilitada, aquella tampoco pudo impugnar temporáneamente, incluso en sede judicial, la liquidación provisional finalmente practicada, lo que redundó en detrimento de su derecho a la tutela judicial efectiva reconocido en el art. 24.1 CE, aun cuando el procedimiento seguido por la administración tributaria no tuviera carácter sancionador.

A pesar de todo lo dicho consideramos, aludiendo al título de este análisis, que aún es un derecho de la ciudadanía la relación por medios electrónicos con las Administraciones Públicas pero que no puede negarse que se encuentre en vías de extinción.

Bibliografía

COTINO HUESO, L., (2021), "La preocupante falta de garantías constitucionales y administrativas en las notificaciones electrónicas», *Revista General de Derecho Administrativo*, núm. 57, Mayo.

DE ALBA BASTARRECHEA, E., (2017), "El uso de medios electrónicos en el procedimiento administrativo", *Asamblea: revista parlamentaria de la Asamblea de Madrid*, núm. 37.

DEL POZO MARMOL, J.M., y RODRIGUEZ CAMPOS, I., (2022), "La actuación administrativa automatizada y la actuación del control en los entornos de gestión", Auditoría pública: revista de los Órganos Autónomos de Control Externo, núm.80.

EXPOSITO GAZQUEZ, A., (2022), "El principio de interoperabilidad como base para las actuaciones y los servicios administrativos personalizados, proactivos y automatizados", *Revista Vasca de Administración Pública,* núm. 122, enero-abril.

GARCÍA LOPEZ, J.C., (2022), "¿Es el órgano judicial un sujeto obligado a relacionarse electrónicamente con la Administración Pública?", *Diario La Ley*, núm. 10097, Sección Tribuna, 24 de Junio de 2022

LOZANO CUTANDA, B., (2021), "El nuevo Reglamento de actuación y funcionamiento del sector público por medios electrónicos: la acreditación y el registro electrónicos de la representación", *Diario La Ley,* núm. 9833, Sección Tribuna, 20 de Abril de 2021.

MARTIN DELGADO, I., (2018), "Algunos aspectos problemáticos de la nueva regulación del uso de los medios electrónicos por las Administraciones Públicas", *Revista jurídica de la Comunidad de Madrid.*

MARTINEZ GUTIERREZ, R., (2021), "La plena eficacia de la e-Administración. Comentario y notas fundamentales del Real Decreto 203/2021, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos", *Derecho Digital e Innovación*, núm. 8, Sección Doctrina, Primer trimestre de 2021

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

PALOMAR OLMEDA, A., (2023), "La relación electrónica y las limitaciones a sus excepciones. La STS de 11 de julio de 2023", *Diario La Ley,* núm. 10341, Sección Doctrina, 5 de Septiembre de 2023.

PAREJO ALFONSO, L., (2016), "A las puertas de su entrada en vigor: algunas cuestiones que suscitan las Leyes 39 y 40 de 2015, examinadas a la luz, en particular, de la autonomía local", *Asamblea: revista parlamentaria de la Asamblea de Madrid*, núm. 34.

RODRIGUEZ-ARANA MUÑOZ, J., y ALVAREZ BARBEITO, J., (2022), "El régimen de subsanación en la Ley 39/2015 y el Real Decreto 203/2021: luces y sombras", *Actualidad Administrativa*, núm. 3, Sección Actualidad, Marzo 2022.

SANCHEZ LAMELAS, A., (2023), "La reciente jurisprudencia sobre la obligación de utilizar medios electrónicos en las relaciones administrativas", *Revista de administración pública*, núm. 220.

ZAFRA ROMERO, L., (2020), "Obligación de presentar recursos administrativos y relacionarse con Administraciones Públicas por medios electrónicos", *Actualidad Jurídica Aranzadi*, núm. 259.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 93-116
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.05

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales. ¿Nuevas perspectivas?*

THE EUROPEAN DIRECTIVE AND THE PRODUCTION AND PRESERVATION ORDERS OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS. NEW INSIGHTS?

Carmen Cuadrado Salinas
Profesora Contratada Doctora (Profesora Titular Acreditada) de Derecho Procesal.
Universidad de Alicante
carmen.cuadrado@ua.es 0000-0001-7824-4791

Recibido: 01 de noviembre de 2023 | Aceptado: 06 de diciembre de 2023

RESUMEN

Las medidas procesales para obtener y conservar pruebas electrónicas son cada vez más importantes a los efectos de las investigaciones y procesos penales a lo largo de la Unión Europea. Si tenemos en cuenta que los datos electrónicos se almacenan a menudo fuera del Estado investigador, o por un prestador de servicios establecido fuera de dicho Estado, es fácil comprender los enormes problemas que puede generar su obtención. El presente estudio analiza los recientemente aprobados instrumentos legales europeos, diseñados para resolver estos problemas: la Directiva y el Reglamento que contiene las Órdenes europeas de Producción y Conservación de pruebas electrónicas.

PALABRAS CLAVE

Obtención de pruebas tecnológicas
Proveedores de servicios
Directiva
Orden Europea de Obtención de Pruebas Electrónicas
Orden Europea de Conservación de Pruebas Electrónicas

ABSTRACT

Procedural measures to obtain and preserve electronic evidence are increasingly important for the purposes of criminal investigation and prosecution across the European Union. If we tale into account that electronic data is often stored outside the investigating State, it is easy to understand the huge problem that gathering of these data, as evidence can generate. This study analyzes the recently approved legal instruments, designed to solve these problems: the Directive and the Regulation on European Production Orders and European Preservation Orders.

KEYWORDS

Gathering of electronic evidence
Service providers
Directive
European Production Orders for Electronic Evidence
European Preservation Orders for Electronic Evidence

* Trabajo realizado en el marco de los Proyectos de Investigación "Empresa y proceso. Investigación y Cooperación" (Ref. PID 2020-119878GB-100) del Ministerio de Ciencia e innovación.

I. Consideraciones previas

El 28 de julio de 2023, el Diario Oficial de la Unión Europea (DOUE) ponía fin al largo camino iniciado en 2016, al publicar la nueva y esperada normativa relativa a la obtención de pruebas transfronteriza dentro de un proceso penal, a través de dos instrumentos conexos muy específicos: por un lado, el Reglamento 2023/1543, de 12 de julio (en adelante el Reglamento), sobre las órdenes europeas de producción y de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de los procesos penales; y, por otro, la Directiva 2023/1544, de 12 de julio (en adelante la Directiva), por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales, ambos del Parlamento Europeo y del Consejo, cuyo plazo de transposición en los ordenamientos de los Estados miembros es el 18 de febrero de 2026, como máximo.

La exigencia de una nueva normativa, a pesar de estar en vigor la Orden de Investigación Europea (OIE)[1], viene originada por varios factores entre los que se encuentra, principalmente, la poca o nula eficacia de este último instrumento a la hora de recabar las pruebas electrónicas, en un ámbito en el que ya está generalizado el uso de dispositivos electrónicos como medio para la comisión de cualquier delito. La naturaleza volatil de los datos electrónicos, por otro lado, no casa bien con las dilaciones derivadas de los plazos y la burocracia provocada por los procedimientos de cooperación judicial en los que se basa la mencionada OIE, y en definitiva, el problema al que nos enfrentábamos era la ausencia de una normativa específica que permitiese la obtención de pruebas electrónicas de ámbito transfronterizo, –puesto que los datos que los investigadores pueden necesitar se encuentra almacenada en servidores distribuidos en distintos Estados– hacía muy difícil, sino imposible, alcanzar estos objetivos con la única ayuda de la OIE (De HOYOS, 2023, p. 101).

Uno de los mayores escollos, pues, en el ámbito de la obtención de pruebas digitales, se encontraba en la ausencia de un régimen común de protección de datos en el ámbito penal entre los Estados miembros, frente al amplio abanico normativo existente, y por ello muy disperso, de estándares legales en las diferentes legislaciones procesales en relación a la obtención de pruebas, y, además, sin la implementación de unas reglas comunes relativas a las garantías procesales mínimas y básicas que el sujeto investigado debía tener en todos y cada uno de los Estados miembros[2]. (PEERS, S., 2010 y SAYERS, D., 2011).

1. Directiva 2014/41/UE del Parlamento y del Consejo, de 3 de abril, relativa a la Orden Europea de Investigación en Materia Penal (DOUI de 1 de mayo de 2014, que se creó con la finalidad de reemplazar dos instrumentos jurídicos hasta entonces vigentes, y con la intención de evitar duplicidades en materia de obtención de pruebas: la Decisión Marco del Consejo de Europa 2003/577/JHA, de 22 de julio, y la Decisión Marco 2008/978/JHA, de 18 de diciembre. La OIE tuvo como base el Programa de Estocolmo, adoptado por la Comisión Europea el 11 de diciembre de 2009. Si bien se recogía el acceso a pruebas electrónicas, la Orden no contenía disposición específica alguna sobre la obtención transfronteriza de pruebas electrónicas.

2. Entre otros pueden verse los informes presentados ante la Comisión Europea de *Fair Trials International* "Fair Trials International's response to a European Member States's legislative initiative for

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

La práctica de los operadores jurídicos durante las labores de búsqueda de elementos probatorios en el proceso penal puso en evidencia que el 85% de las investigaciones penales conlleva el uso de dispositivos electrónicos, y de estos, más de la mitad contienen una petición transfronteriza de acceso a pruebas electrónicas. Por ello, en sus Conclusiones sobre la mejora de la justicia penal en el ciberespacio, el Consejo advirtió de la necesidad de desarrollar acciones concretas basadas en un enfoque común de la UE que facilitasen una asistencia jurídica mutua más eficaz; y lo que resultaba más novedoso pero también más desafiante, basado en el objetivo de establecer vías de cooperación más eficaces entre las autoridades de los Estados miembros y los proveedores de servicios radicados en países no pertenecientes a la UE, así como proponer soluciones al problema de la determinación y aplicación de la jurisdicción en el ciberespacio[3]. En este sentido, como bien señala ROGALSKI, "la propuesta de la Comisión intentaba alcanzar el extremadamente delicado equilibrio entre una eficaz y eficiente investigación penal (para la policía judicial y el juez de instrucción), certeza jurídica (para las compañías tecnológicas), y la protección de los derechos fundamentales (para el sospechoso y otros usuarios)" (ROGALSKI, 2020, p. 335).

Por su parte, el Parlamento Europeo también manifestó expresamente que la creación de un marco jurídico de armonización dirigido a la creación de deberes de colaboración a los proveedores de servicios, con la obligación de dar cumplimiento a las solicitudes cursadas por los jueces, fiscales o fuerzas y cuerpos de seguridad, era todo un reto que había que lograr, abogando por la creación de un marco jurídico europeo armonizado que incluyese salvaguardias para los derechos y las libertades de los interesados[4].

La Comisión propondría, entonces, el 17 de abril de 2018, y mediante una Resolución, la elaboración de dos documentos conexos, uno con forma de propuesta de Reglamento (COM/2018/225) y otro con forma de propuesta de Directiva (COM/2018/226), con la declarada intención de crear la denominada Orden Europea de Entrega (EPOC) y una Orden de Preservación de Pruebas Electrónicas (EPOC-PR), ambas con fuerza vinculante, basadas en la posibilidad de que la autoridad judicial de un Estado Miembro solicite directamente a un proveedor de servicios –que se encuentre ubicado en otra jurisdicción–, los datos electrónicos necesarios para obtener pruebas en los procesos penales iniciados. La EPOC-PR, por su parte, solo permitirá solicitar la conservación de datos que ya se encuentren almacenados en el momento de la recepción de la orden y no podrá ser utilizada, en ningún caso, para acceder a datos producidos antes o tras la recepción de la orden. Ambos instrumentos fueron concebidos, pues, ante la necesidad de obtener pruebas electrónicas de carácter transfronterizo por no existir otros instrumentos eficaces frente al creciente e imparable desarrollo tecnológico y el problema relativo a la aplicación de los conceptos tradicionales en relación con la territorialidad y la jurisdicción (TOSZA, 2020, p. 168).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

---

a Directive on a European Investigation Order", de 29 de junio de 2010 disponible en http://www.statewatch.org/news/2010/jul/eu-eio-ft-briefing.pdf.

3. Conclusiones del Consejo de la Unión Europea, de 9 de junio de 2016, sobre la mejora de la justicia penal en el ciberespacio, ST9579/16.

4. P8_TA(2017)0366.

Con estas propuestas, la Comisión Europea puso en marcha una serie de negociaciones internacionales, en 2018, sobre el acceso a la prueba electrónica transfronteriza, dando así un paso tan decisivo como necesario para perseguir penalmente a organizaciones criminales y terroristas. En octubre de ese mismo año, la Comisión presentó dos propuestas de negociación de directivas: una para negociar con los EEUU[5], con base en un acuerdo bilateral aprobado por el Congreso de los EEUU en relación con la *Clarifying Lawful use of Overseas Data Act*, más conocida como CLOUD Act, de 23 de marzo de 2018. Este acuerdo formaba parte del denominado *Omnibus Spending Bill*, creando, de este modo, una base legal para que el gobierno de los EEUU pueda llegar a acuerdos con otros Estados en relación al acceso de datos contenidos y almacenados por proveedores de servicios norteamericanos y viceversa (FRANSSEN, 2018); y una segunda propuesta para negociar un segundo Protocolo Adicional del Convenio sobre Cibercrimen[6] y relativo a la cooperación reforzada y la revelación de pruebas electrónicas[7].

Este segundo Protocolo reconocía la necesidad de incrementar la cooperación de forma más eficiente, entre los Estados y los proveedores de servicio, en el contexto de obtención de pruebas de los delitos electrónicos, recogiendo ya la exigencia de dotar de una mayor seguridad jurídica a las investigaciones penales en relación con las circunstancias en las que puedan atenderse las solicitudes de las autoridades penales de otros Estados Parte en la revelación de datos electrónicos; así como garantizar una protección más efectiva contra la ciberdelincuencia y en la obtención de pruebas en formato electrónico garantizando, como no podía ser de otro modo, el respeto de los derechos y libertades fundamentales (De HOYOS, 2023, p. 118).

II. La designación de establecimientos y representantes legales a efectos de recabar pruebas para los procesos penales en la Directiva

Los atentados acaecidos en Bruselas el 22 de marzo de 2016[8] provocaron una urgente reunión conjunta de los ministros de Justicia y de Interior de los Estados miembros y de

5. Recomendación para la autorización de negociaciones con vistas a un acuerdo entre la Unión y los EEUU de América sobre acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en asuntos penales, de 5 de febrero de 2019 COM (2019) 70 final. Vide https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf

6. Recomendación para una decisión del Consejo sobre la autorización a participar en las negociaciones de un segundo Protocolo Adicional del Convenio Europeo sobre Cibercrimen (CETS No 185). De 5 de febrero de 2019 COM (2019) 71 final. Vide https://ec.europa.eu/info/sites/info/files/recommendation_budapest_convention.pdf

7. Adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021. Abierto a la firma en Budapest el 23 de noviembre de 2001, España lo firmó el 12 de mayo de 2022. Publicado en el DOUE núm. 63, de 28 de febrero de 2023.

8. Atentado islamita que costó la vida a más de treinta personas y dejó heridos a más de 230. Se trató de un doble atentado que afectó al aeropuerto y el metro, y este último el artefacto explosivo estalló en la estación de Molenbeck, muy cerca del lugar donde está situada la Comisión y el Parlamento Europeo.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

los representantes de instituciones de la UE. Esta reunión sirvió para alcanzar el acuerdo de trabajar sin más dilación en la creación y desarrollo de las vías de actuación necesarias para permitir una cooperación más intensa y eficaz con los proveedores de servicios que operan no solo en el territorio europeo, sino también con terceros países.

La finalidad de fomentar y facilitar una mayor y más eficiente cooperación con los proveedores de servicios se dirigía a posibilitar, no solo la obtención, sino también el aseguramiento, a través de una orden de conservación, de quienes tuviesen la posesión de cualquier dato electrónico que las autoridades investigadoras necesitasen. Y estos acuerdos se volcaron como conclusiones en el Documento que publicó el Consejo de 9 de junio de 2016[9]. Tras ello se solicitó a la Comisión la elaboración de un estudio que sirviese de base a una propuesta con la finalidad de crear una nueva y más eficiente normativa procesal en dicho ámbito, a través del establecimiento de obligaciones para los proveedores de servicios que serían los destinatarios directos de la orden judicial. De esta forma, la idea pivotaba sobre la creación de una cooperación impuesta directamente a los proveedores de servicios como el principal objetivo de la Directiva[10].

La Directiva se traduce, en consecuencia, en el instrumento a través del cual se crea el marco legal que va a dotar de eficacia a la EPOC y a la EPOC-PR" (FRANSSEN, 2018). Y ello porque es en la Directiva donde se establece que los proveedores de servicios son los receptores directos de una orden emitida por un fiscal o por un juez –dependiendo de la naturaleza invasiva de la orden en la esfera de los derechos fundamentales de los usuarios afectados por la orden–. Una vez reciban dichas órdenes, pues, los proveedores quedan obligados a aportar los datos electrónicos que dicho órgano judicial requiera, así como, también (y en caso de ser necesario), adoptar las medidas necesarias para la conservación de datos que puedan resultar útiles a los efectos de una posterior EPOC, o incluso una OIE.

Evidentemente estamos ante la creación de un marco jurídico de deberes y obligaciones que conlleva medidas sancionadoras en caso de incumplimiento. En este sentido, por ejemplo, el artículo 5 de la Directiva ordena a los Estados miembros el establecimiento de un régimen de sanciones aplicable, que según el artículo 15 del Reglamento, podrá consistir en regular una sanción pecuniaria de hasta el 2% del total del volumen anual de negocios mundial del ejercicio precedente del prestador de servicios. Este tipo de sanciones de carácter disuasorio puede en algunos casos no ser eficaz si se tiene en cuenta, por ejemplo, que Google tuvo en el año 2022 un volumen de ingresos de casi 280 mil millones de dólares, los cinco mil seiscientos millones de dólares que debería pagar no va a suponer una cantidad excesiva, o al menos, tan disuasoria como se pretende.

El proveedor de servicios, por otro lado, podrá negarse a entregar los datos requeridos, pero únicamente por las razones y motivos expresamente recogidos en el artículo 12 del Reglamento[11]. Entre otros, por ejemplo, que los datos solicitados estén protegidos

9. ST9579/16.

10. Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo de 12 de julio de 2023. DOUE de 28 de julio de 2023.

11. Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023. DOUE de 28 de julio de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

por inmunidades o privilegios concedidos en virtud del Derecho del Estado de ejecución; o por normas sobre limitación de la responsabilidad penal relacionadas con la libertad de prensa; o porque existan motivos fundados para suponer que la ejecución de la orden supondría una vulneración manifiesta de un derecho fundamental de los recogidos en el artículo 6 del CEDH, y por ello, del derecho a un proceso justo, a la presunción de inocencia y al de defensa.

Se trata, tal y como se cita en el título de la Directiva, de establecer un marco normativo de armonización tanto de aquellas que impongan obligaciones, como de las que recojan sanciones por el no cumplimiento de lo solicitado en la orden, y que pueden imponerse a los proveedores de servicios con vínculos en la UE[12], lo que incluye a terceros países, como los EEUU (a través de los acuerdos bilaterales de los que se hacía mención en apartados anteriores esto es, el CLOUD Act) y que sirve para dejar sin efecto el denominado "Estatuto de Bloqueo", que no es otra cosa que la prohibición legal para los proveedores de servicios americanos de entregar datos electrónicos a otros estados no americanos y que se recoge en la ley *Electronic Communications Privacy Act* de 1986 (FRANSSSEN, 2018).

Y es que, el extraordinario incremento en la utilización –tanto por parte de los servicios de telecomunicaciones tradicionales, como de los consumidores y de las empresas– de los nuevos servicios basados en la red, –que hacen posible la comunicación interpersonal tales como servicios de voz sobre IP, mensajería instantánea de correo electrónico, junto a redes sociales como Facebook y Twitter–, permiten que los datos que compartan los usuarios estén cubiertos, de este modo, por la Directiva. Además, ha de tenerse en cuenta que cada vez resulta más común almacenar los datos en la nube, por lo que no es necesario que los proveedores de servicios tengan servidores en cada jurisdicción, ya que suelen utilizar sistemas centralizados para prestar sus servicios. Las transacciones que realizan las pueden llevar a cabo bien desde el sitio web del mercado en línea o en una página web del comerciante. Todas estas razones explican por qué era tan importante controlar y armonizar la normativa que impusiese obligaciones respecto de los proveedores de servicios, pues es este mercado precisamente el que suele estar en posesión de cualquier tipo de prueba electrónicas que sea necesaria obtener si se abre un proceso penal.

En este sentido, la Directiva es muy clara al señalar que, a los efectos de la obtención de pruebas electrónicas, los obligados a cooperar cuando se emita una orden de producción o de conservación son "los proveedores de servicios de comunicaciones electrónicas[13] y los prestadores de servicios de la sociedad de la información[14]". Respecto de

12. Con base jurídica en los artículos 53 y 62 del TFUE, que prevé la adopción de medidas de coordinación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de establecimiento y de prestación de servicios.

13. De esta forma, la Directiva debe aplicarse a los servicios de comunicación tal y como se definen en la Directiva (UE) 2018/1972 del Parlamento y del Consejo, de 11 de diciembre de 2018, por el que se establece el Código Europeo de las Comunicaciones Electrónicas.

14. Es decir, los prestadores de servicios de la sociedad de la información que puedan calificarse como tales según lo dispuesto en la Directiva (UE) 2015/1535 del Parlamento y del Consejo, de 9 de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

los primeros, la Directiva incluye las prestaciones de servicios de comunicaciones interpersonales tales como servicios de voz sobre IP, servicios de mensajería instantánea y servicios de correo electrónico. Y en relación con los servicios de la sociedad de la información, se refiere a los proveedores que ofrezcan la posibilidad de comunicación entre sujetos, o les ofrezcan servicios que puedan utilizar para almacenar o tratar datos de otro modo en su nombre, y que no puedan calificarse como proveedores de servicios de comunicación.

De esta forma se trata de proveedores que ofrecen servicios, en general, de comunicaciones electrónicas; así como de servicios de información, y de almacenamiento de datos como parte del servicio prestado al usuario, incluidas las redes sociales, los mercados en línea y otros proveedores de servicios de alojamiento de datos; y proveedores de servicios de asignación de nombres y números en internet (artículo 2 de la Directiva). Pero, habrá de tenerse en cuenta, también, que dichas obligaciones tienen implicaciones directas en otras empresas, tales como, por ejemplo, los fabricantes de automóviles que ofrezcan un servicio de navegación por la red o el acceso a emails, lo que resulta cada vez más común.

A los efectos de los obligados, y según el artículo 3 de la Directiva, los proveedores de servicios pueden dividirse, pues, en tres categorías principales: a) los que tengan su sede en un Estado miembro que ofrecen los servicios únicamente en el territorio de dicho Estado miembro; b) los que tengan su sede en un Estado miembro que ofrecen servicios en varios Estados miembros; y c) los que tengan su sede fuera de la UE pero que ofrecen sus servicios en uno o varios Estados miembros, dispongan o no de un establecimiento en uno o en varios Estados miembros. Así, la normativa contenida en la Directiva y en las correspondientes órdenes no sólo va a ser de aplicación a los servidores de servicios con sede en la UE, sino que, al recoger la exigencia de una conexión[15] vinculada a la oferta del servicio con efectos en el mismo ámbito geográfico, se impide una posible laguna legal que dificulte la ejecución de dichos instrumentos (TOSZA, 2020, p. 176). Esta última posibilidad resultará de vital importancia si tenemos en cuenta que los grandes proveedores de servicios, tales como Google y Microsoft, tienen su sede fuera de la UE.

En definitiva, la obligación de designar un establecimiento designado o un representante legal debe aplicarse a los prestadores que ofrezcan sus servicios en la Unión Europea, excluyéndose, a tales efectos, la aplicación de la Directiva a situaciones en las

septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

15. Esta conexión a la que la Directiva llama "sustancial", se refiere, según el considerando número 11 de la Directiva, a la conexión del prestador de servicios "con la Unión. A falta de establecimiento, el criterio de la conexión sustancial debe basarse en criterios fácticos específicos como la existencia de un número significativo de usuarios en uno o más Estados miembros, o la orientación de las actividades hacia uno o más Estados miembros. La orientación de las actividades hacia uno o más Estados miembros ha de determinarse en función de todas las circunstancias pertinentes, incluidos factores como el uso de la lengua o una moneda utilizada generalmente en ese Estado miembro, o la posibilidad de encargar productos o servicios".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

que un prestador de servicios esté establecido en el territorio de un Estado miembro y ofrezca servicios exclusivamente en el territorio de dicho Estado.

III. Las órdenes europeas de entrega y conservación de pruebas electrónicas

Como se ha comentado anteriormente, el Consejo pidió la creación y desarrollo de acciones concretas basadas en un enfoque común de la UE para una asistencia jurídica mutua más eficaz, para mejorar la cooperación entre las autoridades de los Estados miembros y los proveedores de servicios radicados en países no pertenecientes a la UE, y encontrar soluciones al problema de la determinación y aplicación de la jurisdicción en el ciberespacio. Por su parte, el Parlamento Europeo también puso de relieve los retos que, el actualmente fragmentado marco jurídico, puede suponer para los proveedores de servicios que desean dar cumplimiento a los requerimientos legales, e hizo un llamamiento a favor del establecimiento de un marco jurídico europeo que incluyese salvaguardas para los derechos y las libertades de los interesados[16].

La opción de la Comisión por regular estas dos órdenes mediante Reglamento y no mediante Directiva o Decisión, según se declaró en la Exposición de Motivos de la Propuesta de Reglamento, se debía a que las órdenes van a ejecutarse en relación con procedimientos transfronterizos, y ello con buena lógica requiere de normas uniformes y, en consecuencia, la elaboración de un instrumento con forma de Reglamento es lo que va a permitir que, la misma obligación, sea impuesta de forma uniforme en cualquiera de los Estados miembros de la Unión.

La Exposición de Motivos de la Propuesta de Reglamento señalaba que la utilización de las redes sociales, los servicios de correo electrónico y de mensajería y las aplicaciones para comunicarse, trabajar, crear lazos sociales y obtener información se ha convertido en algo habitual en muchas partes del mundo. Estos servicios de mensajería instantánea (WhatsApp, Instagram, pero también e-mail, etc.), conectan entre sí a cientos de millones de usuarios y generan importantes beneficios para el bienestar social y económico de los usuarios en la Unión y fuera de ella. Sin embargo, también sirven como instrumentos para cometer o facilitar delitos de extrema gravedad, como, por ejemplo, atentados terroristas. Y, cuando esto sucede, los proveedores de servicios y las aplicaciones que ofrecen se convierten en el único lugar donde los investigadores pueden hallar indicios que les permitan determinar quién el presunto autor del hecho, y obtener las pruebas de cargo susceptibles de utilizarse en el proceso penal correspondiente.

Como es sabido, las redes sociales ofrecen servicios desde cualquier parte del mundo y a cualquiera que se encuentre en otra parte del mundo distinta, y todo ello sin

16. El fundamento jurídico para adoptar las medidas jurídicas correspondientes recogidas en el Reglamento se basó en el artículo 82, apartado 1 del TFUE, según el cual, podrán adoptarse las medidas que correspondan con arreglo al procedimiento ordinario a fin de establecer la normas y procedimientos que garanticen el reconocimiento en toda la Unión de las sentencias y resoluciones judiciales en todas sus formas.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

necesidad de una infraestructura física ni una presencia empresarial o personal en los Estados miembros en los que se ofrecen, o en el mercado interior en su conjunto. Por otro lado, y por su especial naturaleza, tampoco se requiere una ubicación específica para el almacenamiento de los datos, por lo que ésta suele ser elegida por el proveedor de servicios sobre la base de consideraciones tales como la seguridad de los datos, las economías de escala y la rapidez de acceso. Y, aquí radica la verdadera importancia de este instrumento jurídico: cada vez es más común que en los procesos penales, relativos a todo tipo de delitos, que las autoridades de los Estados miembros necesiten acceder a datos que puedan servir como prueba, pero que están almacenados fuera de su país, o por proveedores de servicios ubicados en otros Estados miembros o en terceros países.

El Reglamento aborda, pues, el problema específico derivado del carácter volátil de las pruebas electrónicas y su dimensión internacional. Es decir, con dicho instrumento se intenta adaptar los mecanismos de cooperación judicial a la era digital, ofreciendo a las autoridades judiciales y policiales las herramientas necesarias para abordar de forma eficaz el ámbito en el que los delincuentes se comunican en la actualidad, y, en consecuencia, enfrentarse de forma eficiente a la investigación de las nuevas formas de delincuencia.

De esta forma, el Reglamento tiene por objeto, por un lado, mejorar la seguridad jurídica para las autoridades, los proveedores de servicios y las personas afectadas, y, por otro lado, mantener un nivel uniforme en lo que respecta a las solicitudes de las autoridades competentes, y todo ello sin merma alguna de la debida protección de los derechos fundamentales, por lo que cualquier medida solicitada deberá estar informada y regida por el principio de necesidad y proporcionalidad[17].

Para la notificación y ejecución de órdenes en virtud de este instrumento, las autoridades deben recurrir al representante legal efectivamente designado por el proveedor de servicios. Se aporta así una solución común para todo el ámbito de la UE para transmitir órdenes a los proveedores de servicios por medio de un representante legal, que, según el artículo 3.7 del Reglamento, deberá ser una persona física o jurídica designada por escrito por un prestador de servicios no establecido en un Estado miembro que participe de un instrumento jurídico contemplado en el artículo 1, apartado 1[18] y en el artículo 3, apartado 1 de la Directiva[19].

17. Según se recoge expresamente en varios considerandos del Reglamento, tales como el 2 y el 49, así como en varios lugares de su articulado, como, por ejemplo, en el artículo 5 donde se establecen las condiciones de emisión de una EPOC.

18. Que dispone que la Directiva "establece las normas relativas a la designación de establecimientos designados y de representantes legales de determinados prestadores de servicios que ofrezcan servicios en la Unión para la recepción, el cumplimiento y la ejecución de las resoluciones y órdenes emitidas por las autoridades competentes de los Estados miembros a efectos de recabar pruebas electrónicas en procesos penales".

19. Según el cual, "Los Estados miembros velarán por que los prestadores de servicios que ofrezcan servicios en la Unión designen al menos un destinatario para la recepción, el cumplimiento y la ejecución de las resoluciones y órdenes que entren en el ámbito de aplicación establecido en el artículo 1, apartado 2 (en lo sucesivo 'resoluciones y órdenes comprendidas en el ámbito de aplicación

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

En relación con las infracciones susceptibles de ser objeto de una EPOC, el artículo 5 del Reglamento establece que podrá emitirse para cualquier infracción punible en el Estado emisor con una pena máxima de privación de libertad de al menos tres años; o bien cuando las infracciones se hayan cometido en su totalidad, o parcialmente, por medio de un sistema de información respecto de las infracciones que, como tal, se definen en: a) la Directiva (UE) 2019/713 del parlamento y del Consejo sobre la lucha contra el fraude y la falsificación de medios de pago distintos al efectivo por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo (transferencias fraudulentas, robo o apropiación indebida de instrumentos de pago, etc.); b) infracciones como las recogidas en la Directiva 2011/93/UE del Parlamento Europeo y del Consejo (relativas a los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, que sustituye la Decisión Marco 2004/68/JAI del Consejo); c) las infracciones recogidas en la Directiva 2013/40/UE del Parlamento Europeo y del Consejo (relativa a los ataques contra los sistemas de información, que sustituye a la Decisión Marco 2005/222/JAI del Consejo); y d) las infracciones recogidas en la Directiva 2017/541 del Parlamento Europeo y del Consejo (relativa a la lucha contra el terrorismo, que sustituye la Decisión Marco 2005/671/JAI del Consejo).

3.1. Tipo de datos que pueden obtenerse como prueba electrónica

En relación con el tipo de datos que pueden obtenerse a través de una EPO o EPOC-PR, ha de tenerse en cuenta que el Reglamento regula únicamente la obtención de datos almacenados por un prestador de servicios en el momento que reciba una orden europea de producción o de conservación. De esta forma, no podrán realizarse investigaciones prospectivas con la intención de obtener datos pasados o futuros. Los datos deberán facilitarse o conservarse independientemente de que estén cifrados o no, y deberá existir una previa imputación en relación con un delito concreto y, en consecuencia, que exista un proceso penal abierto en el momento en el que se soliciten.

Por otro lado, es importante señalar que el Reglamento no define expresamente qué debe entenderse por prueba electrónica, sino que simplemente hace referencia a la clase de datos objeto de la Orden, y en este sentido ha de entenderse que prueba electrónica es "la evidencia almacenada en forma electrónica por o a nombre de un proveedor de servicios en el momento de la recepción de la orden y consistente en una de las cuatro categorías tradicionales de datos: datos de abonado, de acceso, de tráfico y de contenido"[20]. Estas categorías son, en efecto, las que se recogen en el artículo 3

establecido en el artículo 1, apartado 2'), emitidas por las autoridades competentes de los Estados miembro a efectos de recabar pruebas en procesos penales".

20. Según el Informe de la propuesta de regulación publicado por el Parlamento Europeo, en la enmienda núm. 20, se justifica la cobertura de los tipos de datos mencionados por ser las categorías más comunes en muchos de los Estados miembros y en la normativa de la Unión, como la Directiva 2002/58/EC, la jurisprudencia del Tribunal de Justicia, y por supuesto, el Convenio del Cibercrimen. Vide https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

(núm. 9 a 11), de forma que el Reglamento coloca el énfasis en lo que TOSZA denomina "objeto de la Orden", en vez de focalizarlo en la naturaleza jurídica de lo debe entenderse por "prueba electrónica" (TOSZA, 2020, p. 171 y LARO, 2022, p. 291).

En este sentido, en la Propuesta se aseguró que en el Reglamento se recogiese un concepto de datos coherente con los establecidos en otros instrumentos europeos en relación con las comunicaciones electrónicas y, en especial, con lo contenido en el Código Europeo de Comunicaciones Electrónicas creado por la Directiva de 11 de diciembre de 2018[21]. Sin embargo, como señala ROGALSKI, el concepto de lo que ha de entenderse por "abonado" no lo encontramos en la Directiva que acaba de mencionarse, sino en el artículo 2, letra k de la Directiva 2002/21/EC del Parlamento y del Consejo de 7 de marzo de 2002, que fue reemplazada por la anterior, y que definía el termino de abonado como "cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público para la prestación de dichos servicios". Y en este aspecto, es claro que, como señala el citado autor, es importante que, en relación con el tipo de datos que son susceptibles de ser obtenidos y/o conservados, los significados deben ser uniformes en los distintos códigos procesales penales de los Estados miembros (ROGALSKI 2020, pp. 340-341).

En opinión de CORTHAY, sin embargo, el Reglamento se separa de las categorías tradicionales de datos que suele utilizar la Comisión en otros instrumentos jurídicos, por ejemplo, en la Directiva 2002/58/CE del Parlamento y del Consejo de 12 de julio, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, más conocida como la Directiva e-Privacy; y la Directiva 2006/24/CE de Conservación de datos[22] que modifica la anterior. En estos instrumentos se utilizan las categorías de datos de abonado, datos de tráfico y de localización (conocidos como metadatos) y de contenido (CORHAY, 2021, p. 447). Pero el Parlamento rechazó las categorías de datos propuestas por la Comisión, y optó por mantener las categorías tradicionales de datos: de abonado, de tráfico y de contenido (CORHAY, 2021, p. 458).

Así pues, los tipos de datos que recoge el Reglamento son los siguientes:

a) *Datos de los abonados*
   El Reglamento considera datos de los abonados cualquier dato que obre en poder de un prestador de servicios relativo a la suscripción da sus servicios en relación con la identidad del abonado o cliente, como el nombre, fecha de nacimiento, dirección postal o geográfica, facturación y pagos, número de teléfono o dirección de correo electrónico.

21. Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo de 11 de diciembre de 2019 por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DOUE de 17 de diciembre de 2018).

22. Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso o redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE (DOUE núm. 105, de 13 de abril de 2006.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

Y, además de estos, se incluye: el tipo de servicio y su duración, incluidos los datos técnicos que identifiquen las medidas técnicas correspondientes o las interfaces utilizadas o facilitadas al abonado o cliente en el momento del registro o activación inicial, y los datos relativos a la validación del uso del servicio, excluyendo las contraseñas u otros medios de autenticación utilizados en lugar de una contraseña que hayan sido facilitados por un usuario o creados a petición de un usuario.

b) *Datos de identificación del usuario (datos de acceso)*
Tales como las direcciones de IP, los números de acceso y la información conexa. Estos datos pueden constituir un punto de partida esencial para las investigaciones en las que no se conozca la identidad de un sospechoso. Son datos que forman parte de un registro de acontecimientos conocido como registro de servidor que indica el comienzo o fin de la sesión de acceso de un usuario a un servicio. A menudo es una dirección IP (estática o dinámica[23]) y otro identificador el que señala la interfaz de red utilizada durante una sesión de acceso de un usuario a un servicio como los puertos de origen y sello de tiempo, ya que las direcciones de IP suelen compartirse entre usuarios, por ejemplo, cuando se dispone de una traducción de direcciones de redes de alta fiabilidad (CGN), o de equivalentes técnicos. Se trata de un conjunto de mecanismos dirigido a compartir dirección IP entre varios dispositivos. El ejemplo más claro son las conexiones de banda ancha de suscriptores. El proveedor asigna una sola dirección IP a un suscriptor y mediante un dispositivo con capacidades NAT se realiza la traducción del conjunto de direcciones privadas utilizadas en el domicilio del suscriptor, contra la única dirección IP que el proveedor ha asignado al abonado (CASTRO, 2020, p. 5).

Las direcciones de IP dinámicas de acuerdo con la jurisprudencia de la UE deben considerarse datos personales y gozar de plena protección en virtud de materia de protección de datos[24]. Pero, en determinadas circunstancias, las direcciones de IP pueden también considerarse datos de tráfico, por ejemplo, los números de acceso y la información conexa se consideran datos de tráfico en algunos Estados miembros. No obstante, a efectos de una investigación penal específica, las autoridades policiales pueden solicitar una dirección de IP, así como números de acceso e información conexa con el único fin de identificar al usuario antes de que puedan solicitarse al prestador de servicios los datos de los abonados relacionados con ese identificador en tal caso, procede aplicar el mismo régimen que a los datos de los abonados. En este ámbito, sin embargo, y a raíz de una solicitud de la Gran Sala, presentada como cuestión prejudicial planteada por el Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo de Francia, las conclusiones del Abogado General

23. Mientras que las IP estáticas no cambian cuando se asigna a un dispositivo, las dinámicas tienen carácter personal, y cambia con cada nueva conexión a internet, ya que son las que les asigna la red cuando se conectan.

24. Así se estableció en el caso C582/14 Breyer.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

Maciej Szpunar, en el asunto C-470/21, de 23 de marzo de 2023, declaró que una autoridad nacional debería poder acceder a los datos de identidad civil vinculados a las direcciones IP cuando dichos datos constituyen el único método de investigación para identificar a los titulares de esas direcciones sospechosos de vulnerar derechos de propiedad intelectual[25].

c) *Datos de tráfico*

Son los datos relacionados con la prestación de un servicio que sirvan para facilitar información contextual o adicional sobre dicho servicio y sean generados o tratados por un sistema de información contextual o adicional sobre dicho servicio y sean generados o tratados por un sistema de información del prestador del servicio tales como el origen y destino de un mensaje u otro tipo de interacción, el número de teléfono móvil, la ubicación del dispositivo, la fecha, la hora, la duración, el tamaño, la ruta, el formato, el protocolo utilizado y el tipo de compresión, y otros metadatos de las comunicaciones electrónicas y los datos que no sean datos de abonados, relativos al inicio y final de una sesión de acceso del usuario a un servicio, tales como la fecha y hora del acceso, la conexión y desconexión del servicio.

d) *Datos de contenido*

Cualquier dato en formato digital, como texto, voz, videos, imágenes y sonidos que no sean datos de abonados o datos de tráfico.

3.2. Autoridad competente para la obtención y solicitud de conservación de prueba electrónica

Una de las cuestiones más controvertidas y por ello más debatidas por la doctrina tras la publicación de la Propuesta del Reglamento ha sido la cuestión acerca de la determinación de la autoridad competente para emitir tanto una orden de obtención como de conservación de pruebas electrónicas. Y ello porque la Propuesta autorizaba tanto a un órgano judicial, como a un miembro de la Fiscalía, a emitir cualquiera de las órdenes previstas sin diferenciar el tipo de datos y, en consecuencia, de la distinta afectación a los derechos fundamentales del propietario de dichos datos.

En este sentido, el Dictamen del Comité Económico Social Europeo[26] (CESE) señalaba que el Reglamento debía respetar los derechos fundamentales, tanto en relación con los recogidos y reconocidos en el CEDH, como todos los reconocidos en las Constituciones de cada uno de los Estados miembros; en especial, el derecho a la libertad y seguridad, el derecho a la tutela judicial efectiva, y el de protección de los datos de carácter personal.

25. https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-10/cp220172es.pdf

26. Dictamen publicado en el Diario Oficial de la Unión Europea de 10 de octubre de 2018 C 367/88. El Comité Económico y Social Europeo, es el órgano consultivo de la UE, compuesto por los representantes de las organizaciones de trabajadores y empresarios, y que emite dictámenes sobre cuestiones de la UE para la Comisión Europea, el Consejo y el Parlamento Europeo, y actúa como puente entre las instituciones de la UE con capacidad decisoria y los ciudadanos europeos

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

En dicho aspecto, el CESE consideraba que tanto la solicitud de obtención de datos de abonados como la de datos relativos al acceso pertenecen al ámbito de los derechos de carácter personal, por lo que la orden debería estar acordada y emitida por una autoridad judicial y no por un fiscal.

Por su parte, el Supervisor Europeo de la Protección de Datos[27] (EDPS, por sus siglas en inglés), publicada el 6 de noviembre de 2019 como "Opinión 7/2019 sobre la Propuesta de Reglamento de la Orden Europea de obtención y conservación de pruebas electrónicas"[28], realizó recomendaciones dirigidas, por un lado, a que la normativa europea fuese clara y se reforzase la seguridad jurídica, y por otro, que el principio de proporcionalidad se aplicase en el listado de las infracciones susceptibles de ser objeto de una orden (de obtención o de preservación de pruebas).

De esta forma, el EDPS entendía que el límite de tres años de privación de libertad –que recoge el vigente el artículo 5 (4) (a-d) del Reglamento– implicaría que podría solicitarse una orden de este tipo para casi cualquier delito recogido, como tal, en las normativas penales de los Estados miembros, y que podía servir de coladero para otros delitos no recogidos en el listado –anteriormente mencionado–. En dicho aspecto, recordaba que el TJUE, en su decisión C-207/16, ya declaró que "de acuerdo con el principio de proporcionalidad, las graves interferencias por parte del Estado en áreas de la prevención, investigación, detección y persecución penal, sólo puede estar justificado si el delito que se ha cometido puede ser definido como grave, y, únicamente cuando la lucha contra dicha grave criminalidad posibilite justificar al Estado el acceso a datos personales, permitiéndole obtener información relativa a la privacidad de las personas cuyos datos han sido obtenidos". Por otro lado, la exigencia de garantizar la protección a los derechos fundamentales, y en especial, a los datos de carácter personal, es un objetivo esencial. Por ello, las órdenes deberán, en cualquier caso, ser emitidas por una autoridad judicial, no por un fiscal.

En su informe de 2020, investigadores del Centro de Estudios Europeos, insistieron en la necesidad de una validación judicial independiente de las órdenes de obtención y conservación de pruebas digitales y siempre bajo los principios de legalidad, necesidad y proporcionalidad. (Sergio Carrera, M. S. y. V. M., 2020).

Finalmente, en mayo de 2023, pocos meses antes de la publicación de los instrumentos que se están analizando, el European Law Institute, hizo pública una Propuesta de Regulación de la Admisibilidad Mutua de Prueba y Prueba electrónica en los procesos penales dentro de la Unión Europea, en la que recomienda la regulación positiva

27. El EDPS es una institución independiente de la UE y responsable, bajo el artículo 52.2 del Reglamento 2018/1725 de los procesos relacionados con los datos personales para asegurar que los derechos y libertades fundamentales, en particular el derecho fundamental a la protección de datos personales y, bajo el artículo 52.3, para aconsejar a las instituciones de la Unión, así como emitir, por propia iniciativa o, tras la previa solicitud de las instituciones de la Unión, en relación con la protección de datos personales. Vide edps.europa.eu.

28. EDPS Opinion on the Proposals regarding European Production and Preservation Orders of electronic evidence on criminal maters. https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

de ciertos aspectos importantes, - aunque no todos ellos se han recogidos en el vigente Reglamento–, tales como la inclusión de salvaguardas dirigidas a evitar manipulaciones o alteraciones de la integridad y autenticidad de las pruebas electrónicas mediante la posibilidad de que la defensa tenga acceso a todo el material obtenido, y el uso de recursos frente a la obtención de pruebas con infracción de las normas y la regulación de las consecuencias de la declaración de ilicitud de la obtención de pruebas mediante el establecimiento de criterios de inadmisibilidad (MARTINEZ, 2023, p. 11).

Tras todas las consideraciones anteriores, lo cierto es que el Reglamento, en su considerando 10, haciéndose eco de las previas advertencias, reconoce que en el mismo se observa el respeto por los derechos fundamentales y los principios reconocidos en el artículo 6 del CEDH y de los Tratados Internacionales para la Protección de Derechos Humanos, incluyendo el derecho a la libertad y a la seguridad, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de empresa, el derecho a la propiedad, a la tutela judicial efectiva y a un juez imparcial, la presunción de inocencia, el derecho de defensa, y los principios de legalidad y proporcionalidad. Y en su considerando 17, declara que, a fin de garantizar el pleno respeto de los derechos fundamentales, el valor probatorio de las pruebas obtenidas en aplicación del Reglamento deberá ser valorado por un juez competente de conformidad con el Derecho nacional, cuestión esta que era imaginable dada la reticencia del TEDH a establecer una doctrina respecto a cuando debe o no excluirse una prueba por vulnerar el derecho al debido proceso.

De esta forma, al menos el texto final –en relación con la Propuesta inicial– parece haber mejorado mucho al recoger la mayoría de las recomendaciones de los organismos y de la doctrina en relación con las modificaciones que necesitaban operarse en lo que la Propuesta inicialmente contenía.

Así, el artículo 4 del Reglamento, al regular la autoridad emisora, tanto del EPOC, como de la EPOC-PR, señala claramente que la obtención de datos de abonados y de acceso sólo podrán ser recabados por un juez o fiscal competente; y la de datos de tráfico (excepto para obtener datos solicitados con el único fin de identificar al usuario) y de contenido solo podrán ser recabados por un órgano judicial.

Sin embargo, cuando se trata de solicitar la conservación de datos de cualquier tipo, podrá emitirse una orden por un juez, un fiscal o cualquier otra autoridad competente que actúe como investigador en los procesos penales, lo que incluye a los cuerpos y fuerzas de seguridad del Estado. En este último caso, no obstante, la orden deberá ser validada previo examen de su conformidad con las condiciones del Reglamento por un juez o fiscal. En casos de urgencia[29], la policía, o el fiscal podrá solicitar la obtención de

29. Entendiendo por "caso urgente", según el artículo 3.18 del Reglamento, "la situación en la que exista una amenaza inminente para la vida, la integridad física o la seguridad de una persona o para una infraestructura esencial, tal y como se define en el artículo 2, letra a) de la Directiva 2008/114/CE, cuando la perturbación o destrucción de dicha estructura esencial pueda dar lugar a una amenaza inminente para la vida, integridad física o la seguridad de una persona, también mediante perjuicios graves al suministro de productos básicos para la población o para el ejercicio de las funciones esenciales del Estado".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

datos de abonado, con la finalidad de poder identificar al sospechoso sin una previa autorización judicial, pero, ésta deberá emitirse como máximo 48 horas después de la emisión de la orden.

De esta forma, en el proceso de emisión o validación de una orden europea siempre debe intervenir una autoridad judicial. Habida cuenta del carácter especialmente sensible de los datos de tráfico, excepto en el caso de los datos solicitados con el único fin de identificar al usuario, tal y como se definen en el Reglamento, y de los datos de contenido, la emisión o validación de una orden europea de producción para obtener esas categorías de datos requiere el control de un juez. Puesto que los datos de los abonados y los datos solicitados con el único fin de identificar al usuario; tal y como se definen en el Reglamento, son de carácter menos sensible, una orden europea de producción para obtener dichos datos también puede ser emitida o validada por un fiscal competente.

En cuanto a la emisión, la orden se envía al representante legal elegido por el proveedor de servicios y debe tener la forma de certificado, tal y como se señala en el artículo 9 del Reglamento. El certificado es un formulario estandarizado que deberá contener la información a la que se refiere el artículo 5.5 (a-j)[30]. Hay que diferenciar pues, entre la orden y el certificado, puesto que mientras el certificado no exige motivación, la orden sí debiendo ser escrupulosa y razonada en relación con el principio de necesidad y proporcionalidad (TOSZA, 2020, p. 174).

Por último, y respecto del plazo para la preservación de los datos, el Reglamento establece un máximo de 60 días, pero, si se notifica que va a emitirse una orden de obtención de datos (o una OIE), este plazo podrá prorrogarse hasta que se haya emitido la orden correspondiente. En este sentido poco ha cambiado el texto de la Propuesta con el del Reglamento vigente. Ya se criticaba, y con razón, que los datos pueden llegar a estar conservados "el tiempo que sea necesario" (artículo 11.2), lo que en la práctica puede generar problemas en relación con los derechos de los usuarios, de forma que debería haberse establecido un periodo de tiempo limitado para la eliminación de los datos en caso de no solicitase su entrega a la autoridad competente (ROGALSKI, 2020, p. 349).

30. Una orden europea de producción incluirá la información siguiente: (a) la autoridad emisora y, cuando proceda, la autoridad validadora; b) el destinatario de la orden europea de producción a que se refiere el artículo 7; c) el usuario, excepto cuando la única finalidad de la orden sea identificar al usuario, o cualquier otro identificador único como el nombre de usuario, el identificador de inicio de sesión o el nombre de la cuenta a fin de determinar los datos solicitados; d) la categoría de los datos solicitados tal como se definen en el artículo 3, puntos 9 a 12; f) en su caso, el período de tiempo que cubren los datos cuya producción se solicita; g) las disposiciones de Derecho penal aplicables del Estado emisor; en casos urgentes, tales como se definen en el artículo 3, punto 18, las razones debidamente justificadas de la urgencia; h) en los casos en que la orden europea de producción se dirija directamente al prestador de servicios que almacene o trate datos de otro modo en nombre del responsable del tratamiento, una confirmación de que se cumplen las condiciones establecidas en el apartado 6 del presente artículo; i) los motivos para determinar que la orden europea de producción cumple las condiciones de necesidad y proporcionalidad establecidas en el apartado 2; y j) una descripción sucinta del caso.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

3.3. Recursos frente a la Orden Europea de Producción y valoración de la prueba obtenida

El Reglamento recoge, en su artículo 18, la posibilidad de que la persona cuyos datos se hayan solicitado mediante la emisión de una EPOC tendrá la posibilidad de recurrirla. En caso de tratarse del sospechoso o acusado, tendrá derecho a la utilización de vías efectivas de recurso durante la tramitación del proceso penal en el que se estén utilizando los datos.

Este recurso se interpondrá ante el órgano jurisdiccional del Estado emisor y seguirá los cauces establecidos para ello en su Derecho nacional, pero deberá incluir la posibilidad de impugnar la legalidad, la necesidad y la proporcionalidad de la medida. Sin embargo, como De HOYOS entiende muy certeramente, el que los recursos deban solicitarse en el país del Estado emisor de la orden "puede dificultar el ejercicio del derecho de defensa de los afectados cuando sean residentes en el Estado de ejecución" (De HOYOS, 2023, p. 108).

En el apartado 5 del artículo 18, además, se recoge la exigencia de que se respeten los derechos de defensa y equidad del proceso en la valoración de las pruebas obtenidas a través de la orden europea de producción. En este sentido, una vez más, se deja en manos de la normativa nacional la decisión acerca de cuándo debe excluirse una prueba por entenderse obtenida vulnerando derechos fundamentales, cuestión que, como se sabe, no goza de un criterio uniforme en el ámbito de la UE, ni de la doctrina del TEDH.

IV. Conclusiones

Los recientemente promulgados instrumentos europeos con forma de Directiva y de Reglamento, conteniendo las órdenes de producción y de conservación de pruebas electrónicas han introducido, en el ámbito del proceso penal y de la obtención de pruebas electrónicas transfronterizas, una solución inédita y potencialmente más efectiva y eficaz que los variados instrumentos provenientes del Parlamento y la Comisión conocidos hasta el momento.

Y es que, el extraordinario incremento en la utilización –tanto por parte de los servicios de telecomunicaciones tradicionales, como de los consumidores y de las empresas– de los nuevos servicios basados en la red, –que hacen posible la comunicación interpersonal tales como servicios de voz sobre IP, mensajería instantánea de correo electrónico, junto a redes sociales como Facebook y Twitter–, permiten que los datos que compartan los usuarios estén cubiertos, de este modo, por la Directiva. Además, ha de tenerse en cuenta que cada vez resulta más común almacenar los datos en la nube, por lo que no es necesario que los proveedores de servicios tengan servidores en cada jurisdicción, ya que suelen utilizar sistemas centralizados para prestar sus servicios. Las transacciones que realizan las pueden llevar a cabo bien desde el sitio web del mercado en línea o en una página web del comerciante. Todas estas razones explican por qué

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

era tan importante controlar y armonizar la normativa que impusiese obligaciones respecto de los proveedores de servicios, pues es este mercado precisamente el que suele estar en posesión de cualquier tipo de prueba electrónicas que sea necesaria obtener si se abre un proceso penal.

La valoración respecto de la anterior propuesta –en la que no se diferenciaba el tipo de datos y la injerencia en los derechos fundamentales del usuario–, es muy positiva, puesto que, en el vigente Reglamento tanto el proceso de emisión como el de validación de una orden europea queda cubierto por la intervención de una autoridad judicial. Habida cuenta del carácter especialmente sensible de los datos de tráfico, excepto en el caso de los datos solicitados con el único fin de identificar al usuario, tal y como se definen en el Reglamento, y de los datos de contenido, la emisión o validación de una orden europea de producción para obtener esas categorías de datos requiere el control de un juez. Sin embargo, existen otras cuestiones que no alcanzan una valoración tan positiva.

En relación con el valor probatorio de lo obtenido, por ejemplo, y a fin de garantizar el pleno respeto de los derechos fundamentales, se establece que deberá ser valorado por un juez competente de conformidad con el Derecho nacional, y esta cuestión podría haberse resuelto de una vez, estableciendo una normativa uniforme respecto de cuando debe o no excluirse una prueba por vulnerar el derecho al debido proceso, simplemente declarando que la prueba obtenida en circunstancias de urgencia sin el aval posterior de un órgano judicial, por ejemplo, no podrá utilizarse como prueba en ningún tipo de procesos. Por otro lado, también hubiese sido deseable poner un límite temporal al plazo para conservar los datos electrónicos por parte de los proveedores de servicio solicitados. El uso de prórrogas para terminar permitiendo que podrán conservarse los datos "el tiempo que sea necesario" puede generar problemas procesales, pues parece contradecir la prohibición de que dichos datos estén disponibles en el momento de la solicitud de una orden judicial, siempre que exista un proceso penal abierto. Y ello parece que no casar bien con la posibilidad de solicitar la conservación y aseguramiento de una prueba por tiempo indefinido.

Bibliografía

CASTRO SÁNCHEZ, A. (2020). Propuesta de implementación de Carrier-Grade NAT para Guifi.net. Uoc.edu. https://openaccess.uoc.edu/bitstream/10609/118086/7/aaroncastroTFM-0620memoria.pdf

CORHAY, M. (2021). Private Life, personal Data Protection and the Role of Service Providers: The EU E-Evidence Proposal. European Papers, 6.

DE HOYOS SANCHO, M. (2023). Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo". Revista de Estudios Europeos Nº Extraordinario monográfico, *1*.

FRANSSEN, V. (2018). *The European Commission's E-evidence proposal: Toward an EU-wide obligation for service providers to cooperate with law enforcement?* European Law Blog. https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

LARO GONZÁLEZ, E. (2022). Prueba penal transfronteriza: de la orden europea de investigación a las órdenes europeas de entrega y conservación de pruebas electrónicas". Revista de Estudios Europeos, 79.

MARTÍNEZ SANTOS, A. (2023). Admisibilidad mutua de prueba penal transfronteriza en la Unión Europea: La propuesta de Directiva del European Law Institute", en Revista General del Derecho Procesal.

PEERS, S. (2023). *"The proposed European Investigation Order: Assault on human rights and national sovereignty"*, http://www.statewatch.org/analyses/no-96-european-investigation-order.pdf

ROGALSKY, M. (2020). The European commission's e-evidence proposal –critical remarks and proposal for changes. European Jouranl of Crime Criminal Law and Criminal Justice 28(4), 333-353, https://doi.org/10.1163/15718174-bja10018

SAYERS, D. (2011). "*The European Investigation Order. Traveling without a 'roadmap*". En www.ceps.eu.

SERGIO CARRERA, M. S. y. V. M. (2020). *Cross-Border Data Acces in Criminal Proceedings and the Future of Digital Justice. Centre for European Policy Studies* (CEPS). https://www.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf

TOSZA, S. (2020). "*All evidence is equal, but electronic evidence is more equal than any other: the relationship between the European Investigation Order and the European Production Order*". *New Journal of European Criminal la*

Documentos

Conclusiones del Consejo de la Unión Europea, de 9 de junio de 2016, sobre la mejora de la justicia penal en el ciberespacio, ST9579/16.

Dictamen publicado en el Diario Oficial de la Unión Europea de 10 de octubre de 2018 C 367/88

EDPS Opinion on the Proposals regarding European Production and Preservation Orders of electronic evidence on criminal maters. https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf

Fair Trials International "Fair Trials International's response to a European Member States's legislative initiative for a Directive on a European Investigation Order", de 29 de junio de 2010, http://www.statewatch.org/news/2010/jul/eu-eio-ft-briefing.pdf.

Recomendación para la autorización de negociaciones con vistas a un acuerdo entre la Unión y los EEUU de América sobre acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en asuntos penales, de 5 de febrero de 2019 COM (2019) 70 final.https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf

Recomendación para una decisión del Consejo sobre la autorización a participar en las negociaciones de un segundo Protocolo Adicional del Convenio Europeo sobre Cibercrimen (CETS No 185). De 5 de febrero de 2019 COM (2019) 71 final. https://ec.europa.eu/info/sites/info/files/recommendation_budapest_convention.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

Blockchain e implicaciones procesales en materia probatoria*

BLOCKCHAIN AND PROCEDURAL CONSEQUENCES IN THE EVIDENCE

Andrea Martín Meneses
Universidad de la Laguna
alu0101116495@ull.edu.es 0009-0006-9306-6042

Recibido: 16 de octubre de 2023 | Aceptado: 06 de diciembre de 2023.

RESUMEN

La aplicación de las nuevas tecnologías en la Administración de Justicia abre una puerta a la modernización, agilización y simplificación de los trámites procesales. Pese a que muchos consideran que pueden traer consigo una auténtica revolución de esta institución, es fundamental estudiar si realmente estas nuevas tecnologías son compatibles con los principios y garantías inherentes al sistema procesal español y, en caso afirmativo, habría que determinar cuáles son sus límites y en qué procedimientos podría utilizarse.

Una de las más prometedoras actualmente es la tecnología blockchain, un sistema descentralizado basado en el consenso entre los usuarios y caracterizado por la inmutabilidad, la transparencia y la irrevocabilidad. En este trabajo, analizaremos el impacto que la implementación de la tecnología de la cadena de bloques puede ocasionar en el proceso civil, concretamente en materia probatoria, deslindando su caracterización como fuente y medio de prueba en el proceso con base en la normativa hoy vigente.

PALABRAS CLAVE

Blockchain
Nuevas tecnologías
Prueba
Administración de Justicia

ABSTRACT

The application of new technologies in the administration of justice opens the door to the modernisation, streamlining and simplification of court procedures. Although many believe that they can bring about a real revolution in this institution, it is essential to study whether these new technologies are really compatible with the principles and guarantees inherent in the Spanish procedural system and, if so, what their limits are and in which procedures they could be used.

KEYWORDS

Blockchain
New technologies
Evidence
Administration of justice

* Esta publicación es parte del proyecto de I+D+i de Generación de Conocimiento, titulado *Sostenibilidad ambiental, social y económica de la administración de justicia. Retos de la Agenda 2030. (SOST JUST 2030)*, con referencia PID2021-126145OB-I00, financiado por MCIN/AEI/10.13039/501100011033/ y "FEDER Una manera de hacer Europa.

One of the most promising is blockchain technology, a decentralised system based on consensus among users and characterised by immutability, transparency and irrevocability. In this article, we will analyse the impact that the implementation of blockchain technology may have on civil procedure, specifically in terms of evidence, distinguishing its characterisation as a source and means of evidence in the process, taking into account the regulations currently in force.

Blockchain
New technologies
Evidence
Administration of justice

I. Introducción a la tecnología *blockchain*

La tecnología *blockchain* aparece en nuestra sociedad como una auténtica revolución en todos los ámbitos: desde las criptomonedas hasta el sistema sanitario, pasando por las Administraciones Públicas, se ha propuesto su aplicación en infinidad de campos, entre los que destaca el Derecho. *Smart contracts*, *ICOs* (*Initial Coin Offerings*), *DAO (Decentralized Autonomous Organizations*)...son algunas de las fórmulas que han sido ideadas en el ámbito jurídico empleando la tecnología de bloques. Sin embargo, ¿podría esta tecnología implementarse dentro de la Administración Pública, y, en particular, en la Administración de Justicia? Más concretamente, ¿qué papel jugaría la *blockchain* en los procesos judiciales y, en particular, en materia probatoria?

Parece claro que tanto las autoridades europeas, con la aprobación de la *Carta Ética Europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno*, como las españolas así lo creen y consideran fundamental que las Administraciones Públicas se actualicen y hagan uso de todas aquellas tecnologías que puedan agilizar no solo la gestión de la Administración de Justicia, sino también la función jurisdiccional propiamente dicha (Villar Fuentes, 2023, 211), siempre manteniendo todos aquellos principios y garantías que caracterizan a la misma. De hecho, la actual Ministra de Justicia ha destacado que, desde marzo de 2020 hasta junio de este año, gracias a la digitalización de la Justicia, impulsada a raíz de la pandemia, "se han producido más de 920.000 actuaciones procesales no presenciales –entre juicios telemáticos y otros tipos de actuaciones–, lo que ha supuesto un ahorro estimado en desplazamientos de más de 19 millones de euros y se ha evitado la emisión de 9.124 toneladas de CO2, equivalente a 1.382 vueltas al mundo" (Ministerio de Justicia, 2022).

En este sentido, desde hace algunos años se han venido utilizando distintas herramientas electrónicas novedosas de forma satisfactoria, a través de los expedientes electrónicos, que han culminado en el extendido uso de LEXNET[1]. No obstante, aquí no termina la modernización de nuestra Administración de Justicia, ya que en la actualidad se continúa trabajando en esta línea. Ello puede observarse gracias a la tramitación del Proyecto de Ley de Eficiencia Digital del Servicio Público de Justicia, cuyo objetivo

1. Implementado a través del Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia, en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LEXNET.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

fundamental es dar cobertura jurídica y regular la transformación digital del servicio público de Justicia[2]. Sin embargo, la tramitación de este Proyecto de Ley ha quedado suspendida con la convocatoria anticipada de elecciones, por lo que desconocemos si la misma se retomará en el futuro, con la incertidumbre que ello conlleva en este ámbito.

Ahora bien, debe tenerse en cuenta que, a la hora de implementar cualquier tecnología novedosa, cada ordenamiento jurídico, y por lo tanto cada sistema judicial, tiene sus propios principios y estructura. Por ello, es necesario estudiar qué papel puede jugar la tecnología en la Administración de Justicia española. Una de estas tecnologías en auge es la *blockchain*, en relación con la cual se debe ahondar en el impacto que tendría su utilización en la Administración de Justicia española. En particular, debe abordarse el estudio de las consecuencias procesales que traería consigo la aplicación de la cadena de bloques en el seno de la Administración de Justicia, especialmente en materia probatoria con respecto al proceso civil.

Sin embargo, antes de entrar de lleno en los aspectos procesales, conviene explicar primero qué es la tecnología *blockchain*.

II. La *blockchain*

2.1. Breve explicación de la tecnología *blockchain*

La *blockchain* (traducido en español como *cadena de bloques*) es una tecnología novedosa basada en el consenso entre sus usuarios y en la utilización de registros distribuidos (*distributed ledgers*). A lo largo de la historia, todas las transacciones o movimientos entre entidades o personas han sido reflejadas en libros de asientos y anotaciones manejados por Administraciones Públicas, empresas o bancos, entre otros, que actúan como intermediarios o "autoridades centrales" cuando los agentes interesados en la información que ellos manejan la necesitan, por no existir otra forma de acceder a ella debido a que dicha información no es pública o necesita ser validada (Porxas y Conejero, 2018, 25). Por ello, estas "autoridades centrales", poseedoras de información de manera centralizada, se han convertido en intermediarias en quienes todos los usuarios confían, que tienen un control total sobre el sistema e intervienen en todas las transacciones (Boucher, 2017, 5).

Sin embargo, la tecnología *blockchain* pretende revolucionar esta realidad, optando por un sistema descentralizado caracterizado por la inexistencia de una "autoridad central". Se trata de un sistema basado en el consenso entre los usuarios (nodos) que gestionan una base de datos gigante, en vez de en la confianza hacia la entidad poseedora y garante de la información. Por ello, la *blockchain* puede definirse como una tecnología que se fundamenta en una *"base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente"* (Preukschat, 2027, 14 y 15); es decir, es una base de

2. Proyecto de Ley de Eficiencia Digital del Servicio Público de Justicia de 12 de septiembre de 2022. Recuperado de: https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-116-1.PDF

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

datos descentralizada y distribuida que no puede ser alterada. Concretamente, se basa en un modelo que permite que sus usuarios, sin necesidad de que confíen plenamente los unos en los otros, puedan mantener un consenso acerca de la existencia, el estado y la evolución de la cadena de bloques de que se trate, así como de la información que en ella se contiene. De esta manera, se prescinde de la confianza depositada tradicionalmente en las instituciones intermediarias o "autoridades centrales" para transferir esta confianza directamente a la red de nodos que configuran la red *blockchain* y elaboran un registro digital consensuado.

Imaginemos como ejemplo que dos personas (A y B) quieren transferirse mutuamente una cantidad X de dinero. Actualmente, el procedimiento normal sería trasladar dicha cantidad a través de un banco, que actúa como intermediario o "autoridad central", de tal manera que A da la orden a su banco de que transfiera de su cuenta corriente una cantidad de dinero X a la cuenta corriente del banco de B. Esta transferencia, que no se materializa con la transferencia de dinero material sino simplemente con un cambio de saldo de las cuentas de cada uno de los sujetos a través de un programa informático, puede tardar incluso días en realizarse. De hecho, A y B no tienen control alguno sobre este proceso de transferencia de dinero, ya que son los bancos los que controlan toda la operación. Sin embargo, con la tecnología *blockchain* sería posible eliminar estos intermediarios, siendo los propios usuarios, entre los que se encontrarían A y B, los que controlarían el proceso. Este ejemplo no solo es aplicable a transferencias bancarias, sino que también podría serlo a otro tipo de transacciones.

Tal y como explica BARRIO ANDRÉS, la *blockchain "permite a las partes enviar, recibir y almacenar valor o información a través de una red distribuida peer-to-peer de varios ordenadores (o nodos). Cada transacción se reparte por toda la red y se registra en un bloque solo cuando el resto de la red ratifica la validez de la operación basándose en transacciones pasadas teniendo en cuenta los bloques anteriores. Cada bloque sigue al otro sucesivamente, y esto es lo que crea la cadena de bloques*" (Barrio Andrés, 2022, 81).

La tecnología *blockchain* surge en el año 2009 de la mano de Satoshi Nakamoto, quien describió por primera vez un sistema electrónico de pagos sin terceros de confianza y que hizo público bajo el nombre de "*Bitcoin*". Dicho sistema se caracterizaba por la privacidad, volatilidad y descentralización, todo ello a través de una serie de cadenas de bloques que son, en realidad, una compilación de diferentes tecnologías conocidas desde hace tiempo, las cuales sin embargo no habían sido combinadas para su funcionamiento conjunto hasta entonces (redes Peer-to-peer, criptografía asimétrica…) (Gallego Fernández, 2018, 99).

De esta manera, la *blockchain* permite realizar operaciones o transacciones seguras sin la necesidad de recurrir a un intermediario centralizado. A pesar de que su utilidad primigenia estuvo ligada a la actividad económica, tras haberse descubierto sus beneficios relativos a la seguridad, inmutabilidad, transparencia y confianza, se fue aplicando en otros sectores, como el sanitario, el bancario, el energético, el logístico, el asegurador y el legal, entre otros (Badiola Coca, 2022, 290).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

2.2. Principios caracterizadores de la *blockchain*

Como hemos indicado, la *blockchain* se trata de un libro digital compartido, conformado por una serie de bloques conectados y almacenados en una red distribuida, descentralizada y protegida mediante criptografía, siendo un depósito de información que se almacena de forma incorruptible e irreversible (Pacheco Jiménez, 2019, 63). De esta definición se desprenden los siguientes principios caracterizadores de esta tecnología (Porxas y Conejero, 2018, 28):

a) Principio de inmutabilidad. Como hemos señalado, la tecnología *blockchain* se basa en el encadenamiento sucesivo de bloques mediante la criptografía (a través del empleo de *hashes*[3]). Este encadenamiento sucesivo es inmutable ya que, si un nodo decidiera modificar el contenido de la cadena de bloques alterando una transacción que ya se ha realizado y se ha incluido en un bloque, ello sería detectado inmediatamente, debido a que el contenido de su versión del libro registro variará. De esta forma, el resto de nodos denegarán el registro de cualquier otra nueva transacción que pretenda incluir este nodo en su versión, debido a que esta no coincidirá con el contenido del libro registro que tienen el resto de nodos.
b) Principio de irrevocabilidad. Debido a lo anteriormente indicado, cuando una información se incorpora a una red *blockchain*, no es posible eliminarla (salvo ciertas excepciones), ya que desde que esta se incorpora a la red, esta información es poseída por todos los usuarios, debido a que se distribuye de manera automática a todos y cada uno de los nodos que intervienen en la red.
c) Principio de transparencia. En una red *blockchain*, todos los usuarios tienen acceso al que se ha denominado libro registro (o libro digital compartido), por lo que todos ellos tienen acceso a la información sobre todas las transacciones efectuadas. De hecho, en determinados tipos de redes, existe la posibilidad de que incluso los usuarios que no forman parte de la red puedan también consultar el contenido de la cadena de bloques, como es el caso de las redes públicas de Bitcoin o Ethereum. Todo ello ocurre debido a que se emplea un protocolo informático de código abierto, que hace accesible la red de manera prácticamente universal.

Sin embargo, esta transparencia no supone la identificación del autor de las transacciones en todos y cada uno de los casos, debido a que en algunas de las redes, los usuarios no se identifican de forma personal para acceder y operar en la red *blockchain*.

3. Un *hash* es una concatenación de caracteres alfanuméricos resultantes de aplicar un algoritmo matemático sobre un archivo u objeto digital, siendo único el *hash* para cada archivo u objeto al que se le aplica, por lo que tienen una función de identificación de cada uno de los bloques de datos. De esta manera, cada *hash* es inmutable además de unidireccional, por lo que puede calcularse el *hash* de un archivo mediante el algoritmo aplicable, mientras que no puede obtenerse el archivo digital a partir del *hash*. En caso de que se modifique el contenido del archivo, el *hash* asociado a este variará también. En un lenguaje coloquial, podríamos decir que el *hash* de un archivo u objeto digital es como la matrícula que identifica a un coche.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

En estos casos, las transacciones son visibles a todos los que acceden a la red, pero se vinculan a un código de identificación que, en muchas ocasiones, no revela la identidad concreta del sujeto que realiza la transacción.

Estos principios característicos de la tecnología *blockchain* deben completarse con las características propias de los distintos tipos de redes *blockchain* que existen en la actualidad, tal y como explicaremos a continuación.

2.3. Tipos de redes *blockchain*

Una vez explicada de manera sucinta qué es la tecnología *blockchain* y cuáles son sus características básicas, podemos adentrarnos en los tipos de redes blockchain, que actualmente son dos: las públicas y las privadas (Preukschat, 2017, 18 a 20).

a) *Blockchains* públicas. Las redes *blockchain* públicas (*blockchain* sin permiso o *permisionless,* en inglés) se caracterizan porque cualquier persona, sin ser usuario, puede acceder y consultar las transacciones efectuadas en la cadena de bloques. Este tipo de redes son abiertas, de tal manera que cualquiera puede convertirse en usuario (nodo). Asimismo, se caracterizan por su descentralización, es decir, que no existen usuarios que tengan más poder que otros en la red ya que todos los nodos son, una vez incorporados en la red, iguales entre sí, por lo que no existe una jerarquía entre ellos. Otra de las características de las redes públicas es que son pseudo anónimas, es decir, que los nodos que realizan las transacciones no son identificables personalmente, aunque sí pueden rastrearse sus direcciones. Cualquiera, en este tipo de redes, puede consultar la información almacenada en ella, incorporar nueva información realizando transacciones o incluso participar en la construcción de la propia cadena mediante el minado de bloques (Gallego Fernández, 2018, 121). Un ejemplo de cadena de bloques pública es Bitcoin, ya que es libremente accesible por cualquiera, sin más requisitos que disponer de un dispositivo adecuado y conexión a internet.
b) *Blockchains* privadas. A diferencia de las *blockchain* públicas, las redes *blockchain* privadas (*blockchain* con permiso o *permissioned*, en inglés), las transacciones realizadas y datos almacenados solo pueden ser consultados por los participantes o usuarios de la red, de tal manera que se dice que son redes cerradas, debido a que solo las personas o entidades invitadas a participar en ellas adquieren la condición de usuarios, que pueden situarse en diversos niveles dependiendo de los accesos concedidos, motivo por el que unos usuarios pueden ser registradores (cuando se les concede la capacidad de registrar información), otros ser exclusivamente verificadores de los cambios producidos en la cadena de bloques, mientras que otros pueden tener prohibida estas facultades y solo se les da la posibilidad de consultar la información previamente registrada y verificada. Debido a sus características, todos los nodos se conocen, aunque una *blockchain* privada puede establecer el nivel de anonimato que se necesite para

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

realizar o proteger transacciones, motivo por el que los usuarios que registran anotaciones pueden estar o no identificados.

Como diferencia fundamental entre ambos tipos de redes podemos destacar que, mientras que la *blockchain* privada es distribuida, puesto que es una base de datos repartida entre varios nodos, la pública es descentralizada, ya que en ella no se controla quién participa en la misma, motivo por el que cualquier usuario puede participar en ella libremente. Teniendo en cuenta el desarrollo de las redes de cadenas de bloques, es probable que en un futuro no solo existan este tipo de redes, sino que se creen nuevos tipos de *blockchain, l*os cuales adquirirán la caracterización de redes híbridas, al adoptar características de ambos tipos de *blockchain*, dependiendo del tipo de uso para el que fueren creadas.

2.4. Posibles aplicaciones de *la blockchain*

A pesar de que la *blockchain* es una tecnología novedosa, han sido muchas las interesantes aplicaciones propuestas para ella en distintos sectores económicos, entre los que podemos destacar:

— **Criptomonedas:** en la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, en su artículo primero apartado d) se define a las "monedas virtuales" como la "*representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos*" (Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018). Estas monedas se han venido desarrollando mediante la aplicación de la tecnología *blockchain*, cuyo objetivo es precisamente el prescindir de una "autoridad central" o intermediario, a través de un sistema de apuntes contables en un registro electrónico digital compartido entre los usuarios de la red, quienes les atribuyen un valor. Encontramos cientos de criptomonedas, siendo la más conocida Bitcoin, creada en 2009 y diseñada como medio de pago entre aquellos que aceptan esta moneda como tal, con un número de emisión finito de 21 millones de BTC, y Ethereum, creada en 2015 y con una emisión anual limitada de 18 millones de unidades (Irish Department of Finance, 2018, 2). En este caso, la red Ethereum permite operaciones más allá del mero pago, admitiendo que sobre su estructura operen ciertos *smart contracts* (Porxas y Conejero, 2018, 29 y 30).

— ***Smart contracts:*** se define como el contrato celebrado "*a través de una página web accesible para las partes cuya forma está constituida por la interfaz de usuario de la aplicación externa y uno o varios programas autoejecutables (smart contracts) residentes en la cadena de bloques con capacidad para actuar recíprocamente con*

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

dicha interfaz" (Tur Faúndez, 2018, 60). En su etapa inicial, su creador, Nick Szabo (Szabo, 1997) los concebía como programas ejecutables que, mediante protocolos informáticos, automatizarían la ejecución de una serie de cláusulas contractuales previamente acordadas por las partes, quienes son desconocidas entre sí, cuando se dieran una serie de condiciones. Un ejemplo de *smart contract* en su etapa primitiva son las máquinas de *vending* o máquinas expendedoras, en la que las partes realizan una compraventa sin la necesidad de conocerse y coincidir en el espacio y el tiempo. Sin embargo, en la actualidad, los *smart contracts* se alejan un poco de la idea inicial de Szabo, ya que realmente se trata de algoritmos informáticos que ejecutan automáticamente una serie de operaciones en caso de que se verifique la concurrencia de las condiciones predefinidas por las partes. Por este motivo, se discute si los *smart contracts* tienen verdadera naturaleza contractual; en este sentido, aunque la mayoría de la doctrina coincide en que pese a que su naturaleza no es puramente contractual, esta aplicación del *blockchain* sí que puede ayudar a la ejecución de los contratos, permitiendo un ahorro significativo en costes operativos y asociados a la ejecución de los mismos (Viedma Cabrera, 2021, 624). De hecho, se ha planteado la posibilidad de aplicar la tecnología de los *smart contracts* al pago de indemnizaciones por parte de las compañías aseguradoras de manera automática cuando se verifique la concurrencia de las condiciones pactadas por las partes, tal y como propuso, por ejemplo, la compañía aseguradora AXA, que ofrecía un seguro de viaje que automatizaba la liberación de compensaciones a los pasajeros de un vuelo si se comprobaba que este llegaba a su destino con un retraso superior a lo estipulado (Viedma Cabrera, 2021, 659). Asimismo, se ha propuesto la utilización de esta tecnología para los préstamos dirigidos a financiar la compra de un coche, de tal forma que si el prestatario incumple una mensualidad, el algoritmo del *smart contract* impediría el uso del coche (Barrio Andrés, 2022, 83). Los *smart contracts* podrían, de esta forma, agilizar e incluso evitar la necesidad de acudir a un proceso judicial declarativo y de ejecución, ya que permitirían la ejecución privada del contrato, suponiendo una medida muy interesante para la agilización procesal de la Administración de Justicia que tanto se necesita actualmente.

— **ICO *(Initial Coin Offerings)*:** se trata de una vía de financiación empresarial consistente en la oferta de *tokens* a cambio de criptomonedas, realizada por empresas de reciente creación con el objetivo de buscar capital para desarrollar su proyecto. Mediante las ICO, estas empresas ofrecen *tokens* en vez de acciones de manera global a inversores de todo el mundo, por lo que los adquirentes de aquellos se convierten en un nuevo tipo de "accionistas", cuyos tokens pueden representar capital o deuda de la empresa como inversión simbolizando la propiedad de un activo, lo que daría derecho a un interés participativo en futuros ingresos o en el posible aumento de valor de la entidad emisora o negocio (tokens de valor o *security tokens*) o un derecho de uso de un producto o servicio (tokens de utilidad o *utility tokens*), sin ser una inversión sino, más bien, un modo de acceso futuro a un producto o servicio aún no lanzado al mercado. Sin

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

embargo, la participación en una ICO no da derecho a unas acciones ya que no implica la participación en dividendos ni tampoco se trata de un *crowdfunding* como tal, sino que es una nueva fórmula en la que el inversor adquiere un token que le confiere un derecho de uso sobre una nueva plataforma o negocio, los cuales en la mayoría de los casos ni siquiera existen en el momento de la inversión. Actualmente, las ICOs se caracterizan por su incertidumbre regulatoria, ya que a pesar de que en algunos países como China o Corea del Sur han sido declaradas ilegales, en otros como Estados Unidos, Suiza o Reino Unido no lo han sido, pero tampoco están reguladas de manera clara. En España, por su parte, se han elaborado una serie de documentos para establecer una regulación mínima de bases por la Comisión Nacional del Mercado de Valores (CNMV) (Pacheco Jiménez, 2019, 69 a 74). Por todo ello, y teniendo en cuenta lo arriesgado y volátil del producto, las amenazas de seguridad, la posibilidad de evasión fiscal y fraude, consideramos que debe desarrollarse y regularse aún más para que esta aplicación de la tecnología *blockchain* esté dotada de la suficiente seguridad jurídica y pueda llegar a tener relevancia en nuestro mercado empresarial.

— **DAO *(Decentralized Autonomous Organizations)*:** este tipo de estructuras se trata de sociedades sin personalidad jurídica y descentralizadas, en las que el poder de decisión reside en los titulares de tokens que han sido emitidos a través de una ICO, quienes pueden presentar, aceptar y ejecutar propuestas, modificar reglas de votación e incluso transferir rendimientos de la sociedad. De esta manera, se elimina el factor humano, al considerar que estos son más proclives a la vulneración de las normas y a la comisión de delitos, por lo que la gestión de la entidad se realiza mediante el empleo de *smart contracts*, automatizando la mayoría de procesos y decisiones que se vienen tomando por los administradores o socios de una sociedad convencional (Pacheco Jiménez, 2019, 80 a 82). Las DAO cuentan con unos estatutos formalizados y codificados a través de *blockchain,* los cuales solo pueden ser modificados en caso de que una cantidad determinada de los titulares de tokens de la organización voten a favor de dicha alteración (Navarro Lérida, 2018, 3). Se prevé que aumenten su importancia en un futuro, aunque actualmente, como hemos visto, se caracterizan por su vulnerabilidad en materia de seguridad frente a hackeos, así como en su falta de regulación jurídica.

— **Registro de trazabilidad:** gracias a la inmutabilidad de las transacciones anotadas en la red otorgada por la tecnología *blockchain,* esta permite la creación de una "identidad digital" para cada elemento que se registra en la cadena de bloques, permitiendo la elaboración de un historial propio y trazable, especialmente aplicable para la identificación y seguimiento del origen y cadena de custodia de bienes materiales (ej: tabaco, alimentos, bienes de gran valor…). También podría emplearse esta tecnología para el seguimiento de bienes inmateriales, como las obras artísticas en soporte digital, pudiendo verificar y acreditar su autenticidad, autor, transmisiones, actos de explotación, licencias obtenidas… De hecho, muchos autores consideran que este registro de trazabilidad,

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

complementado con las monedas virtuales y *smart contracts* podrían facilitar la gestión de derechos económicos y de explotación de las obras con derechos de autor (Porxas y Conejero, 2018, 32). Asimismo, se ha planteado la posibilidad de creación de nuevos tipos de registros, concretamente aquellos dedicados a activos de cierto valor, como pueden ser los diamantes u otros activos de especial valor que actualmente son casi imposibles de rastrear (Arruñada, 2018, 18), como sugiere la iniciativa *Everledger* [4].

Además de todas estas aplicaciones de la tecnología *blockchain* vinculadas al mundo del Derecho, podemos destacar diversos usos relevantes tanto en esta área como en otras ramas de conocimiento, como la de la salud, el sector automovilístico, el bancario, etc. Sin embargo, centraremos nuestro estudio en la posible aplicación de la *blockchain* en el ámbito de la Administración de Justicia española.

III. Aplicación de la *blockchain* en la administración de justicia española

Con el paso de los años, nuestra sociedad se va desarrollando e incorporando paulatinamente nuevos elementos tecnológicos que le permiten mejorar los procesos que en ella se producen. Echando la vista atrás, podemos ver como todas las revoluciones que la humanidad ha vivido, y especialmente tras la tercera revolución o "Revolución digital" que tuvo lugar a finales del siglo XX con la llegada de las telecomunicaciones, la tecnología de la información y la electrónica, han supuesto un avance gigantesco en distintos ámbitos de la vida. De esta manera, se demuestra que la sociedad siempre está en movimiento, se va reinventando y acogiendo nuevas formas de hacer las cosas. Sin embargo, parece que la Administración de Justicia española aún no ha sido testigo de esta gran transformación ya que, pese a que se han ido incorporando distintas novedades tecnológicas que han supuesto una mejora sustancial en sus procesos internos, tal y como explica el Proyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia con la introducción de innovaciones en los Tribunales como son la incorporación de la ofimática en los Juzgados (Barona Vilar, 2023, 1), la Sede Judicial Electrónica, LEXNET, las subastas judiciales electrónicas, etc., su "revolución" no termina de fraguar. Es por ello que ahora, en la cresta de la ola de la "Cuarta revolución industrial", que estamos viviendo actualmente, en la que destacan tecnologías como la robótica, la inteligencia artificial o el *blockchain*, entre otros, es el momento perfecto para plantearnos no solo qué tipo de sociedad queremos y estamos construyendo, sino también qué tipo de Justicia es la que queremos diseñar, consolidar y garantizar (Barona Vilar, 2022, 77).

4. *Everledger* es un libro de contabilidad (ledger) global y digital que monitorea y protege artículos de valor mediante la *blockchain*. Fue una iniciativa que ganó el concurso de startups de BBVA y que fue incluida en el ranking The FinTech 50 del año 2016.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

Sin embargo, la aplicación de las nuevas tecnologías en el ámbito de la Administración de Justicia puede no solo provocar un aumento de la efectividad, eficacia y una mejora en el acceso a la Justicia por parte de los ciudadanos, sino que además puede negar, limitar y restringir derechos inherentes a los mismos. De hecho, la implementación de novedades tecnológicas en este ámbito es todo un reto para el derecho procesal, ya que herramientas como la *blockchain* pueden ser utilizadas para incorporar en el proceso civil la prueba sobre la existencia de un documento, sobre su fecha exacta, su contenido concreto, permitiendo analizar su trazabilidad y su veracidad. No obstante, al no existir actualmente una regulación en relación con su incorporación al proceso de las nuevas tecnologías, es fundamental estudiar las consecuencias que la utilización de las mismas en los tribunales de justicia pueda tener sobre los derechos y garantías que asisten a los ciudadanos.

En este trabajo nos centraremos exclusivamente en la implementación de la tecnología *blockchain* en el proceso ya que, en caso de que pueda afirmarse que existe una inmediata correlación entre la información que accede a dicha base de datos y la autenticidad de su contenido por el mero hecho de hallarse registrada en una cadena de bloques, sería una auténtica revolución en el sistema probatorio (Ríos López, 2022).

No obstante, antes de entrar a valorar en qué medida la *blockchain* puede emplearse como prueba en el proceso, debemos traer a colación la distinción que hace CARNELUTTI (Carnelutti, 1955) entre las fuentes y los medios de prueba en el Derecho Procesal.

En este sentido, GÓMEZ COLOMER explica que es necesario distinguir entre los hechos de la vida y cómo introducir estos hechos en el proceso.

El primer punto hace referencia a las fuentes de prueba, a los hechos, datos y circunstancias de la vida (Gómez Colomer, 2022, 234). Son fuentes de prueba todos aquellos instrumentos que contienen información o datos relevantes al margen de la realidad procesal, siendo estas un concepto extrajurídico que se corresponde con una realidad anterior y distinta al proceso.

Por su parte, cómo se introducen estos hechos en el proceso hace referencia a los medios de prueba. Los medios de prueba son todos aquellos instrumentos que la legislación procesal reconoce como mecanismos aptos para introducir las fuentes de prueba en el proceso, permitiendo a las partes con el Juez, o excepcionalmente a este solo, llegar a la convicción de la certeza positiva o negativa de las afirmaciones fácticas que se han de fijar como verdaderas, falsas o dudosas, a los efectos del proceso (Díaz Martínez, 2021, 394). Son, por tanto, un concepto jurídico que solo existe en el proceso y que determina cuáles son los instrumentos o actividad que permiten la introducción de las fuentes de prueba en el proceso judicial, cuya finalidad es la de convencer al juzgador de la existencia o no del hecho objeto de prueba. Los medios de prueba admitidos en el proceso civil son los reconocidos en el artículo 299 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante, LEC), es decir: (i) interrogatorio de partes, (ii) documentos públicos, (iii) documentos privados, (iv) dictamen pericial, (v) reconocimiento judicial, (vi) interrogatorio de testigos y (vii) medios de reproducción del sonido o la imagen e instrumentos de archivo.

Asimismo, el apartado tercero de este artículo permite que, cuando por cualquier otro medio no expresamente previsto en los apartados anteriores se pudiera obtener

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias. Este último inciso deriva del art. 24 CE, en el que se promulga como derecho fundamental el que todas las personas puedan hacer valer los medios de prueba pertinentes en aras de impulsar una actividad probatoria de acuerdo con sus intereses[5]. Sin embargo, el mismo ha causado una discusión doctrinal sobre si constituye un *numerus apertus o un numerus clausus* de medios de prueba. Si bien del tenor literal puede entenderse que el mismo constituye una enumeración abierta de medios de prueba, autores como GIMENO SENDRA consideran que existe una posibilidad muy infrecuente de "inventar" el juez nuevos medios de prueba, por lo que dicho apartado no debe entenderse a favor de la opción de numerus apertus de los mismos (Gómez Colomer, 2022, 235).

La *blockchain* da constancia de varios hechos relevantes de la transacción, como son la realidad, el sujeto titular y el sellado de tiempo de la misma. Estos tres aspectos pueden ser introducidos en el procedimiento mediante la utilización del soporte electrónico en el que los mismos se encuentran registrados. Sin embargo, es importante estudiar no solo su consideración como medio de prueba en el proceso, sino también como fuente de la misma.

3.1. La cadena de bloques como fuente de prueba

Teniendo en cuenta las características inherentes a la tecnología *blockchain,* como pueden ser su inmutabilidad, irrevocabilidad y transparencia, entendemos que esta puede utilizarse como fuente de prueba, similar a cualquier otro soporte electrónico. De hecho, desde el punto de vista del derecho probatorio, el valor de esta fuente de prueba es indiscutible, pues ¿qué fuente de prueba es mejor que una inmutable por definición (Badiola Coca, 2022, 309)?

Son varios los autores que opinan que la tecnología *blockchain* puede tener valor probatorio, más teniendo en cuenta que, como hemos indicado, debido a su inmutabilidad, proporciona una seguridad jurídica relevante al no poder alterarse los datos contenidos en la cadena de bloques, siendo especialmente útiles a la hora de probar la identidad de las partes de la operación llevada a cabo mediante la tecnología de la cadena de bloques[6], el contenido de los datos registrados, la autenticidad de las firmas (Ibáñez Jiménez, 2018, 4) y la fecha y hora de la operación, debido a que cada *hash* posee una firma con registro temporal o *time stamping,* que determina este extremo (Llopis Benlloch, 2017). Puede afirmarse, por tanto, que la tecnología *blockchain* garantiza la integridad de la información contenida en la cadena de bloques al no poder modificarse,

5. Véase F.J 3º de SSTC 173/2000, de 26 de enero y F.J. 2º de SSTC 1/2004, de 14 de enero.

6. Pese a que puede pensarse que la cadena de bloques otorga anonimato con respecto al nodo, es preciso destacar que en realidad se trata de una pseudoanonimidad, ya que en todos los casos, los nodos pueden identificarse mediante las direcciones IP (en caso de redes públicas anónimas) o directamente conociendo los datos del usuario (en la mayoría de redes privadas, en las que suelen conocerse los nodos actuantes en la red).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

lo cual serviría para afianzar la veracidad y certeza de determinados medios de prueba, siendo una tecnología útil tanto para el juez como para las partes en el juicio (Cerdá Meseguer, 2020, 146).

Sin embargo, otros autores como BUENO DE MATA, destacan que la *blockchain* es una fuente de prueba difícil de encajar en alguno de los medios de prueba recogidos en el art. 299 LEC, motivo por el que no están de acuerdo con que se introduzca en el proceso por medio de la documental electrónica, ya que de esta manera se lanzaría un mensaje erróneo a la sociedad, haciendo pensar que todo puede documentarse, algo que la tecnología *blockchain* pretende evitar (Bueno de Mata, 2021).

La primera postura, en la que se considera que la *blockchain* puede tener valor probatorio e incorporarse en el proceso tal y como indicaremos a continuación, es la que consideramos más acertada teniendo en cuenta que el derecho procesal debe adaptarse a la realidad existente e ir adoptando nuevas fuentes de prueba que, además proporcionan mayor inmutabilidad y, por tanto, seguridad jurídica.

La información que se contiene en los distintos bloques validados en la red se encuentra distribuida entre una cantidad enorme de mineros, ya que cada integrante de la cadena tiene en su ordenador, una copia de todas y cada una de las operaciones que se han llevado a cabo en la red por lo que no puede en ningún caso hablarse de "anonimato" de las operaciones, ya que de las mismas quedará inequívoca constancia y no solo en uno o dos soportes, sino en todos los que integran la cadena de bloques en la que se ha llevado a cabo dicha transacción. De ahí su reconocida "eficacia probatoria" en el caso de que alguna red blockchain o smart contract deba llegar a juicio (Calaza López, 2022, 252).

Ahora bien, en ningún caso puede pensarse que la introducción de la *blockchain* en el proceso es una cuestión fácil de dirimir, ya que la misma plantea una serie de interrogantes y cuestiones que, como veremos, para nada están resueltos ni serán fáciles de resolver.

3.2. La cadena de bloques como medio de prueba

Pese a la discusión doctrinal planteada, está claro que, por el momento, la tecnología *blockchain* es una fuente de prueba aún muy novedosa, por lo que en caso de que fuera necesaria su introducción en el proceso, muchos entienden que lo más probable es que se inserte mediante una documental (ya que, en esencia, podría encajar como un registro de datos distribuido compuesto por la concatenación de distintas transacciones digitales) y una pericial informática, que proporcionará al juez los conocimientos necesarios para poder interpretar la cadena de bloques, así como para determinar su autenticidad e inmutabilidad.

La prueba documental supone un soporte apto para incorporar al proceso las fuentes de prueba electrónicas, ya que toda la información registrada en la cadena de bloques no deja de conformar un documento, con la singularidad de que aparece plasmado en un soporte informático (Ríos López, 2022, 6). En nuestro ordenamiento jurídico podemos distinguir dos tipos de pruebas documentales: la pública y la privada.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

3.2.1. La *blockchain* como documento público

Una de las posibilidades que se manejan es la de otorgar a la cadena de bloques el valor probatorio que la normativa procesal concede al documento público, siendo estos, tal y como expone el listado de *numerus clausus* contenido en el art. 317 LEC, aquellos expedidos por autoridades, ya sean judiciales, notariales o registradores, legitimadas para certificar, en el ámbito de sus competencias, la autenticidad de dichos contenidos.

Al no certificarse las redes *blockchain* por fedatario público, atendiendo al tenor literal de la ley, no podría ser equiparado a la documental pública, la cual haría prueba, aun contra tercero, del hecho que motiva su otorgamiento y de la fecha de este.

Un ejemplo sería el de las certificaciones registrales, tradicionalmente aportadas como prueba documental en juicio. El artículo 319 LEC establece que las certificaciones expedidas por los registros de la propiedad de los asientos registrales harán prueba plena del derecho, acto o estado de cosas que documenten, la fecha en que se produce esa documentación y de la identidad de los fedatarios y demás personas que intervengan en ella. En este sentido, es posible plantearse si, con la aplicación de la tecnología *blockchain* en el sistema registral español, tal y como se ha venido proponiendo por diversos autores con la creación de redes *blockchain* en las que los notarios y registradores participaran en la misma como nodos validadores, esta presunción legal podría verse afectada.

Atendiendo al artículo 41 del Reglamento (UE) 910/2014, de 23 de julio, sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior, solo los sellos de tiempo electrónico verificados por un prestador cualificado de servicios de confianza gozan de presunción legal de exactitud respecto a la fecha, hora indicada y los datos vinculados. Por tanto, en el caso de la *blockchain*, al no existir tal prestador, no regirá esta presunción de exactitud. Sin embargo, la doctrina viene entendiendo que el documento público electrónico notarial produce efectos probatorios plenos ya que, gracias a la intervención del fedatario público, se le puede aplicar esta presunción de exactitud.

Es por ello que, *lege ferenda*, en el caso de que se propusiera en juicio como prueba un documento público electrónico registral o notarial basado en la *blockchain* privada o híbrida en la que estos profesionales actuaran como nodos en la red, debería regir esta misma presunción de exactitud ya que, ante la imposibilidad de que la cadena de bloques sustituya al registro de la propiedad, el registrador deberá continuar con su función calificadora cada vez que se pretenda registrar un título o derecho, por lo que encontraríamos la figura verificadora necesaria para la aplicación de la presunción legal de exactitud que se viene imputando a los prestadores de servicios de confianza *lege lata*. Entendemos que esta previa labor calificadora del registrador, junto con las características de seguridad, inmutabilidad, trazabilidad, irrevocabilidad y transparencia inherentes a la tecnología *blockchain*, son suficientes para justificar la aplicación de la presunción de exactitud y prueba plena que actualmente se viene aplicando a la documental pública *ex* art. 319 LEC, a aquellos documentos públicos expedidos por el registrador de la propiedad y notarios, entre otros, que incorporen la tecnología *blockchain*

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

en su sistema interno, ya que ello proporcionará una seguridad jurídica aún superior a la que ya ofrecen estas instituciones públicas ante los tribunales de justicia y en el tráfico jurídico en general.

3.2.2. La *blockchain* como documento privado

Pese a que actualmente no existe jurisprudencia en España que reconozca expresamente el valor probatorio del contenido de la *blockchain* (aunque nada impide que se pueda aceptar), parte de la doctrina considera que la opción más adecuada para introducir una red *blockchain* como prueba en un procedimiento judicial será como documento electrónico con valor de documento privado *ex* art. 326 LEC, en relación con los artículos 23 y 24 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante, la LSSICE) (Bandín Barreiro y Molina Álvarez, 2020, 102 y 104), que establecen que la forma electrónica equivale a la forma escrita, añadiendo que el soporte electrónico en el que conste un contrato electrónico será admisible en juicio como prueba documental.

En el caso de la *blockchain,* la aportación de la misma al proceso como prueba documental privada se haría mediante la impresión del "*hash*", es decir, de la clave alfanumérica asociada al contenido en concreto, así como su "traducción al lenguaje humano" (Ríos López, 2022, 6).

Ahora bien, hay que tener en cuenta, atendiendo a lo dispuesto en el art. 326.1 LEC, que los documentos privados hacen prueba plena en el proceso, siempre y cuando su autenticidad no sea impugnada por la parte a quien perjudiquen. Pese a que la probabilidad de impugnación de la autenticidad de la firma de la *blockchain* es baja dada las características inherentes a esta tecnología, como hemos mencionado, el artículo 326.2.II LEC permite la proposición de cualquier medio de prueba que resulte sirva para impugnar la autenticidad de las documentales privadas (Ibánez Jiménez, 2018, 4), cuando resulte útil y pertinente al efecto.

Para poder conocer si se ha mantenido la cadena de custodia de un archivo digital propuesto como prueba en el procedimiento, suele emplearse una prueba pericial informática que determina si en la práctica de la prueba se está ante el mismo archivo electrónico que se propuso en su día. Para ello, se utiliza el código *hash*, obtenido mediante la aplicación de un algoritmo del cual se consigue un valor alfanumérico inmutable. En caso de que se haya modificado un solo aspecto del conjunto de datos sobre el que se ha aplicado el algoritmo que da lugar al *hash,* este variará, por lo que se determinará si la evidencia digital se ha mantenido indemne, y por tanto sirve como prueba, o si, por el contrario, ha sido manipulada, evidenciando una ruptura de la cadena de custodia. En caso de que se verifique la falta de coincidencia entre el archivo original y aquel sobre el que se practica la prueba, ello sería suficiente para desvirtuar el resultado probatorio en juicio.

Autores como SÁNCHEZ-RUBIO aconsejan, debido a que la parte que aporta la evidencia electrónica es la que tiene la carga de probar su autenticidad en caso de impugnación *ex*

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

art. 326.2 LEC, la realización de una copia exacta del contenido de la prueba electrónica incluso antes de su impugnación mediante un clonado de la misma ante testigos o fedatario público, empleando los instrumentos tecnológicos y procedimientos adecuados para ello. El trabajo del perito informático, en su caso, consistirá tanto en el cálculo del *hash,* para observar si ha sido o no manipulada la prueba electrónica, como en la preservación de la fuente de prueba (Sánchez Rubio, 2019, 296).

Por otro lado, hay que tener en cuenta que, en caso de que no se pudiera deducir su autenticidad o no se hubiera propuesto prueba alguna, el art. 326.2 *in fine* LEC determina que el tribunal lo valorará conforme a las reglas de la sana crítica.

Finalmente, cabe destacar que, en la actualidad, en nuestro sistema procesal y de cara a evitar posibles impugnaciones, es conveniente que el documento privado aportado al proceso se acompañe de un dictamen pericial elaborado por un técnico experto en *blockchain*, de cara a certificar la autenticidad de los datos incorporados en la cadena de bloques, en particular los aspectos criptográficos, así como la equivalencia entre la huella digital y el dato que existe en el mundo "real".

Sin embargo, la conveniencia o necesidad de aportar este dictamen pericial no supone la exclusión de la posible valoración del medio de prueba documental por parte del juez, sin necesidad de aportación de dictámenes adicionales (Ríos López, 2022, 7 y 8).

IV. Evolución previsible y principales interrogantes a plantear

La utilización de la tecnología *blockchain* como medio de prueba en la Administración de Justicia española plantea aún interrogantes, aunque son especialmente preocupantes dos de ellos:

El primero es el reto derivado del anonimato de los usuarios, ya que cualquier sujeto que registra transacciones a través de la *blockchain* pública, opera mediante claves criptográficas públicas y privadas que garantizan la privacidad del usuario, lo cual puede impedir establecer una conexión entre la persona física que actúa y el usuario que accede a la red, es decir, una correlación entre la identidad física y la identidad virtual (Ríos López, 2022, 5). Sin embargo, a pesar del temor por dicha especie de "anonimato" es importante tener en cuenta que realmente se trata de una pseudoanonimidad, ya que en todos los casos, los nodos pueden identificarse mediante las direcciones IP de los ordenadores desde los que actúan (en caso de redes públicas anónimas) o directamente conociendo los datos del usuario (en la mayoría de redes privadas, en las que suelen conocerse los nodos actuantes en la red).

Otro interrogante que surge es el de la integridad del contenido de la cadena de bloques. Al no acceder a la cadena de bloques el documento completo, sino simplemente la huella digital o el "*hash*" que lo representa, la autenticidad del contenido se limita a que la misma se traduzca al lenguaje natural mediante la clave criptográfica alfanumérica que lo revela, por lo que una de las cuestiones es también que dicha traducción se realice de forma correcta mediante su decodificación por un perito informático.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

En segundo lugar, otra de las cuestiones problemáticas que se suscitan se centra en el coste que supone el minado de los bloques en la actual red *blockchain*. De hecho, para minar un solo bloque dentro de la red Bitcoin, se estima que el proceso dura aproximadamente unos 10 minutos. Por ello, son muchos los que consideran que los costes de procesamiento y "traducción" de los *hashes*, así como la energía que se requiere para ello, son demasiado elevados, algo que debe tenerse en cuenta a la hora de determinar si realmente es apropiado implementar la tecnología *blockchain* en procedimientos tan reiterados y numerosos como los que se llevan a cabo tanto en las instituciones públicas como en la Administración de Justicia. Sin embargo, debe tenerse en cuenta que la tecnología de la cadena de bloques es aún muy novedosa, por lo que en el futuro probablemente se desarrollen métodos para disminuir los costes actuales y agilizar mucho más el proceso de minado. De hecho, poco a poco van creándose sistemas con un funcionamiento similar a la *blockchain* pero con mejoras, como puede ser el *Hashgraph*, una tecnología mucho más rápida que la cadena de bloques, en la que cada nodo puede difundir información sellada por medio de eventos sobre transacciones creadas y recibidas de unos a otros nodos elegidos al azar, proceso que se repite hasta que todos los nodos conocen la información creada o recibida al principio, llegando la nueva información a cada nodo de la red de una manera más rápida, prescindiendo de los mineros característicos de la *blockchain*, ya que en el caso de *Hashgraph*, los nodos están constantemente compartiendo la información que conocen y el estado de la red de manera aleatoria. De esta forma, *Hashgraph* promete ser un sistema que permite un ahorro energético, eficacia y sostenibilidad comparada considerable, aunque manteniendo las características que hacen atractiva a la tecnología de la cadena de bloques.

Con esto queremos decir que parece que el avance de la tecnología podría solventar algunas de las cuestiones que la aplicación de la red *blockchain* en la Administración de Justicia pudiera plantear, llegando incluso a la automaticidad del minado y su "traducción" a lenguaje natural en un futuro.

Por ello, todas las posibilidades de utilización de la tecnología *blockchain* en nuestro sistema judicial consignadas en páginas anteriores, serían una suerte de paso previo o incipiente, pero necesario para la implementación de esta revolución en su estado más puro, caracterizado por la inmutabilidad, consenso, ausencia de autoridades centrales… Para ello, no sería suficiente con llevar a cabo una modificación legislativa, sino que sería necesaria una reforma profunda de nuestro sistema jurídico procesal, de cara a que el mismo aprovechara todas las ventajas que las nuevas tecnologías nos ofrecen.

Sin embargo, debemos resaltar que es imprescindible hacer un juicio valorativo sobre si realmente convendría llevar a cabo esta redefinición completa de nuestro sistema jurídico procesal en aras de implementar la tecnología *blockchain* en su estado "puro", como sustitución total de las "autoridades centrales", que es en realidad el propósito para el que, en un principio, fue creado. Es decir, debemos sopesar si sería proporcionado y conveniente realizar una inversión de recursos tanto económicos como técnicos, con las reformas legislativas que habría que realizar, para que la tecnología *blockchain* fuera aplicada en toda su plenitud.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

Quizás no sea tan necesaria esa gran redefinición del sistema para poder aplicar la tecnología *blockchain* en el ámbito procesal español, sino que sería suficiente con adoptar una fórmula intermedia, como la explicada anteriormente, que permitiera beneficiarnos de las ventajas que esta ofrece con los recursos y normativa vigentes en la actualidad.

IV. Conclusiones

La *blockchain* es una tecnología basada en el consenso entre los nodos y el empleo de registros distribuidos (*distributed ledgers*) protegidos criptográficamente y organizados en bloques, con el objetivo inicial de desplazar a las "autoridades centrales" a la hora de realizar distintas transacciones. Esta tecnología se caracteriza por la inmutabilidad, irrevocabilidad y transparencia, principios de gran interés a la hora de plantear su posible aplicación en el ámbito de la Administración de Justicia.

La tecnología *blockchain* se viene aplicando en numerosos campos. Las criptomonedas, las *DAO*, los *Smartcontracts*, *NFT*s, registros de trazabilidad… son algunas de las utilidades que podemos encontrar en la actualidad. Si bien es cierto que muchos de ellos ponen de relieve las carencias de la actual cadena de bloques, el constante y vertiginoso desarrollo de la tecnología puede mejorar muchos de los inconvenientes que pueden observarse todavía, como ocurre gracias al desarrollo de nuevas redes, como el *Hashgraph,* tecnología que promete solventar el problema de los costes energéticos y tardanza del minado de un bloque en la red *blockchain*.

Una de estas aplicaciones sería la de su implementación en la Administración de Justicia española, con la cual se prevé un aumento en la efectividad, eficacia y una mejora en el acceso a la justicia por parte de los ciudadanos. Ahora bien, es preciso tener en cuenta las consecuencias que su utilización en los tribunales de justicia puede ocasionar, especialmente, mediante la introducción de la misma como fuente y medio de prueba en el proceso.

La cadena de bloques puede considerarse como fuente de prueba con valor probatorio considerando sus características inherentes, que proporcionan una seguridad jurídica relevante al no poder alterarse los datos contenidos en la misma, siendo especialmente útiles a la hora de probar la identidad de las partes de la operación llevada a cabo mediante la tecnología de la cadena de bloques (con las especialidades de pseudoanonimidad ya comentadas), el contenido de los datos registrados, la autenticidad de las firmas (Ibánez Jiménez, 2018, 4) y la fecha y hora de la operación, debido a que cada *hash* posee una firma con registro temporal o *time stamping,* que determina este extremo.

Por otro lado, en cuanto a la introducción de la tecnología *blockchain* en el proceso como medio de prueba, existe una discusión doctrinal sobre si puede o no introducirse en el proceso y cómo. Muchos autores entienden que lo más correcto sería su introducción mediante prueba documental. Como sabemos, nuestra normativa actual distingue entre la prueba documental pública y privada.

Con respecto a la posibilidad de incorporarla como documental pública, tal y como hemos indicado, de *lege ferenda*, en el caso de que se propusiera en juicio como prueba

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

un documento público electrónico registral o notarial basado en la *blockchain* privada o híbrida en la que estos profesionales actuaran como nodos en la red, debería regir la misma presunción de exactitud de la que actualmente goza la documental pública en virtud del art. 319 LEC. La aplicación de la tecnología *blockchain* en el registro de la propiedad o notarías, entre otros, vendría a reforzar esa presunción legal de exactitud, ya que nos encontraríamos ante la unión de las características inherentes de seguridad, inmutabilidad, irrevocabilidad y transparencia de la cadena de bloques, con la labor calificadora profesional del registrador y de asesoramiento del notario. Por ello entendemos que, pese a que la tecnología *blockchain* no se recoge explícitamente como medio de prueba admitido en la LEC, sí que deberá aplicarse la misma presunción de exactitud a aquellos asientos registrales insertados en la cadena de bloques cuando se pretenda hacerlos valer en juicio.

Por otro lado, con respecto a su introducción como documental privada, entendemos que, ciñéndonos a la normativa actual, es posible que la misma se introduzca en el proceso como documental privada, mediante la impresión del "*hash*", es decir, de la clave alfanumérica asociada al contenido en concreto, así como su "traducción al lenguaje humano" (Ríos López, 2022, 6).

Ahora bien, hay que tener en cuenta, atendiendo a lo dispuesto en el art. 326.1 LEC, los documentos privados hacen prueba plena en el proceso, siempre y cuando su autenticidad no sea impugnada por la parte a quien perjudique, por lo que es probable que deba acudirse a una pericial informática de cara a determinar si en la práctica de la prueba se está ante el mismo archivo electrónico que se propuso en su día.

Por último, y a modo de conclusión final, consideramos que la utilización de la tecnología *blockchain* en el ámbito judicial plantea aún varios interrogantes, como son el reto derivado del anonimato de los usuarios y el de la integridad del contenido de la cadena de bloques, entre otros. Sin embargo, la cadena de bloques es aún una tecnología muy incipiente que se encuentra en pleno desarrollo, por lo que deberemos esperar a que el paso del tiempo y la perfección de la misma hagan su trabajo.

Bibliografía

ARRUÑADA, BENITO. (2018): "Limitaciones del *blockchain* en contratos y propiedad", en *Revista Crítica de Derecho Inmobiliario*, vol. 94, nº 769.

BADIOLA COCA, SILVIA (2022): "La prueba de los hechos acaecidos en el entorno de la tecnología Blockchain como medio de prueba en el proceso civil español", en *Blockchain: aspectos jurídicos de su utilización*, (dir. VALPUESTA GASTAMINZA, EDUARDO), La Ley, Madrid, p.p. 284 - 315.

BANDÍN BARREIRO, ISABEL y MOLINA ÁLVAREZ, INÉS (2020): "*Blockchain:* eficacia probatoria en los Tribunales españoles y análisis del derecho comparado", en *Comunicaciones en propiedad industrial y derecho de competencia*, nº 91.

BARONA VILAR, SILVIA (2022) "La digitalización y la algoritmización, claves del nuevo paradigma de justicia eficiente y sostenible" en *Uso de la información y de los datos personales en*

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

los procesos: los cambios en la era digital (dir. COLOMER HERNÁNDEZ, IGNACIO), Pamplona, Aranzadi, p.p. 75 - 115.

BARONA VILAR, SILVIA (2023): "Ecosistema digital de Justicia eficiente (De la Justicia digital orientada al documento a la Justicia orientada al dato)", en *Actualidad Civil,* Nº 5, Mayo de 2023, Editorial LA LEY.

BARRIO ANDRÉS, MOISÉS (2022): *Manual de Derecho Digital*, Tirant Lo Blanch, Valencia.

BOUCHER, PHILIP (2017): "How *blockchain* technology could change our lives", en *In-depth Analysis, European Parliamentary Research Service*, http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf.

BUENO DE MATA, FEDERICO: (21-22 de abril de 2021). ''*Inteligencia artificial y medidas de investigación en la era post Covid"* [Sesión de videoconferencia], Jornada Jóvenes Investigadores: Investigación y proceso penal en el Siglo XXI. Nuevas tecnologías y protección de datos, Girona, España. Disponible en: https://www.youtube.com/watch?v=GScnXuglBg8.

CALAZA LÓPEZ, SONIA (2022): "*Blockchain* y *smart contracts:* ¿un ecosistema digital seguro al margen de la ley?" en *Uso de la información y de los datos personales en los procesos: los cambios en la era digital* (dir. COLOMER HERNÁNDEZ, IGNACIO), Aranzadi, Navarra, p. 229 - 258.

CARNELUTTI, FRANCESCO (1955) *La prueba civil*, Buenos Aires, Arayu.

CERDÁ MESEGUER, JUAN IGNACIO. (2020): "*Blockchain* y Administración de Justicia: ¿un reto posible de alcanzar?", en F*ODERTICS 8.0 estudios sobre tecnologías disruptivas y justicia* (dir. BUENO DE MATA, FEDERICO), 1ª edición, Granada, Comares.

DÍAZ MARTÍNEZ, MANUEL (2021): "Procedimiento probatorio y medios de prueba" en *Derecho Procesal Civil. Parte General* (coord. GIMENO SENDRA, VICENTE y CALAZA LÓPEZ, SONIA), Tirant Lo Blanch, Valencia, pp.389 - 394.

Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018. Recuperada de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32018L0843

GALLEGO FERNÁNDEZ, LUIS ANTONIO (2018): "Cadenas de bloques y Registros de derechos", en *Revista Crítica de Derecho Inmobiliario, nº 765.*

GÓMEZ COLOMER, JUAN LUIS (2022). "La prueba. Aspectos comunes" en *Proceso Civil. Derecho Procesal II* (Coord. GÓMEZ COLOMER, JUAN LUIS y BARONA VILAR, SILVIA), 2ª Edición, Tirant Lo Blanch, Valencia, p. 219 - 235).

IBÁÑEZ JIMÉNEZ, JAVIER W. (2018): "Cuestiones jurídicas en torno a la cadena de bloques («*blockchain*») y a los contratos inteligentes ("*smart contracts*")", en *Icade. Revista de la Facultad de Derecho*, nº 101. Disponible en: https://revistas.comillas.edu/index.php/revistaicade/article/view/8407. (fecha de última consulta: 22 de octubre de 2023).

IRISH DEPARTMENT OF FINANCE (2018): *Discussion Paper: Virtual Currencies and Blockchain Technology*, Recuperado de http://www.finance.gov.ie/wp-content/uploads/2018/03/VirtualCurrencies-and-Blockchain-Technology-March-2018.pdf

LLOPIS BENLLOCH, JOSÉ CARMELO (2017): "*Blockchain* y profesión notarial". *El notario del siglo XXI: Revista del Colegio Notarial de Madrid*, nº 71. Disponible en http://www.elnotario.es/index.php/hemeroteca/revista-70/7106-blockchain-y-profesion-notarial (fecha de última consulta: 23 de octubre de 2023).

MINISTERIO DE JUSTICIA (2022) *El Gobierno aprueba el Proyecto de Ley de Eficiencia Digital del Servicio Público de Justicia. Ministerio de Justicia.* Recuperado el 28 de agosto de 2023, de: https://www.mjusticia.gob.es/es/institucional/gabinete-comunicacion/noticias-ministerio/ley-eficiencia-digital.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

NAVARRO LÉRIDA, MARÍA DEL SAGRARIO. (2018): "Gobierno corporativo, *blockchain* y *smart contracts:* Digitalización de las empresas y nuevos modelos descentralizados (DAOs)", en *Revista de Derecho del Mercado de Valores*, nº 23.

PACHECO JIMÉNEZ, MARÍA NIEVES (2019): "De la tecnología *blockchain* a la economía del token", en *Revista de la Facultad de Derecho PUCP*, nº 83.

PREUKSCHAT, ALEXANDER (2017): *Blockchain: la revolución industrial de internet*, Gestión 2000, Barcelona.

PORXAS, NURIA y CONEJERO, MARÍA (2018): "Tecnología *blockchain:* funcionamiento, aplicaciones y retos jurídicos relacionados", en *Actualidad Jurídica Uría Menéndez*, nº 48. Recuperado de: https://www.uria.com/documentos/publicaciones/5799/documento/art02.pdf?id=7875 (fecha de última consulta 30 de octubre de 2023).

RÍOS LÓPEZ, YOLANDA (2022) "*Blockchain, smart contracts y Administración de Justicia*" en https://blockchainintelligence.es/wp-content/uploads/2021/02/BLOCKCHAIN-SMART-CONTRACTS-Y-ADMINISTRACION-DE-JUSTICIA_YOLANDA-RIOS.pdf (fecha de última consulta 19 de octubre de 2023).

SÁNCHEZ RUBIO, ANA (2019): "Cadena de custodia y prueba electrónica: la mismidad del hash como requisito para la fiabilidad probatoria" en *FODERTICS 7.0 estudios sobre derecho digital* (dir. BUENO DE MATA, FEDERICO), 1ª edición, Comares, Granada.

SZABO, NICK (1997): "Formalizing and Securing Relationships on Public Networks", en *First Monday,* vol. II, núm 9. Recuperado de: https://doi.org/10.5210/fm.v2i9.548

TUR FAÚNDEZ, CARLOS (2018): *Smart contracts, análisis jurídico*, Reus, Madrid.

VIEDMA CABRERA, PABLO. (2021): "La disrupción del *Blockchain* en los mercados financieros y tokenización de activos" en *Estudios sobre Derecho Digital* (coord. PEREA ORTEGA, RAFAEL), 1º edición, Aranzadi, Navarra.

VILLAR FUENTES, ISABEL (2023). "Proceso Civil y los *Smart Contracts* en *Blockchain", Revista de la Asociación de Profesores de Derecho Procesal de las Universidades Españolas,* vol nº 7, Valencia, pp. 209 a 250.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 136-156
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.07

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los *deepfakes**

THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE IN THE INVESTIGATION OF GENDER CYBERCRIME: THE RISE OF DEEPFAKES

Irene González Pulido
Investigadora postdoctoral "Margarita Salas"
Área de Derecho procesal.
Universidad de Salamanca/ Universidad de Extremadura
irenegopu@usal.es 0000-0001-8098-350X

Recibido: 03 de noviembre de 2023 | Aceptado: 08 de diciembre de 2023.

RESUMEN

El auge de la inteligencia artificial generativa ha condicionado el devenir de los modus operandi de los ciberdelitos de género; destacando la utilización de los deepfakes. En la actualidad, preocupa la rápida adecuación y adaptación por parte de los ciberdelincuentes, en contraposición al lento desarrollo de una regulación de los diferentes sistemas de IA. El empleo de las tecnologías más novedosas para la comisión de ciberdelitos de género aumenta los obstáculos que ya encontraban las autoridades policiales y judiciales en la práctica de investigaciones en Internet. Estas cuestiones han determinado que en el presente estudio se apueste por analizar la necesidad de implementar los sistemas de IA generativa como herramientas de investigación tecnológicas, proponiendo diferentes líneas de actuación a corto, medio y largo plazo para conseguir materializar investigaciones salvaguardando todas las garantías y, por consiguiente, finalizar este tipo de procesos penales con éxito.

PALABRAS CLAVE

Inteligencia artificial
Generativa
Deepfakes
Ciberdelincuencia
Violencia de género
Investigación tecnológica

* Actualmente en el centro de destino del primer año: Área de Derecho procesal de la Universidad de Extremadura. Beneficiaria de una ayuda para la recualificación del sistema universitario español para 2021-2023, modalidad "Margarita Salas". Resolución Complementaria de 30 de junio de 2021 de la Universidad de Salamanca, en el marco del Real Decreto 289/2021, de 20 de abril, (BOE núm. 26 de 22 de abril de 2021), así como en la Orden del Ministerio de Universidades UNI/551/2021 de 26 de mayo. Instrumento Europeo de Recuperación («Next Generation EU»).

ABSTRACT

The rise of generative artificial intelligence has conditioned the evolution of the modus operandi of gender cybercrime, especially the use of deepfakes. Currently, there is concern about the rapid adaptation by cybercriminals, as opposed to the slow development of regulation of AI systems. The use of the latest technologies for the commission of gender-based cybercrime increases the obstacles already encountered by law enforcement and judicial authorities in the practice of Internet research. The present study focuses on analyzing the need to implement generative AI systems as technological research tools, proposing different lines of action in the short, medium and long term in order to carry out investigations that safeguard all the guarantees and, consequently, this type of criminal proceedings.

KEYWORDS

Generative artificial
Intelligence
Deepfakes
Cybercrime
Gender violence
Technological research

I. Aproximación a la inteligencia artificial generativa

Para realizar una aproximación a la inteligencia artificial generativa, tenemos que destacar tres ideas principales. La primera está relacionada con las funciones de la inteligencia artificial (en adelante, IA) y, en particular, con el alcance de la IA generativa, ya que solo de este modo podremos dar paso a las otras dos ideas, basadas respectivamente en su previsión legal y en su incorporación a los *modus operandi* de los ciberdelitos de género.

Como hemos señalado, la segunda de las ideas que se abordará en el presente estudio está relacionada con la apuesta por una regulación a nivel europeo que prevea unas condiciones y unas prohibiciones que permitan a la comunidad europea controlar los sistemas IA que se están implementando y que están siendo utilizados por su ciudadanía. Sistemas IA entre los que se han incluido algunas funciones relativas a la posibilidad de falsificación que ofrecen los sistemas de IA generativa y, más recientemente, la mención expresa de este tipo de IA, así como de los modelos fundacionales.

La tercera idea está relacionada con la acogida de estos sistemas por parte de la ciudadanía y con la adaptación de los ciberdelincuentes ante estas nuevas tecnologías. Por un lado, la utilización de este tipo de IA favorecerá el progreso tecnológico, su implementación a nivel de la UE, pero, por otro lado, también supondrá un obstáculo para la consecución de los objetivos de las autoridades policiales y judiciales que deben perseguir los ciberdelitos que se sirven de estas tecnologías; en el presente estudio atenderemos a los que han sido denominados ciberdelitos de género. El motivo de esta elección se debe a la tendencia al alza de la utilización de esta tecnología en los últimos meses (del Castillo, 18 de septiembre de 2023; Navarro, 21 de diciembre de 2022; Viejo, 3 de octubre de 2023) atentando contra los derechos de mujeres y niñas[1].

1. Sin perjuicio de que también los niños están siendo víctimas de algunas conductas delictivas de esta índole, la victimización es mayor en el caso de niñas. Véase, por ejemplo, el documento de enmiendas realizadas por la Comisión de Derechos de las Mujeres e Igualdad de género a la Propuesta

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

Desde hace varias décadas se han identificado múltiples funciones de la IA. En la Comunicación de la Comisión Europea de 2021 se destacaron, por un lado, como *software* sus funciones de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento facial y de voz, asistentes de voz, traducción de textos, generación de subtítulos, identificación y bloqueo de spam, etc. Y, por otro, se incluyó la posibilidad de incorporar la IA a dispositivos *hardware* desarrollando robots avanzados, automóviles autónomos, drones o aplicaciones del Internet de las cosas, etc. Desde este primer momento se identificó que podría favorecer, en general, a la Administración de Justicia y, en particular, la lucha contra la delincuencia, combatiendo incluso formas graves con mayor eficacia[2]. Por ejemplo, se manifestó que podría contribuir a la lucha contra la delincuencia organizada destacando su potencial para analizar grandes cantidades de datos y para la práctica de investigaciones en la *darkweb* (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025, 14 de abril de 2021). No obstante, desde el momento en el que se apostó por este tipo de tecnología también se detectaron los riesgos y las amenazas que podrían emerger del desarrollo y la expansión de la IA.

Con carácter específico, en atención a las enmiendas a la Propuesta de Reglamento de IA para la UE, aprobadas el 14 de junio de 2023 por el Parlamento Europeo, podemos definir la IA generativa como los "sistemas de IA destinados específicamente a generar, con distintos niveles de autonomía, contenidos como texto, imágenes, audio o vídeo complejos" (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023). Por lo tanto, en el marco de la IA generativa encontramos diversas herramientas diseñadas para la práctica de diferentes funciones, entre las que destacaremos algunas de las que se han considerado más relevantes para el presente estudio.

Por un lado, encontramos modelos de lenguaje generativo, entre los que desataca ChatGPT, que a priori no responde preguntas clasificadas como dañinas o ilícitas, pero sin embargo, se ha demostrado que utilizando algunas estrategias específicas para orientar los *prompts* o indicaciones se podrían eludir las medidas de seguridad. Continuamente se está desarrollando y mejorando la *prompt engineering* (Europol, 27

---

de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores. Enmiendas 46-536. 8 de mayo de 2023. 2022/0155(COD).

Las propuestas aquí analizadas perseguirán su implementación para la protección de todas las víctimas menores de edad, ya que como se ha incorporado en las enmiendas a la última propuesta de Reglamento en la que se apuesta por reforzar la lucha contra el abuso sexual de menores, nos encontramos ante una amenaza grave que afecta particularmente a la UE. Véase enmienda 286, de 30 de mayo de 2023, realizada por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior. 2022/0155(COD).

2. Se señaló que "La IA puede ayudar a luchar contra la delincuencia y el terrorismo, y permitir a las fuerzas o cuerpos de seguridad seguir el ritmo del rápido desarrollo de las tecnologías utilizadas por los delincuentes y sus actividades transfronterizas" (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Fomentar un planteamiento europeo en materia de inteligencia artificial, 21 de abril de 2021).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

de marzo de 2023). Por otro lado, encontramos aplicaciones que se sirven de sistemas IA que funcionan generando imágenes a partir de una entrada de texto; otras que sirven para manipular imágenes preexistentes; para combinarlas e incluso para superponer imágenes diferentes o para insertarlas en un vídeo específico; el desarrollo de este tipo de aplicaciones está siendo exponencial, las combinaciones son múltiples y los resultados cada vez están más mejorados, aproximándose cada día más a la realidad sin manipular[3].

En este marco de análisis tenemos que destacar el auge, a lo largo del último año, de algunas aplicaciones que se sirven de sistemas de IA generativa, ejemplo de ello lo encontramos en el "Chat GPT-4" o "Midjourney". Este auge y desarrollo exponencial de la IA generativa ha provocado que los expertos se cuestionen ante qué tipología de sistemas IA nos encontramos cuando implementamos estos programas que, día tras días, son más numerosos y variados. Parece que la propuesta de Reglamento original se redactó en términos de funcionalidad, es decir, persiguiendo evitar la obsolescencia de la tecnología apostando por clasificar los sistemas IA en función de su aplicación específica, bien haciendo referencia a un sector, como la Administración de Justicia, o bien en atención a la acción específica que permite, como podría ser la perfilación (Villatoro González y Camblor Echanove, 16 de junio de 2023).

No obstante, este planteamiento parecía no dar respuesta a este tipo de sistemas, por lo tanto, el Parlamento europeo ha apostado por aprobar una serie de enmiendas al respecto, el pasado 14 de junio de 2023. Se ha incluido, en primer lugar, la definición de los "modelos fundacionales", que caracterizan el funcionamiento de los sistemas de IA generativa[4], como modelos entrenados con grandes volúmenes de datos, diseñados para la producción de información y para la práctica de una gran variedad de tareas. En este mismo sentido se ha incluido la definición de "Sistema de IA de uso general" para dar cobertura jurídica a los que no se han diseñado específicamente para realizar una función concreta en un ámbito localizado, sino que "puede utilizarse en aplicaciones muy diversas". En este sentido se han recogido diversas funciones y obligaciones inherentes a los proveedores o implementadores de este tipo de sistemas de IA o modelos fundacionales.

En definitiva, tras dichas enmiendas a la Propuesta de Reglamento de IA de la Unión Europea parece clara la apuesta por la regulación de este tipo de sistemas de IA generativa, con el objetivo de que se cumplan los principios y las obligaciones necesarias para garantizar un uso de esta tecnología salvaguardando los valores de la UE y los derechos de su ciudadanía. Sin perjuicio de que esta propuesta esté en curso y se prevea que el próximo año estará vigente, la adecuación de la ciberdelincuencia de nuevo se

3. Desde Trend Micro se apuesta por clasificar estos *deepfake* en atención a la manipulación realizada: reemplazo de la cara de una persona por la de otra; reconstrucción facial; generación de rostros totalmente ficticios; generación de contenido de audio o de voz; creación de falsificaciones audiovisuales; etc.

4. Se hace mención expresa a esta vinculación de los modelos fundacionales y la IA generativa en el artículo 28 ter relativo a las obligaciones del proveedor de un modelo fundacional, en su apartado cuatro. (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

ha adelantado al desarrollo normativo y, en este sentido, continuaremos con la última idea de esta breve aproximación.

En este contexto, por lo tanto, tenemos que destacar que la IA se presenta como una oportunidad para los ciberdelincuentes; mejoran sus ataques, obtienen más beneficios en menos tiempo, acceden a nuevas víctimas, crean medios de ataque más innovadores, refuerzan su anonimato y pueden hacer uso de estos sistemas con pocos conocimientos técnicos, incluso pudiendo practicar técnicas de hackeo (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). En el marco de la ciberdelincuencia pura o de alta tecnología, la implementación de la IA podría favorecer la ocultación del *malware,* su activación y la práctica de ataques persistentes. Por supuesto, también se ha puesto de manifiesto la posible mejora de los *malware* empleados en el marco de la ingeniería social con la utilización de la IA (Europol, 2020). En este contexto delictivo, también va a ser relevante el desarrollo de la IA generativa, como analizaremos a continuación.

En este mismo sentido, se ha identificado que los ataques *ransomware,* posicionados en la cúspide de las ciberamenazas de alta tecnología y que también comprometen las infraestructuras críticas, si se acompañan por inteligencia artificial podrían tener efectos devastadores, ya que optimizaría la infección y sus efectos. En este sentido se podrían ver comprometidos servicios esenciales y tener graves consecuencias en la vida *offline* (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

En atención a la posibilidad de sortear mecanismos de seguridad con sistemas basados en IA, se ha identificado un *software* que permite atacar al sistema de seguridad CAPTCHA, favoreciendo el acceso automático a bases de datos, acceso de sistemas IA a esta información e incluso se emplea para el acceso automatizado a foros u otras plataformas de interacción. Junto a esto se podrían sortear los sistemas existentes para la detección de redes de *bots*, lo que favorecería la simulación de actividad humana en determinados contextos, cuando esta puede ser inexistente, por ejemplo, en redes sociales (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

Este tipo de ciberataques basados en el engaño, como ha sido publicado por Trend Micro, también suponen una amenaza para la industria de los *eSport*, tanto con ánimo de lucro como con el objetivo de blanquear dinero. También los sistemas de los juegos en línea podrían ser atacados mediando la utilización de IA. Con esta misma finalidad, destacan las herramientas IA, generalmente *bots* que se utilizan para el comercio financiero, para el comercio de criptomonedas, empleando el análisis de estrategias de negociación y realizando predicciones de las operaciones (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). La obtención de financiación y el blanqueo de capitales han sido actividades clave para el mantenimiento de grandes organizaciones criminales, sin perjuicio de que puedan perpetrarse estos ataques por otro tipo de delincuentes al margen de dichas organizaciones. En este sentido, es destacable que la IA puede servir para potenciar la práctica de otras actividades transversales necesarias

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

para materializar los ciberdelitos de género, ya sea con carácter previo o posterior, entre las que destacan la ya citada financiación o el blanqueo de los beneficios obtenidos.

También se ha previsto por los investigadores la utilización de sistemas IA para la obtención de claves y contraseñas que pueden permitir el acceso a plataformas, aplicaciones o sistemas (Europol, 2020). Este tipo de actuación podría dar lugar a la comisión de toda una variedad de conductas delictivas, en atención al contenido al que se pudiera acceder (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020), incluyendo ciberdelitos de género entre las mismas.

La IA además puede ser utilizada para proteger la propia infraestructura delictiva y eliminar evidencias, permitiendo la programación y destrucción automática (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). Esta cuestión complicaría la práctica de investigaciones que impliquen diligencias de investigación tecnológicas complejas; como son el agente encubierto informático o el registro remoto. Sin perjuicio de que, con carácter general, se obstaculizaría la obtención de cualquier tipo de evidencia y, por consiguiente, se comprometería el éxito de la investigación y del proceso penal en su totalidad.

En definitiva, podemos afirmar que las funciones que ofrece la IA a la ciudadanía en general no han quedado al margen de la actuación de los ciberdelincuentes, sino que los últimos avances en materia de IA se están empleando para atentar contra múltiples bienes jurídicos, persiguiendo diferentes objetivos. De este modo, como hemos apuntado, las autoridades competentes para practicar la investigación de los delitos que se perpetren utilizando este tipo de sistemas encontrarán numerosas dificultades, añadidas a las que ya existían en el marco de la persecución de los ciberdelitos más tradicionales que se cometían a través de Internet desde su aparición.

II. IA generativa como método utilizado para la comisión de ciberdelitos

Como se ha señalado en la Propuesta de Reglamento de IA de la UE, esta tecnología puede servir para optimizar y personalizar las operaciones, incluidas las policiales y judiciales, pero también su desarrollo nos obliga a identificar nuevos riesgos. En particular, como se ha introducido en el epígrafe anterior, en lo que respecta a la IA generativa, detectamos cambios y adaptaciones en los *modus operandi* de determinados tipos delictivos.

En el reciente estudio elaborado por Europol se han identificado algunas utilizaciones de sistemas de IA generativa que pueden fomentar, facilitar o mejorar la comisión de determinados tipos delictivos. Como modelo de lenguaje generativo por excelencia destacamos de nuevo el ChatGPT, tanto su versión 3,5 como la 4, podría utilizarse con finalidades ilícitas; tanto para la práctica de algunas conductas más leves como de otras más graves, siendo útil para complementar delitos de terrorismo, de abuso sexual de menores o ciberdelitos que han sido considerados como puros (Europol, 27 de marzo

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

de 2023). Entre las funciones claves detectadas por Europol, por un lado, es destacable la capacidad de redacción de textos de un modo similar al que lo harían los humanos, siguiendo modelos específicos y adecuándose a necesidades o situaciones concretas. Por lo tanto, se puede favorecer la suplantación de identidad y del estilo de escritura y, por consiguiente, se pueden perfeccionar las técnicas de ingeniería social, el *phishing* y, de este modo, se mejoran algunas tipologías delictivas que llevan años practicándose, como los fraudes en línea; como puede ser el fraude del CEO. Asimismo, eludiendo las restricciones del sistema podría facilitarse la redacción de textos que fomenten la desinformación, la incitación al odio, el adoctrinamiento terrorista, etc. (Europol, 27 de marzo de 2023). Las estafas en las que se utiliza ingeniería social también podrían optimizarse, facilitando el trabajo y favoreciendo el éxito de los ciberdelincuentes (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

Por otro lado, desde la aparición en noviembre de 2022 del ChatGPT, una de las cuestiones que más ha preocupado ha sido su capacidad para generar código en diferentes lenguajes de programación, esta función del ChatGPT podría ser utilizada con fines maliciosos para la comisión de múltiples actividades delictivas, incluso por personas que no son expertas en informática para el desarrollo de *malware*. No obstante, se apunta que en la actualidad el desarrollo de esta función es bastante sencilla, pero se estima que en un futuro este tipo de sistemas se mejoren, como ya se ha hecho con respecto a la primera versión que se publicó del chat (Europol, 27 de marzo de 2023). En la actualidad se ha detectado lo que se denominan "alucinaciones" de forma coloquial, debido a algunas imprecisiones en su uso habitual (Retana Gil, 19 de octubre de 2023).

La mejora de *malware* es una de las características que va a permitir aumentar la eficacia de las actividades ilícitas; por ejemplo, los sistemas de lenguaje o gramática generativa pueden ayudar a sortear los filtros del spam y acceder a un mayor número de víctimas sin ser identificados (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). Es decir, se podrá implementar este tipo de sistemas de IA generativa, basados en lenguaje, para eludir mecanismos de seguridad y control que llevan años establecidos. En este mismo sentido, investigadores han demostrado que se podría camuflar *malware,* pasando desapercibido ante los antivirus, incluso de aquellos que se sirvan de IA para mejorar su eficacia (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

Desde el estudio de investigación que ha publicado Trend Micro respecto a las amenazas de la IA y al abuso de estos sistemas también se ha recogido como la IA generativa podría implementar las llamadas automáticas para cometer estafas de diversa índole, incluso simulando la voz de personas conocidas; para generar voces y quebrantar sistemas de seguridad que funcionan por autenticación de voz en entidades bancarias (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020); entre otras modalidades delictivas que podrían surgir del desarrollo y la evolución de este tipo de sistemas.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

Entre las posibilidades de empleo de la IA generativa, son destacables los *deepfakes* o vídeos ultra falsos que se ha identificado que son producto de la manipulación de material multimedia preexistente o bien de su generación a través de técnicas de *machine learning,* con el objetivo de reemplazar a otras personas, simulando que son reales; se pueden encontrar imágenes, vídeos, audio... Es decir, con este tipo de tecnología se puede conseguir mostrar de forma convincente a personas que existen, han existido o que nunca existieron, haciendo y/o diciendo cosas que nunca hicieron y/o dijeron (Europol Innovation Lab, 2022). En concreto, no podemos afirmar que no existiera esta técnica con carácter previo al desarrollo de la IA, sin embargo, sí podemos concretar que se ha facilitado, agilizado y extendido su posible práctica gracias a las ventajas de este tipo de sistemas (Simó Soler, 2023).

La generación de *deepfakes* es una de las utilidades de la IA que ha sido identificada como una de las más empleadas con fines maliciosos y como una de las más dañinas, advirtiendo de que el desarrollo y la evolución de esta tecnología dificulta que los seres humanos llevemos a cabo la diferenciación de este tipo de contenido artificial o simulado, con respecto a los auténticos u originales (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). La evolución y la mejora de la tecnología no cesa, sin embargo, la apuesta por herramientas y mecanismos que permitan su detección o utilización por autoridades policiales y judiciales no lo hace al mismo ritmo, de este modo el nuevo panorama de la ciberdelincuencia compromete los recursos de investigación preexistentes en la normativa vigente[5].

Esta tecnología, además, se sirve de herramientas que existen en el marco de Internet desde hace décadas y de las propias características inherentes al ciberespacio; se sirven de las redes sociales, aplicaciones de mensajería y otros canales de difusión para llegar en un corto plazo de tiempo a millones de personas situadas en diferentes lugares del mundo (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). En este mismo sentido, se identificó que mejora las técnicas que los ciberdelincuentes llevan décadas empleando; por ejemplo, como ya se han señalado, las relativas a ingeniería social (Aider, Patrini, Cavalli, Cullen (Deeptrace Labs), 2019). Asimismo, se ha mencionado la posibilidad de combinar el *Crime as a service* y el comercio con sistemas de IA o servicios de creación de *deepfakes* directamente a través de mercados ilícitos (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). Por lo tanto, la expansión de la IA y el desarrollo de múltiples aplicaciones favorece el acceso de cualquier persona a IA generativa, permitiendo y facilitando la generación de *deepfakes,* también con fines ilícitos.

Con la combinación de este tipo de tecnología con las ventajas que ofrece la actuación en el ciberespacio, algunas de las cuales han sido señaladas, se pueden perseguir múltiples finalidades maliciosas, entre las que destacan: destruir la imagen y la credibi-

5. Como afirman desde EUROPOL: "As a result, they are always one step ahead of law enforcement in their implementation, use and adaptation of these technologies" (Europol Innovation Lab, 2022).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

lidad individual; acosar o humillar a personas en línea; perpetrar extorsión y fraude; falsificar documentos de identidad; suplantar identidades en línea; falsificar y manipular pruebas electrónicas; distribuir desinformación; incitar a la violencia, odio u otros mensajes extremistas o terroristas; interrumpir mercados financieros; incluso podríamos encontrarnos con otras consecuencias que provocasen enfrentamientos entre diferentes Estados (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

Teniendo en cuenta el alcance y la repercusión de estas técnicas, en el siguiente apartado analizaremos algunas particularidades de estos *deepfakes* en atención a la comisión y a la investigación de ciberdelitos de género. Los *deepfakes* también han sido utilizados y aprovechados para atentar contra los derechos de las mujeres, siendo destacable el material pornográfico generado con diversas intenciones delictivas y persiguiendo toda una variedad de objetivos, como analizaremos más en profundidad a continuación (Secretaría General de la Organización de los Estados Americanos, s.f.).

2.1. IA generativa y ciberdelincuencia de género

Desde que surgieron los primeros instrumentos y desarrollos tecnológicos los delincuentes han sido rápidos adecuando su *modus operandi* para conseguir el mayor éxito delictivo. Como ha sido señalado, lo mismo ha ocurrido con la expansión y el auge de la IA generativa.

Tenemos que considerar que en este caso la tecnología se estaría utilizando para atentar contra los derechos fundamentales de las personas, para manipular a grupos vulnerables concretos, pudiendo provocar perjuicios psíquicos e incluso físicos en las víctimas. Por lo tanto, estaríamos ante prácticas prohibidas, catalogadas como de riesgo inaceptable en la propuesta de Reglamento IA de la UE. Siendo destacable todo el elenco de modalidades delictivas que podrán perpetrarse o complementarse con la utilización de la IA generativa.

En este sentido, podemos encontrarnos diferentes delitos que podrían cometerse, como los ciberdelitos de género. En primer lugar, definiremos la ciberdelincuencia de género como aquellos delitos cometidos a través de Internet por razón de género prevaliéndose el agresor del alcance y la especial lesividad de los medios tecnológicos, tanto en el ámbito público como en el ámbito privado, con independencia de la relación preexistente con la víctima (González Pulido, 2017). Por ejemplo, encontraríamos la generación de material de abuso sexual infantil o la generación y distribución de material sexual explícito de adultos, falso y sin consentimiento. Por lo tanto, algunas de las conductas que tendrían cabida en la citada definición están consideradas como graves y así se han contemplado en el marco de los instrumentos aprobados a nivel de la UE e incluso a nivel internacional.

En este momento, en atención a las apreciaciones realizadas, es oportuno comenzar a señalar que en la propuesta de Reglamento de IA de la UE, se supedita la utilización de algunos de los sistemas de IA previstos en su articulado a la gravedad y a la autorización

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

judicial[6], por lo que parecería que cuando nos encontremos ante determinadas conductas de ciberdelincuencia de género el Reglamento si favorecería la implementación de sistemas de IA policiales y judiciales para luchar contra estos fenómenos.

Como características más relevantes de la IA generativa para utilizarla para la comisión de este tipo de ciberdelitos de género destacan: la utilidad de modelos de lenguaje generativo para suplantar la identidad y la capacidad de estos modelos para favorecer que los ciberdelincuentes se ganen la confianza de las víctimas (Europol, 27 de marzo de 2023); la utilización de *deepfakes* basados en imágenes, vídeos o audio; también la posible combinación de diferentes técnicas de IA generativa buscando la mayor efectividad; entre otros. Sin perjuicio de que también pueda combinarse la utilización de otro tipo de sistemas de IA para obtener material o incluso para su difusión, en función de la conducta a realizar y el objetivo perseguido por el delincuente, ya se abordaron previamente algunas posibles ventajas de los *software* que se sirven de estas tecnologías.

En particular, es destacable en el marco de este estudio cómo preocupan a la comunidad internacional los sistemas de IA que han sido catalogados como multimodales, ya que son sistemas de IA capaces de integrar y procesar "múltiples modalidades de información o fuentes de datos de diversos tipos […]: texto, audio, imagen/vídeo, profundidad, térmica y movimiento" (Loredo, 2023). Estos sistemas de IA generativa pueden fomentar la creación de *deepfakes* muy convincentes y que pueden servir para la comisión de múltiples tipologías delictivas (Europol, 27 de marzo de 2023).

Estas funciones podrían mejorar y favorecer las prácticas de algunos ciberdelitos e incluso utilizar la posible generación de vídeo y audio para engañar o embaucar a menores o mujeres con el fin último de captar víctimas de otros eventuales delitos o bien directamente con el objetivo de perpetrar un delito sexual en el medio físico *offline*. No se trata de la aparición de nuevos delitos, sino de herramientas que agilizan y promueven su práctica, ya que la principal ventaja de la IA generativa es que facilita y mejora la calidad del material audiovisual.

Ejemplo de esta cuestión la encontramos en el análisis de la realidad actual, ya que pone de manifiesto que no nos encontramos ante ideas hipotéticas de futuro, sino que este tipo de criminales ya se están aprovechando de las ventajas de la IA generativa para poder perpetrar sus delitos, en particular, para la comisión de este tipo de ciberdelitos que atentan contra las mujeres, por el mero hecho de serlo, con una mayor incidencia. En particular, los *deepfakes* ya fueron identificados hace años como un riesgo para los derechos de las mujeres y como una manifestación más de la cosificación de las mismas (Cerdán Martínez, Padilla Castillo, 2019).

6. Véase, por ejemplo, el considerando 18 tras la enmienda aprobada el 14 de junio de 2023, que señala estos requisitos para la utilización excepcional de sistemas IA para la identificación biométrica en imágenes grabadas en espacios de acceso público. Indicando que deberá ser estrictamente necesario para investigar un delito grave, que ya se haya cometido, y solo previa autorización judicial. Cuestión regulada en el artículo 5, apartado 1, letra d quinquies.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

A finales del año 2017 ya encontrábamos el caso del usuario anónimo de Reddit que publicó vídeos de diferentes actrices famosas, en los que había superpuesto a cuerpos de otras mujeres sus caras para crear películas pornográficas, así como es destacable la consiguiente creación de *FakeApp* u otras aplicaciones (Cerdán Martínez, Padilla Castillo, 2019; Aider, Patrini, Cavalli, Cullen (Deeptrace Labs), 2019). Nos encontramos en este caso ante la utilización de IA generativa con fines de generación de material pornográfico no consentido. Es preciso apuntar que el desarrollo que han experimentado estas técnicas desde 2017 ha sido muy significativo, no obstante, es relevante recoger este mediático caso que pone de manifiesto el empleo de esta tecnología.

Además, el desarrollo de este tipo de aplicaciones generó la creación de algunas específicas como *Deepnude,* focalizada concretamente en desnudar a mujeres (Aider, Patrini, Cavalli, Cullen (Deeptrace Labs), 2019). Como señala el estudio de *Deeptrace Labs* sus creadores eliminaron el sitio web oficial pero el código quedó en Internet, e incluso se crearon nuevas versiones mejoradas que cobraban por su utilización.

Es preciso incidir en el mencionado informe elaborado por *Deeptrace Labs,* uno de los informes referentes en el marco de los *deepfakes,* publicado en el año 2019, en este se registró que la mayoría de los vídeos *deepfake* eran vídeos pornográficos, un 96%, frente al 4% que no lo eran. Además, destacaron que en este tipo de vídeos las protagonistas eran mujeres, frente a los vídeos que no tenían contenido pornográfico donde los protagonistas eran hombres (Aider, Patrini, Cavalli, Cullen (Deeptrace Labs), 2019).

Junto con las dificultades inherentes a la detección de los delitos que se sirven de la IA para su comisión, se ha destacado como la elaboración anónima que ofrecen las herramientas de IA generativa puede obstaculizar la actuación de las autoridades competentes (Europol Innovation Lab, 2022). Uno de los principales objetivos tras la detección de un hecho delictivo es la identificación de los responsables, cuestión que favorecerá también la represión del delito y la reparación del daño. En Internet, desde su aparición, esta cuestión se configura como una dificultad significativa y, además, parece agravarse con el uso de la IA.

En definitiva, cada vez son más numerosos los informes, los documentos o las noticias que de forma directa o indirecta identifican que nos encontramos ante una amenaza que favorece la ciberdelincuencia de género.

Además, se ha detectado que los sistemas de IA generativa se están implementando para cometer delitos contra víctimas menores de edad, siendo destacables el embaucamiento de menores o la creación de materiales relacionados con el abuso sexual infantil en línea. En estos casos podemos encontrar una amplia variedad de ejemplos en los que la IA generativa se ha utilizado para la comisión de estos hechos delictivos. En primer lugar, la simulación de una identidad falsa, bien de otra persona o bien de un menor de edad, ha sido empleada para favorecer el acercamiento y para ganarse la confianza de las víctimas menores, incluso para la obtención de material de contenido sexual explícito autogenerado por estos menores. De igual modo, ya se ha detectado y detenido a un sujeto en España que utilizaba un sistema de IA generativa en el que añadía una descripción de texto y se generaban imágenes en atención a las preferencias y descripciones que realizaba en el citado texto. Por lo tanto, empleaba este tipo de IA para la

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

producción de materiales relacionados con el abuso sexual infantil en línea, material pornográfico de menores; generaba archivos de "extrema dureza" en los que se "representaban imágenes reales de niñas de muy corta edad siendo violadas y utilizando órganos y juguetes sexuales desproporcionados" ("La Policía Nacional detiene a un pedófilo que utilizaba inteligencia artificial para crear material de abuso sexual infantil de extrema dureza", 21 de diciembre de 2022).

De igual modo, podríamos encontrarnos incluso con ciberdelincuencia de género en el marco de la delincuencia organizada, se ha identificado que los *deepfakes* pueden favorecer el fraude documental, lo que puede facilitar la práctica de otros delitos como la trata de seres humanos, el tráfico de personas e incluso algunas actividades relativas al terrorismo (Europol Innovation Lab, 2022), contribuyendo no solo a la captación sino también al transporte de mujeres y menores con diferentes fines.

En este sentido, la realidad actual pone de manifiesto la preocupación de la comunidad internacional por regular este fenómeno, tipificar estas conductas y favorecer la represión de las mismas. Podemos reseñar brevemente como se han incluido preceptos en recientes propuestas o se han registrado enmiendas en este sentido, sin perjuicio de las que ya han sido señaladas en la Propuesta de Reglamento de IA de la UE y que serán analizadas con más profundidad en los epígrafes posteriores.

En primer lugar, en la Propuesta de Directiva sobre la lucha contra la violencia contra las mujeres y la violencia doméstica se ha recogido, en el considerando 19 y en el artículo 7, la necesidad de tipificar la producción, manipulación o difusión no consentida de material íntimo o manipulado. Se ha incluido expresamente la alusión a la edición o fabricación de *deepfakes*[7].

En este mismo sentido, se han recogido enmiendas a la propuesta de Reglamento por el que se establecen normas para prevenir y combatir el abuso sexual de los menores que identifican la necesidad de considerar que existe una mayor probabilidad de que las niñas sean víctimas, afectando "la desigualdad de género, la violencia estructural y la discriminación contra las mujeres" en algunas tipologías delictivas, como en el abuso sexual infantil en línea (Comisión de Derechos de las Mujeres e Igualdad de género a la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores, 8 de mayo de 2023). Desde la aprobación hace décadas de otros instrumentos se ha considerado delictiva la representación visual o la existencia de imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita (Ratificación del Convenio sobre la Ciberdelincuencia, 17 de septiembre de 2010) o

7. Se hace referencia en el considerando 19 a "la fabricación de ultrafalsificaciones (deepfakes), en las que el material se parezca sensiblemente a una persona, a objetos, lugares u otras entidades o acontecimientos existentes, representando actividades sexuales de otra persona, y pueda dar a otros la impresión falsa de que es auténtico o veraz".

Además, se persigue la protección de la amenaza: "En aras de una protección eficaz de las víctimas de estas conductas, también debe regularse la amenaza de llevarlas a cabo".

(Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica. Estrasburgo, 8 de marzo de 2022)

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

imágenes realistas de los órganos sexuales de un menor con fines principalmente sexuales (Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, 17 de diciembre de 2011, artículo 2), casuística entre la que tendría cabida la creación de material a través de sistemas de IA generativa[8]. Sin perjuicio de que si se utilizan imágenes reales de menores o se manipula material audiovisual con esta tecnología también será considerada delictiva incluso su producción, oferta, difusión, adquisición o posesión, entre otras.

En definitiva, podemos afirmar que la IA generativa está siendo utilizada para perpetuar y facilitar la práctica de todo un elenco de ciberdelitos de género. Debido a ello, se están sumando algunas dificultades adicionales a las investigaciones tradiciones, las cuales debemos considerar como cuestiones urgentes a atender, ya que nos podemos encontrar ante fenómenos delictivos globales y graves. En los siguientes apartados analizaremos cuáles son las perspectivas de futuro existentes en el marco de la UE y qué desafíos no se han contemplado pero que son necesarios para poder aprovechar las ventajas tecnológicas de la IA con el objetivo de minimizar la impunidad y la cifra negra de estos ciberdelitos.

III. IA generativa como recurso para la investigación de autoridades policiales y judiciales

En algunos de los anteriores instrumentos señalados ya se recogieron medidas de investigación tecnológicas para hacer frente a diferentes ciberdelitos, por ejemplo, en el marco del Convenio sobre la ciberdelincuencia se incluyeron algunos tipos de interceptación, registro, conservación u obtención de diferentes tipos de datos (Ratificación del Convenio sobre la Ciberdelincuencia, 17 de septiembre de 2010). En este mismo sentido, a nivel europeo, se ha apostado por las órdenes europeas de investigación para la obtención de prueba transfronteriza, incorporando expresamente la intervención de las telecomunicaciones (Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, 1 de mayo de 2014), aunque quedándose escuetos en lo que respecta a la previsión exhaustiva de las diligencias tecnológicas más novedosas y óptimas para los ciberdelitos actuales. Por otro lado, en atención a otros instrumentos específicos, como los señalados en materia de abuso sexual infantil en línea o la reciente propuesta de Directiva relativa a violencia sobre la mujer, no han centrado su atención en lo que respecta a las diligencias de investigación tecnológicas, sin perjuicio de que instasen a los Estados a adoptar las medidas necesarias para su esclarecimiento y enjuiciamiento (Propuesta

8. Se hizo referencia a la denominada "pornografía virtual", como "creación artificial pero realista" (Circular 2/2015, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015, 19 de junio de 2015)

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica. Estrasburgo, 8 de marzo de 2022; Propuesta de Reglamento para prevenir y combatir el abuso sexual de los menores, 8 de mayo de 2023; Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, 17 de diciembre de 2011).

En atención a las propuestas existentes, podemos afirmar que la actuación de la Unión Europea está encaminada a establecer una regulación en materia de IA e incluso a contemplar las actividades delictivas en las que pueda mediar su utilización. No obstante, todavía no está suficientemente desarrollada la posibilidad de implementar los diferentes tipos de sistemas de IA para la investigación policial y judicial.

Desde la Unión Europea, entre las razones y los objetivos de la propuesta de Reglamento de IA se ha hecho mención a su intención de conseguir un equilibrio entre la apuesta por la tecnología y la salvaguarda de los valores, derechos fundamentales y principios de la UE (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, 21 de abril de 2021). En el contexto de la investigación policial y judicial no se prohíbe su utilización, sino que se prevé su regulación en atención a la necesaria salvaguarda de todos los derechos y garantías inherentes al proceso. En este sentido continuaremos el presente análisis, centrándonos en la implementación de la IA en el marco de la actuación policial y judicial para hacer frente a la ciberdelincuencia de género.

Se abordará esta cuestión sin perjuicio de que también se haya identificado la necesidad de preparar a las autoridades competentes para conocer el alcance de la utilización de la IA tanto con fines maliciosos como con otra intención no delictiva; como hace referencia Europol en el marco de análisis de la técnica de los *deepfakes* (Europol Innovation Lab, 2022). Como ha ocurrido con otros desarrollos tecnológicos la capacitación y formación también es necesaria para poder actuar contra los fenómenos delictivos emergentes.

En el marco del proceso penal se han planteado múltiples posibilidades de aplicación de la IA[9]. En los últimos años, muchas han sido las apuestas por la utilización de la IA para la investigación policial y judicial, habiendo destacado en el campo de la predicción, prevención y actuación policial (Dolz Lago, 2022; González-Álvarez, Santos-Hermoso, Camacho-Collados, 2020; Martín Diz, 2020a; Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)), 24 de marzo de 2022). En particular, también se ha apostado por su utilización en el

9. MARTÍN DIZ (2020a) señala que existen múltiples posibilidades como su implementación para "la obtención de datos para la investigación criminal, la valoración o el razonamiento de los resultados de la prueba o el cotejo de la adecuación del perito y su dictamen en la prueba pericial junto a las posibilidades predictivas".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

marco de la investigación criminal a través de la identificación biométrica, la realidad aumentada e incluso se han implementado sistemas de IA para la investigación de la ciberdelincuencia y detección de amenazas (Cuatrecasas Monforte, 2022; Martín Ríos, 2022; Richard González, 2023). Asimismo, con carácter todavía más específico, ya se ha apostado por la utilización de la IA para mejorar la investigación policial en casos de violencia de género (Magro Servet, 2021).

Con carácter general, con la propuesta de Reglamento de IA en la UE se persigue el establecimiento de una base sólida que nos permita armonizar la normativa relativa al desarrollo, funcionamiento y utilización de los sistemas de IA. Además, establece diferentes categorías en base al riesgo, proponiendo unas líneas de actuaciones proporcionadas en atención al mismo.

En el considerando 38 de la propuesta de Reglamento de IA, incluso en las enmiendas, se reconoce que "procede considerar de alto riesgo a múltiples sistemas de IA diseñados para usarse con fines de aplicación de la ley", en atención concretamente a la "precisión, fiabilidad y transparencia" que se deben garantizar. Asimismo, enumeran algunos de los sistemas que se incluiría: "polígrafos y herramientas similares, en la medida en que su uso esté permitido conforme a la legislación de la Unión y nacional pertinente, para evaluar la fiabilidad de las pruebas en un proceso penal; para elaborar perfiles durante la detección, la investigación o el enjuiciamiento de infracciones penales, y para realizar análisis penales en relación con personas físicas" (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023).

De igual modo, entre los sistemas de IA de alto riesgo contemplados en el anexo III de la propuesta inicial se incluyeron otros que podrían utilizarse en el marco de la investigación que se ha encomendado por ley a las autoridades policiales y judiciales. En este sentido, destacaron los sistemas biométricos y basados en la biometría; sistemas IA de apoyo a las autoridades encargadas de aplicar la ley para examinar grandes cantidades de datos, disponibles en distintas fuentes o formatos, para detectar modelos desconocidos o descubrir relaciones ocultas; sistemas IA empleados por autoridades públicas para verificar autenticidad de documentos y detectar documentos falsos; sistemas IA para detectar ultrafalsificaciones; y, entre otros, en el punto ocho es destacable la mención a "sistemas de IA destinados a ser utilizados por una autoridad judicial […], o en su nombre, para ayudar a una autoridad judicial o un órgano administrativo 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" (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, 21 de abril de 2021). Aunque algunas citaciones concretas a estos sistemas IA al servicio de las autoridades encargadas de hacer cumplir la ley se suprimen, agrupan o modifican por parte del Parlamento europeo en las últimas enmiendas (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023).

Es importante la aclaración que se realiza en atención a que "los sistemas de IA de alto riesgo no están prohibidos ni deben considerarse indeseables", sino que apuntan

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

que "por el contrario, el cumplimiento de los requisitos de conformidad establecidos en el Reglamento hace que dichos sistemas sean más fiables y tengan más probabilidades de tener éxito en el mercado europeo" (Parlamento Europeo, 22 de mayo de 2023). En definitiva, no se está excluyendo a que autoridades competentes a nivel nacional puedan hacer uso de estos para la práctica de las investigaciones.

Destacan los sistemas de IA generativa, que se han incorporado en la propuesta de IA de la UE bajo la denominación de "robots conversacionales" o "ultrafalsificaciones", definiéndolos como "un contenido de sonido, imagen o vídeo manipulado o sintético que puede inducir erróneamente a pensar que es auténtico o verídico, y que muestra representaciones de personas que parecen decir o hacer cosas que no han dicho ni hecho, producido utilizando técnicas de IA, incluido el aprendizaje automático y el aprendizaje profundo", por lo tanto, incluyendo cualquier sistema de IA que genere o manipule de texto, sonidos o vídeos (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023, artículo 3, apartado 44 quinquies). Para estos sistemas se han establecido unas obligaciones en materia de transparencia, enfocadas principalmente a la identificación de los mismos. Cuando los fines sean delictivos está claro que se omitirán estas obligaciones por parte de los ciberdelincuentes.

Por supuesto, ya se ha previsto que cuando sean las autoridades policiales y/o judiciales en el marco de sus funciones de detección, prevención, investigación o enjuiciamiento de infracciones penales, podrán omitir la obligación de que las personas que interactúan con determinados sistemas IA o material generado con esta tecnología conozcan realmente que se encuentran ante el producto o sistemas de IA generativa (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, 21 de abril de 2021). Desde la aparición de la propuesta ya se detectó que, por ejemplo, podría estar pensado para la utilización de "materiales camuflados o creados artificialmente por agentes encubiertos informáticos" (Bueno de Mata, 2021).

Aunque esta aclaración parece haberse modificado con la aprobación de las últimas enmiendas, ya que se permite directamente obviar esta obligación cuando esté el sistema IA previsto y autorizado en la legislación vigente (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023), por lo tanto, sería idóneo contar con una legislación que habilitara expresamente a la utilización de esta tecnología, ya que se evitarían problemas derivados de la falta de exhaustividad y seguridad jurídica.

De igual modo, se ha señalado que no se impide que las autoridades competentes utilicen sistemas IA para detectar dichas falsificaciones y para prevenir, investigar y enjuiciar las infracciones penales relacionadas con su uso. Por lo tanto, parece que sí se está instando a la necesidad de perseguir los delitos que se sirven de la IA generativa, pero no se prevé expresamente que esta tecnología se incluya en el marco de las diligencias de investigación tecnológicas.

Por parte de Europol, también se han realizado apuestas específicas que instan al estudio de los nuevos modelos de IA, como pueden ser los modelos de lenguaje

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

generativo, en aras a implementarlos de un modo específico en el marco de sus actuaciones, entrenando a estos sistemas de IA generativa privados con sus propios datos y salvaguardando la integridad y confidencialidad de los datos utilizados para su entrenamiento (Europol, 27 de marzo de 2023).

Cuando se introduce la IA en la Administración de Justicia se requieren datos de calidad y una incorporación de los mismos con precisión, con el objetivo de implementar "buenas tecnologías" (Magro Servet, 2018). Por su parte, en el caso de que los sistemas de IA que se utilizarán para realizar investigaciones criminales se apuesta por un control de calidad mucho mayor, en atención a todos los derechos fundamentales pueden verse comprometidos (Cuatrecasas Monforte, 2022).

Es importante atender a la utilización de sistemas IA también para investigar otros sistemas y técnicas delictivas basadas en IA que simulan comportamientos humanos o de otra índole (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). La probabilidad de detección podrá ser mayor si se recurre a esta misma tecnología, debido a ello es importante plantearse la IA como herramienta también de investigación. Urge esta consideración en atención al desarrollo exponencial de la tecnología y al alto grado de adaptación que están demostrando los delincuentes y organizaciones.

Asimismo, en la propuesta de Reglamento de IA de la UE original estos sistemas de IA empleados para detectar las ultrafalsificaciones por parte de las autoridades encargadas de la aplicación de la ley, es decir, por parte de las autoridades policiales y judiciales, se incluían en el anexo III de un modo expreso como sistemas IA de alto riesgo. Sin embargo, en las enmiendas del Parlamento, los sistemas IA empleados por autoridades policiales en el marco de una investigación podrían tener cabida en el apartado 8, letra a), relativo a "la utilización de esta tecnología para la investigación o interpretación de hechos y de la ley". Sin perjuicio de la mención expresa en la modificación propuesta por el Parlamento del artículo 52, apartado 3 bis, que ha sido previamente señalada[10]. Quizá se persigue evitar la obsolescencia los sistemas de alto riesgo, pero sí se realiza en otros ámbitos una enumeración más detallada y exhaustiva que otorgaría una mayor seguridad y garantía a las autoridades competentes en materia de investigación de la ciberdelincuencia. No obstante, es destacable en este sentido que desde la propuesta inicial se ha previsto la modificación y actualización del anexo III, relativo a los sistemas IA de alto riesgo, cuando se detecte que en atención al riesgo, a la gravedad y a la probabilidad de ocurrencia sea relevante y proporcionada su incorporación, en ponderación con los perjuicios que se podrían derivar de la aplicación de dichos sistemas IA (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023, artículo 7, apartado 1). En el caso de implementar sistemas de IA generativa en el marco de la investigación policial y judicial o bien sistemas para investigar los delitos

10. Se señala que "Asimismo, no impedirá que las autoridades encargadas de la aplicación de la ley utilicen sistemas de IA destinados a detectar ultrafalsificaciones y a prevenir, investigar y enjuiciar las infracciones penales relacionadas con su uso". (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

cometidos con IA generativa, en atención a la injerencia sobre los derechos fundamentales podría haberse condicionado su previsión específica en el anexo III. Sin perjuicio de que tenga cabida, como se ha señalado, en otros preceptos. Parece que la tendencia, tras las enmiendas del Parlamento, insta a una regulación genérica que necesitará una previsión legal exhaustiva a nivel nacional y en el marco de instrumentos de investigación transfronteriza.

En definitiva, la utilización de la IA generativa en el marco de la investigación de ciberdelitos de género corresponde a la implementación de sistemas IA de alto riesgo, por lo que deberá acogerse a los requisitos previstos en los artículos 8 y siguientes para este tipo de sistemas. Para ello, deberá implantar y mantener un sistema de gestión de riesgos; emplearán prácticas idóneas respecto a la gobernanza y gestión de datos; elaboración y mantenimiento de la documentación técnica y los registros actualizados; garantizarán un nivel elevado de transparencia, sin perjuicio de las citadas excepciones que se prevén para la práctica de investigaciones policiales y judiciales; se diseñarán en atención al requerimiento de que se pueda realizar una efectiva vigilancia humana de su actividad, previendo la minimización de las consecuencias negativas derivadas de la utilización de un sistema de IA generativa que puede suponer una injerencia sobre derechos fundamentales de las personas investigadas. Asimismo, estos sistemas deben contar con un nivel adecuado de precisión, solidez, seguridad y ciberseguridad, evitando y corrigiendo, asimismo, posibles sesgos (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023, capítulo 2; 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, 21 de abril de 2021, capítulo 2).

Es relevante el cumplimiento de todas estas cuestiones ya que en el marco de un proceso penal incoado por motivo de un ciberdelito, será importante también salvaguardar los derechos de las personas investigadas. En este sentido, en las enmiendas aprobadas con respecto a la propuesta de Reglamento de IA, se ha incluido que las autoridades competentes deben tener en consideración "el impacto del uso de herramientas de IA en los derechos de defensa de los sospechosos, en especial la dificultad para obtener información significativa sobre su funcionamiento y la consiguiente dificultad para impugnar sus resultados ante los tribunales" (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023, considerando 38, enmienda 69). Con carácter general, son muchos los derechos fundamentales y principios inherentes al proceso penal que se podrían ver comprometidos sino se incorpora este tipo de tecnología salvaguardando todos los requisitos relativos al funcionamiento de la IA y todas las garantías procesales (Martín Diz, 2020b).

Todas estas cuestiones deben considerarse sin perjuicio de que como también se ha señalado se pueda utilizar otro tipo de sistemas IA que favorezcan la verificación de material audiovisual o probatorio, como por ejemplo, se hace referencia por Europol a la necesidad futura de mejorar la detección de *deepfakes* comprobando una serie de marcadores de autenticidad (Europol Innovation Lab, 2022). No nos encontramos ante una novedad para las autoridades policiales y judiciales, ya que la elaboración de documentación o

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

material probatorio falso ya existía con carácter previo al desarrollo de la IA, no obstante, se requiere apostar por nuevas herramientas para hacer frente a técnicas que mejoran su práctica ilícita y que dificultan su detección. Por lo tanto, parece clave la utilización de la tecnología para también detectar lo que la tecnología ha creado.

Urge aprobar una regulación exhaustiva e internacional que contemple el funcionamiento y la utilización de todos los tipos de sistemas de IA, en particular de los sistemas de IA generativa en atención a las ventajas que ofrecen, ya que, como hemos señalado anteriormente, la falta de regulación de estas tecnologías va a suponer un mayor obstáculo para que fuerzas y cuerpos de seguridad puedan cumplir sus funciones y practicar investigaciones eficaces (Europol Innovation Lab, 2022).

IV. Líneas de actuación futuras para implementar la IA generativa: recomendaciones para actuar a corto, medio y largo plazo

Para finalizar el presente estudio se destacarán algunas líneas de actuación futuras que deben seguirse para poder implementar la IA generativa en el marco de actuación de las autoridades policiales y judiciales, pero también para que estas autoridades competentes en materia de investigación puedan atajar las amenazas que se están transformando debido a la implementación de este tipo de sistemas IA en los *modus operandi* de los diferentes delitos.

En primer lugar, ya se apunta desde Europol, que urge la necesidad de visibilizar el alcance de estos sistemas de IA generativa. Como ya se ha señalado, es necesaria la capacitación de las autoridades señaladas y la comprensión por estas de los nuevos fenómenos delictivos. Nos encontramos ante una realidad presente, que se ha magnificado en los últimos meses y solo de este modo se podrá avanzar hacia la consecución de una prevención, detección, investigación y enjuiciamiento eficaces (Europol, 27 de marzo de 2023). Es clave la capacitación y financiación para apostar por nuevas tecnologías que permitan atajar nuevas amenazas clave que perpetúan la desigualdad de género, como es este tipo de ciberdelincuencia.

Como también se ha apuntado a lo largo del presente estudio, el potencial que desarrollarán este tipo de sistemas de IA generativa en los próximos años favorecerá la actuación de los delincuentes, mejorando el éxito delictivo, principalmente protegiendo su identidad y obstaculizando las investigaciones delictivas, las cuales encontrarán mayores dificultades. La tecnología no cesa, la evolución y mejora de la IA y, en particular, de la IA generativa compromete la protección de los derechos de los internautas y las autoridades competentes deben contar con herramientas técnicas y legales que les permitan practicar actuaciones de alto nivel técnico, que sean eficaces y garantes.

A corto plazo, la implementación de los sistemas de IA generativa podría optimizar la utilización de algunas diligencias de investigación ya preexistentes; por ejemplo, la práctica del agente encubierto informático. En este sentido, sistemas multimodales podrían optimizar la actuación de las autoridades policiales y judiciales, favoreciendo la

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

protección de víctimas y de los propios agentes involucrados, por ejemplo, a través de perfiles e identidades falsas[11]. Por lo tanto, la tecnología se presenta ofreciendo unos recursos que permiten continuar con la adopción de técnicas de investigación que habían sido consideradas idóneas, por ejemplo, para la lucha contra la creación y distribución de material relativo a abuso infantil en línea.

En este concreto ejemplo, por un lado, nos encontramos con que se ha detectado la idoneidad de la utilización del agente encubierto informático y los diferentes tipos de registros, remoto y de dispositivos de almacenamiento masivo (Rodríguez Tirado, 2018), para la persecución de los delitos relativos a explotación sexual infantil en línea y a la distribución de material de abuso de menores y, asimismo, se ha identificado la necesidad de intercambiar material ilícito para obtener la confianza necesaria (Carou García, 2018) y poder acceder a los grupos u organizaciones, así como para concretar la autoría de este tipo de hechos delictivos. En este sentido también se han previsto epígrafes específicos en nuestra legislación vigente[12]. Encontramos en estos casos varios momentos en los que podríamos recurrir a la IA generativa; a sistemas que generen imagen, audio y vídeo para simular la identidad del agente; a sistemas de lenguaje para favorecer la interacción entre agente y presunto autor; e incluso a sistemas de IA generativa que generen el material que se requiere para intercambiar (Bueno de Mata, 2021).

Se ha detectado que la regulación preexistente en materia de diligencias de investigación tecnológicas podría servir como base para implementar este tipo de tecnología como herramienta en la investigación criminal, ya que se ha previsto la salvaguarda de los principios de especialidad, idoneidad, necesidad, excepcionalidad y proporcionalidad para autorizar su adopción con todas las garantías (Cuatrecasas Monforte, 2022). De igual modo, sería la opción más viable a corto plazo también para los sistemas de IA generativa.

En este mismo sentido podríamos enumerar otros ejemplos relativos a la utilización de esta herramienta para la investigación de los ciberdelitos de género que se cometan, por ejemplo, en el marco de organizaciones criminales. O bien se podría requerir la utilización de sistemas de IA generativa para el desarrollo de *software* policiales o judiciales que favorezcan la práctica de ciberrastreos u otras diligencias tradicionales; como puede ser el desarrollo de programas de detección de material de abuso sexual infantil en línea o bien *spyware* específicos para cursar registros remotos.

En atención a la complejidad y a las circunstancias del caso, se puede requerir que la investigación inicial que se está efectuando con un sistema de IA generativa se complemente con otras diligencias, que a su vez se pueden agilizar y mejorar utilizando otro tipo de sistemas IA. Por ejemplo, en el marco de actuación de un agente encubierto se puede necesitar la práctica de un registro remoto o un registro de dispositivos de

11. MARTÍN RÍOS (2022) ya señalaba: "En el marco de la represión policial de la pederastia, también se utiliza IA para construir perfiles falsos".

12. Véase artículo 282 bis 6 de la Ley de Enjuiciamiento Criminal española: "El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

almacenamiento masivo. En el citado ejemplo, el agente se podría beneficiar de la utilización de *malware* programado con tecnología IA para indagaciones remotas o bien de la capacidad de un *software* para tratar grandes cantidades de datos tras un registro físico u *online*.

La ausencia de fronteras y la inmediatez que ofrece Internet son dos características clave de las que se sirven los creadores y los que utilizan estas nuevas técnicas de IA, incluidos los delincuentes que perpetran ciberdelitos de género, los cuales ya identificaron estas particularidades como ventajas hace décadas. En este sentido, es preciso que se prevea con mayor exhaustividad la posibilidad de aplicar sistemas IA para realizar investigaciones transfronterizas. En el marco de análisis que nos ocupa, tenemos que destacar que la problemática de los *deepfakes* está consolidada en la actualidad a nivel global, expandiéndose de forma exponencial. En este mismo sentido, la práctica de investigaciones en Internet con frecuencia requiere el recurso a medios de investigación tecnológica que permitan la obtención de prueba transfronteriza. Sin perjuicio de que a corto plazo, como apuntamos a nivel nacional, se pueda utilizar la IA y la IA generativa para favorecer la práctica de estas diligencias ya preexistentes, sería oportuno que a largo plazo se concreten todos los requisitos, principios y extremos necesarios para poder implementar IA por parte de las autoridades policiales y judiciales. Incluso se puede aprovechar esta apuesta por la regulación de la IA como herramienta de investigación para crear nuevas diligencias, otorgando suficiente seguridad jurídica a estas prácticas que cada vez deberán ser más frecuentes y que tendrán que ser eficaces y salvaguardar los derechos fundamentales de las personas investigadas.

Por otro lado, también sería recomendable a medio plazo, debido a la complejidad que ello requiere, actualizar los instrumentos referentes en materia de tipificación y lucha contra la ciberdelincuencia; por ejemplo, el Convenio sobre la ciberdelincuencia. Y también apostar, a nivel regional, en la UE por concretar las propuestas en materia de regulación de los sistemas de IA de forma urgente, así como otras que de un modo más específico persiguen minimizar amenazas consolidadas que se están agravando debido al desarrollo tecnológico. Para ello, se requiere prestar atención a diferentes enmiendas que persiguen una lucha contra la ciberdelincuencia efectiva, sin dispersar las herramientas existentes o reiterar el desarrollo de las mismas, optimizando los recursos y agilizando la cooperación para este tipo de casos de investigación tecnológica.

La ciberdelincuencia, incluyendo en ella los delitos cometidos por razón de género que se dirigen con mayor frecuencia contra mujeres y niñas, se está convirtiendo en una herramienta clave para complementar otros delitos en el medio *offline* e incluso para la delincuencia organizada internacional. Ante esta realidad, podríamos encontrarnos ante el momento idóneo para apostar por la regulación de unas técnicas y medidas de investigación específicas para la ciberdelincuencia, que consideren todas las particularidades y obstáculos que se presentan en Internet y que se agravan con el desarrollo de los sistemas de IA. De este modo se unificarían los recursos disponibles y se podrían concretar los extremos necesarios para implementar los sistemas de IA en la investigación policial y judicial; en particular, debiéndose incluir los requisitos necesarios para cumplir con los principios y garantías procesales en este medio *online*.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

Bibliografía

AIDER, H., PATRINI, G., CAVALLI, F., CULLEN, L. (DEEPTRACE LABS). (2019). *The State of Deepfakes: Landscape, Threats, and Impact*.

BUENO DE MATA, F. (2021). "Protección de datos, investigación de infracciones penales e inteligencia artificial: novedades y desafíos a nivel nacional y europeo en la era postcovid". *La Ley Penal,* nº 150.

CAROU GARCÍA, S. (2018). "El agente encubierto como instrumento de lucha contra la pornografía infantil en Internet". *Cuadernos de la Guardia Civil,* nº 56, pp. 23-40. ISSN: 2341-3263.

CERDÁN MARTÍNEZ, V., PADILLA CASTILLO, G. (2019). "Historia del *fake* audiovisual: *deepfake* y la mujer en un imaginario falsificado y perverso". *Historia y comunicación social,* 24 (2), pp. 505-520. ISSN–e 1988-3056.

Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015. FIS-C-2015-00002.

Comisión de Derechos de las Mujeres e Igualdad de género a la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores. Enmiendas 46-536. 8 de mayo de 2023. 2022/0155(COD).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Fomentar un planteamiento europeo en materia de inteligencia artificial. COM/2021/205 final. Bruselas, 21 de abril de 2021.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025. COM (2021) 170 final. Bruselas, 14 de abril de 2021.

CUATRECASAS MONFORTE, C. (2022). "La inteligencia artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional". *La Ley*.

DEL CASTILLO, C. (18 de septiembre de 2023). "Un negocio con lista de espera: la app usada para 'desnudar' a menores en Badajoz cobra 9 euros por 25 fotos". ElDiario.es.

Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo. «DOUE» núm. 335, de 17 de diciembre de 2011, pp. 1 - 14.

Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal. OJ L 130, 1 de mayo de 2014, pp. 1–36.

DOLZ LAGO, J.M. (2022). "Una aproximación jurídica a la Inteligencia Artificial". *Diario La Ley,* nº 10096.

EUROPOL. (27 de marzo de 2023). ChatGPT. The impact of Large Language Models on Law Enforcement. Luxembourg: Publications Office of the European Union.

EUROPOL (EUROPOL INNOVATION LAB). (2022). Facing reality? Law enforcement and the challenge of deepfakes. Luxembourg: European Union Agency for Law Enforcement Cooperation. ISBN 978-92-95220-40-9.

EUROPOL. (2020). Internet organised crime threat assessment (IOCTA). Consultado en: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf (Fecha de consulta: 01/10/2023).

GONZÁLEZ-ÁLVAREZ, J. L., SANTOS-HERMOSO, J. & CAMACHO-COLLADOS. (2020). "Policía predictiva en España. Aplicación y retos de futuro". *Behavior & Law Journal*, 6(1), pp. 26-41.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

GONZÁLEZ PULIDO, I. (2017). "Avances y desafíos en materia de ciberdelincuencia de género a nivel europeo". *FODERTICS 6.0. Los nuevos retos del derecho ante la era digital*. Granada: Editorial Comares, pp. 149-160.

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. «BOE» núm. 226, de 17 de septiembre de 2010, pp. 78847-78896.

LOREDO, A. (14 de junio de 2023). "IA multimodales, metaverse y más". Consultado en: https://www.linkedin.com/pulse/ia-multimodal-metaverse-y-m%C3%A1s-all%C3%A1-alejandro-loredo/?trk=pulse-article&originalSubdomain=es (Fecha de consulta: 01/10/2023).

MAGRO SERVET, V. (2018). "La aplicación de la inteligencia artificial en la Administración de Justicia". *Diario La Ley,* nº 9268, sección doctrina.

MAGRO SERVET, V. (2021). "La inteligencia artificial para mejorar la lucha contra la violencia de género". *Diario La Ley,* nº 9898.

MARTÍN DIZ, F. (2020a). "Aplicaciones de inteligencia artificial en procesos penales por delitos relacionados con la corrupción". *Corrupción: Compliance, represión y recuperación de activos*. Valencia: Tirant lo Blanch, pp. 533-568.

MARTÍN DIZ, F. (2020b). "Capítulo XLV. Inteligencia artificial y proceso: garantías frente a eficiencia en el entorno de los derechos procesales fundamentales". Justicia: ¿Garantías versus Eficiencia? (Coord.: DE LUIS GARCÍA, E., BELLIDO PENADÉS, R., LLOPIS NADAL, P., JIMÉNEZ CONDE, F.). Valencia: Tirant lo Blanch, pp. 815-827.

MARTÍN RÍOS, P. (2022). "Empleo de *big data* y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras". *Revista de Internet, Derecho y Política,* nº 36, pp. 1-13.

NAVARRO, J. (21 de diciembre de 2022). "Detenido un pedófilo que usaba inteligencia artificial para crear material de abuso sexual infantil". *El País*.

PARLAMENTO EUROPEO. (22 de mayo de 2023). Informe sobre la 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. COM (2021) 0206.

PARLAMENTO EUROPEO. Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la 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 (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)). 14 de junio de 2023. Consultado en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.pdf (Fecha de consulta: 01/10/2023).

Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica. Estrasburgo, 8 de marzo de 2022. COM (2022) 105 final.

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. Bruselas, 21 de abril de 2021. COM (2021) 206 final.

Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)). OJ C 132, 24 de marzo de 2022, pp. 17–26.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

RETANA GIL, C. (2023). "Diálogos para el futuro judicial LX. IA Generativa y legalidad: ¿futuro o ciencia ficción? *Diario La Ley*, nº 10371.

RICHARD GONZÁLEZ, M. (2023). "Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial". *Justicia,* nº 1, pp. 147-281.

RODRÍGUEZ TIRADO, ANA M. (2018). "Las víctimas menores de delitos de pornografía infantil y de delitos de child grooming y su protección en el proceso penal. Las TICs y las diligencias de investigación tecnológica". *Justicia,* nº 1, pp. 137-199.

SECRETARIA GENERAL DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. (s.f.). *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*. ISBN 978-0-8270-7306-7

SIMÓ SOLER, E. (2023). "Retos jurídicos derivados de la Inteligencia Artificial Generativa: *deepfakes* y violencia contra las mujeres como supuesto de hecho". *InDret*. 2. DOI: 10.31009/InDret.2023.i2.11.

TREND MICRO RESEARCH, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI), EUROPOL'S EUROPEAN CYBERCRIME CENTRE (EC3). (2020). Malicious uses and abuse of Artificial Intelligence. *Trend Micro Research*.

VIEJO, M. (3 de octubre de 2023). "El caso de los desnudos con IA de Almendralejo se dispara: 26 menores implicados y 21 chicas afectadas". *El País*. 3 de octubre de 2023.

VILLATORO GONZÁLEZ, T., CAMBLOR ECHANOVE, G. (16 de junio de 2023). "La propuesta de reglamento europeo sobre inteligencia artificial para mitigar los riesgos de ChatGPT". *El País*.

—. (21 de diciembre de 2022). "La Policía Nacional detiene a un pedófilo que utilizaba inteligencia artificial para crear material de abuso sexual infantil de extrema dureza". *Gabinete de prensa de la Dirección General de la Policía*. Consultado en: https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=14981# (Última consulta: 01/10/2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

Compliance institucional y riesgo transnacional digital en la Unión Europea: ¿avanzamos hacia la prevención uniforme?

INSTITUTIONAL COMPLIANCE AND TRANSNATIONAL DIGITAL RISK IN THE EUROPEAN UNION: ARE WE MOVING TOWARDS UNIFORM PREVENTION?

Juan Ignacio Leo-Castela[1]
Profesor Ayudante Doctor. Universidad de Salamanca
leocastela@usal.es 0000-0003-2936-6017

Recibido: 29 de octubre de 2023 | Aceptado: 02 de diciembre de 2023

RESUMEN

En este trabajo se aborda, desde una perspectiva jurídico-económica, la gestión del riesgo transnacional digital por parte de la Unión Europea considerando la importancia creciente del compliance en el ámbito institucional como una herramienta innovadora y de extraordinaria utilidad para la gobernanza global de este riesgo. En este contexto, el trabajo se orienta hacia la búsqueda de respuestas que permitan aportar certidumbre en relación con los posibles avances de la Unión hacia un nuevo modelo de prevención uniforme.

PALABRAS CLAVE

Compliance
Unión Europea
Riesgo transnacional digital

ABSTRACT

This work addresses, from a legal-economic perspective, the European Union transnational digital risk management, considering the growing importance of compliance in the institutional field as an innovative and extraordinarily useful tool for the global risk's governance. In this context, the work is oriented towards the search for answers that allow us to provide certainty in relation to the possible European Union progress towards a new uniform prevention model.

KEYWORDS

Compliance
European Union
Transnational digital risk

1. Profesor Ayudante Doctor acreditado a Contratado Doctor en la Facultad de Derecho de la Universidad de Salamanca, despacho 113. Departamento de Economía Aplicada. Paseo Tomás y Valiente s/n, Campus Unamuno. CP 37007, Salamanca (Salamanca). Investigador en el Centro de Investigación para la Gobernanza Global (CIGG) de la Universidad de Salamanca. La elaboración de este trabajo de investigación se ha realizado en el marco del Proyecto I+D del Ministerio de Ciencia, Innovación y Universidades: "Cumplimiento normativo y protección penal de la Administración Pública".

I. Introducción

La demanda de herramientas idóneas para una adecuada gestión de los riesgos legales ha crecido exponencialmente a medida que la comunidad internacional se ha ido volviendo cada vez más vulnerable frente a los retos y desafíos globales de nuestro tiempo. Nos hallamos inmersos en la llamada "cuarta revolución industrial" (Schwab, 2017). Una revolución marcada por la aceleración digital (pre y post pandemia) y por el auge del "dato" como elemento vertebrador de un nuevo orden social, jurídico y económico[2]. En este contexto, la Unión Europea pretende avanzar hacia la búsqueda de soluciones comunes para la adecuada gestión de los riesgos legales en el panorama comunitario. De manera particular, en relación con aquellos que está propiciando la transformación digital.

El nivel de globalización alcanzado en los últimos años ha traído consigo importantes avances cuyo impacto resulta innegable en términos de bienestar social y progreso. Sin embargo, en la otra cara de la moneda la globalización representa también la necesidad de contar con instrumentos idóneos (cada vez más sofisticados) con los que alcanzar una prevención eficaz y uniforme en ámbitos tan complejos como la delincuencia transnacional, el cambio climático, la protección de los derechos humanos, o la ciberdelincuencia, entre otros[3].

Bajo mi punto de vista el papel de las autoridades comunitarias frente a los retos globales que nos rodean se ha enfocado excesivamente en la producción legislativa de un Derecho cada vez más técnico, indeterminado y complejo cuya aplicación en la práctica no solo resulta tediosa para los operadores jurídicos, sino que a menudo termina frustrando la finalidad de la norma[4]. Si bien es cierto que este afán de la Unión Europea por promulgar normativas en tiempo récord ha estado orientado a la siempre bienintencionada protección de bienes jurídicos expuestos a situaciones de riesgo, no es menos cierto que esta premura ha condicionado en cierta medida la calidad del paraguas jurídico de protección ocasionando alguna que otra gotera. No sería justo obviar que el contexto socioeconómico reciente no ha sido precisamente el más favorable[5] y que, al mismo tiempo, la

2. En este sentido se expresa el *European Data Market study measuring the size and trends of the EU data economy*. Disponible en: https://digital-strategy.ec.europa.eu/en/library/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy. Fecha de última consulta: 24 de agosto de 2023.

3. Estos y otros riesgos globales han sido recopilados por el Eurobarómetro 2022 sobre el futuro de Europa disponible en: https://www.europarl.europa.eu/news/es/press-room/20220119IPR21314/futuro-de-europa-el-cambio-climatico-es-el-mayor-reto-para-la-ue. Fecha de última consulta: 24 de agosto de 2023.

4. En este sentido, la evolución del Derecho digital comunitario resulta tan innegable como la complejidad técnica de algunas de sus normas. Sirva de ejemplo la reciente aprobación del Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo de 31 de mayo de 2023 relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n. º 1093/2010 y (UE) n. º 1095/2010 y las Directivas 2013/36 UE y (UE) 2019/1937. Disponible en: https://www.boe.es/doue/2023/150/L00040-00205.pdf Fecha de última consulta: 24 de agosto de 2023.

5. Según Eurostat la evolución del crecimiento económico de la Unión Europea-27 desde 2020 ha estado realmente muy limitada. La serie histórica completa se encuentra disponible

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

inmediatez con la que a veces se materializan algunos de estos riesgos globales deja muy poco margen de maniobra para que el Derecho comunitario y los mecanismos multilaterales de la Unión (a menudo costosos) puedan desplegar a tiempo su verdadera eficacia. En este contexto debo detenerme un instante a reflexionar sobre la conveniencia de actualizar la configuración tradicional de las normas jurídicas y su capacidad para garantizar el orden y la convivencia social (prevención del daño social) a la luz de este problema que en los últimos tiempos parece estar haciéndose más evidente.

En otras palabras, la producción normativa tradicional respondía a una serie de criterios más o menos satisfactorios que tal vez por inercia (o, sencillamente, por falta de necesidad) se fueron replicando mecánicamente a lo largo del tiempo, pero este planteamiento, a la vista de realidad actual, quizás haya quedado obsoleto. Para comprender mejor este posicionamiento conviene prestar atención al concepto de "sociedades del riesgo" acuñado por Ulrich Beck en pleno apogeo del fenómeno de la globalización a principios de los años noventa (Beck, 1992, 51)[6]. Siguiendo a este autor, los riesgos se definen como la probabilidad de que exista un daño o impacto. En términos agregados cuando hablamos del conjunto de una sociedad, un daño o impacto social. Aunque la opinión de Beck es que su origen puede responder a factores de lo más diverso bajo mi punto de vista y al menos a efectos de cuanto aquí se expone, podríamos dividirlos en dos grandes grupos: aquellos en los que interviene el factor tecnológico y aquellos en los que no.

Siguiendo este razonamiento podría decirse que el hecho de que en los últimos tiempos se hayan incrementado los riesgos (probabilidad de que exista un daño social, entre otras razones, a causa de haber alcanzado un nivel récord de globalización), podría justificar la necesidad de elevar el "listón preventivo" por parte de las autoridades comunitarias para una mejor protección de los bienes jurídicos en juego. Como se verá a lo largo de estas páginas, este planteamiento ya ha calado en la nueva forma de legislar de la Unión Europea modificando, en parte, el paradigma tradicional e incorporando aspectos tan novedosos como la medición de los niveles de riesgo, las evaluaciones de impacto o los mecanismos de compliance (corporativo y/o institucional). De manera particular, cuando se trata prevenir un daño social en ámbitos tan relevantes o con tanta sensibilidad social como los referidos anteriormente[7].

---

en: https://ec.europa.eu/eurostat/databrowser/view/NAMQ_10_GDP__custom_7680558/bookmark/table?lang=en&bookmarkId=a4ce6a9d-7ef1-48f1-a5bf-e23a717fcf75 Fecha de última consulta: 26 de agosto de 2023.

6. El concepto "sociedades del riesgo" fue actualizado por el mismo autor en el año 2009. Con anterioridad a los trabajos de Beck, Simon (1987) describió la gobernanza de la sociedad del riesgo como un "zumbido de circuitos integrados" en el que se interrelacionan diferentes tipos de riesgo (y ésta es precisamente una de las dificultades más importantes para su adecuada gobernanza y gestión. Al otro lado de la doctrina encontramos autores más cercanos en el tiempo como O'Malley (2002) que sostiene que la adecuada gestión del riesgo no es más que una técnica de gobernanza que permite mejorar la eficacia en la sociedad.

7. Véase en este sentido la nota informativa sobre la importancia de las evaluaciones de impacto en los procesos de producción normativa de la Unión Europea, disponible en: https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/impact-assessments_es Fecha de última consulta: 29 de agosto de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

En paralelo, la irrupción de la responsabilidad legal de las personas jurídicas en los ordenamientos internos de cada Estado miembro (ya sea en sede civil, penal, o administrativa) ha modificado la manera de entender la responsabilidad de las organizaciones hacia la sociedad y su entorno. Entre los factores determinantes de este cambio de paradigma no podemos obviar la influencia internacional de organismos tan relevantes como la OCDE o Naciones Unidas que, al margen de la Unión Europea, también han liderado un empuje hacia la consideración de las personas jurídicas como sujetos legalmente responsables[8].

La configuración de todo este nuevo marco legal entorno al nuevo *status* jurídico de las corporaciones y empresas supone la incorporación de importantes obligaciones en materia de buen gobierno corporativo, ética y cumplimiento que han ido calando con mayor o menor protagonismo en las diferentes ramas del Derecho (de manera mayoritaria en el ámbito penal, administrativo y tributario). No solo a nivel interno en los diferentes Estados miembros sino, también en el Derecho comunitario. La puesta en marcha de protocolos y procedimientos normalizados para el control, el registro y el reporte de riesgos ha dejado de ser una cuestión exclusivamente interna de las organizaciones y empresas a partir del momento en que los organismos internacionales han comenzado a considerar su utilidad potencial para la prevención de riesgos transnacionales como los que se expondrán enseguida. Sin embargo, las autoridades nacionales y supranacionales se enfrentan al importante reto de gestionar procesos y flujos de información sensible mediante el empleo de recursos que, desafortunadamente, a menudo resultan escasos. En esta tarea las tecnologías de la información y la comunicación han irrumpido con fuerza desplegando un amplio abanico de bondades entre las que sobresale, sin duda, la agilización y el ahorro de costes. La progresiva digitalización del compliance corporativo e institucional responde precisamente a la necesidad de gestionar los riesgos de la manera más eficiente posible.

En vista de todo ello parece razonable reflexionar no solo sobre el papel que está desempeñando la tecnología en la mayor o menor gravedad del riesgo transnacional presente en la Unión Europea si no, al mismo tiempo, también en la gestión que se realiza (tanto a nivel interno en cada Estado miembro como a nivel supranacional) de estos riesgos.

II. El riesgo transnacional digital

2.1. Riesgo transnacional digital y evaluaciones de impacto

Entre las dificultades a las que se enfrenta la Unión Europea a la hora de prevenir y mitigar los riesgos legales que eventualmente pudieran tener un impacto sobre sus

8. Sirvan de ejemplo, entre otros textos internacionales, la Convención para Combatir el Cohecho de Servidores Públicos Extranjeros en Transacciones Comerciales Internacionales de la OCDE. Disponible en: https://www.oecd.org/daf/anti-bribery/convcombatbribery_spanish.pdf; la Convención de Naciones Unidas contra la Corrupción (2004); la Directiva 2008/99/CE del Parlamento Europeo y del Consejo, de 19 de noviembre de 2008, sobre protección del medio ambiente mediante el Derecho penal; o, en el ámbito del *softlaw* las normas ISO 19600, 19601, 19602 e ISO 37001 y 37301 (todas ellas en materia de sistemas de gestión de *compliance* y antisoborno).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

objetivos e intereses destaca sin duda su carácter transnacional. No en vano, como expondré más adelante, la fragmentación geográfica ha representado tradicionalmente un importante aliado para la delincuencia transnacional. Sin embargo, este viejo problema adquiere un nuevo matiz cuando además del componente transnacional se incorpora el elemento digital. En este sentido no han tardado en ponerse de manifiesto los problemas para atajar la ciberdelincuencia en el espacio transnacional. El uso de recursos informáticos y tecnológicos específicamente diseñados para la mejor (peor) perpetración de actos ilícitos es ya una realidad incontestable cuyo impacto sobre el mercado único y sobre los intereses particulares de los ciudadanos comunitarios hemos podido comprobar, por ejemplo, a propósito del auge de los criptoactivos y de la inseguridad jurídica que propiciaba su desregulación inicial.

Este hecho conduce irremediablemente a que las autoridades e instituciones públicas hayan comenzado a considerar el empleo de la tecnología con la finalidad de combatir de una manera eficaz este tipo de amenazas globales. En este sentido, como se verá a lo largo de las páginas que siguen, el diseño de los mecanismos internacionales de cooperación-prevención ha ido incorporando progresivamente componente tecnológicos y digitales para tratar de acomodarse a la realidad actual. Por un lado, esto nos permite contar con herramientas más sofisticadas (y, probablemente, más eficaces). Sin embargo, por otro lado, no es menos cierto que por la misma razón su utilización se está volviendo cada vez más compleja para los operadores jurídicos y los organismos públicos implicados.

Junto a esta novedad quiero referirme ahora, aunque sea brevemente, a la irrupción del concepto "evaluación de impacto" en el Derecho comunitario y a la importancia que representa no solo a la hora de gobernar y gestionar los riesgos en la Unión Europea sino, muy especialmente, a la hora de afrontar su prevención uniforme. Podría decirse que este concepto aterriza de manera más evidente en el ordenamiento comunitario a partir de la aprobación del Reglamento 2016/679 en materia de protección de datos de carácter personal[9]. Su finalidad esencial no es otra que la de introducir la posibilidad de evaluar, atajar, gestionar, y gobernar a priori situaciones de riesgo mayor que bajo para los derechos de las personas físicas en el ámbito de la protección de sus datos. Cuya vulneración, por cierto, se produce con cada vez más frecuencia en el espacio virtual.

La propia doctrina también se ha referido al concepto como "un proceso o metodología para determinar los riesgos o impactos que una propuesta o proyecto tiene en la privacidad de los individuos, así como para determinar los medios o soluciones para mitigar o evitar dichos riesgos o impactos negativos" (Puyol, 2018, 351). La utilidad de este recurso hace que resulte cuanto menos interesante detenerse a reflexionar sobre su posible incorporación a otras materias en las que, por su especial naturaleza, también resulte conveniente realizar este tipo de evaluaciones previas. Entre otras, el Derecho medioambiental (Quintana *et al*, 2014, 267), el Derecho fiscal y tributario o, como en el caso que nos ocupa, el Derecho digital.

9. Véanse en este sentido el artículo 35 y siguientes del Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Como se verá a continuación la importancia que la Unión Europea le confiere a este instrumento incide de manera directa en la prevención transnacional de cualquier tipo de riesgo en un sentido positivo, esto es, minimizando su daño o impacto social. Conviene tener muy en cuenta que la existencia de riesgos globales que trascienden del ámbito interno tiene un efecto multiplicador sobre el daño social potencialmente asociado y que, en este sentido, toda evaluación previa resultará bienvenida.

Desde este enfoque la Unión Europea parece orientarse hacia la consolidación de una prevención en origen (desde la producción de las normas) fomentando una cultura de prevención a partir de la regulación de una serie de obligaciones previas de vigilancia y control sobre la que edificar toda una arquitectura global para la gobernanza del riesgo. No puede negarse que, al menos en los primeros textos, los enfoques socioeconómico y medioambiental parecen prevalecer sobre el resto. En este punto quiero advertir que el hecho de no considerar su potencial preventivo en otras áreas del Derecho puede hacer que la Unión Europea pierda este tren hacia la configuración de un nuevo modelo de cooperación-prevención. Aún es pronto para saberlo puesto que apenas se ha comenzado con esta andadura y, por tanto, aún no abundan las iniciativas legislativas que incorporan este nuevo enfoque. Pero me atrevería a pronosticar que dada su utilidad preventiva y más allá del posicionamiento que finalmente adopten las autoridades comunitarias el recurso hacia las evaluaciones previas de impacto será una práctica frecuente en la era del dato.

Por otro lado, no quiero dejar de mencionar el hecho de que la producción normativa haya sido casi exclusivamente el único recurso empleado por la Unión Europea en la lucha contra el riesgo transnacional digital. Como se viene indicando la complejidad de esta realidad tiene un claro reflejo en la producción de normas comunitarias cada vez más complejas lo cual ha propiciado la aparición de dos nuevos problemas que se suman a los citados anteriormente. El primero es el relativo a las dificultades propias de su integración en el acervo comunitario. Y el segundo, tanto o más importante, es la sobrecarga de trabajo en la interpretación de estas normas que a la postre ha asumido el Tribunal de Justicia de la Unión Europea (TJUE) como último intérprete y garante de la coherencia entre las diferentes normas que integran el Derecho comunitario.

De manera paralela los intentos del legislador nacional por abordar jurídicamente los riesgos que representa la revolución digital han desencadenado una diarrea legislativa en dos sentidos. El primero a iniciativa propia y, el segundo, por la necesidad de trasponer e integrar en el derecho interno la normativa comunitaria. La crítica que cabe exponer frente a esta nueva realidad pasa de nuevo por recalcar la importancia de pensar antes de legislar. O, dicho en otras palabras, la importancia de evaluar el impacto que tendrá en la comunidad jurídica y en la sociedad general la aprobación de una determinada norma. De manera particular, si su complejidad radica en las dificultades del legislador para tratar de dotar a la sociedad de instrumentos idóneos para la gobernanza de según qué riesgos legales. En consecuencia, nos encontramos frente a un poder judicial cada vez más sobrecargado y ante una sumisión pericial que parece que ya es imparable en la revolución digital.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Quizás la solución pase por un cambio de mentalidad o simplemente por una evolución cultural que nos permita poner en valor la importancia de la valoración apriorística del riesgo digital y su potencial impacto dañino sobre determinados bienes jurídicos dignos de protección. No solo por razones de seguridad jurídica (que también) sino acaso en términos económicos y de bienestar social. En cierta medida la eficacia de las evaluaciones de impacto depende de su contenido y alcance, pero no es menos cierto que existen otros aspectos como su obligatoriedad o su mayor o menor carácter vinculante que quedan a expensas de un legislador que a menudo carece de los conocimientos propios de una ciencia que le puede resultar tan ajena o lejana como la informática, la ingeniería, o la inteligencia artificial. En este sentido quiero subrayar que la importancia que el legislador le confiera a los resultados derivados del proceso de evaluación tiene un impacto directo sobre el diseño de las políticas públicas y el resto de las medidas (no estrictamente legales) con las que se pretenda combatir cada riesgo.

Desde esta perspectiva con este trabajo pretendo abordar la necesidad de avanzar hacia una prevención uniforme del riesgo transnacional digital en la Unión Europea. De entre las múltiples iniciativas puestas en marcha hasta la fecha dirigiré mi análisis a la innovación por la que recientemente parece estar apostado la Unión desde el compliance institucional para el conjunto de los Estados miembros ya que, como trataré de exponer enseguida, parece posicionarse como la herramienta contemporánea más efectiva para esta lucha.

2.2. Riesgo transnacional digital y compliance institucional. La experiencia de la OCDE y sus implicaciones para la Unión Europea

Coincidiendo con el nuevo escenario que dibuja la transformación digital y a propósito del riesgo transnacional digital, las transacciones realizadas *online* por parte de los ciudadanos de la Unión Europea están alcanzado niveles desconocidos hasta la fecha. No solo en sus relaciones comerciales con oferentes y productores comunitarios sino también con terceros países. El modelo tradicional de integración económica también se ha "contaminado" de la nueva realidad digital como ha reconocido la propia Unión Europea en su estrategia para el mercado único digital[10]. La gran pregunta que a mi juicio procede plantearse ahora es si contamos en el plano supranacional con la estructura jurídico-social necesaria para la protección de los ciudadanos comunitarios frente a los riesgos que entraña la extraordinaria expansión de la revolución digital. Bajo mi punto de vista lo ideal sería contar con una herramienta cooperativa multiplataforma desde la que poder gestionar eficazmente cualquier manifestación del riesgo transnacional digital. Quizás, comenzando por los que representan un mayor nivel de peligrosidad o tienen una mayor probabilidad de impactar sobre intereses y objetivos comunes. Entre ellos podemos citar algunos de los típicamente asociados a las conductas propias de las

10. Disponible en: https://eufordigital.eu/discover-eu/eu-digital-single-market/ Fecha de última consulta: 4 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

personas físicas como, por ejemplo, el riesgo de sufrir una estafa en una compra *online*, el riesgo de sufrir una vulneración en la protección de datos de carácter personal, o el riesgo en la formalización de operaciones con criptoactivos en el espacio comunitario. Sin embargo, también resulta interesante atender desde la perspectiva del compliance corporativo al riesgo típicamente asociado a las conductas propias de las personas jurídicas como, por ejemplo, el riesgo de blanqueo de capitales mediante operaciones realizadas en línea, el riesgo de soborno o extorsión en la red, el riesgo de financiación ilegal, etcétera.

En todas estas modalidades coinciden el elemento transnacional y el elemento digital haciendo que todas estas conductas representen un nivel de riesgo mayor que bajo para la ciudadanía europea. Cualquier gestión eficaz de este tipo de riesgos precisará bajo mi punto de vista de mecanismos idóneos de vigilancia y control global que permitan alcanzar estándares de seguridad aceptables (habida cuenta que el riesgo cero no existe). Estas medidas forman parte de lo que podríamos considerar como compliance institucional o, en otras palabras, mecanismos de cooperación-prevención interinstitucional diseñados para la protección de todos aquellos riesgos que por exceder de las fronteras de un Estado miembro podamos catalogar como transnacionales. Esta idea no se encuentra en el acervo comunitario tradicional y tampoco es exclusiva de la Unión Europea (aunque parece que empieza a aplicarse en algunas de sus estrategias para la gobernanza global). Pero sí podemos identificarla, por ejemplo, en otros organismos internacionales como la OCDE.

La experiencia piloto de la OCDE con la activación en 2019 de su plataforma multilateral de compliance y aseguramiento de riesgos fiscales[11] representa uno de los primeros ejemplos para la gobernanza del riesgo transnacional a partir del compliance, aplicable también en el plano de lo digital. En este caso, en materia fiscal y tributaria. La acción número trece del Proyecto BEPS de la OCDE[12] se orientaba hacia una autoevaluación de riesgos que realizaba la persona jurídica contribuyente haciendo un especial hincapié en la documentación sobre precios de transferencia[13] de acuerdo con el principio de plena competencia (*arm's length principle)* (Keuschnigg y Devereux, 2013, 436). Sin perjuicio de las críticas señaladas por la doctrina a propósito de este modelo y de sus posibles perjuicios en los intercambios intragrupo (Witterndorff, 2010, 343), considero que su potencial disuasorio a la hora de evitar riesgos relacionados con la erosión de la base imponible del impuesto de sociedades resulta satisfactorio. En sintonía con esta iniciativa de

11. OCDE (2019): *International Compliance Assurance Programme* (2019). En línea: http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/international-compliance-assurance-programme-pilot-handbook-2.0.pdf Fecha de última consulta: 8 de septiembre de 2023.

12. OCDE (2015): *Plan de Acción BEPS*. En línea: https://read.oecd-ilibrary.org/taxation/plan-de-accion-contra-la-erosion-de-la-base-imponible-y-el-traslado-de-beneficios_9789264207813-es#page2 Fecha de última consulta: 8 de septiembre de 2023.

13. Documentación sobre precios de transferencia e informe país por país, Acción 13. Recurso disponible en: https://read.oecd-ilibrary.org/taxation/documentacion-sobre-precios-de-transferencia-e-informe-pais-por-pais-accion-13-informe-final-2015_9789264267909-es#page19 Fecha de última consulta: 8 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

la OCDE la doctrina señala otras de similar naturaleza como las normas internacionales para el control fiscal de empresas extranjeras (*controlled foreign company*, CFC) (Haufler, *et al*, 2018, 31), el diseño de mecanismos para la neutralización de los efectos derivados de instrumentos híbridos, o el proyecto CRS (*Common Reporting Standard*), entre otros (Belmonte, 2016, 103; Vérguez, 2016, 75).

El reflejo de estos instrumentos en la Unión Europea para la gobernanza del riesgo transnacional se ha ido dejando ver poco a poco (sobre todo a partir de la necesidad de gestionar los riesgos fiscales en el plano supranacional) en diferentes textos y Directivas comunitarias que han ido allanando el camino hacia la configuración de un modelo de compliance institucional de cooperación-prevención. Entre otras, podemos citar la Directiva 2014/107/UE del Consejo de 9 de diciembre de 2014[14], o la Directiva (UE) 2018/822 del Consejo, de 25 de mayo del 2018[15]. Ambas en relación con el intercambio automático y obligatorio de información en el ámbito de la fiscalidad en relación con los mecanismos transfronterizos sujetos a comunicación de información.

El éxito en la iniciativa de la OCDE radica en primer lugar en el número de Estados miembro acogidos a su plataforma internacional. Inicialmente, en 2019 contaba con las administraciones tributarias y los grupos empresariales (grandes contribuyentes) de ocho países de la OCDE[16]. Como podrá comprender el lector el éxito en la gestión de un riesgo transnacional es directamente proporcional al número de Estados que participan en el mecanismo propuesto para su adecuada gestión. A la luz de esta experiencia me propongo finalizar este epígrafe analizando algunos de los problemas que estuvieron (y siguen estando) presentes en el diseño y la aplicación de este tipo de plataformas. Pues, como se verá en el siguiente apartado resultan igualmente válidos para cualquier mecanismo de compliance institucional que se proponga en la Unión Europea para la gestión del riesgo transnacional digital.

El primer aspecto controvertido es la siempre temida pérdida de soberanía o de poder decisorio por parte de los Estados adheridos. Este viejo problema (del que es consciente la Unión Europea tal y como se aprecia en su derecho originario) adquiere ahora un nuevo matiz cuando se trata de gestionar los riesgos propios de la revolución digital. Aspectos como las diferencias en el nivel de alfabetización digital entre los diferentes Estados miembros de la Unión Europea[17], el acceso a internet, o las diferentes fuerzas con las que cada Estado se enfrenta a este tipo de riesgo a nivel interno generan asimetrías y desigualdades que comprometen sin duda la prevención uniforme. Para tratar de salvar este obstáculo la Unión cuenta desde hace décadas con mecanismos de cohesión que pretenden precisamente corregir este tipo de desequilibrios territoriales.

14. Directiva 2014/107/UE del Consejo de 9 de diciembre de 2014, disponible en: https://www.boe.es/doue/2014/359/L00001-00029.pdf. Fecha de última consulta: 17 de septiembre de 2023.

15. Directiva (UE) 2018/822 del Consejo, de 25 de mayo del 2018, disponible en: https://www.boe.es/doue/2018/139/L00001-00013.pdf. Fecha de última consulta: 17 de septiembre de 2023.

16. Australia, Canadá, Italia, Japón, Reino Unido, EE. UU., Países Bajos y España.

17. Recogidos entre otros indicadores en el *EU-DESI Index 2022*. Disponible en: https://digital-strategy.ec.europa.eu/es/library/digital-economy-and-society-index-desi-2022 Fecha de última consulta: 17 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Sin embargo, su impacto real sobre la mejora en el desempeño digital de algunas regiones y territorios sigue siendo muy limitado y, en consecuencia, sigue condicionando el acceso de estos ciudadanos al mercado único digital. Como posible solución al temor de la pérdida de soberanía a mi juicio debemos optar por mecanismos complementarios de compliance institucional y nunca sustitutivos de las medidas internas que en cada caso quiera adoptar cada Estado miembro. De tal manera (y este es el reto) que se establezcan criterios claros para aquellos casos de incompatibilidad y/o conflicto siempre en aras de la mejor prevención y/o mitigación posible del riesgo transnacional para el conjunto de los Estados miembros.

A propósito de este problema la doctrina señala que una posible vía para el combate eficaz de los problemas propios de las sociedades del riesgo es la puesta en valor del autogobierno o, si se prefiere, la autogobernanza. Es decir, la posibilidad de establecer políticas públicas que impliquen obligaciones que afecten a comportamientos individuales. Pues, en definitiva, el comportamiento de una sociedad no es más que la agregación de un conjunto de comportamientos individuales (Ericson y Haggerty, 1997, 83). No es menos cierto que estos aspectos, de una u otra manera ya están presentes en buena parte de los modelos de autorregulación regulada que ha ido incorporando el legislador nacional en los diferentes Estados miembros de la Unión Europea desde que se produjo el cambio de siglo. Y, que con independencia de que se hayan llevado por la vía penal, civil, o administrativa, impactan en el comportamiento de organizaciones y empresas que también actúan en el plano internacional.

En segundo lugar, cualquier mecanismo de estas características debe contar necesariamente con incentivos. A pesar de las ventajas derivadas del cumplimiento normativo en cualquiera de sus ámbitos no es menos cierto que existen costes que los Estados y las empresas no siempre están dispuestos a asumir. Entre otros, el coste de coordinar una actuación uniforme entre un conjunto de Estados con diferencias notables entre sí. La dificultad en este caso se nos presenta cuando existen diferencias importantes entre el estándar óptimo de prevención global y el que venía aplicando o pretendía aplicar cada Estado. Este hecho puede acabar obligando a uno o varios países a elevar las condiciones que venía exigiendo en su ámbito interno (shock asimétrico). Al igual que ocurre en el ámbito que nos ocupa existen otros muchos en los que la existencia de regímenes menos estrictos o más beneficiosos actúa como refugio para según qué prácticas o actos ilícitos propiciando la aparición de "focos de riesgo" en un territorio concreto, pero con efectos y consecuencias transnacionales para todos. Son precisamente estos focos los que a menudo nos pueden dificultar el consenso.

El reto en este punto pasa necesariamente por diseñar una plataforma multilateral que resulte atractiva para todos los Estados miembros con independencia de cuál sea su punto de partida. En este punto la Unión Europea se enfrenta al reto de diseñar un sistema de compliance institucional capaz de asumir que los *dispute-prevention efforts* deben ser una prioridad y que la estrategia de pretender una solución demasiado exigente puede acabar desembocando en un incentivo para que aquellos países con peor situación de partida terminen abandonando el proyecto. En relación con todo ello no debemos obviar que la integración de la tecnología y los principios que rigen el funcionamiento electrónico de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

las relaciones entre particulares y empresas presenta también diferencias notables que pueden estar propiciando la aparición de riesgos digitales potencialmente transnacionales en territorios concretos de la Unión Europea.

III. Compliance, riesgo transnacional y prevención de la delincuencia organizada en la Unión Europea

La estrategia comunitaria para la gobernanza de los riesgos transnacionales se ha centrado tradicionalmente en identificar aquellas actividades en cuyo ámbito pudiera resultar más probable la aparición de estos riesgos para, en un momento posterior, tratar de diseñar e implementar las medidas de vigilancia, monitoreo y control necesarias para alcanzar un determinado nivel de "prevención" y/o "seguridad". En este sentido la traslación de elementos más propios del compliance privado al ámbito público o institucional representa una oportunidad para la adecuada gestión de los riesgos (Nieto y Calatayud, 2015) no solo a nivel interno de cada Estado miembro sino, con cada vez más frecuencia, también en el plano internacional como se aprecia en las políticas públicas de la OCDE o, como se verá a continuación, en la nueva tendencia que parece estar iniciándose en la Unión Europea. Bajo esta premisa aludo al término compliance institucional en referencia a esta maniobra recordando que se trata de un concepto no estrictamente jurídico sino más bien interdisciplinar en el que se combina la ciencia jurídica con otras disciplinas como la economía, la gestión de riesgos, la sociología, o las nuevas tecnologías.

De entre las múltiples actividades que eventualmente pueden dar lugar a la aparición de riesgos transnacionales en la Unión Europea en este trabajo me centraré en una de las que, a mi juicio, resulta más preocupante en el momento actual: la delincuencia organizada. De manera particular atendiendo a sus diferentes manifestaciones en la realidad digital de nuestros días. Como ya anticipaba en el apartado anterior, la adecuada gestión y el tratamiento del riesgo transnacional digital encuentra un importante aliado precisamente en la incorporación de las nuevas tecnologías a las recientes medidas de vigilancia y control que nos ofrece el compliance en el ámbito público.

Debo especificar que a efectos de este trabajo me referiré a dos tipos de estrategias adoptadas por la Unión Europea para la prevención del riesgo asociado a la delincuencia transnacional: *ad intra* y *ad extra*. O si se prefiere en otras palabras: la acción exterior y la acción interior de la Unión. Como trataré de exponer a lo largo de estas páginas esta diferenciación resulta determinante a la hora de seleccionar las medidas preventivas con las que la Unión afronta este reto en uno y otro escenario, de evaluar su idoneidad, y de explorar las posibles sinergias o relaciones de complementariedad que se puedan establecer entre ellas en aras de la máxima aspiración de la Unión: la prevención uniforme. De la misma manera la diferenciación entre ambas resulta también pertinente a la hora de abordar las posibilidades de digitalización que nos ofrece la gestión de este tipo de riesgos en uno y otro escenario.

A lo largo de este trabajo me centraré mayoritariamente en la vertiente *ad intra* de la gestión del riesgo transnacional en la Unión Europea a partir de las diferentes amenazas y

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

desafíos que representa la sociedad digital. En este abordaje me propongo hacer hincapié en la eficacia preventiva de los nuevos elementos de compliance institucional incorporados recientemente por las autoridades comunitarias para tratar de aportar claridad sobre algunos de los interrogantes que considero más relevantes en esta materia. ¿Caminamos verdaderamente hacia una prevención uniforme del riesgo transnacional en el seno interno de la Unión? ¿Estamos ante el diseño de una nueva arquitectura de cooperación-prevención o, por el contrario, nos encontramos más bien ante una mera reformulación estética del modelo anterior? De encontrarnos en el primer escenario, ¿qué significado tienen entonces las nuevas medidas propuestas por las autoridades comunitarias? Y, lo que es más importante aún, ¿hacia dónde nos dirigimos ahora con este nuevo modelo?

3.1. La gestión del riesgo transnacional *ad extra*

Para una mejor comprensión del enfoque propuesto, de su sentido y alcance, conviene también atender siquiera sucintamente a esa otra dimensión exterior en la que la Unión ha desplegado tradicionalmente sus mecanismos para la gobernanza global de este riesgo. En este segundo escenario los esfuerzos de la Unión Europea se han concentrado tradicionalmente en tratar de gobernar, en sentido amplio, cualquier riesgo asociado a la criminalidad transnacional con origen en un territorio extracomunitario cuyo impacto pudiera resultar potencialmente dañino para los intereses de la Unión. En este sentido, la acción preventiva exterior se ha dirigido hacia aquellos países que, a juicio de las autoridades comunitarias, podían representar mayores niveles de riesgo. Destacan en este contexto los diferentes programas y acuerdos de cooperación (cooperación-prevención) suscritos durante los últimos años con América Latina. Por citar algunos ejemplos recientes me referiré, en primer lugar, al Programa de Asistencia contra el Crimen Transnacional Organizado 2017-2022 (en adelante, PAcCTO)[18] cuya finalidad esencial no ha sido otra que la de proporcionar asistencia técnica a los Estados de América Latina incluidos en el programa para la prevención eficaz del crimen organizado.

En mi opinión, desde su suscripción en el año 2017 el programa ha resultado fiel a su propósito y ha cubierto las expectativas. Incluso, como trataré de exponer, arrojando resultados y oportunidades para la cooperación internacional que representan importantes avances en esta materia. Seis años después de su inauguración puede afirmarse que el PAcCTO ha favorecido la cooperación estratégica entre la Unión Europea y América Latina para la prevención del riesgo de delincuencia transnacional. A mayores me gustaría señalar que este marco general de prevención constituye un apoyo importante sobre el que fundamentar cualquier medida de cumplimiento institucional y que también puede resultar especialmente útil cuando se trata de prevenir la vulneración de bienes jurídicos en el espacio virtual.

18. Países incluidos en el PAcCTO: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay, Venezuela.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Es de justicia reseñar que la cooperación policial y judicial se han posicionado como ejes vertebradores del PAcCTO gracias a la implicación de Europol y Eurojust. Como se verá en el siguiente apartado esta cooperación ha sido particularmente estrecha y, al menos bajo mi punto de vista, altamente satisfactoria. Tanto es así que ha permitido la conexión de algunos países de América Latina con otros mecanismos más propios de la gobernanza global de este tipo de riesgos *ad intra*. Aunque esta conexión no se haya materializado al mismo nivel al que rige para los Estados miembros su análisis resulta, a mi modo de ver, bastante interesante desde la perspectiva de la complementariedad entre los instrumentos preventivos *ad intra* y *ad extra* a la que me refería anteriormente. La importancia que representa este análisis justifica su abordaje en el apartado siguiente dedicado a la vertiente *ad intra*.

Como segundo ejemplo quiero referirme un instante al oportuno estrechamiento del cerco que se está produciendo a lo largo de este año 2023 entre la Unión Europea y el Comité Latinoamericano de Seguridad Interior (en adelante, CLASI) para la prevención transatlántica del riesgo de delincuencia transnacional. Con especial atención a la lucha contra el narcotráfico, la trata de seres humanos, el abuso sexual de menores, la corrupción y el blanqueo de capitales, los delitos contra el medio ambiente, el tráfico de armas de fuego, la ciberdelincuencia, o el tráfico ilícito de migrantes. Este nuevo marco de cooperación resulta particularmente interesante cuando se trata de analizar la comisión de estas conductas ilícitas en el espacio virtual.

El acercamiento responde a la misma línea de acción estratégica inaugurada en el PAcCTO y aspira a reforzar la cooperación para la prevención de la delincuencia transnacional mediante el establecimiento de marcos de colaboración permanentes entre la Unión Europea (y sus diferentes organismos y agencias de seguridad y justicia implicados en la gestión de este riesgo; entre ellos, Europol, Eurojust, y Frontex) y América Latina (y sus correspondientes agencias y organismos homólogos; de manera particular, la agencia policial latinoamericana Ameripol). De nuevo, la importancia de analizar este segundo hito histórico se pondrá de manifiesto en el siguiente apartado a propósito del estudio de la vertiente *ad intra* tanto en el plano *online* como *offline* y de sus posibles interacciones con este escenario de acción exterior de la Unión.

Antes de adentrarme en la segunda vertiente quiero referir que si algo caracteriza a esta acción exterior de la Unión es la prevención en origen (presente en ambos ejemplos). Esto es, la importancia de la identificación y la detección temprana de cualquier situación potencialmente dañina a partir de un refuerzo de la vigilancia en origen. Bajo mi punto de vista esta estrategia entronca en cierto modo con la doctrina anglosajona del *Tort Law* o Derecho de daños en la que la apreciación de responsabilidades legales se realiza a partir de la ubicación del origen de un riesgo en la fuente del daño (McBride y Bagshaw, 2008, 30). Si el origen de la responsabilidad es el daño cualquier prevención deberá dirigirse entonces hacia el origen del daño. Como expondré en el apartado dedicado al estudio de los elementos de compliance institucional presentes en la estrategia comunitaria para la prevención del riesgo de delincuencia transnacional, la apreciación (y en su caso la atribución) de responsabilidades penales para el caso de las personas jurídicas, pasa precisamente en este contexto por la adecuación o

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

inadecuación de las medidas internas de vigilancia y control llevadas a cabo para prevenir, reducir o mitigar riesgos legales. Medidas que, a través de los correspondientes sistemas de gestión de compliance, irán dirigidas con más o menos acierto hacia la identificación del riesgo como fuente de origen del daño. En otras palabras, lo habitual es que siguiendo esta teoría en términos generales se trate de orientar cualquier acción preventiva (corporativa o institucional) hacia la circunstancia o actividad concreta generadora del daño alcanzando así lo que se ha dado en llamar la prevención en origen. En este sentido sería razonable que desde la Unión Europea se fomentase la prevención uniforme en origen orientando cada acción preventiva hacia el origen del daño.

3.2. La gestión del riesgo transnacional *ad intra*

De entre las diferentes figuras delictivas que salen a escena cuando hablamos de prevenir el riesgo transnacional en la Unión Europea en este apartado me propongo abordar el asociado al crimen organizado transnacional (especialmente en su vertiente digital) por la importancia creciente que las autoridades comunitarias le han ido confiriendo en los últimos años a la necesidad de articular una red de cooperación-prevención uniforme entre los Estados miembros que optimice los recursos digitales con los que cuenta la Unión.

El interés de la Unión por diseñar una arquitectura eficaz de cooperación-prevención en esta materia se remonta al año 2014, fecha en la que el Consejo de Europa publica el libro blanco sobre el crimen organizado transnacional[19]. En este momento ya se empieza a alertar sobre el impacto de las nuevas tecnologías en la comisión de nuevas modalidades delictivas en la escena transnacional y de la conveniencia de aplicar igualmente los recursos tecnológicos a cualquier estrategia preventiva. Conviene recordar que por aquel entonces la Unión ya estaba inmersa en la preparación de su estrategia para el mercado único digital y que la protección de este mercado y la creación de un espacio virtual de confianza recíproca para oferentes y demandantes precisaba de mecanismos para la prevención de cualquier tipo de riesgo transnacional digital. Bajo esta premisa la importancia de prevenir y gestionar eficazmente este tipo de riesgos se va convirtiendo poco a poco en una prioridad para el correcto funcionamiento del mercado.

La publicación de este libro blanco representa toda una declaración de intenciones por parte de las autoridades comunitarias al incluir, por primera vez, un diagnóstico de situación (fallos y problemas detectados) y un paquete específico de acciones posibles consideradas idóneas para una prevención eficaz y uniforme entre todos los Estados miembros. A mi modo de ver con esta iniciativa el Consejo de Europa hace un llamamiento a los Estados miembros poniendo de manifiesto dos grandes problemas que han dificultado (y que, al menos a mi juicio, continúan dificultando) la gobernanza del riesgo transnacional en el seno interno de la Unión.

El primero de ellos es la fragmentación geográfica y sus consecuencias desde el punto de vista del riesgo ya que, como es sabido, en no pocas ocasiones ha propi-

19. Disponible en: https://rm.coe.int/168070e545. Fecha de última consulta: 21 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

ciado la aparición de focos de riesgo en determinados territorios o regiones que por reunir ciertas características o circunstancias particulares resultan más atractivos para el crimen. Aspecto que desaparece por completo cuando nos movemos en el espacio virtual.

Y, el segundo, es la ausencia de acuerdos multilaterales y de otros mecanismos legales de cooperación-prevención que resulten verdaderamente eficaces en el plano transnacional. Incluyendo, por supuesto, la prevención del riesgo transnacional digital.

3.2.1. ¿Por qué es necesaria una prevención uniforme?

Entre los factores que han alimentado la preocupación de las autoridades comunitarias por alcanzar estándares óptimos de cooperación-prevención en esta materia vale la pena reflexionar un instante sobre su impacto económico. La delincuencia transnacional (*online* y *offline*) a menudo aparece vinculada a la comisión de delitos económicos donde la necesidad de cooperar es, si cabe, aún más intensa cuando además de procesar a los autores se persigue la recuperación de los beneficios derivados de su actividad ilícita.

La localización de estos activos por parte de los autores en diferentes ubicaciones geográficas ha puesto de manifiesto las dificultades reales de la Unión Europea en relación con el comiso y embargo de las ganancias derivadas del crimen organizado transnacional aun cuando estas se materializan en el plano *offline*. De manera similar, cuando nos encontramos en el espacio virtual el rastreo de la actividad delictiva y la búsqueda de estas ganancias precisan de herramientas digitales que nos permitan reconocer la trazabilidad de esos activos.

A propósito de ello me propongo subrayar las consecuencias jurídicas, económicas y sociales que ha desencadenado esta realidad en la última década y realizar un juicio crítico sobre la estrategia comunitaria para su abordaje desde el compliance institucional. Abordaré la primera cuestión a lo largo de este apartado y me dedicaré a la segunda en el apartado siguiente.

Como punto de partida debo advertir que las dificultades a la hora de localizar y recuperar las ganancias procedentes del crimen organizado en el espacio *offline* derivadas de la fragmentación geográfica tienen a su vez un efecto multiplicador que retroalimenta este tipo de delincuencia transnacional. Y que, en ocasiones, fomenta su reingreso en el espacio *online*. Las consecuencias de este tipo de prácticas no son exclusivamente económicas, sino que inciden de manera directa en el comportamiento social y político haciendo del crimen organizado una especie de "colectivo" con capacidad para influir en la sociedad. Como demuestran los informes de INTERPOL[20] en la mayoría de los casos estas ganancias se "invierten" en nuevas actividades delictivas como la corrupción o el propio crimen organizado (revierten en la propia red), nutren

20. Disponibles en: https://www.interpol.int/es/Delitos/Ciberdelincuencia. Fecha de última consulta: 16 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

a otros grupos organizados, financian actos de terrorismo y, en definitiva, fortalecen la delincuencia transnacional.

En este contexto la posibilidad de refugiar estas ganancias en el espacio *online* constituye un aliciente para la ciberdelincuencia que, sin duda, incrementa el riesgo transnacional digital. La Unión Europea, consciente de esta realidad, se ha rearmado modernizando sus técnicas de investigación y fomentando la creación de unidades específicas de ciber vigilancia y la aplicación de recursos informáticos que le permitan identificar el rastro digital de las ganancias económicas derivadas del crimen. En relación con todo ello, en el siguiente apartado expondré las herramientas concretas (jurídicas y extrajurídicas) que recientemente ha incorporado la Unión para su lucha contra el riesgo transnacional digital.

Como segunda derivada y ya en el plano estrictamente económico el fortalecimiento del crimen organizado a partir de este sistema de financiación tiene al menos dos consecuencias directas. La primera es el desequilibrio en la competencia de los diferentes agentes que operan en el mercado global. Y, la segunda, su impacto sobre la economía pública también en términos de confianza y reputación. Este aspecto entronca con la necesidad de alinear cualquier estrategia para la gobernanza del riesgo transnacional asociado a la delincuencia organizada con las políticas públicas comunitarias sobre transparencia y buen gobierno y con otras líneas para la prevención de delitos como la prevención del blanqueo de capitales, los actos de corrupción o el soborno a funcionario público extranjero. Pues, en todos estos casos, se trata de prevenir riesgos contra la administración pública. Y, en todos ellos, puede estar presente directa o indirectamente el componente digital.

A la vista de todo ello se hace aún más necesaria si cabe la búsqueda de nuevas herramientas e instrumentos preventivos multilaterales que nos permitan estar a la altura de este desafío global. Como se verá a continuación, el nuevo modelo de cooperación-prevención diseñado por la Unión Europea combina elementos de compliance institucional con diferentes iniciativas legislativas que representan avances verdaderamente significativos respecto de las herramientas jurídicas tradicionales[21] que si bien han resultado extraordinariamente útiles a mi juicio precisaban ya de un nuevo empuje.

3.2.2. Antecedentes y evolución de la estrategia comunitaria

La respuesta de las autoridades comunitarias frente al desafío global que representa el riesgo transnacional digital ha ido evolucionando desde 2010 hasta nuestros días priorizando una acción conjunta *ad intra* basada en dos ejes fundamentales que podemos considerar prioritarios en el combate de la delincuencia transnacional. El primero de ellos consiste en el establecimiento de mecanismos legales y extralegales para la mejora

21. Entre ellas no quiero dejar de citar el Convenio del Consejo de Europa relativo al blanqueo, seguimiento, embargo y decomiso de los productos del delito y a la financiación del terrorismo de 2005, la Convención UNTOC, o la Convención contra la Corrupción; entre otros.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

en la recuperación de activos procedentes de actividades ilícitas haciendo especial hincapié en la recuperación de los activos digitales. Y, el segundo, consiste en el diseño e implementación de instrumentos multilaterales de cooperación conjunta para la prevención del riesgo transnacional digital.

El primer paso hacia esta nueva dirección lo identifico en los compases previos a la publicación del libro blanco sobre el crimen organizado transnacional del Consejo de Europa en 2014. Concretamente, en los años 2012 y 2013 cuando la Unión puso en marcha por primera vez el llamado ciclo de actuación contra la delincuencia organizada. Podría decirse que este ciclo representa la primera piedra sobre la que, como trataré de exponer, se ha ido edificando toda una política comunitaria para la prevención uniforme del riesgo transnacional. En esta ocasión, asociado al crimen organizado[22].

El principal problema que a mi juicio presenta esta receta de "café para todos" es que la realidad jurídica, económica, digital y social de cada Estado miembro es diferente del resto. Y, por lo tanto, los niveles de riesgo transnacional (digital y no digital) no son homogéneos. En este punto tiene sentido reflexionar un instante sobre dos posibles vías de comprender y aplicar la prevención uniforme.

La primera sería entender que existe prevención uniforme en la aplicación de medidas preventivas globales cuya aplicación se realiza por igual entre y para todos los Estados miembros. Ello aun con independencia de los niveles de riesgo que se presenten en cada uno de ellos. Esta estrategia de máximos nos llevaría quizás que dos Estados con diferentes niveles de riesgo se vieran obligados a aplicar las mismas medidas. Sin embargo, la segunda consistiría en comprender que existe prevención uniforme cuando ante iguales niveles de riesgo se reacciona con las mismas medidas. Este segundo enfoque obliga a que previamente se haya realizado una exhaustiva labor de identificación de riesgos. Aun siendo consciente de que se trata de un camino costoso y seguramente más lento que el anterior bajo mi punto de vista podría resultar más acorde con la realidad socioeconómica actual de los Estados miembros.

A partir de la experiencia adquirida con este ciclo de actuación la Unión Europea da un paso más allá en el año 2021 con la finalidad de mejorar la eficacia de su acción preventiva frente al riesgo transnacional. De esta manera el ciclo de actuación diseñado en 2010 fue reformulado mediante acuerdo del Consejo de 26 de febrero de 2021 pasando a su denominación actual: *European Multidisciplinary Platform Against Criminal Threats* (en adelante EMPACT), o Plataforma Multidisciplinar Europea Contra las Amenazas Delictivas.

Esta plataforma, más actual y por lo tanto más acorde con la realidad social de nuestros días, incorpora novedades metodológicas interesantes para la prevención,

22. La versión inicial de este ciclo se orientó hacia diez figuras delictivas: la ciberdelincuencia, el tráfico de drogas, la facilitación de migración ilegal a la Unión Europea, el robo organizado, la trata de seres humanos, el fraude de impuestos especiales y del operador desapercibido, el tráfico de armas de fuego, la delincuencia medioambiental, las operaciones financieras delictivas, y el fraude documental. Documento disponible en: https://op.europa.eu/en/publication-detail/-/publication/9984824a-7509-448e-8ed8-ea7a54ff5ad6/ Fecha de última consulta: 23 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

el tratamiento y la gestión del riesgo transnacional, también en su versión digital. El nuevo modelo se inspira en cierta medida en la vieja idea del ciclo de *Deming* (PDCA, *Plan-Do-Check-Act*) que ha inspirado el diseño de los sistemas de compliance contemporáneos. A través de esta plataforma se pretende establecer y evaluar prioridades y objetivos de actuación en función de los diferentes niveles de riesgo identificados. Esta nueva política preventiva de la Unión Europea es coherente, como indicaba antes, con la línea seguida por otros organismos internacionales como la OCDE en su plataforma *ICAP*[23]. Y, en este sentido, permite la conexión con la vertiente *ad extra* del riesgo transnacional. La importancia de esta conexión radica en el hecho de que nos encontramos en una economía con niveles récord de globalización y cada día más digitalizada. Por lo tanto, esta evolución de la multilateralidad en el panorama internacional resulta crucial para afrontar con éxito estos desafíos. Tengamos en cuenta que según ha informado recientemente la Comisión Europea el riesgo transnacional asociado al crimen organizado está presente en al menos tres Estados miembros en el 70 de cada 100 casos. Con todo ello, la plataforma EMPACT se encuentra actualmente en el ecuador del marco plurianual 2022-2025[24] y, aunque aún es pronto para evaluar resultados, contamos con algunos indicios interesantes que trataré de exponer a continuación.

Como segunda novedad relevante la plataforma plantea la creación de nuevos servicios de cooperación internacional, inteligencia, y prevención e incorpora nuevas obligaciones de colaboración *ad intra* y *ad extra* para una gestión más eficaz del riesgo transnacional. En este nuevo enfoque está muy presente el daño económico que representa el riesgo transnacional asociado al delito de organización criminal para los ciudadanos y las instituciones europeas. La propia Comisión Europea ha cuantificado los ingresos derivados de la delincuencia organizada en 139.000 millones de euros en 2019. Esta cifra representa el 1% de todo el PIB comunitario y se asocia con una cierta tendencia al alza que, en resumidas cuentas, no es sino la confirmación de que el riesgo transnacional asociado al crimen organizado también está al alza.

En tercer lugar, la metodología propuesta en esta plataforma se basa en un modelo secuencial en cuatro pasos que aspira a servir como marco global para la cooperación-prevención *ad intra*. Al análisis crítico de este modelo me dedicaré en el apartado siguiente.

23. Acceso al documento para el desarrollo completo de la plataforma *ICAP* de la OCDE disponible en: http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/international-compliance-assurance-programme-pilot-handbook-2.0.pdf Fecha de última consulta: 17 de septiembre de 2023.

24. Prioridades EMPACT 2022-2025 disponibles en: https://www.consilium.europa.eu/es/press/press-releases/2021/05/26/fight-against-organised-crime-council-sets-out-10-priorities-for-the-next-4-years/ Fecha de última consulta: 17 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

3.2.3. Breve análisis de la plataforma comunitaria EMPACT desde la perspectiva del compliance institucional. ¿Un recurso útil para la gestión del riesgo transnacional DIGITAL?

En relación con la idoneidad del modelo contenido en la plataforma comunitaria para la prevención del riesgo transnacional asociado al crimen organizado dedicaré este apartado al análisis de su eficacia en el espacio *online* a partir de los elementos de compliance institucional que identifico en su configuración. A lo largo de esta exposición me propongo realizar algunas aportaciones desde la crítica constructiva sobre aquellos aspectos en los que considero que existe algún margen para la mejora.

La primera podríamos localizarla en la fase del modelo dedicada a la elaboración de políticas. Este elemento resulta clave en cualquier sistema de gestión de compliance por su utilidad para la prevención de cualquier tipo de riesgo. Tomando como base la segunda interpretación del concepto de prevención uniforme a la que me referí anteriormente la identificación previa de diferentes niveles de riesgo (en diferentes territorios y/o Estados) puede acabar determinando la eficacia de cualquier medida preventiva. En otras palabras, la elaboración de políticas requiere siempre de una evaluación previa del riesgo. Sin embargo, al menos sobre el papel, no parece que en el diseño originario de esta plataforma se le haya conferido esta relevancia a la identificación previa del riesgo como elemento clave de la elaboración de políticas. Bajo mi punto de vista resultaría conveniente que, al menos en la práctica, se incorporase este enfoque ya que puede resultar particularmente útil en el espacio virtual. Por otro lado, el hecho de que no se le haya conferido esta importancia a la gestión apriorística del riesgo en la fase de elaboración de políticas resulta cuanto menos chocante con la intención del propio Consejo de hacer de esta fase una herramienta útil para la evaluación de amenazas de delincuencia organizada en sentido amplio respecto de cualquier riesgo potencialmente dañino para la Unión Europea. De hecho, las figuras delictivas comprendidas en el ámbito de actuación de la plataforma tienen una extraordinaria capacidad para transformarse, como ocurre con cada vez más frecuencia, al confluir elementos digitales o informáticos en la comisión del delito. El hecho de que puedan intervenir estos elementos justificaría, a mi modo de ver, no solo un enfoque más centrado en el riesgo sino también más centrado en la revisión periódica y en la actualización de los diferentes niveles de riesgo. En consecuencia, los controles internos y las medidas de compliance institucional de la Unión deberían acomodarse con relativa rapidez a cualquier cambio identificado en los niveles de riesgo.

Por último, este hecho podría comprometer la efectividad de las evaluaciones de impacto que analizamos anteriormente. Una de las debilidades de cualquier modelo secuencial es precisamente su incapacidad para adaptarse con rapidez a los cambios. La aparición de nuevos riesgos no detectados o la modificación de los ya existentes puede comprometer el resto de las etapas del ciclo. En este sentido se echa en falta quizás un compromiso menos tibio de las autoridades comunitarias con la acomodación del modelo a la realidad digital de nuestros días. Digo menos tibio porque, en honor a la verdad, debe reconocerse que la implicación de EUROPOL en la cooperación entre

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Estados miembros para la detección temprana de riesgos ha sido creciente desde el año 2021. Y, a mayores, el sistema prevé el reporte de informes periódicos desde EUROPOL al Consejo.

En segundo lugar, procedería reflexionar ahora a propósito de la primera interpretación del concepto de prevención uniforme referido anteriormente en relación con los planes estratégicos plurianuales previstos por este modelo. También llamados *General Multi-Annual Strategic Plan* (en adelante, G-MASP). En pocas palabras, se trata de una planificación de metas horizontales comunes (el Consejo se refiere a ellas como *Common Horizontal Strategic Goals*, CHSG) en las que todo parece indicar que se ha optado de nuevo por una receta de café para todos.

De nuevo aflora la cuestión de qué ocurre cuando en uno o varios Estados o regiones de la Unión Europea se presentan niveles particulares de riesgo (nacional y/o transnacional) que precisen de medidas concretas o que no puedan prevenirse, mitigarse, o gestionarse con la receta global. Las CHSG podrían haber previsto esta situación, pero es posible que la reacción que contemplen no sea la más adecuada para ese país o región en concreto. En otras palabras, la cauterización de ese punto caliente podría requerir de medidas complementarias o independientes de las previstas por el plan general y, bajo mi punto de vista, esta posibilidad debería estar incluida con mayor nitidez en la estrategia comunitaria. No como un incentivo hacia la inequidad horizontal (aspecto que habrá que trabajar aparte) pero sí como una posible solución frente a los casos concretos. La previsión de esta posibilidad no tendría por qué comprometer, al menos no necesariamente, la uniformidad de la prevención. Pues, al preverse para situaciones concretas que eventualmente pudieran presentarse en el conjunto de los países incluidos en la plataforma, procedería su aplicación para cualquiera de ellas con independencia del factor geográfico. De la misma manera sería recomendable buscar la complementariedad entre la plataforma EMPACT y las medidas internas que en cada caso pudiera haber previsto cada Estado miembro respetando siempre los principios que rigen las relaciones entre las competencias nacionales y supranacionales en la Unión Europea.

En tercer lugar, la plataforma incorpora un comité bautizado como "de cooperación operacional y seguridad interna" (COSI, *Committee on Operational Cooperation on Internal Security*) para una mejor prevención de la delincuencia transnacional en las diez áreas seleccionadas como prioritarias[25]. Como se puede observar en la mayoría de estas áreas existe la posibilidad de toparnos con conductas y riesgos en el espacio virtual. En este sentido el recurso hacia redes seguras para el intercambio de información entre Estados miembros y hacia las autoridades comunitarias se hace inevitable. Este hecho ha impulsado, como trataré de exponer en el apartado siguiente, algunas iniciativas legislativas en la Unión Europea para adecuar nuestro marco jurídico a las nuevas necesidades de intercambio de información que ha puesto de manifiesto nuestra realidad digital. La red europea SIENA opera en este contexto como un recurso digital coadyuvante en la

25. Acceso al documento completo (con descripción de las áreas) de la estrategia de prevención EU-EMPACT 2022-2025 disponible en: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact Fecha de última consulta: 21 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

prevención del riesgo transnacional. Sin embargo, en no pocas ocasiones desafortunadamente la configuración de estas redes y la redacción de estas normas presenta vulnerabilidades y riesgos que comentaré más adelante y que también pueden condicionar la gestión del riesgo transnacional en la Unión.

En cuarto lugar, me detendré en la necesidad de evaluar de manera independiente e imparcial el funcionamiento general del modelo. Este es un aspecto que a menudo sobresale en cualquier sistema de gestión de compliance corporativo y que en el plano institucional aparece, bajo mi punto de vista, con menor intensidad. Posiblemente la envergadura del modelo, el volumen de información y las características del riesgo al que nos enfrentamos en el plano supranacional puedan explicar en alguna medida el porqué de este hecho. Lo cierto es que en la plataforma que nos ocupa se menciona este aspecto sucintamente por parte de las autoridades comunitarias, pero al menos bajo mi óptica, no se concreta nítidamente la manera de llevarlo a la práctica y esta es quizás la crítica más evidente.

IV. Hacia un modelo de compliance institucional para la prevención (¿uniforme?) del riesgo transnacional digital en la Unión Europea

A partir del análisis previo procede adentrarse ahora en los elementos de compliance institucional presentes en las diferentes herramientas jurídicas y extrajurídicas con las que cuenta hasta la fecha la Unión Europea para la prevención del riesgo transnacional (incluida su versión digital).

Para una mejor comprensión de cuanto se expone a continuación procede acotar siquiera sucintamente el concepto de riesgo transnacional digital sin perjuicio de cuanto ya se ha ido avanzando al respecto en las páginas precedentes. La coincidencia de estos tres elementos en este concepto responde a la necesidad de delimitar una realidad que sin apellidos podríamos considerar infinita. Si comenzamos por el primer elemento lo cierto es que en relación con el acervo comunitario puede generar la misma sensación que tenemos cuando se nos presenta en casa una visita inesperada. Las referencias hacia el concepto de riesgo no resultan precisamente abundantes en el derecho comunitario (salvo en alguna que otra regulación sectorial) precisamente por la dificultad conceptual que representa. No en vano se trata de un concepto interdisciplinar.

Sin embargo, la evolución del Derecho digital en la Unión Europea ha impulsado su incorporación en cada vez más textos normativos desde una perspectiva basada en el fenómeno anglosajón del *risk management* o la gestión de riesgos[26]. Al menos hasta el momento en ninguno de los textos legales que ha ido aprobando y proponiendo la Unión se especifica con claridad qué debe entenderse por "riesgo". Sin embargo, si acudimos a las fuentes de *softlaw* encontramos que el estándar ISO 37301:2021 sobre sistemas de

26. En este sentido discurren, por ejemplo, las nuevas directivas propuestas en materia de ciberseguridad, resiliencia y protección frente a ciberataques de la Unión Europea que se analizarán en seguida.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

gestión de compliance (requisitos con orientación para su uso) define el riesgo como el "efecto de la incertidumbre sobre los objetivos"[27]. Siguiendo esta definición la cuestión espacial me aboca a emplear el adjetivo transnacional para acotar este efecto a este espacio geográfico concreto (con todas sus connotaciones en el panorama comunitario) en contraposición, por ejemplo, a otros efectos que pudiera tener la incertidumbre en cualquier otro escenario. De la misma manera el adjetivo digital. Así, en definitiva, bajo la óptica que aquí se propone se encontrarían comprendidos en el concepto de riesgo transnacional digital todos aquellos efectos de la incertidumbre en los que concurra el elemento digital y que pudieran manifestarse más allá de las fronteras de cada Estado miembro. Sin ánimo de ahondar más en esta cuestión terminológica por el momento y sin obviar su interés académico tomaré como válida esta delimitación del concepto tan brevemente esbozada únicamente a los efectos de cuanto se pretende con este apartado.

Partiendo entonces de esta definición procede ahora realizar la aproximación hacia el impulso del compliance institucional previsto por la reciente regulación de la Unión Europea en materia de Derecho digital y prevención de ciberamenazas. Por cuestiones de espacio me centraré en el paquete formado por las siguientes cuatro normas comunitarias: (1) El Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 20 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad»)[28]. (2) La propuesta de Reglamento de Ciberresiliencia de la Comisión Europea de 15 de septiembre de 2022[29]. (3) La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (en adelante, Directiva SRI 1)[30]. (4) La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a

27. La propia norma ISO 37301:2021 aclara sobre la base de este concepto cuatro elementos que nos permiten delimitar su alcance. En ese sentido se indica que un efecto es "una desviación de lo esperado ya sea positiva o negativa". La incertidumbre es "el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su probabilidad". Seguidamente se indica que "con frecuencia el riesgo se caracteriza por referencia a eventos potenciales (como se define en la Guía ISO 73) y consecuencias (como se define en la Guía ISO 73), o a una combinación de estos". Por último, se añade que "con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios de las circunstancias) y la "probabilidad" (como se define en la Guía ISO 73) asociada de que ocurra".

28. Texto completo del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 20 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad») disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881 Fecha de última consulta: 29 de septiembre de 2023.

29. Versión en castellano disponible en: https://data.consilium.europa.eu/doc/document/ST-12429-2022-INIT/es/pdf Fecha de última consulta: 29 de septiembre de 2023.

30. Texto completo de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (en adelante, Directiva SRI 2)[31].

Comenzando por el Reglamento 2019/881 lo primero que debo advertir es que establece una serie de competencias, obligaciones y facultades en materia de ciberseguridad y prevención de riesgos digitales para la ENISA (Agencia de la Unión Europea para la ciberseguridad)[32] con una doble finalidad. La primera es garantizar un estándar óptimo de ciberseguridad y ciberresiliencia en el conjunto de la Unión Europea y, la segunda, proteger el mercado interior. Se establece así la existencia de un órgano autónomo (institución pública) con competencias propias al que la Unión Europea le confía la máxima autoridad en esta materia.

Como primer aspecto relevante el Reglamento define el concepto de incidente (artículo 2.6) por remisión a la Directiva SRI 1 que se comentará a continuación (artículo 4.7) como "todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información". Podríamos analizar las semejanzas entre este concepto y el concepto de riesgo referido en la norma ISO 37307:2021 y citado anteriormente si no fuera porque la misma Directiva SRI 1 incorpora en su artículo 4.9 su propio concepto de riesgo y lo define como "toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información". De nuevo la posibilidad de identificar el riesgo en términos razonables es lo que nos permite diferenciarlo de otras categorías jurídicas como el incidente. Como es sabido la Directiva SRI 1 fue derogada en 2022 por la Directiva SRI 2 en la que, a propósito de los conceptos de riesgo e incidente sorprenden algunas diferencias notables en relación con la Directiva SRI 1[33]. En mi opinión estas diferencias nos dan buena muestra de la evolución digital sufrida en la Unión Europea durante esos seis años y de cómo el dato pasa a ubicarse ahora en el centro de la regulación de la prevención de incidentes y riesgos relacionados con la ciberseguridad. Este aspecto ha propiciado el refuerzo de ENISA cuyas funciones en materia de compliance y control interno representan un claro avance institucional hacia la prevención uniforme.

redes y sistemas de información en la Unión (Directiva SRI 1) disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148 Fecha de última consulta: 29 de septiembre de 2023.

31. Texto completo de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555&qid=1689114036076 Fecha de última consulta: 29 de septiembre de 2023.

32. Sitio web oficial ENISA: https://www.enisa.europa.eu/about-enisa/about/es

33. En la Directiva SRI 2 se define el incidente como: "todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos". En la misma Directiva SRI 2 se define el riesgo como: "la posible pérdida o perturbación causada por un incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal incidente".

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

El Reglamento se centra en la labor de ENISA y le atribuye competencias concretas en relación con los incidentes y su gestión. De manera particular en dos sentidos: la detección de incidentes y la asistencia y apoyo a los Estados miembros para su gestión. Así su función de vigilancia y control se basa fundamentalmente en un modelo de cooperación *ad intra* y se combina con una acción exterior (acaso más discreta) de manera muy similar a los sistemas de gestión de compliance corporativos referidos en la norma ISO 37307:2021. De manera complementaria a la labor de la ENISA el Reglamento refuerza el papel de la red CSIRT[34] en la Unión Europea. Conviene recordar que esta red tiene como finalidad principal el establecimiento de equipos nacionales en cada Estado miembro para responder frente a posibles incidentes y analizar los riesgos que se produzcan en el espacio virtual. En segunda instancia, la red CSIRT alerta sobre estos riesgos facilitando su detección temprana en otros Estados miembros (componente transnacional) y aportando soluciones para mitigar sus efectos desde su propia experiencia[35]. En este sentido nos encontramos ante otro elemento institucional de compliance que también sale reforzado tras la aprobación del Reglamento comunitario.

Por lo que respecta a la Directiva SRI 1 de 2016, su análisis nos puede resultar interesante como predecesora de la Directiva SRI 2 que la deroga y rige desde 2022. Ya se ha referido que se orientaba a la consecución de un determinado nivel de seguridad en las redes y sistemas de información de la Unión y en este sentido incorpora elementos interesantes como el concepto de incidente, el concepto de riesgo, o la creación de la red CSIRT (nacional y supranacional). El establecimiento de obligaciones de cooperación nacional e internacional en esta Directiva resulta clave para comprender la estructura de compliance y ciberseguridad institucional que se persigue en ella. En pocas palabras, la Directiva articula una suerte de colaboración entre las autoridades comunitarias, ENISA, y la red CSIRT orientada a la detección temprana de cualquier efecto perturbador significativo en el mercado interior. De esta manera la prevención del riesgo transnacional digital encuentra un importante aliado en la acción encomendada a los equipos de respuesta a incidentes de seguridad cuya labor, como refería anteriormente, se ha visto reforzada con el Reglamento (UE) 2019/881. Con esta estrategia la Unión afronta la prevención del riesgo transnacional digital desde una doble perspectiva. En primer lugar, fomentando la creación de nuevos organismos e instituciones con perfiles profesionales especializados en el campo de la informática, la ciberseguridad y la gestión de información sensible. Y, en segundo lugar, dotando a estos órganos de competencias en materia de vigilancia, supervisión, reporte y control interno del riesgo asociado a los incidentes de seguridad en la red. Esta estrategia representa un avance significativo en términos de compliance y seguridad institucional en un campo, el del Derecho digital, donde esta demanda era una de las asignaturas pendientes del legislador.

34. De las siglas en inglés *Computer Security Incident Response Teams*. La regulación de esta red se encuentra en el artículo 1.2.c) y en el artículo 9 de la Directiva SRI 1.

35. En el caso de España, en el año 2022 existían más de una docena de equipos integrados en la red CSIRT dependientes directamente del Ministerio de Transformación Digital.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Abordando ya por el último el caso de la Directiva SRI 2 de 2022 se observa que esta tendencia continúa al alza. En primer lugar, la Directiva reformula los conceptos clásicos de riesgo e incidente presentes en la Directiva SRI 1 a partir de un nuevo elemento clave: el dato. En este sentido se habla por primera vez de autenticidad, integridad y confidencialidad de los datos para referirse al concepto de incidente (y cuasiincidente) cuando éstas se vean comprometidas. Y para referirse también al concepto de riesgo al hacerlo depender de la existencia de un incidente. La Directiva hereda la regulación de la red CSIRT que ya introdujo la SRI 1 y, sobre esta base, añade una serie de obligaciones y competencias en materia de prevención de riesgos (artículo 11) muy centradas en la cooperación transnacional de los Estados miembros. En otras palabras, en la aspiración de alcanzar una cierta prevención uniforme.

En este camino hacia la creación de nuevos organismos e instituciones para dotarlos de competencias en materia de vigilancia, control y gestión de riesgos, la Directiva SRI 2 crea en su artículo 16 la red europea de organizaciones de enlace para las crisis de ciberseguridad, en adelante EU-CyCLONe. Sorprende que ni la Directiva SRI 1, ni la SRI 2, ni el Reglamento (UE) 2019/881 hayan definido qué debe entenderse por crisis de ciberseguridad. La aproximación teórica más cercana a este concepto la encontramos en la Recomendación (UE) 2017/1584 de la Comisión de 13 de septiembre de 2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala[36]. Sin embargo, la Directiva SRI 2 establece la obligación de que cada Estado miembro designe a una autoridad nacional competente para gestionar estas crisis (artículo 9).

Para finalizar, me referiré brevemente al capítulo IV de la Directiva SRI 2 sobre medidas para la gestión de los riesgos de ciberseguridad y obligaciones de notificación. Este capítulo establece todo un paquete de medidas que bajo mi punto de vista resultan perfectamente aplicables a la gobernanza *ad intra* del riesgo transnacional digital en la Unión. En él concurren entre otros elementos interesantes de compliance institucional, la obligación de monitorear, reportar y notificar cualquier tipo de riesgo en el sentido indicado por la Directiva SRI 2, la evaluación coordinada y conjunta de esos riesgos, el recurso hacia la certificación de esquemas de ciberseguridad, o la normalización. El hecho de que la Unión haya decidido por fin incorporar una regulación de estas características responde a mi modo de ver a dos factores fundamentales. El primero, la utilidad práctica que incorporan este tipo de medidas de cumplimiento normativo, prevención y seguridad. En su mayoría, presentes ya en el derecho interno de los Estados miembros a propósito de la responsabilidad legal de las personas jurídicas y de otros aspectos jurídicos afines a ella. Este hecho facilita, en este momento, su regulación comunitaria con una terminología y unos procedimientos ciertamente similares. Y, el segundo, la envergadura del desafío digital al que nos enfrentamos cuando se trata de abordar este tipo

36. Recomendación (UE) 2017/1584 de la Comisión de 13 de septiembre de 2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017H1584 Fecha de última consulta: 30 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

de riesgos más allá de las fronteras nacionales. La conjunción de ambos factores hace de la Directiva SRI 2 un instrumento jurídico necesario, pero al mismo tiempo, al menos a mi juicio, insuficiente.

V. Conclusiones

Del análisis realizado a lo largo de estas páginas se extrae como primera idea fundamental que la realidad digital de nuestros días ha superado cualquier expectativa del legislador nacional y comunitario. La aparición y propagación del riesgo digital a lo largo y ancho de la Unión Europea constituye hoy un desafío de primer orden que coloca a la ciencia jurídica en una posición realmente comprometida. En primer lugar, porque se demandan respuestas cada vez más rápidas y eficaces para tratar de regular jurídicamente una realidad cada día más cambiante y volátil; aspecto que de por sí resulta difícil de conciliar con los procesos legislativos comunitarios que a menudo precisan de consensos y tramitaciones realmente lentas. Y, segundo lugar, porque la complejidad de la materia objeto de regulación está tecnificando el Derecho comunitario hasta extremos inimaginables. Incorporando, con cada vez más frecuencia, conceptos y razonamientos más propios de otras disciplinas como la ingeniería informática, la gestión de riesgos, la economía, o la inteligencia artificial. Este hecho dificulta la aplicación y la interpretación de este nuevo Derecho comunitario por parte de todos los operadores jurídicos e introduce la posibilidad de que esta dificultad termine frustrando la finalidad de estas normas.

En segundo lugar, podemos concluir que la Unión Europea es consciente de esta realidad y ha apostado claramente por evolucionar su Derecho en este sentido. Prueba de ello son los diferentes Reglamentos y Directivas comunitarios aprobados en los últimos años en materias tan novedosas como la ciberseguridad, los criptoactivos, o la protección del denunciante de infracciones del Derecho de la Unión. Sin embargo, la magnitud del desafío global al que nos enfrentamos no se conforma con una respuesta jurídica. Si no que, bajo mi punto de vista, precisa también de una reacción comunitaria que, sin apartarse del poder legislativo, incorpore jurídica o extra jurídicamente elementos eficaces e idóneos para la gobernanza y la gestión de estos riesgos. Es aquí donde la traslación de mecanismos de compliance (diseñados inicialmente para el sector privado) hacia el ámbito de las instituciones públicas adquiere un nuevo sentido.

En tercer lugar, el riesgo transnacional digital se caracteriza por representar una amenaza global que en mi opinión sólo se podrá combatir con éxito desde una actuación que ya no puede ser únicamente conjunta o cooperativa, sino que además debe ser necesariamente uniforme. Esta exigencia choca de manera frontal con las características propias de cada Estado miembro y con la indiscutible disparidad entre los recursos y riesgos que existen en cada territorio. No quiero decir con ello que los Estados miembros deban afrontar este reto desde una misma posición de partida, pero sí que al menos se avance de manera más significativa hacia la corrección de las posibles desigualdades entre ellos en aras de una mayor uniformidad preventiva tal y como ya se

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

hace, por cierto, en otros ámbitos comunitarios donde podemos identificar fácilmente las bondades de los mecanismos de cohesión.

En cuarto lugar y en relación con lo anterior, en honor a la verdad debe reconocerse tras todo lo expuesto que existen importantes avances en materia de cooperación para la prevención del riesgo transnacional en la Unión y que si por algo se caracteriza este nuevo rumbo es por el compromiso de las autoridades comunitarias con el diseño de una respuesta común más transversal y acorde con la realidad que vivimos. Sin embargo, hablar en este momento de prevención uniforme me resulta un ejercicio un tanto forzado. En primer lugar, porque los niveles de prevención alcanzados internamente en cada Estado miembro siguen estando condicionados por la mayor o menor eficacia de su Derecho interno en la lucha frente a este tipo de riesgos. En segundo lugar, porque bajo mi punto de vista la corrección de esta disparidad no puede alcanzarse exclusivamente desde el Derecho, sino que precisa de otros cambios culturales, sociales y económicos en los que ya se está trabajando tanto a nivel interno como desde la Unión Europea. Y, en tercer y último lugar, porque los recursos económicos, técnicos y materiales de los que se dispone en relación con este desafío son limitados y, a la luz de los hechos, podríamos decir que insuficientes.

En quinto y último lugar, la prevención del riesgo transnacional digital (y no digital) no puede afrontarse desde un posicionamiento exclusivamente jurídico. La complejidad de este reto demanda la aplicación de herramientas interdisciplinares y la implicación de las autoridades comunitarias, pero también de las nacionales en cada Estado miembro. En este contexto el compliance institucional entra en escena como un recurso innovador e interesante que puede resultar extraordinariamente útil en ambos planos cuya finalidad no es otra que la de completar esa laguna allá donde el Derecho no puede llegar aportando soluciones desde la gestión y la gobernanza del riesgo que pasan, necesariamente, por tres ejes principales. Un cambio en la cultura y en la manera tradicional de entender la prevención (que quizás fuera válida en otros momentos o contextos históricos de la Unión pero que a todas luces ha quedado obsoleta frente a la realidad actual), la implicación del legislador nacional y comunitario pero también del resto de los poderes públicos para la mejor aplicación posible de sus mecanismos e instrumentos; y, por último, la colaboración eficaz entre todas las partes interesadas (agentes sociales, sector privado, fuerzas y cuerpos de seguridad, autoridades supranacionales, poderes públicos, *policy makers* y sociedad civil) en la implementación y el seguimiento de todos los recursos a su alcance.

Bibliografía

Agencia Europea para la ciberseguridad (2023). Reporte anual en materia de ciberseguridad. Recuperado el 7 de septiembre de 2023 de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

BECK, U. (1992). *Risk Society: Towards a New Modernity*. (London: Sage).

BECK, U. (2009). "Critical theory of world risk society: a cosmopolitan vision". *Constellations*, vol. 16, n. º 1.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

BELMONTE, P. (2016). "El nuevo estándar global de intercambio automático de información sobre cuentas financieras de la OCDE ("*CRS, Common Reporting Standard*"): estructura y funcionamiento. Aplicación del mismo en la Unión Europea: Directiva 2014/107/UE del Consejo de 9 de diciembre de 2014". *Crónica tributaria*, Vol. 159 (103-130).

Comisión Europea (2017). Report Study. *European Data Market study measuring the size and trends of the EU data economy*. Recuperado el 7 de septiembre de 2023 de https://digital-strategy.ec.europa.eu/en/library/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy

CONSEJO DE EUROPA (2014). Libro blanco sobre el crimen organizado transnacional.

Directiva (UE) 2018/822 del Consejo, de 25 de mayo del 2018, que modifica la Directiva 2011/16/UE por lo que se refiere al intercambio automático y obligatorio de información en el ámbito de la fiscalidad en relación con los mecanismos transfronterizos sujetos a comunicación de información. Recuperado el 16 de septiembre de 2023 de https://www.boe.es/doue/2018/139/L00001-00013.pdf

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148.

Directiva 2008/99/CE del Parlamento Europeo y del Consejo, de 19 de noviembre de 2008, sobre protección del medio ambiente mediante el Derecho penal.

ERICSON, R. V., y HAGGERTY, K. D. (1997). Policing the risk society. (London: Clarendon Press).

EU4Digital (2021). EU Digital Strategy. Recuperado el 13 de septiembre de 2023 de https://eufordigital.eu/discover-eu/eu-digital-single-market/

HAUFLER, A., MARDAN, M., y SCHINDLER, D. (2018). "Double tax discrimination to attract FDI and fight profit shifting: The role of CFC rules". *Journal of International Economics*, Vol. 114 (25-43).

INTERPOL (2023). La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad. Recuperado el 11 de septiembre de 2023 de https://www.interpol.int/es/Delitos/Ciberdelincuencia

ISO (2021). Norma ISO 37301:2021 sobre Sistemas de gestión del compliance. Requisitos con orientación para su uso.

KEUSCHNIGG, C., y DEVEREUX, M. (2013). "The arm's length principle and distortions to multinational firm organization". *Journal of International Economics*, Vol. 89, n. º 2 (432-440).

MCBRIDE, N., y BAGSHAW, R. (2008). *Tort law*. (London: Pearson Education).

NIETO, A. y CALATAYUD, M. (2015). *Public Compliance: Prevención de la corrupción en administraciones públicas y partidos políticos* (Vol. 13). Ediciones de la Universidad de Castilla La Mancha.

NACIONES UNIDAS (2004). Convención de Naciones Unidas contra la Corrupción. Recuperado el 21 de septiembre de 2023 de https://www.unodc.org/pdf/corruption/publications_unodc_convention-s.pdf

O'MALLEY, P. (2002). Risk societies and the government of crime. In *Dangerous offenders* (pp. 27-44). Routledge.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

OCDE (1997). Convención para Combatir el Cohecho de Servidores Públicos Extranjeros en Transacciones Comerciales Internacionales de la OCDE. Recuperado el 23 de septiembre de 2023 de https://www.oecd.org/daf/anti-bribery/convcombatbribery_spanish.pdf

OCDE (2015). *Plan de Acción BEPS*. Recuperado el 17 de septiembre de 2023 de https://read.oecd-ilibrary.org/taxation/plan-de-accion-contra-la-erosion-de-la-base-imponible-y-el-traslado-de-beneficios_9789264207813-es#page2

OCDE (2019). *International Compliance Assurance Programme* (2019). Recuperado el 17 de septiembre de 2023 de http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/international-compliance-assurance-programme-pilot-handbook-2.0.pdf

PUYOL, J. (2018). El Modelo de Evaluación de Riesgos en la Protección de Datos EIPD/PIA's. (Valencia: Tirant lo Blanch).

QUINTANA, T. y CASARES, A. (2014). *Evaluación de Impacto Ambiental y Evaluación Estratégica*. (Valencia: Tirant lo Blanch).

Recomendación (UE) 2017/1584 de la Comisión de 13 de septiembre de 2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala.

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 20 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad»).

Reglamento 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

SCHWAB, K. (2017). *The fourth industrial revolution*. (New York: Crown Business Publishing).

SIMON, J. (1987). The Emergence of a Risk Society-Insurance, Law, and the State. *Socialist Review*, (95), 60-89.

VÉRGEZ, J. (2016). "Alcance de la acción 2 del plan BEPS: recomendaciones relativas al diseño de las medidas nacionales y los tratados fiscales para neutralizar los efectos de los acuerdos de desajuste híbrido". *Fórum fiscal: la revista tributaria de Álava, Bizkaia y Gipuzkoa*, n. º 217 (75-88).

WITTENDORFF, J. (2010). *Transfer pricing and the arm's length principle in international tax law* (Vol. 35). Netherlands: Kluwer Law International BV.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

COMENTARIOS

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

The role of artificial intelligence in combating cyber terrorism

EL PAPEL DE LA INTELIGENCIA ARTIFICIAL EN LA LUCHA CONTRA EL CIBERTERRORISMO

Madaoui Nadjia
Lounici Ali, University of Blida2, Algeria
madaoui.nadjia99@yahoo.com 0009-0005-1096-211X

Recibido: 29 de octubre de 2023 | Aceptado: 08 de diciembre de 2023

ABSTRACT

This study aims at identifying the effects of technology on crime, as it is a double-edged sword, in which it can help in committing crimes, however it also contributes to preventing, detecting and suppressing them. Besides, technological development has had two prominent effects, one of them is negative, which was manifested in the dangers that threaten the security of states and individuals, particularly the phenomenon of terrorism, whose danger has steadily increased with technological and technical progress.
Therefore, the method of managing terrorism has become more sophisticated, as terrorist groups using cyberspace to launch attacks using the Internet and complex programs, thus terrorism has shifted from traditional based on hard power to cyber terrorism based on soft power. As for the positive impact of technological development, it is represented in the artificial intelligence technology used in the prevention and control of crimes, including cyber terrorism crimes.

KEYWORDS

Cyber terrorism
Artificial intelligence
technology
Combating
Prevention

RESUMEN

Este estudio tiene como objetivo identificar los efectos de la tecnología en la delincuencia, ya que es un arma de doble filo, en la que puede ayudar en la comisión de delitos, sin embargo, también contribuye a prevenirlos, detectarlos y reprimirlos. Además, el desarrollo tecnológico ha tenido dos efectos destacados, uno de ellos negativo, que se manifestó en los peligros que amenazan la seguridad de los Estados y de los individuos, en particular el fenómeno del terrorismo, cuyo peligro se ha incrementado constantemente con la tecnología.
Por lo tanto, el método de gestión del terrorismo se ha vuelto más sofisticado, ya que los grupos terroristas utilizan el ciberespacio para lanzar ataques utilizando Internet y programas complejos, por lo que el terrorismo ha pasado de ser tradicional basado en el poder duro al ciberterrorismo basado en

PALABRAS CLAVE

Ciberterrorismo
Tecnología de inteligencia artificial
Lucha contra la prevención
Prevención

el poder blando. En cuanto al impacto positivo del desarrollo tecnológico, está representado en la tecnología de inteligencia artificial utilizada en la prevención y control de delitos, incluidos los delitos de ciberterrorismo.

1. Introduction

Cyberspace has become of great significance in the international system, as it affects the nature of that system after the increasing reliance on technology. Besides, it helped to end the monopoly of power in the traditional sense of hard power, through the emergence of a new type of power, which is electronic or virtual power. Furthermore, this power became accessible to everyone who possesses technological knowledge and has the ability to use it to achieve his goals. However, it is not only used peacefully, but also by terrorist groups to conduct their attacks. Moreover, it is used by individuals and non-state actors to penetrate information networks or espionage and other offensive purposes.

As it is well known, cybercrime evolves as society develops, becoming more dangerous than ordinary crime. Especially with the spread of modern technology, and the increasing dependence of the world on computers and the Internet, the terrorist only needs, for example, a computer and secure his connection to the Internet company to carry out terrorist acts. In addition to, the crime of terrorism by electronic means has become a threat to the whole world, as the danger lies in its ease of use, in which it is employed by the terrorist while he is at home, office or hotel room away from the attention of the authority and society.

In a little more than two decades, the rapid growth of the Internet and information and communication technologies has enabled economic growth and expanded access to vital services. However, it also created new opportunities for criminal activities. As criminals have become the unintended beneficiaries of new technology and globalization because those developments have enabled them to commit and profit from crimes by exploiting transnational activities, as well as to expand their illegal activities and actions through digital platforms in a way that reduces risks, especially exposure. On the other hand, current technologies offer new opportunities for law enforcement, criminal investigation and prosecution, and fight cyber-crimes, including cyber terrorism, so as to improve public safety and enable law enforcement and criminal justice agencies to prevent and combat crime through technological progress and technology as well as artificial intelligence which has a positive impact in preventing or confronting cyber terrorism.

The significance of this study stems from our existence within the realm of the technological revolution, a period marked not only by its positive impacts but also by negative consequences. The convergence of terrorism and cyberspace has given rise to the explicit notion of cyber terrorism. This phenomenon is anticipated to be the most alarming criminal development in the coming years, with the potential for terrorists to exploit the Internet for destructive purposes, resulting in more severe consequences compared to traditional methods.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

The research aims at identifying the concept of cyber terrorism, its characteristics and causes, and then highlighting the other aspect that resulted from technological development, which is artificial intelligence as a means of preventing and combating this type of crime.

From the above, the main question of the study revolves around how to use artificial intelligence techniques and expert systems in preventing and combating cyber terrorism?

The descriptive analytical approach was adopted, through the analysis and extrapolation of jurisprudential opinions, and data collection, benefiting from the results of previous research, writings and studies that were published in the field of this study.

Therefore, we will attempt to answer the problematic of the study by dividing the research paper into two main sections:

— First - the concept of cyber terrorism and its causes.
— Second - the use of artificial intelligence technology to combat cyber terrorism.

II. The concept of cyber terrorism and its causes

Everyone recognizes the difficulty of giving a specific concept of terrorism, due to the lack of a unified agreement among specialists on this complex term of a changing nature, according to some, it is due to the overlap of the concept of terrorism with other concepts, such as political violence, political crime or organized crime. Furthermore, it is also a dynamic and evolving concept whose forms and motives vary in different places and time periods. Thus, the concepts of terrorism have varied and differed, according to the varying premises of researchers on the subject. However the common factor among them is that the terrorist act is a form of violence that targets the entity of society (Ben Amrouche, 2018, p. 218).

In an attempt to give a definition of cyber terrorism, we will discuss its definition linguistically, then jurisprudentially, and explain its characteristics and perpetrators, and try to determine their motives (VERRE, 2011, p. 24 et S).

2.1. The definition of cyber terrorism and its characteristics

There are many different definitions and opinions about cyber terrorism, as the international community has not determined yet an agreed comprehensive definition of terrorism, due to the diversity of its forms and manifestations, the multiplicity of its methods and patterns, the different international views and political trends around it, in addition to the various beliefs and ideologies espoused by states towards it, while some see it as terrorism, while others as a legitimate act.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

2.1.1. Linguistic and terminological definition of cyber terrorism

The term "Cyber terrorism" consists of two words, a familiar and common word "Cyber" which means the Internet, and the other word "Terrorism" which means violent, criminal acts, however until now it has not been defined in a specific way. Ibn Faris said in Mu'jam al-Lughah: "Ra', Ha', and Ba'a are two principles: one of them indicates fear, and the other refers to accuracy and lightness (Ibn Faris, 1999, p. 401)." in Taj Al Arous: (El Irhab – by Al Kasr - disturbing and frightening) (Al-Zubaidi, 1987, p. 50). The Academy of the Arabic Language in Cairo indicated that terrorists are a description given to those who use the way of violence to achieve their political goals (The Arabic Language Academy, s.d, p. 282). From the foregoing, it is clear that the meaning of terrorism in the language indicates intimidation, frightening and horrifying (Sharqi & Gharib, 2020, p. 561).

As for the definition of terrorism terminologically, there are many definitions of terrorism where opinions regarding it are varied and differed. However, the international community has not found yet a comprehensive and unified definition of terrorism. This is due to the diversity of its forms and manifestations, the multiplicity of its methods and patterns, the different international opinions and political trends around it, as well as the different beliefs and ideologies espoused by states towards it.

We can mention the most significant definitions of this term as follows:

> The International Islamic Fiqh Academy of the Organization of the Islamic Conference defines terrorism as: aggression, intimidation, or threat, whether material or moral, issued by states, groups or individuals against a person, in his religion, self, honour, mind or money without right, in various forms of violence and forms of corruption on land. (Al-Mukarramah, 5-10/1/2002)

Despite the numerous efforts at the international level to define terrorism, there is no single, comprehensive definition of the concept of terrorism. The most prominent of them is the one of the political encyclopaedia; which defined terrorism as: "the use of illegal violence, or the threat in its various forms, such as assassination, mutilation, torture, sabotage and bombing, in order to achieve a specific political goal, such as breaking the spirit of resistance and commitment among individuals, and destroying morale among organizations and institutions, or as a means of obtaining information or money. In general, it is the use of coercion to subjugate an opposing party to the will of the terrorist entity (Al Kayali, 1994, p. 562).

Barry Collins also defines it as "an electronic attack whose purpose is to threaten or attack governments, in pursuit of religious, political, or ideological goals, and that the attack must have a devastating and disruptive effect equivalent to the physical acts of terrorism. (Sharqi & Gharib, 2020, p. 562)"

Cyber terrorism can be defined as the illegal activity of a party by digital electronic technology through its networks to achieve a specific purpose (Mustafa, 2009, p. 5).

Furthermore, it is defined by Dergham Jaber Attoush as "aggression, intimidation, or physical or moral threat using electronic means issued by states, groups, or individuals

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

against a person in his religion, self, honour, or intellect, without right in all kinds and forms of corruption on land" (Al-Mawash, 2017, p. 9).

2.1.2 Characteristics of cyber terrorism

Cyber terrorism is characterized by many features that distinguish it from terrorism in its traditional form, which ultimately endeavours to achieve illegal goals, as follows:

Cyber terrorism is a transcontinental and cross-border terrorism, therefore is not subject to any specific geographical scope. It is one of the most serious types of terrorism, as it negatively affects the national security of the target country and the lack of a high degree of certainty in the results of those attacks. Besides, in traditional attacks, the target location is specific where the damages can be expected, however they can be repaired quickly because it is easier to discover the sources of defects, unlike electronic attacks (Sharqi & Gharib, 2020, p. 562).

What distinguishes cyber terrorism is the ability to conceal and obscure the sources of information: one of them is the difficulty of tracing the perpetrator of the cyber terrorism incident, as there are many difficulties that stand in the way of obtaining physical evidence linking the perpetrator to the incident. Besides, cyber terrorism crimes are characterized as being difficult to prove because there is no clear physical evidence, as well as the case of traditional attacks. However, the difficulty of proving them is due to many reasons: they are committed by a person with a high degree of competence, deception and misinformation has, in addition to the difference in time, place and the applicable law in the country in which it was committed.

The vulnerability to dangers, as the computer has a very significant role in contemporary life, and a base on which the work of many important facilities "hospitals - airports - banks…", this statement highlights the susceptibility to threats due to the pivotal role that computers play in modern life. The term "base" refers to the foundational reliance on computers, serving as a critical infrastructure for the functioning of essential facilities such as hospitals, airports, banks, and more. In other words, these important institutions and services heavily depend on computer systems for their operations. The interconnectedness of these sectors with computer technology makes them vulnerable to various risks and dangers, emphasizing the critical need for robust cyber security measures to safeguard against potential disruptions or attacks on these vital systems. therefore in the event of a malfunction in computers, this may lead to disasters, and then computers became widely targeted and an attractive target for terrorist groups. However, we no longer need to launch missiles and explosions to destroy a city, but it is enough to disable the transportation network or disable the computers of the stock exchange in that city.

The computer is the tool used in cyber-terror attacks: as it falls under the umbrella of cybercrime, which naturally occurs in a digital environment, and therefore the perpetrator needs to use a computer.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

Cyber-terror attacks are also characterized by low cost, as they require only a person with competence and technical expertise (Ben Amrouche, 2018, p. 221). Moreover, cyber-attack is a cross-border activity, thus it is a global activity which depends on deception and misinformation. Furthermore, there is difficulty in technical retention of its effects, and it is hard for the traditional investigator to deal with it. In addition, the motives of electronic terrorism are mainly political.

Calm environment: Cyber terrorism takes place in a calm environment that does not require force, violence (Abdel-Sadiq, 2009, p. 112) and the use of weapons. Therefore, it is called soft crimes. All it needs is a computer and the Internet, thus transferring data from a computer or cyber burglary does not need violence or shooting (Waquaf, 2006, p. 12).

Furthermore, one of the features of cyber terrorism is the multiplicity of actors in the use of cyber terrorist attacks, where terrorists resort to using cyberspace so as to collect information, recruit, plan, coordinate and finance, this will be dealt with in detail in the third section. Besides, the terrorists have a tremendous ability to use and employ the Internet to achieve their goals. Among the most prominent groups that have used this weapon are Al-Qaeda and, more recently, the most dangerous terrorist organization at all, "the Islamic State of Iraq and the Levant" "ISIS".

In addition to terrorist groups, countries use cyber terrorist attacks against hostile countries to achieve certain goals, as there are different ways to use cyber terrorism by the state, it may be used in the field of intelligence, or cooperation with individuals or terrorist groups to damage another country. Moreover, the state's use of this type is more dangerous than the one of terrorist groups, given the enormous capabilities of the state, which far exceeds the capabilities of the former.

Moreover, considering the widespread accessibility of the Internet to millions of users, its profound influence on public opinion becomes increasingly significant. As a result, there are individuals who sympathize with both the perspectives advocated by the state and those aligned with terrorist groups, encompassing their ideologies and associated issues.

2.2 The causes of cyber terrorism

The causes and motives of terrorism vary in the degree of their significance according to political trends, economic conditions, social conditions, as well as religious and ideological differences. We can summarize the causes of the phenomenon of terrorism as follows:

2.2.1 Personal and ideological motives

The personal and psychological factor is closely related to political, ideological and economic factors. As the marginalized youth who lose the meaning of life in the developing world for reasons related to injustice, inequity, unemployment, poverty and lack of a decent life are vulnerable to deviation and entry into the world of crime and terrorism. This is due to:

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

— A person's lack of the significance of his role in the family and society and his failure in family life, which leads to the acquisition of some bad qualities, including a lack of sense of belonging and loyalty to the homeland.
— The desire to appear and the love of fame, as a person is not qualified, therefore he searches for what qualifies him in vain, thus he feels aggression, sabotage and destruction.
— The person's resentment against the society in which he lives as a result of injustice and the violation of rights.
— The role of the media in stimulating the psychological factors of the individual and fuelling the spirit of a person's revenge.
— On the cultural level, the peoples of the developing world suffer from the negative repercussions created by globalization represented in cultural dependency and the identity crisis, as this led to the creation of cultural conflicts within the same society (Al-Huwaidi, 2011, p. 13).

With regard to ideological and intellectual motives, the misunderstanding of the principles and provisions of religion and its misinterpretation, and the dependence of young people on each other without referring to scholars, as well as the intellectual void and ignorance of the true religion rules, ignorance of the purposes of Sharia, extremism and radicalization in thought are all intellectual motives that led to an increase in the phenomenon of terrorism. Thus, the ideological motives leading to the phenomenon of terrorism vary, the most important of them can be stated as follows:

1. Ignorance of the objectives of Islamic law represented by conjecture not by certainty and confirmation, misunderstanding and misinterpretation of religion, and the ignorance of the rules, etiquette and behaviour of the true religion.
2. The various intellectual divisions between the diverse and different trends.
3. Extremism, which is very dangerous in any field, especially intellectual domains.

Among the most prominent causes and political motives for the phenomenon of terrorism, we find the following:

— The political motive is one of the stimulating motives for terrorism, as the unjust policies pursued by some people.
— States against their citizens, the political repression that they exercise, the marginalization of the citizen's role, the violation of his rights, and the failure to meet the requirements of social balance, all them represent a strong motive for the practice of terrorism in order to get rid of these conditions.
— In addition to the absence of social justice, inequality in the distribution of national wealth, disparity in the distribution of services and public utilities, and the negligence of citizens' needs.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

2.2.2 Political and technical motives

One of the political motives for the phenomenon of terrorism is the suffering of some international societies and peoples from injustice, persecution, colonial control, theft of funds, and violation of international laws and charters, which push peoples to extremism and radicalization.

Facts have also proven that the existing conflicts between two countries often lead to the exchange of electronic terrorist operations, as the case of the existing conflict between America and Cuba, in which the American political class attempted to link the Cuban island to cyber terrorism, and that was a few days after the receipt of (George W. Bush) the authority arguing that Cuba represents an indirect threat to the national security of the United States, and has the ability to launch cyber-attacks on the infrastructure of the superpower (Alejandro, 2012, pp. 154-155).

Among the technical reasons that facilitate cyber terrorism, we find:

1. The low cost of electronic mechanisms combined with the traditional tools with which terrorist operations are carried out, such as bombs, explosives, and developed weapons (Shafiq, 2016, pp. 36--37).
2. The lack of geographical borders and spatial barriers in cyberspace is an appropriate opportunity for terrorists.
3. The weakness of the information network structure and its penetrability provides terrorists with a way to attack them to achieve their goals. As terrorist groups may attack the computer networks of governments, private companies, or individuals.
4. The lack of control and oversight over information networks is one of the main reasons for the spread of cyber terrorism. In many cases, it is difficult for the police to pursue those who carry out cyber terrorism operations and to determine their identity.
5. The difficulty of proving these aspects is considered as one of the strongest motives helping to commit terrorist crimes, because it gives the criminal a hope of escaping punishment. Besides, the regulatory and legislative vacuum in crimes that are used in electronic crimes helped to increase this crime. Furthermore, the absence of a unified central authority that controls what is offered on the network and its inputs and outputs is an important reason for the spread of this crime (Ben Amrouche, 2018, p. 221); (Carole, 2019, p. 2).

The use of artificial intelligence technology to combat cyber terrorism.

The roots of artificial intelligence go back to the forties with the spread of computers, where Dan. W. Patterson defined it as "a type of computer science that is concerned with the study and formation of computer systems which show some forms of intelligence, as these systems have the ability to draw very useful conclusions about the problem set. Furthermore, these systems can also understand natural languages or living perception, and other capabilities that need intelligence when implemented by humans (Sheikh, 2018, p. 82).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

The term artificial intelligence has increased in use recently in light of the technical renaissance that the world is witnessing in the field of machine development. Although it was just a dream put forward by directors in fantasy films until the middle of the twentieth century, today it has become a tangible reality that we resort to many times, even if we sometimes do not realize it.

2.3 The definition of artificial intelligence and its characteristics

Artificial intelligence is one of the modern and innovative sciences that rely mainly on computers and its programs. It is the cornerstone in making programmed and computerized machines perform tasks similar to the human intelligence processes, which are learning, deduction and decision-making, it is characterized by a set of features

2.3.1 The definition of Artificial Intelligence

There is no specific definition of intelligence, therefore we find **Marvin Minsky**, who is one of the most famous scientists specialized in administrative and cognitive sciences in the field of artificial intelligence, in his book "Steps Towards Artificial Intelligence", defines it as "A branch of science that is concerned with machines that can solve the kind of problems that a person resorts to when solving them to his intelligence" (Suleiman, s.d, p. 3).

Mohammed Ali Al-Sharqawi defines artificial intelligence in his book as "Artificial Intelligence and Neural Networks" as "that branch of computer science through which it is possible to create and design computer programs that simulate the method of human intelligence so that the computer can perform some tasks instead of the human being that requires thinking, comprehension, hearing, speaking, and movement" (Al-Sharqawi, 1996, p. 24).

It is also defined as a technology dedicated to programming the machine to perform tasks that require human intelligence to solve, i.e. simulating the intelligent behaviour of humans. It is also described as an attempt to build machines that think and act like humans, so that they are able to learn and use their knowledge to solve problems alone (Al-Hamdani, 2008, p. 260).

2.3.2 The characteristics of artificial intelligence

Artificial intelligence has many characteristics that made it an effective investment in many areas, such as its application to devices and machines that enable it to plan and analyse problems using logic (Khaza'leh, 2015,), where machine is programmed by human and works well, however in many cases its work is more elaborate than the human.

It also recognizes sounds, speech and the ability to move things:

> The use of artificial intelligence contains many areas, including the field of robots that speak, move and distinguish sounds, which makes humans benefit from them

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

in the future, especially in the field of crime control, by recording sounds, movement and images and using them as evidence in proving or denying crimes, which helps to achieve justice.

In addition to the possibility of machines which carry out their work continuously without feeling tired or bored, as well as the stability of their ability to produce at all times without regard to the time or circumstances surrounding the work (Bana, 2020).

Furthermore, the devices that adopt artificial intelligence can understand the input and analyse it well to provide outputs that meet the user's needs with high efficiency (Khaza'leh, 2015,), such as entering information about a person by the police, thus the results are quickly given from the computer programmed for this process. Therefore, this makes it easier for the police to work easily and not to waste time, especially since the speed in proving crimes is among the things that help to achieve justice and not allowing criminals to evade them.

Moreover, artificial intelligence is also characterized by the ability to process the huge amount of information that is presented (sans référence), where, for example, the police can search for a person's name on a computer with just the touch of a button the result will be available, knowing that the device may contain hundreds of thousands of people's (Victor, Kenneth, & Big, 2013)names, which is considered a tremendous development and service to humans that exceeds their intelligence, as they cannot reach the level of machine intelligence no matter what they do, because the human mind is very limited.

Besides, the machine can find similarities and differences between the cases recorded in its brain or programmed, as well as it cannot forget unless a technical failure occurs, thus it helps to achieve justice.

2.4. Combating cyber terrorism through artificial intelligence

Artificial intelligence techniques play a pivotal role in predicting terrorist operations through the analysis of big data of citizens (Kathleen, August 2019), however at the same time, they face challenges related to human rights, and the implications of their practical applications, which raise questions about the limits of their predictive uses in combating terrorism, and the implications of opportunities and risks (Kathleen, August 2019).

By relying on the use of security surveillance cameras networks to monitor hundreds of thousands of faces on a daily basis in search of any suspected terrorist, where terrorist crimes can be reduced. In addition to using the characteristics of previous attacks, training in identifying terrorists in crowded areas, introducing artificial intelligence systems to analyse surveillance videos in criminal investigations, identifying suspected persons targeting major events, determining vehicle models and analysing suspicious financial transactions, and automatically detecting people who appear unusual behaviour such as frequently visiting a particular site or staying in one place, or suspicious items that have been abandoned.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

2.4.1 Methods of neutralizing cyber terrorist attacks

There are two ways to prevent terrorist attacks (Kathleen, August 2019); The first is deterrence, by protecting infrastructure, and implementing security controls, forecasting contributes to the physical protection of infrastructure, and it can also be a way to improve resource allocation to locations that are likely targets for terrorists.

The second aspect involves preventing the initiation of attacks, by arresting terrorists before they carry out their plans, combating future terrorist recruitment and extremism, imposing restrictions on the movement and freedom of individuals. Furthermore, effective prediction helps in the use of force or coercive restrictions against violent terrorists, whereas restorative measures are used with individuals prone to extremism.

Counter-terrorism predictability requires a type of artificial intelligence that enables knowledge and predictions to be extracted from diverse, large digital data. As algorithms that support predictive models are self-programmed based on data handling. In many cases, it would be impossible to analyse data without such an approach, and it would be impossible to build models without data (Kathleen, August 2019). However, the problem is that predicting terrorist operations imposes the need to expand the surveillance space for people in contravention of human rights, and exposes governments and intelligence services to human rights problems. Thus, in the near future, good predictions based on artificial intelligence techniques about whom or what to monitor can contribute to reducing the wholesale misuse of technical aspects of monitoring.

2.4.2 Applications of cyber counter-terrorism

Artificial intelligence can be used to make predictions about terrorism by analysing communications metadata, information about financial transactions, travel patterns, and web browsing activities. Furthermore, it can also be employed to analyse social network data to counter negative phenomena (Olivier, 2017), whether represented in combating extremist content on the Internet (Dr. Haider & Dr. Mahmoud, 2014, p. 19). Moreover, there is a growing interest by security authorities in using **Social Analytics** to analyse social network data to discover the possibility of riots and demonstrations in a given region (Dr. Al-Salmi, 1999, p. 43).

The Artificial Intelligence and Computer Science Laboratory at the Massachusetts Institute of Technology designed an algorithm that analysed more than 600 hours of YouTube videos with the aim of studying human behaviour. The algorithm was then able to correctly predict human actions in 43% of the test samples, which is less than the ability of humans by only 28% (Tolba & Fahmy, 2005, p. 38).

Artificial intelligence analyses the "big data" of individuals, which is the huge amounts of personal and professional information that can be analysed to identify developments in human behaviour patterns and interactions, as this data is very complex, which helps in a deep understanding of societies, in which it allows more ability to monitor collective and individual human behaviour, and predict their future trends (Shadi, Al-Ghitan, & Yahya, p. 12).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

Artificial intelligence endeavours to determine terrorists by distinguishing between what characterizes the activity of a particular subgroup on these media. Furthermore, machine learning methods allow interpreting and analysing patterns that are inaccessible with large amounts of data. These methods include analysing relationships between entities or more complex tools for image or sound recognition. In this regard, some examples of the ability of artificial intelligence to predict (Kathleen M., 2019), are represented as follows:

A. Predicting the timing and location of attacks: Models have been developed to predict the location and timing of terrorist attacks. In 2015, for example, a tech start-up (PredictifyMe) claimed that its model, which contains more than 170 data points, was able to predict suicide attacks with 72% accuracy. Furthermore, some other models have relied on open source data for individuals using social media and apps on their mobile phones include the Early Event Recognition System (EMBERS), which integrates the results of various separate predictive models in order to predict events such as disease outbreaks and civil disturbance events.

B. Fragility and vulnerability to extremism: Some technology companies have developed tools to assess vulnerability to violent extremist ideologies; Like Alphabet Inc's Jigsaw (formerly Google Ideas) which announced its project called "Redirect", that targets users of video-sharing sites who may be vulnerable to propaganda from terrorist groups such as "ISIS", as the project redirects them to videos that adopt an authoritative and anti-regulatory narrative.

C. Identification of terrorists: Some leaked details of a US National Security Agency (SKYNET) program indicate that an artificial intelligence-based algorithm was used to analyse metadata from 55 million local Pakistani mobile phone users in 2007, the result was that a percentage of only 0.008% of cases are mistaken as potential terrorists, which is about 15,000 people out of Pakistan's total population of 200 million at the time. Although the model used was not effective, it illustrates the predictive value of the data when identifying close links with terrorism.

Even though the prediction is not accurate at this time, with the development and improvement of machine recognition technology, we may reach a high rate of accuracy that makes us use this technology one day to correctly predict human actions, which we believe will contribute significantly to improving the level of security in cities.

III. Scope for future work

Cyber security needs much more attention. Given human limitations and the fact that agents such as computer viruses and worms are intelligent, network-centric environments require intelligent cyber sensor agents (or computer-generated forces) which will detect, evaluate and respond to cyber-attacks in a timely manner. The application of AI techniques in cyber defense will need planning and future research. One of the challenges is knowledge management in network-centric warfare, hence a promising area for research is introduction of modular and hierarchical knowledge architecture

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

in the decision making software. Rapid situation assessment and decision superiority can only be guaranteed with automated knowledge management. It is also foreseeable that the grand goal of AI research – development of artificial general intelligence - can be reached in not so distant future which would lead to Singularity described as "the technological creation of smarter-than-human intelligence". Nevertheless, it is of crucial importance that we have the ability to use better AI technology in cyber defense than the one offender possess. Furthermore, a lot more research needs to be done before we are able to construct trustworthy, deployable intelligent agent systems that can manage distributed infrastructures. Future work must search for a theory of group utility function to allow groups of agents to make decisions. (Dilek, S, Çakır, H., Aydın, M. 2015. P33-34).

The role of artificial intelligence (AI) in combating cyber terrorism constitutes a critical and evolving field with considerable scope for future research. One promising avenue for exploration involves advancing the capabilities of AI-driven predictive models for early detection and prevention of cyber threats associated with terrorism. Future research could delve into the development of more sophisticated algorithms and machine learning techniques, enhancing the accuracy and efficiency of AI systems in identifying emerging cyber threats and potential terrorist activities. Furthermore, there is a pressing need to investigate the integration of AI in cyber security strategies employed by governments, organizations, and security agencies. This research could focus on understanding how AI technologies can be effectively incorporated into existing frameworks to bolster cyber defenses against evolving and sophisticated cyber threats associated with terrorist activities. Examining the practical implementation of AI-powered cyber security measures and their effectiveness in real-world scenarios would provide valuable insights for policymakers and practitioners.

The ethical and legal dimensions of AI in the context of combating cyber terrorism present a complex and multifaceted area for future inquiry. Research in this domain could explore the development of ethical frameworks and regulatory guidelines governing the responsible use of AI in counterterrorism efforts. Understanding the ethical considerations and legal implications associated with AI technologies would contribute to the establishment of robust governance mechanisms that balance security imperatives with individual rights and privacy concerns. Additionally, as AI technologies continue to advance, there is potential for research on the vulnerabilities and countermeasures specific to AI systems themselves. Investigating the susceptibility of AI algorithms to adversarial attacks and developing techniques to enhance the resilience of AI-powered cyber security solutions would be crucial for ensuring the reliability and trustworthiness of these systems in the fight against cyber terrorism.

An interdisciplinary approach to studying the socio-technical aspects of AI in combating cyber terrorism is another promising direction for future research. Examining the human factors involved, such as user interactions with AI-based security systems and the socio-political implications of widespread AI adoption in counterterrorism could provide a comprehensive understanding of the broader impact of AI technologies on security practices.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

In conclusion, the future scope for research in the role of AI in combating cyber terrorism is vast and multifaceted. From technical enhancements and practical implementations to ethical considerations and societal implications, researchers have the opportunity to contribute significantly to the advancement of knowledge in this critical domain. As AI technologies and cyber threats continue to evolve, ongoing research endeavors will be essential for developing effective and responsible strategies to safeguard against cyber terrorism.

IV. Conclusion

We addressed in this study a significant subject that has become a current event, which is cyber terrorism, and the role of artificial intelligence technology systems in preventing and combating it, as it is a very thorny and complex subject.

Cyber terrorism is one of the most serious types of terrorism in the world, especially since the phenomenon of cyberspace has played a strategic role in the international community at the economic, political, cultural, security and social levels.

The danger of cyber terrorist acts lies in their reliance on advanced technologies such as devices that eavesdrop on communication networks, encryption software, to penetrate network and computer security systems. Furthermore, a single automated network may include tens, hundreds of thousands, or millions of computers or devices connected to the Internet that can be used to launch various attacks for criminal purposes such as sabotage, terrorism, threats and extortion.

We concluded a set of results, the most important are:

- Cyber terrorism is a deliberate activity or attack with political motives aiming to influence government decisions or public opinion by exploiting cyberspace in the implementation process with the intent of intimidating individuals by threatening them or causing actual damage to them.
- The fundamental reasons for the spread of this kind of terrorist acts are: the political reasons represented in the dictatorship of the regime and the lack of political participation of citizens. Moreover, the economic reasons which are due to social inequality, and the spread of unemployment. As for the technological reasons, it is mainly due to the weakness of the information network system. Therefore, it is easy to penetrate by terrorist groups, in addition to its ease of use, low risks and cost.
- The methods and means used by terrorist groups to exploit cyberspace in carrying out their terrorist acts are represented in coordination and communication, in addition to media promotion, as well as spying on and destroying websites, and finally, propaganda war which aimed at attracting and recruiting many individuals, especially minors, as well as obtaining support and financial resources.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

— Advancement in the field of artificial intelligence has made robots more intelligent and able to perform many functions and tasks instead of humans, it also has encouraged an increasing number of law enforcement agencies to take advantage of these technological advances in a variety of their operations.
— Artificial intelligence is very much a double-edged sword, as it can lead to important changes in the way justice agencies deal with the task of policing, however it also enhances the working methods of terrorist groups, and can even facilitate the emergence of new forms of crime and the priority must be to enhance policing using AI techniques to combat AI-based crime.

At the end of the research, we recommend the following:

— Giving special significance to identifying ways and means to enable criminal justice and law enforcement personnel to employ advanced technologies, such as artificial intelligence, information and communication technologies, including big data, as well as to make full use of them in combating the crime of cyber terrorism.
— Countries of the world should identify and address existing gaps in their legal systems to ensure effective investigation and prosecution of technology-facilitated crimes, including adopting new laws and/or updating existing laws with technology-neutral language, and promoting international cooperation.
— States should promote and expand partnerships and synergies with international and regional organizations, civil society, the private sector and academia, in order to enhance research, innovation, development and use of technology in the areas of law enforcement and criminal justice in the context of preventing and combating terrorist cybercrime.
— Working to constantly improve new technologies to ensure preparedness to address their problems; and to promote the application of ethical standards in the use of these technologies.

Bibliography list

ABDEL-SADIQ, A. (2009). *Cyber Terrorism: The Power in International Relations, a New Pattern and a Contrasting App*. Cairo: Center for Political and Strategic Studies.

AL KAYALI, A. W. (1994). *Political Encyclopedia, part 7*. Beirut: the Arab Foundation for Studies and Publishing.

AL-SHARQAWI, M. A. (1996). *Artificial Intelligence and Neural Networks* (éd. 1). Egypt: The Modern Egyptian Office Press

AL-ZUBAIDI. (1987). *Taj al-'arūs min jawāhir al-Qāmūs* (éd. 2). (A. Hilali, Éd.) Kuwait.

AL-HAMDANI, B. H. (2008). Al-Bakry, Riyad Hamza, *The reality of development in light of scientific progress and the concept of artificial intelligence*. Journal of Comprehensive Management Accounting, College of Management and Economics.

AL-HUWAIDI, O. (2011). *Combating Terrorism Crimes*. Amman: Dar Wael Li Al Nasher.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

AL-MAWASH, D. J. (2017). *The Crime of Information Espionage (a comparative study)* (éd. 1). Egypt: Longitudinal Center for Scientific Studies and Research.

AL-MUKARRAMAH, T. d. (5-10/1/2002). *(Makkah Al-Mukarramah: the Islamic Fiqh Council of the Muslim World League in its sixteenth session.*

AL-SALMI, A. A.-R. (1999). *Information Systems and Artificial Intelligence*. Amman: Dar Al-Manhaj for Publishing and Distribution.

ALEJANDRO, C. A. (2012). *The Empire of Terror* (éd. 1). (W. Ibrahim, Trad.) Beirut: Publications Company for Distribution and Publishing.

BANA, D. (2020, January 14). Consulté le November 16, 2021, sur https://mawdoo3.com

BEN AMROUCHE, F. (2018). *Electronic Terrorism: A Study in Conceptual and Dimensional Problems*. Algerian Journal of Social and Human Sciences, 8(2).

CAROLE, M. (2019). Laurent Guille*, Intelligence Artificielle Et Cybersécurité*. Wavestone.

DILEK, S., ÇAKIR, H., & AYDIN, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications (IJAIA), 6(1).

HAIDER, S. A.-B., & Dr. MAHMOUD, H. A.-H. (2014). *Technology and Information Systems in Contemporary Organizations* "A Technological Administrative Perspective." Cairo: Published by Mahmoud Hassan Jomaa Foundation.

IBN FARIS. (1999). *A Dictionary of Language Standards* (éd. 1). Beirut: Dar al-Kotob al-Ilmiya.

KATHLEEN, M. (2019, October 9). *Predicting Attacks: Opportunities and Risks of Using Artificial Intelligence* in. Récupéré sur https://futureuae.com/ar/Mainpage/Item/5022/%D8%A7%D9%84%D8%AA%D9%86 %D8%A8%D8%A4-%D8%A8%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA.

KATHLEEN, M. (August 2019). *Artificial Intelligence Prediction And Counterterrorism*. Britain: Chattam House.

KHAZA'LEH, S. (2015, August 15). *The Characteristics of Artificial Intelligence*. Consulté le November 16, 2021, sur https://mawdoo3.com.

MUSTAFA, M. M. (2009). *Electronic Terrorism (legal, security, psychological, and social study)* (éd. 1). Cairo: Egyptian National Books and Documents House.

OLIVIER, T. (2017, June 6). *Artificial Intelligence Will Save Us From Cyberterrorism*. Consulté le August 12, 2020, sur https://Www.Telerama.Fr/Medias/L-Intelligence-Artificielle-Va-Nous-Sauver-Du-Terrorisme'159806.Php.

sans référence. (s.d.).

SHADI, A.-W., Al-GHITAN, I., & YAHYA, S. (s.d.). *Opportunities and Threats of Artificial Intelligence in the Next Ten Years.*

SHAFIQ, N. (2016). *The Impact of Cyber Threats on International Relations: A Study in the Dimensions of Cyber Security* (éd. 1). Cairo: al-Maktab al-'Arabī lil-Ma'ārif.

SHARQI, S., & Gharib, H. (2020). *Electronic Terrorism and the Transformation of the Concept of Power*. Al-Bahith Journal for Academic Studies,, 7(2).

SHEIKH, H. (2018). *The role of artificial intelligence in managing the electronic customer relationship of the Algerian People's Credit* CPA. Academic Journal of Human and Social Studies,(20).

SULEIMAN, Y. A.-F. (s.d). *Artificial intelligence*. Syria: Al-Badr Magazine.

The Arabic Language Academy. (s.d). *The Intermediate Lexicon*. (I. Mustafa, & others, Éds.) Turkey: the Islamic Library.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

TOLBA, D., & FAHMY, M. (2005). *Computer Knowledge Department*. Alexandria: Modern Egyptian Office Press.

VERRE, D. (2011). *Cyberspace And Actors Of Cyberconflict* (Edition Bermes Science ed.). Paris: La Voisier.

VICTOR, M.-S., KENNETH, C., & BIG, D. (2013). *A Revolution That Will Transform How We Live. Work And Think* (London, John Murray).

WAQUAF, A.A. (2006). *Combating Terrorism Between Politics and Law*. Algeria: Dar Al-Kheldonia Publishing and Distribution.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 211-227
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

El preocupante clausulado de la Ley Modelo de Neuroderechos del Parlatino*

THE WORRYING CLAUSES OF THE PARLATINO NEURORIGHTS MODEL LAW

Diego Borbón
Universidad Externado de Colombia
diego.borbon1@uexternado.edu.co 0000-0002-2115-2105
Luisa Borbón
Universidad de los Andes
luisaborbon.ro@gmail.com 0000-0003-2220-4277
Ximena Mora-Gómez
Universidad Externado de Colombia
leidy.mora@uexternado.edu.co 0009-0009-9683-0036
Sandra Villamil-Mayoral
Universidad Externado de Colombia
sandra.villamil1@uexternado.edu.co 0009-0009-3546-655X

Recibido: 23 de octubre de 2023 | Aceptado: 06 de diciembre de 2023

RESUMEN

Recientemente, el Parlamento Latinoamericano y Caribeño (Parlatino) promulgó una Ley Modelo sobre Neuroderechos con el propósito de crear las bases para que los países miembros legislen en esa materia. Sin embargo, los documentos presentados por el Parlatino podrían adolecer de serios vicios de fundamentación teórica, conceptual y científica, así como de contener, y desconocer, importantes debates neuroéticos. En este artículo buscamos

PALABRAS CLAVE

Neuroderechos
Neuroderecho
Neuroética
Libertad cognitiva
Neurociencias
Mejora cognitiva

* El presente artículo es un producto del Grupo de Investigación en Ciencias Biológicas y Derecho del Centro de Estudios sobre Genética y Derecho de la Universidad Externado de Colombia, reconocido por el Ministerio de Ciencia, Tecnología e Innovación del Gobierno de Colombia: https://scienti.minciencias.gov.co/gruplac/jsp/visualiza/visualizagr.jsp?nro=00000000020449.

El orden de los autores fue decidido conforme su contribución al texto. D.B. y L.B. estructuraron el artículo y contribuyeron a su redacción principal; X.M.G. aportó un análisis concreto al problema del consentimiento informado; S.V.M contribuyó a los comentarios críticos; X.M.G; S.V.M; L.B. y D.B. revisaron y corrigieron la redacción final del mismo y aprobaron el texto para su publicación en coautoría.

poner de presente los principales reparos frente al documento presentado para servir como Ley Modelo, así como del Anexo "Marco teórico conceptual general". En ese sentido, hacemos un especial llamado al debate académico, científico y político, sin incurrir en proposiciones normativas apresuradas e inadecuadas. Por tales consideraciones, sugerimos no incorporar la Ley Modelo propuesta. Por el contrario, proponemos que, en lugar de crear normas ambiguas, abstractas y generales, se legislen y se lleguen a acuerdos internacionales en materias concretas con base en los riesgos reales de la neurotecnología, de tal manera que las regulaciones verdaderamente protejan. Hasta entonces, los comentarios críticos que desde la academia se han planteado, son una necesaria crítica que disputa el papel de los neuroderechos en el entorno político global.

ABSTRACT

Recently, the Latin American and Caribbean Parliament (Parlatino) promulgated a Model Law on Neurorights with the purpose of creating the bases for member countries to legislate on this matter. However, the documents presented by the Parlatino could suffer from serious defects in theoretical, conceptual and scientific foundation, as well as containing, and ignoring, important neuroethical debates. In this article we seek to highlight the main objections to the document presented to serve as a Model Law, as well as the Annex "General conceptual theoretical framework". In this sense, we make a special call for academic, scientific and political debate, without incurring in hasty and inadequate normative proposals. For such considerations, we suggest not incorporating the proposed Model Law. On the contrary, we propose that, instead of creating ambiguous, abstract and general regulations, international agreements be legislated and reached on specific matters based on the real risks of neurotechnology, in such a way that the regulations truly protect. Until then, the critical comments that have been raised from academia are a necessary critique that disputes the role of neurorights in the global political environment.

KEYWORDS

Neurorights
Neurolaw
Neuroethics
Cognitive Liberty
Neuroscience
Cognitive enhancement

I. Introducción

En la frontera de la ciencia y la tecnología, las neurociencias están avanzando a un ritmo sin precedentes. Desde las innovaciones en neurología clínica hasta la aplicación de neurotecnologías con fines recreativos y comerciales, se abre una nueva posibilidad, no sólo para comprender y monitorizar la actividad cerebral, sino, también para manipularla. En esa dirección, los avances en esta materia no están exentos de cuestionamientos éticos y legales. A medida que la cognición humana se integra cada vez más con nuevas tecnologías, resulta imperativo considerar las implicaciones para la privacidad, la autonomía, la integridad y la dignidad humana. Bajo este importante marco tecnológico es que surgen los denominados "neuroderechos".

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

Los neuroderechos, como concepto emergente, hacen referencia a una serie de nuevos derechos fundamentales propuestos para abordar los desafíos éticos y legales que plantea el avance de la neurociencia humana y las neurotecnologías. Estos nuevos derechos buscan proteger la integridad de la mente humana, empleando conceptos como la libertad cognitiva, la privacidad mental, la integridad mental y la continuidad psicológica.

En esencia, los neuroderechos buscan proporcionar, y promover, un nuevo marco regulatorio como un conjunto de principios propuestos para protegernos de los avances tecnológicos en materia de neurociencias. Así, los neuroderechos se centran en abordar y regular el uso de tecnologías que tienen el potencial de afectar o manipular la función cerebral, los procesos cognitivos, o incluso la identidad personal de un sujeto. De la misma manera, estos nuevos derechos se han propuesto con alcances incluso para el desarrollo de la inteligencia artificial (IA) sin sesgos algorítmicos.

En tal dirección, son varios países, organizaciones internacionales y organismos regionales, como se verá más adelante, los que han adelantado varias iniciativas de neuroderechos. Al respecto, Chile, Brasil, Argentina, España, Francia y México son algunos ejemplos de Estados que han adoptado, o están adelantando, proyectos al respecto. A nivel internacional, la Organización de Naciones Unidas, en sede de la UNESCO y la Asamblea General, ha adelantado y encomendado estudios en materia de neurociencias y derechos humanos. En organismos regionales, por su parte, la Organización de Estados Americanos, y particularmente el Comité Jurídico Interamericano, ha realizado declaraciones y emitido unos principios interamericanos en la materia. Por último, el Parlamento Latinoamericano y Caribeño (en adelante Parlatino), promulgó una Ley Modelo para que los países miembros cuenten con las bases para legislar en dicha materia.

Con las anteriores consideraciones, este artículo se propone abordar un estudio crítico de la "Ley Modelo de Neuroderechos para Latinoamérica y el Caribe" emitida por el Parlatino (2023), así como su Anexo "Marco Teórico Conceptual General". Se realizará una aproximación crítica con el empleo de una metodología de investigación sociojurídica documental con fuentes jurídicas formales, como leyes e iniciativas normativas de neuroderechos, así como el uso de fuentes secundarias, especialmente libros, artículos y documentos con referencia a la intersección entre neurociencias y derechos humanos. Posteriormente, se traerán a colación las principales observaciones críticas que desde la academia se han formulado a las actuales iniciativas de neuroderechos, para señalar las numerosas preocupaciones que pueden advertirse del clausulado propuesto en la Ley Modelo del Parlatino, así como las deficiencias técnicas, metodológicas y conceptuales del Anexo que fundamenta la propuesta.

El artículo concluye que, en atención a las múltiples deficiencias conceptuales, técnicas y metodológicas de esta propuesta, los países de Latinoamérica y el Caribe no deberían incorporar la Ley Modelo del Parlatino en sus legislaciones, o por lo menos no con la redacción textual propuesta. Justamente, lejos del *boom* mediático, la academia ha planteado serios e importantes comentarios que parecen ser desconocidos por buena parte de las iniciativas de neuroderechos, tanto así que los más importantes

neuroeticistas y juristas alrededor del mundo han alzado voces críticas para construir mejores regulaciones. Si las iniciativas tuviesen en cuenta dichos comentarios y observaciones, sin duda podríamos construir propuestas mucho más robustas y acertadas favor de todas las personas. Por lo tanto, sugerimos dar mayor apertura al debate desde instancias sociales y políticas, con especial atención a las sendas observaciones que se han formulado desde la academia, y resaltamos la importancia de no legislar de maneras erráticas y apresuradas.

II. Contexto del surgimiento de los neuroderechos

Comprender el surgimiento de los neuroderechos requiere, previamente, un sumario contexto a propósito de la neuroética y el neuroderecho. Por ello, como propuesta para crear una nueva categoría de derechos fundamentales, los neuroderechos se basan en antecedentes académicos y filosóficos desarrollados desde la neuroética. Así, por ejemplo, conceptos como la libertad cognitiva se han construido justamente en discusiones propias de este campo.

Pues bien, cuando el editor en jefe, Neil Levy, publicó la carta editorial del primer volumen de la prestigiosa revista Neuroethics, hoy una de las más importantes en la materia, consideró que la neuroética se refiere a dos grandes temas estrechamente relacionados.

En primer lugar, la neuroética comprendería la reflexión ética sobre las nuevas tecnologías y técnicas producidas por la neurociencia. Las preguntas que surgen en dicha interacción también tienen relación con preguntas bioéticas sobre la aplicación de nuevas técnicas biomédicas y el desarrollo de biotecnologías (Levy, 2008). Si bien son cuestiones similares, Levy (2008) sostuvo que la bioética y la neuroética eran lo suficientemente diferentes para justificar la creación de una nueva disciplina.

La segunda rama de la neuroética, para Levy (2008), conserva aún más diferencias con la bioética. Se refiere, en ese sentido, a las formas en las que el nuevo conocimiento que surge de las ciencias cognitivas impacta en temas filosóficos tradicionales, como la naturaleza de la moralidad, el autocontrol, las creencias y la búsqueda del conocimiento (Levy, 2008). Preguntas que no tienen realmente un análogo en la bioética. De esa manera, concluyó que:

> Las dos ramas de la neuroética interactúan, produciendo una disciplina generalmente nueva, una a la que los bioeticistas tienen mucho que contribuir, pero que es igualmente la provincia de neurocientíficos, filósofos, psicólogos, sociólogos y abogados (p.2).

Véase, en ese sentido, que el debate neurocientífico no solo permea cuestiones éticas, sino que también podría tener impacto en materia legal y jurídica. En esa dirección, ya en 1991 Taylor, Harp, y Elliott, estimaron el surgimiento de una nueva disciplina: el neuroderecho –neurolaw–. Para Taylor, Harp, y Elliott (1991), los *neuropsicólogos* y los *neuroabogados* cumplirán una función importante en el litigio civil. Estos autores

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

consideraban especialmente importante el vínculo en materia de responsabilidad civil, por ejemplo, en casos de lesiones cerebrales traumáticas. Así, para Taylor, Harp, y Elliott (1991), "el neuroabogado es aquél que presenta evidencia neuropsicológica en los tribunales de justicia" (p.298). Por otra parte, para Petoft (2015) el neuroderecho es un intento de conocer la relación entre derecho y el cerebro teniendo en cuenta los hallazgos de la neurociencia, explorando los efectos de los descubrimientos de la neurociencia en las normas jurídicas. En síntesis, para Cáceres Nieto y López Olvera (2022), el neuroderecho es la:

> [...] interdisciplina encargada de estudiar la regulación jurídica de la investigación en neurociencias y su aplicación al derecho (derecho de las neurociencias), así como los factores neurológicos que intervienen en los procesos cognitivos y comportamentales de los operadores jurídicos (neurociencia del derecho) y la forma en que las neurociencias pueden auxiliar a la práctica jurídica (neurociencias auxiliares del derecho) (p.75).

Sobre la aplicación concreta del neuroderecho, acogemos lo propuesto por Meynen (2019) de dividir esta disciplina en tres áreas concretas: revisión, evaluación e intervención. La primera área se refiere a la revisión de la ley y las prácticas legales ya que la neurociencia puede proporcionar motivos para reconsiderar y reformar elementos del derecho. El segundo dominio se refiere a la evaluación a los individuos que utilizan técnicas de neurociencia en el derecho, como las personas procesadas en una causa penal. La intervención es la tercera área de investigación del neuroderecho que considera el sí y el cómo de las intervenciones cerebrales directas en el sistema de justicia penal (Meynen, 2019). El tema de los neuroderechos estaría inmerso, especialmente, en el área de la revisión.

En esa dirección, para Ienca (2021), a lo largo de la década de 1990 y principios de la de 2000, los temas principales abordados por la neuroética y el neuroderecho, se enfocaron en cuatro grandes familias temáticas sobre la permisibilidad de la mejora cognitiva con nootrópicos, las implicaciones filosóficas y jurídicas de la neurociencia del libre albedrío, la ética de las neuroimágenes y la lectura de la mente, y la validez de la evidencia neurocientífica en tribunales de justicia.

Ahora bien, para Ienca (2021), en la actualidad y en las últimas dos décadas, el progreso tecnológico en neurociencias, y su extrapolación a sectores por fuera de la medicina, como el derecho, la guerra o el mercado recreativo, ha dado lugar a un creciente interés en las implicaciones éticas y sociales de las neurotecnologías. Así, siguiendo a Ienca (2021):

> Desde principios del presente siglo ha surgido una quinta y complementaria área de investigación neuroética y neurojurídica, que ha comenzado a mirar los desafíos ético-jurídicos en neurociencia y neurotecnología en términos de principios normativos de alto nivel, como derechos, facultades y deberes asociados. Esta forma de analizar las implicaciones éticas y jurídicas de la neurociencia ha llegado a conocerse como "neuroderechos". Los neuroderechos pueden definirse como los principios éticos, legales, sociales o naturales de libertad o derecho relacionados con el dominio cerebral y mental

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

> de una persona; es decir, las reglas normativas fundamentales para la protección y preservación del cerebro y la mente humanos (p.2).

Así las cosas, con estos contextos, en el año 2017 nace la propuesta formal de crear una nueva categoría de derechos fundamentales bajo la etiqueta de 'neuro'derechos. De esa manera, el artículo seminal de Ienca y Andorno (2017) marca el punto de partida en esta materia. La base conceptual de los neuroderechos, tal como lo reseña Ienca (2021), habría comenzado a principios de la década de 2000, con el trabajo de neuroeticistas como Boire y Sententia sobre la *libertad cognitiva*, argumentaron que debería considerarse como un derecho fundamental, parte integral de cualquier otra libertad.

Ienca y Andorno (2017) sostuvieron que la creciente sensibilidad y disponibilidad de los neurodispositivos requerirán la aparición de nuevos derechos o el desarrollo de derechos tradicionales para abordar específicamente los desafíos planteados por la neurociencia y la neurotecnología (Ienca y Andorno, 2017). Sugieren que los derechos humanos han surgido históricamente en respuesta a amenazas a los intereses humanos fundamentales o a la dignidad humana, y que el mismo proceso puede ocurrir con la neurociencia. De esa manera, Ienca y Andorno (2017) proponen cuatro neuroderechos, incluido el derecho a la libertad cognitiva, el derecho a la privacidad mental, el derecho a la integridad mental y el derecho a la continuidad psicológica. Argumentan que estos derechos cumplen con los requisitos para justificar nuevos derechos humanos y no plantean el riesgo de inflación de derechos.

En ese sentido, para Ienca y Andorno (2017) el derecho a la libertad cognitiva se refiere a la protección de los individuos contra el uso coercitivo y no consentido de tecnologías que pueden afectar la cognición. Por su parte, el derecho a la privacidad mental implica la protección de la información privada o sensible en la mente de una persona contra la recopilación, almacenamiento, uso o incluso eliminación no autorizados. Adicionalmente, el derecho a la integridad mental se refiere a la protección de los individuos contra las intervenciones no autorizadas en su bienestar mental realizadas a través del uso de neurotecnología, especialmente si dichas intervenciones resultan en daño físico o mental para el usuario de la neurotecnología. Finalmente, el derecho a la continuidad psicológica aborda la protección de la identidad personal y la coherencia del comportamiento individual contra la modificación no consentida por parte de terceros (Ienca y Andorno, 2017).

En el mismo año, el equipo encabezado por el neurobiólogo español, Rafael Yuste, publicó un breve comentario en la revista Nature, donde ponen de presente varios retos éticos de las neurotecnologías y la inteligencia artificial (IA), destacando la necesidad de respetar y preservar la privacidad, identidad, agencia e igualdad de las personas. En esa dirección Yuste et al. (2017) señalan que, aunque la tecnología de interfaces cerebro computadoras (BCI) actual se centra principalmente en los resultados terapéuticos, como ayudar a las personas con lesiones de la médula espinal, la tecnología está avanzando hacia una mayor interpretación de la actividad neural y la posibilidad de manipulación cerebral directa.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

En ese sentido, Yuste et al. (2017) argumentan que, aunque estas tecnologías podrían revolucionar el tratamiento de muchas afecciones y mejorar la experiencia humana, "la tecnología también podría exacerbar las desigualdades sociales y ofrecer a las corporaciones, piratas informáticos, gobiernos o cualquier otra persona nuevas formas de explotar y manipular a las personas" (p. 160). Además, advierten que estas tecnologías podrían alterar profundamente algunas características humanas fundamentales, como "la vida mental privada, la agencia individual y una comprensión de los individuos como entidades unidas por sus cuerpos" (p. 160).

Por tales razones, Yuste el at. (2017) identifican cuatro retos éticos particulares que requerirían la creación de nuevos derechos humanos. En primer lugar, sobre la privacidad y el consentimiento, las prácticas actuales a menudo involucran a personas que, sin saberlo, renuncian a sus derechos de privacidad, por lo que las soluciones propuestas incluyen establecer un valor predeterminado de exclusión voluntaria para compartir datos neuronales, regular la transferencia comercial y el uso de datos neuronales e implementar tecnologías para garantizar la privacidad de los datos (Yuste et al. 2017). Por otra parte, en materia de agencia e identidad, Yuste et al. (2017) identifican que las neurotecnologías pueden alterar el sentido de identidad y agencia de las personas, lo que genera problemas relacionados con la responsabilidad personal, por lo que proponen que se deben implementar protecciones para defender la identidad y la agencia individual como derechos humanos básicos.

Por otra parte, en materia de mejora cognitiva o aumento (enhancement), Yuste et al. (2017) sostienen que las mejoras de la neurotecnología que aumentan la resistencia o las habilidades cognitivas podrían desencadenar la presión social para adoptar estas mejoras y potencialmente conducir a nuevas formas de discriminación. Por lo tanto, proponen que debieran establecerse directrices tanto a nivel internacional como nacional para fijar límites a las tecnologías de aumento y definir sus contextos de uso aceptables (Yuste et al. 2017). Finalmente, en materia de sesgos de los algoritmos de inteligencia artificial, sostienen que estos podrían incorporarse involuntariamente dentro de las tecnologías, privilegiando a ciertos grupos sobre otros. Por lo anterior, la propuesta sería establecer, como regla general contramedidas a los sesgos, para garantizar que los grupos marginados, participen en el diseño de algoritmos y dispositivos (Yuste et al. 2017). Por estas razones, Yuste et al. (2017) sostienen que: "Recomendamos agregar cláusulas que protejan tales derechos ('neuroderechos') a los tratados internacionales, como la Declaración Universal de los Derechos Humanos de 1948" (p.162).

Con este antecedente, nació la NeuroRigths Initiative, hoy NeuroRights Foundation, en cabeza de Yuste, que parte de un taller de tres días en la Universidad de Columbia, organizado por el Grupo Morningside, en el que líderes académicos se reunieron para discutir las preocupaciones éticas de la neurotecnología y la inteligencia artificial (NeuroRights Foundation, s.f.). Como resultado del taller, dos años después, se fundó la Iniciativa NeuroRights (NRI) en la Universidad de Columbia, con el objetivo de servir como una organización de derechos humanos para desarrollar directrices sobre la innovación neurotecnológica, que derivó, finalmente, en la Fundación NeuroRights,

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

que incorporó a la NRI en su estructura (NeuroRights Foundation, s.f.). Esta iniciativa propone crear cinco neuroderechos:

> Privacidad Mental: Cualquier NeuroDato obtenido de la medición de la actividad neuronal debe mantenerse en privado. Si se almacena, debe existir el derecho a que se elimine a petición del sujeto. La venta, la transferencia comercial y el uso de datos neuronales deben estar estrictamente regulados.
>
> Identidad personal: Se deben desarrollar límites para prohibir que la tecnología interrumpa el sentido de uno mismo. Cuando la neurotecnología conecta a las personas con redes digitales, podría desdibujar la línea entre la conciencia de una persona y los insumos tecnológicos externos.
>
> Libre albedrío: Las personas deben tener el control final sobre su propia toma de decisiones, sin manipulación desconocida de neurotecnologías externas.
>
> Acceso Justo al Aumento Mental: Deberían establecerse directrices tanto a nivel internacional como nacional que regulen el uso de las neurotecnologías de mejora mental. Estas directrices deben basarse en el principio de justicia y garantizar la igualdad de acceso.
>
> Protección contra el sesgo: Las contramedidas para combatir el sesgo deberían ser la norma para los algoritmos en neurotecnología. El diseño del algoritmo debe incluir aportes de grupos de usuarios para abordar de manera fundamental el sesgo (NeuroRights Foundation, s.f., s.p.).

De esa manera, los neuroderechos se postulan como propuestas para crear una nueva categoría de derechos humanos que protejan a las personas de los riesgos planteados por el exacerbado avance de las neurotecnologías y la inteligencia artificial.

III. Los neuroderechos: lejos del consenso y cerca de las críticas de la academia

El propósito mismo del título de este artículo busca señalar, de inmediato, que una materia tan novel y compleja como los *neuroderechos* no puede tomarse a la ligera. Nadie puede desconocer los inmensos retos éticos que presenta la neurotecnología contemporánea, pero la cuestión está en los detalles. Hoy, nos atrevemos a sostener, no se discute si la neurociencia debe ser regulada; se discute el cómo. Muy a pesar del *boom* mediático y político, en esta materia estamos lejos tener un consenso. En tal sentido, la academia ha planteado serios e importantes comentarios que parecen ser desconocidos por gran parte de las iniciativas de neuroderechos, tanto así que los más importantes neuroeticistas y juristas alrededor del mundo han alzado voces críticas para construir mejores regulaciones.

Uno de los más enérgicos y contundentes críticos ha sido Christoph Bublitz, quien, en un reciente artículo, criticó los neuroderechos, particularmente, los propuestos por la Neurorights Foundation. Bublitz (2022) señaló que los neuroderechos no deberían adoptarse y que el *lobby* en su favor debería detenerse. En ese sentido, argumentó que la propuesta tiende a promover la inflación de derechos, carece de fundamentación en la investigación académica relevante y está contaminada por el *neuroexcepcionalismo* y

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

el *neuroesencialismo*. En lugar de crear nuevos derechos humanos, Bublitz (2022) sugiere que los derechos existentes deben desarrollarse aún más en respuesta a los cambios en las circunstancias sociales y las posibilidades tecnológicas.

En ese sentido, en primer lugar, Bublitz (2022) expresa preocupación por la inflación y devaluación de los derechos humanos, argumentando que la propuesta de añadir cinco nuevos "neuroderechos" a las listas internacionales, aunque audaz, potencialmente debilita la naturaleza fundamental y prioritaria de los derechos humanos existentes. En lugar de desestimar los derechos humanos ya reconocidos, y crear nuevos, Bublitz (2022) aboga por un enfoque *parsimonioso*, similar a la Navaja de Occam, en el que los derechos humanos no deben multiplicarse sin necesidad, y la carga argumentativa para crear nuevos, recaería en el proponente; cosa que la NeuroRights Foundation no ha logrado realmente, muy a pesar del entusiasmo mediático y político.

En segundo lugar, Bublitz (2022) plantea una preocupación sobre la distinción entre la academia y el activismo en la propuesta de la iniciativa de Neuroderechos de Yuste y colaboradores. Subraya que las reformas legales deben cumplir con ciertas condiciones, como provenir de las disciplinas relevantes o estar respaldadas por la investigación en campos pertinentes. La propuesta de la NeuroRights Foundation, aunque está situada en el campo de la ciencia y, aparentemente, proviene de personas que trabajan en neurociencia, no se encuentra entre las disciplinas principalmente relevantes para redactar y discutir derechos humanos o constitucionales (Bublitz, 2022). En tal sentido, argumenta Bublitz (2022), la experiencia en el campo de la neurociencia, no debe confundirse con la experiencia en técnica legal, que requiere una necesaria familiaridad con la ley. Además, señala que los derechos propuestos no están fundamentados en la técnica legislativa y critica la falta de trabajo conceptual y discusiones críticas, argumentando que su defensa parece, en gran medida, imposible sin algún fundamento legal real (Bublitz, 2022).

En tercer lugar, Bublitz (2022) destaca que la creación de nuevos derechos no es siempre positiva, ya que impone deberes y puede restringir la toma de decisiones democráticas, además de tener consecuencias complejas que requieren un razonamiento cuidadoso. Además, critica la propuesta de la Iniciativa Neurorights por no cumplir con los estándares de transparencia, trabajo previo de preparación integral y evaluación de consecuencias, así como cuestiona su falta de compromiso con las leyes ya existentes. La propuesta de neuroderechos, para Bublitz (2022), es vista más como una proclamación elevada que un análisis serio de las leyes, y se argumenta que lo que se necesita, realmente, son propuestas de políticas públicas y regulaciones mejor pensadas y consideradas, en lugar de la adopción de los neuroderechos propuestos.

En cuarto lugar, Bublitz (2022) argumenta que la propuesta de los neuroderechos exhibe, más bien, una sobrevaloración del aspecto *neuro*, lo cual se manifiesta en la denominación misma de estos derechos, aunque los problemas que abordan no son exclusivamente causados por el avance de la neurotecnología. Este enfoque corresponde a lo que se ha llamado *síndrome de exageración cerebral* que, según Bublitz (2022), puede estar relacionado con el *neuroesencialismo*, que asume que las explicaciones definitivas de eventos mentales o sociales se encuentran en el nivel cerebral; lo *neuro* es

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

lo esencial. La propuesta de neuroderechos, para Bublitz (2022), también involucra un fenómeno conocido como neuroexcepcionalismo, que es, básicamente, considerar que todo lo *neuro* es excepcional.

Aquí vale la pena preguntarse, por ejemplo, en materia de privacidad de los neurodatos, ¿qué diferencia, realmente, los datos cerebrales, de otro tipo de datos fisiológicos, genéticos, psicológicos, de las decisiones como consumidores, o de la información en general, como para justificar la creación de nuevos derechos humanos? ¿También debemos crear nuevos derechos humanos para otro tipo de tecnologías emergentes? ¿Debemos legislar en favor de nuevas categorías para todas las tecnologías disruptivas que surjan y planteen retos ético-legales?

Retomando el artículo de Bublitz (2022), el autor plantea una preocupación sobre el *neurohype*, donde la propuesta podría estar basada en una evaluación poco realista de las tecnologías, creando una sensación de urgencia que podría limitar el debate y la deliberación. En dicho sentido, la recomendación de Bublitz (2022) es, más bien:

> En lugar de alimentar tales narrativas y reforzar tales tendencias, el asesoramiento académico debería ponerlas en contexto, separando la ciencia de la ficción, diferenciando entre los resultados de la investigación, las hipótesis subyacentes, las implicaciones más amplias de las hipótesis si se verifican y las predicciones sobre trayectorias futuras (p.8).

Finalmente, para Bublitz (2022), los derechos propuestos, como el derecho a la identidad personal, el derecho al libre albedrío, el derecho a la privacidad mental, la protección especial de los neurodatos, el derecho al acceso igualitario a la mejora y el derecho a la protección contra el sesgo algorítmico, se encuentran en gran medida vagos, redundantes o fundamentalmente imprecisos. Algunos, sin duda, parecen repetir derechos existentes, mientras que otros plantean cuestiones que requieren un análisis más detallado y contextualizado. Por lo tanto, para Bublitz (2022), ninguno de los derechos propuestos supera el control de calidad necesario para crear nuevos derechos humanos, y la propuesta en sí misma no parece tomar en serio los derechos humanos, ya que no se ajusta al paisaje normativo existente, y está teñida de profundos vicios.

En conclusión: lo único recomendable es detener el lobby en favor de los neuroderechos, tomarse en serio la discusión y, en su lugar "se debe promover una academia más profunda y sustantiva sobre los muchos desafíos que la neurociencia y otras tecnologías plantean para la ley" (Bublitz, 2022, p.12). Lo que realmente se necesita, siguiendo a Bublitz (2022), son argumentos sobre cuestiones sustantivas como equilibrar los intereses gubernamentales en la aplicación de la ley con la privacidad individual, en lugar de la declaraciones de nuevos, pero vacíos, derechos humanos. Por lo tanto, sugiere que deberíamos enfocarnos en definiciones más precisas de los alcances y fortalezas de los derechos existentes en diferentes contextos, así como en propuestas políticas más detalladas. Además, es menester abogar por un enfoque que atienda a cuestiones legales concretas y desarrollando soluciones a nivel de derecho positivo ordinario, así como analizando cómo los derechos humanos existentes se aplican, buscando formas

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

plausibles de avanzarlos, en lugar de conjurar nuevos derechos en gran medida vacíos (Bublitz, 2022).

En este punto, antes de introducir nuevas críticas de otro autor, permítasenos traer a colación que, a nivel global, la International Neuroethics Society, fundada en 2006 y que desde entonces agrupa a buena parte de los más reputados académicos en neuroética y neuroderecho, marcó un hito en la institucionalización de estas disciplinas académicas, según señala el mismo Marcello Ienca (2021). Tres lustros después, según Ienca (2021), la International Neuroethics Society constituye la mayor sociedad académica comprometida con el estudio de las implicaciones sociales, legales, éticas y políticas de los avances en neurociencia en el mundo.

En dicho sentido, no otro que el mismo Joseph J. Fins, quien, no sobra decir, ostenta la posición como el Presidente de la International Neuroethics Society para el periodo 2021–2023, publicó un artículo a propósito de la reforma constitucional de neuroderechos en Chile, argumentando, en esencia, que la mencionada reforma era vaga y prematura, que requiere mayor deliberación académica, y que, en consecuencia, no debería ser adoptada por ninguna otra jurisdicción (Fins, 2022)

En tal sentido, Fins (2022) evalúa críticamente las normas propuestas para la Constitución chilena en relación con los neuroderechos, enfocándose en los desafíos que la neurociencia plantea para la ley y cómo podrían afectar a individuos con trastornos de la conciencia. Argumenta que la iniciativa de neuroderechos en Chile podría tener consecuencias no deseadas, como detener la investigación que podría aliviar condiciones psiquiátricas y entrar en conflicto con los derechos de las personas con discapacidades. El autor aboga por una visión más amplia de los neuroderechos que esté en armonía con las normas internacionales de derechos humanos y discapacidad, en lugar de adoptar prohibiciones protectoras unilaterales que podrían socavar la capacidad restauradora de las neurotecnologías.

En dicha dirección, Fins (2022) afirma que la legislación de neuroderechos en Chile podría representar un obstáculo para el diagnóstico y tratamiento de trastornos de la conciencia, como el coma y el estado vegetativo. Destaca cómo la preocupación por la libertad cognitiva y la integridad mental en la legislación podría obstaculizar la investigación y la atención clínica en áreas como el pronóstico, el diagnóstico y la terapéutica. En particular, para Fins (2022), la identificación de la conciencia encubierta en pacientes aparentemente no responsivos y la restauración de la comunicación funcional podrían verse afectadas por las disposiciones sobre integridad mental y consentimiento. En dicho sentido, para Fins (2022), la incongruencia entre las preocupaciones teóricas y las capacidades actuales de la neurotecnología, se constituyen en reacciones irreflexivas, exageradas y prematuras por parte de los legisladores chilenos.

Más adelante, Fins (2022) aborda los desafíos éticos y regulatorios del consentimiento en la investigación con sujetos que carecen de capacidad para tomar decisiones, en el contexto de la legislación de neuroderechos en Chile. Por lo que concluye que, muy a pesar de los logros en la aprobación ética y regulatoria para ensayos invasivos en sujetos incapaces de dar su consentimiento, el modelo chileno de neuroderechos podría revertir o ralentizar dicho progreso. Fins (2022) argumenta que el consentimiento informado no

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

debe ser visto como el único medio para promover el respeto por las personas y que la identificación de la conciencia encubierta y la promoción de la comunicación funcional son demostraciones vívidas de dicho respeto. En tal sentido, Fins (2022) afirma que la propuesta de neuroderechos en Chile podría constituir una distracción infortunada, desinformada, vaga y prematura que desvía los esfuerzos de la ciencia y el tratamiento, hacia los tribunales, en lugar de la atención al paciente.

Por lo tanto, para Fins (2022), la fórmula chilena presenta un desequilibrio al promover derechos negativos sobre los positivos, anticipando un advenimiento distópico y apocalíptico de la neurociencia, limitando su progreso beneficioso, sin contar con real evidencia de los riesgos reales que representaría el avance neurotecnológicos. En síntesis, la iniciativa de Chile se enmarca en un momento político complejo y turbulento, con posibles implicancias negativas para los derechos sociales y la atención médica de personas con discapacidades neurológicas graves. A pesar de la esperanza que algunos ven en el proceso constitucional chileno, la actual formulación de neuroderechos es, sin duda, vaga y prematura, y no satisface criterios clave como el equilibrio entre derechos positivos y negativos, la orientación futura informada por la ciencia y la armonización con las normas internacionales de derechos humanos (Fins, 2022).

En dicho sentido, no hay que olvidar que la reforma fue incorporada en la constitución pasada de Chile y que dicho país está adelantando esfuerzos constitucionales, por lo que está por verse si se mantiene la reforma de neuroderechos en el nuevo texto constitucional que potencialmente se apruebe.

En una dirección similar, Ruiz et al. (2021) habían sostenido que la introducción de neuroderechos en Chile, con el objetivo de salvaguardar la privacidad e integridad mental y psíquica contra el uso indebido de las neurotecnologías, suscitaba importantes inquietudes, tales como definiciones ambiguas y complejas, perspectivas reduccionistas de la neurociencia cognitiva, y posibles duplicidades con derechos ya garantizados. Además, Ruiz et al. (2021) destacan que la prohibición del uso de neurotecnologías en individuos que no puedan dar su consentimiento podría tener repercusiones perjudiciales en la investigación en neurociencias y en la práctica clínica, y examina cómo legislaciones previas en Chile, como la Ley N°20.584, han limitado la investigación en enfermedades neuropsiquiátricas.

En tal sentido, Ruiz et al. (2021) sostienen que la Ley de Neuroderechos, actualmente en tramitación, repite un error similar al de la Ley 20.584, promulgada en 2012, que ha sido criticada por excluir a personas vulnerables de estudios sobre sus propias enfermedades y por ser interpretada como discriminatoria e inconstitucional. La nueva ley podría tener consecuencias negativas en la investigación y práctica médica, afectando la aplicación de Interfaces Cerebro-Computadoras (ICC) en pacientes con enfermedades neurológicas severas y potencialmente interfiriendo con terapias y monitoreos neurológicos habituales. En síntesis, para Ruiz et al. (2021), la formulación actual de la ley podría amenazar tanto la investigación científica en neurociencias como tratamientos esenciales, necesitando un análisis y ajuste meticulosos para prevenir un retroceso en la práctica clínica y el avance futuro de la medicina en Chile.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

Por otra parte, Moreu Carbonell (2021), se muestra, en general, de acuerdo con las críticas en contra de la consagración constitucional de los neuroderechos, como ha hecho Chile, argumentando que dicha reforma no está realmente justificada. Moreu Carbonell (2021) reconoce que los derechos humanos están cada vez más vulnerables debido al avance de las neurotecnologías y la inteligencia artificial, pero sostiene que no hay nada en los neuroderechos que permita identificarlos como derechos *nuevos*. En lugar de crear más derechos, Moreu Carbonell (2021) aboga por la adaptación y protección de los derechos humanos existentes contra las nuevas amenazas, señalando que la creación de nuevas reglas para un campo con hallazgos tan incipientes es inapropiada.

En su conclusión, Moreu Carbonell (2021) enfatiza que la propuesta de crear una carta de neuroderechos es sugerente, pero no necesaria en este momento, ya que sería prematuro. Argumenta que la creación de neuroderechos podría desviar recursos que serían mejor utilizados en la mejora de las garantías de los derechos humanos ya existentes. En lugar de esbozar nuevos neuroderechos, aboga por garantizar los derechos existentes contra los riesgos de la neurotecnología, adaptándolos o moldeándolos según sus propias características. La autora también destaca la necesidad de una regulación internacional y la aprobación de códigos éticos y medidas educativas para reflejar las implicancias sociales, médicas y bioéticas de la neurotecnología.

Por parte de López-Silva y Madrid (2021), si bien la modificación constitucional para incluir neuroderechos les parecería técnicamente innecesaria, la presentación de un proyecto de ley sobre el tema resultaría aconsejable. En tal sentido, un proyecto de esta naturaleza, de acuerdo con López-Silva y Madrid (2021) debe ser cauteloso en su técnica legislativa, ya que una consagración legal inadecuada podría conllevar consecuencias jurídicas nefastas si dichas reformas se manifiestan normativamente de un modo frívolo o poco preciso.

En otras líneas, De Asís (2022), luego de resumir de manera completa las principales críticas, citando a numerosos autores, afirma que la crítica más acertada es la falta de un debate académico profundo y amplio sobre el tema. El autor enfatiza la necesidad de llevar a cabo una discusión multidisciplinaria y abierta que permita determinar si los instrumentos de garantía actuales son suficientes o si es necesario establecer un catálogo de neuroderechos con un sistema de garantías eficaz.

Además, en materia del uso de neurotecnologías en los sistemas penales, Fyfe, Lanphier y Peterson (2022) abordan la complejidad de los *neuroderechos* en el contexto penitenciario, enfocándose en tres aspectos principales: la inflación de derechos, la deflación de derechos y los *acertijos* conceptuales. La sección sobre la inflación de derechos cuestiona la incorporación de neuroderechos junto a los derechos humanos tradicionales, sugiriendo que podría llevar a una devaluación de derechos más fundamentales. La deflación de derechos examina las restricciones a la autonomía y la libertad en el contexto carcelario, argumentando que la atención a los neuroderechos podría desviar la vista de problemas más urgentes y reales en el sistema penitenciario.

Finalmente, frente a los problemas conceptuales, plantean preguntas sobre la posibilidad de violar la privacidad y la libertad mental, cuestionando si las neurotecnologías pueden, realmente, transgredir estos derechos. La crítica concluye con una llamada a

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

una mayor claridad y consideración de estos temas complejos en el análisis y aplicación de los neuroderechos (Fyfe, Lanphier y Peterson, 2022). En tal sentido, sostienen que, si bien apoyan la protección de la privacidad y la libertad, tanto en general como en entornos penitenciarios, son escépticos de que la expansión de los llamados neuroderechos logre objetivos de protección y, en cambio, puede inflar los actuales derechos humanos de manera que disminuya la capacidad material y real de hacerlos cumplir (Fyfe, Lanphier y Peterson, 2022).

Para Ligthart et al. (2023), las diferencias sustanciales en la forma en que los académicos entienden los fundamentos filosóficos y éticos de los neuroderechos en todas las disciplinas, vuelve discutible hasta qué punto es deseable y necesario traducirlas y condensarlas en derechos específicos a nivel internacional, así como integrarlas en las normas existentes de los sistemas de derechos humanos. Lo anterior en razón a que estas ideas pueden conceptualizarse de manera diferente en cuanto a sus fundamentos filosóficos y éticos (Ligthart et al. 2023).

En otro ámbito, Cornejo-Plaza y Saracini (2023) si bien no se oponen a la propuesta general de neuroderechos, sí plantean importantes observaciones en materia del derecho a la mejora cognitiva con neurofármacos. En tal sentido, señalan que la implementación del derecho a la mejora cognitiva va más allá de los desafíos regulatorios y requiere un consenso sobre el concepto de *mejora* y un debate profundo sobre quién debería tener acceso a diferentes tipos de mejora cognitiva, ya sea desde una perspectiva terapéutica, recreativa o comercial (Cornejo-Plaza y Saracini, 2023). Mencionan que dicha cuestión es controvertida y plantea preguntas fundamentales sobre el papel del estado en las mejoras no terapéuticas, cómo se define la *normalidad*, y si el estado debería garantizar, subsidiar o financiar estas mejoras, así como cómo manejar los riesgos y consecuencias futuras, como la adicción o enfermedades resultantes del uso de neuroestimulantes (Cornejo-Plaza y Saracini, 2023). Además, afirman que se debe considerar la expansión silenciosa de la mejora cognitiva farmacológica, que está ocurriendo en ausencia de regulación ética y neuroética coherente. Por lo que, en resumen, la mejora cognitiva neurofarmacológica requiere una discusión exhaustiva para enfocarse en su contribución a la sociedad (Cornejo-Plaza y Saracini, 2023).

Además, si bien Herrerá-Ferrá et al. (2022) dicen estar de acuerdo en que se deben proteger universalmente derechos específicos relacionados con el cerebro y la mente, instan a reflexionar sobre la inclusión proactiva de consideraciones e inquietudes transnacionales, transculturales y contextuales para contribuir y enriquecer el discurso global hacia una definición internacional. En tal sentido, Herrerá-Ferrá et al. (2022) señalan que la comprensión polarizada sobre los neuroderechos podría sesgar un verdadero discurso global sobre las preocupaciones emergentes relacionadas con la neurotecnología. En ese sentido, argumentan que se requieren consideraciones adicionales en las definiciones de consenso para algunos neuroderechos propuestos, como la libertad cognitiva, la integridad mental, la identidad personal y la agencia, ya que ciertas culturas podrían no percibir estos conceptos como en amenaza, y mucho menos como un requisito legal universal de protección. A manera de ejemplo, resaltan culturas para

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

las cuales un estado alterado de conciencia a través de la etnofarmacología es fundamental para la identidad cultural.

En otras palabras, el relativismo contextual y cultural llama a considerar una posible comprensión y prioridad no-universal al conocimiento neurocientífico actual, por lo que cualquier marco regulatorio debe ser contextual y culturalmente consciente, responsable, respetuoso e inclusivo de la diversidad cultural neurocognitiva (Herrerá-Ferrá et al. 2022).

Varios de los argumentos críticos también habían sido señalados en una serie de artículos publicados desde el año 2020 por Borbón y colaboradores. Así, en Borbón, Borbón y Laverde (2020), artículo publicado en esta misma revista, se afirma que el prematuro desarrollo de los debates académicos deriva en una necesaria cautela, y el imperativo de ampliar las discusiones en foros académicos, sociales y políticos. De la misma manera, se señala que la propuesta de la NeuroRights Initiative de incorporar neuroderechos al libre albedrío y al acceso equitativo a tecnologías es especialmente problemática en términos conceptuales y prácticos (Borbón, Borbón y Laverde, 2020). Más adelante, en Borbón, Borbón y León (2021) se afirma que un neuroderecho al acceso a tecnologías de mejora cognitiva puede generar desigualdad, pérdida de diversidad y presiones sociales además de problemas fiscales y desafíos en la implementación de este tipo de iniciativas con tintes transhumanistas, adoptando una posición escéptica y crítica ante el aparente entusiasmo, proponiendo no incorporar dicho derecho. Una posición similar respecto a ese neuroderecho apareció recientemente con otros argumentos en Muñoz y Borbón (2023).

Posteriormente, en Borbón y Borbón (2021) se sostiene una crítica a todos los cinco neuroderechos propuestos por la NeuroRights Foundation, señalando los inconvenientes conceptuales del libre albedrío, que también pueden encontrarse en Muñoz (2019), y los problemas prácticos y éticos relacionados con la mejora, la privacidad, la identidad y el sesgo, se destacan las posibles antinomias que puedan surgir, así como se argumenta que son jurídicamente innecesarios. Más adelante, en Díaz-Soto y Borbón (2022) se señala que, en materia penal, los neuroderechos no serían idóneos para limitar aplicaciones tecnológicas en materia de neuropredicción y detección de mentiras, pues los mismos autores que proponen los neuroderechos, han dicho que estos se pueden relativizar para que las tecnologías sean empleadas coercitivamente, sin consentimiento en casos graves, en nombre de la seguridad pública.

IV. Recepción internacional y regional de los neuroderechos

A pesar de los numerosos comentarios valiosos de la academia, ya varias naciones y organizaciones internacionales de todo el mundo han comenzado a legislar en favor de los neuroderechos, algunos sin tener muy en cuenta los comentarios y críticas. En cambio, otros ejemplos, como el caso de Argentina, sí parecen tomar en cuenta estas observaciones, como veremos en el penúltimo apartado de este artículo.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

Así, en la vanguardia de la promoción de los neuroderechos se encuentra Chile, que ha demostrado su interés con las nuevas iniciativas legislativas. En ese sentido, Chile hizo un esfuerzo importante con la inclusión de una breve protección de la integridad mental, los datos cerebrales y la actividad cerebral, como se ve en la reciente reforma del artículo 19 de su Constitución:

> El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella (Biblioteca del Congreso Nacional de Chile, 2021, s.p.).

Además de la reforma constitucional, el Senado de Chile (2021) ha estado avanzando con un proyecto de ley de neuroprotección que incluía, en su redacción original, alguna aproximación a los cinco derechos propuestos por la NeuroRights Foundation, proyecto que ha tenido varios cambios y su avance ha sido relativamente lento.

Por otra parte, Brasil avanza con un proyecto de ley (PL 522/2022) para definir los datos neuronales y establecer reglas para su protección. En tal sentido, el Proyecto de Ley 522/22 busca regular la información obtenida directa o indirectamente de la actividad del sistema nervioso central mediante interfaces cerebro-computadora u otras tecnologías, invasivas o no invasivas (Câmara dos Deputados, 2022). Así las cosas, el proyecto incorpora medidas a la Ley General de Protección de Datos Personales (LGPD) estableciendo que el tratamiento de datos neurales solo se realizará con el consentimiento expreso del titular, y establece la prohibición del uso compartido de datos neurales con fines de lucro. Por otra parte, se prohíben métodos que puedan causar daños a la identidad, autonomía o integridad psicológica de la persona y se establecen medidas para asegurar el acceso equitativo a los avances en neurotecnología (Câmara dos Deputados, 2022).

Por su parte, Argentina está promoviendo el proyecto de ley 0339-D-2022, que agregaría salvaguardias y requeriría consentimiento previo y una orden judicial antes de utilizar la neurotecnología en procesos penales pues la reforma al artículo 134 del Código Procesal Penal Federal de la Nación establecería que estas tecnologías "Sólo podrán ser empleados por orden judicial y con el consentimiento explícito de la persona, que previamente deberá ser informada sobre sus finalidades y alcances (Diputados Argentina, 2022, p.1).

En Europa, España tiene una nueva Carta de Derechos Digitales, no vinculante legalmente, pero con un enfoque de soft law sobre los neuroderechos, incorporando los cinco propuestos por la Neurorights Initiative (Gobierno de España, 2021). Adicionalmente, Francia incorporó la nueva Ley 2021-1017 relacionada con la bioética estableciendo que:

> Los actos, procesos, técnicas, métodos y equipos que tengan por efecto modificar la actividad cerebral y presenten un peligro grave o una sospecha de peligro grave para la salud humana pueden ser prohibidos por decreto, previa consulta a la Alta Autoridad Sanitaria. Cualquier decisión de levantar la prohibición se toma de la misma forma. (Gobierno de Francia, 2021, s.p.).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

Mucho más recientemente, en México, una Diputada Federal propuso un proyecto para añadir un párrafo al artículo 4 de la Constitución Federal que establece que:

> Toda persona tiene derecho a la identidad individual plena e integral, así como a la integridad física y psíquica como condiciones de su libertad. El estado garantizará el respeto a la privacidad y la integridad mental de las personas. Ninguna autoridad o particular podrá, mediante el uso de cualquier mecanismo tecnológico, modificar, reducir o afectar dicha integridad e identidad (Prensa Diputados Morena, 2023, s.p.)

Por otro lado, las organizaciones internacionales también reconocen la importancia de los neuroderechos. Por ejemplo, las Naciones Unidas produjo un informe sobre cuestiones éticas de la neurotecnología, adoptado por la (UNESCO, 2021), y promulgaron la reciente resolución A/HRC/RES/51/3 del Consejo de Derechos Humanos, aprobada el 6 de octubre de 2022 (Consejo de Derechos Humanos, 2022), en la que se encarga un estudio sobre las repercusiones de la neurotecnología en los derechos humanos. A nivel regional, la Organización de los Estados Americanos emitió en 2021 una declaración sobre los neuroderechos que contiene una serie de recomendaciones (Comité Jurídico Interamericano, 2021), seguida de una declaración de Principios Interamericanos sobre Neurociencias y Derechos Humanos aprobada en 2023 (Comité Jurídico Interamericano, 2023). En este sentido, la Ley Modelo del Parlatino constituye uno de los más recientes avances en esta materia.

V. ¿Hacia la uniformidad en América Latina y el Caribe?

El Parlamento Latinoamericano y Caribeño, conocido como Parlatino, es un organismo regional compuesto por los Congresos, Parlamentos o Asambleas Legislativas nacionales de los Estados Parte de los países de América Latina y el Caribe que firmaron el Tratado de Institucionalización en 1987 en Lima, Perú (Parlatino, sf.). El Parlatino se rige por principios como la defensa de la democracia, la integración latinoamericana, la no intervención y la autodeterminación de los pueblos. Sus propósitos incluyen promover el desarrollo integral de la comunidad latinoamericana, defender la libertad y la justicia social, velar por los derechos humanos fundamentales y luchar contra el colonialismo y la discriminación (Parlatino, s.f.). El Parlatino es un organismo compuesto por la Asamblea, la Junta Directiva, las Comisiones Permanentes y la Secretaría General, y cuenta con la participación de los países miembros de América Latina y el Caribe, incluyendo Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, República Dominicana, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay, Venezuela, Aruba y Curazao.

Una de las funciones que más ejecuta el Parlatino es la de promulgar leyes modelo, que a la fecha suma más de 110 documentos, y que busca fomentar un proceso de integración y armonización legislativa en Latinoamérica. Para cumplir con esta función, el Parlatino cuenta con dos documentos relevantes, siendo, el primero de estos, los Lineamientos Metodológicos para la realización de Estudios de armonización Legislativa, revisado en el año 2003, y el Procedimiento para la Elaboración, Discusión y Aprobación de Leyes Modelo. aprobado en las reuniones de Junta Directiva y Asamblea, en noviembre de 2017.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

Sobre el primer documento, el esquema metodológico de armonización legislativa se basa en cinco actividades principales: el estudio de legislación comparada, la definición de principios y fundamentos clave, propuestas de armonización relativa, propuestas de armonización absoluta y la elaboración de códigos y otros cuerpos jurídicos de carácter marco (Parlatino, 2003). Dicho documento resalta la importancia de la unificación de las leyes y códigos jurídicos en ciertas materias donde exista una gran coincidencia en los principios generales y cuyo objetivo final del proceso es la creación de una legislación común para todos los países latinoamericanos como una parte esencial de un esquema comunitario de integración subregional o regional (Parlatino, 2003).

Frente al segundo documento, el Parlatino (2017) detalla el procedimiento para la elaboración, discusión y aprobación de proyectos de leyes modelo. En ese sentido, las Comisiones Permanentes del Parlatino son los organismos especializados encargados de analizar y desarrollar estos proyectos. En dicho documento, el Parlatino (2017) destaca que la iniciativa para estas leyes puede surgir en cualquier Comisión Permanente del Parlatino y luego son discutidas, modificadas si es necesario y aprobadas dentro de estas mismas. Posteriormente, la Junta Directiva, se avoca el proyecto de Ley Modelo, y podrá rechazarlo; devolverlo o aprobarlo para que sea estudiado por la Asamblea, que podrá aprobarlo con la mayoría de los votos presentes. Una vez aprobado el proyecto de Ley Modelo, será girado a los Parlamentos Miembros para su conocimiento y tratamiento que estimen corresponder. Sobre los requisitos de las leyes modelo, éstas deben tener un título que represente su objeto, un preámbulo explicativo, un ordenamiento sistemático, y un lenguaje normativo claro.

Con esto considerado, el pasado mes de junio de 2023, fue aprobada la Ley Modelo de Neuroderechos, bajo un documento que, según reza el último folio, proviene de una redacción de noviembre de 2022. La mencionada Ley modelo contiene un preámbulo, un clausulado de 13 artículos y un *Anexo Marco Teórico Conceptual General*.

En cuanto al articulado, la Ley Modelo de Neuroderechos del Parlatino (2023) establece que el objeto del documento es crear las condiciones para que los países miembros cuenten con las bases para legislar y reglamentar esta materia (Art. 1). Consagra que la Ley deja un amplio margen para que se puedan incorporar avances siempre y cuando se respeten las "bases filosóficas y conceptuales que se encuentran en el Anexo, el cual forma parte inseparable de la ley" (Art.2, p.4), y establece el ámbito de aplicación al territorio nacional del país correspondiente (Art.3).

Adicionalmente, como disposiciones generales, establece que el objetivo de la Ley es posibilidad el compromiso por la promoción de los neuroderechos dentro del criterio de la neuroética (Art.4), establece que los neuroderechos se basan en principios éticos de validez universal, entre ellos la "neuroética", que debe incluir y preservar los siguientes derechos fundamentales sin perjuicio de incluir otros:

a) Derecho a la privacidad mental (los datos cerebrales de las personas)
b) Derecho a la identidad y autonomía personal
c) Derecho al libre albedrío y a la autodeterminación
d) Derecho al acceso equitativo a la aumentación cognitiva o al desarrollo cognitivo.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

e) Derecho a la protección de sesgos de algoritmos o procesos automatizados de toma de decisiones.
f) El derecho inalienable a no ser objeto de cualquier forma de intervención de las conexiones neuronales o cualquier forma de intrusión a nivel cerebral mediante el uso de neurotecnología, interfaz cerebro computadora o cualquier otro sistema o dispositivo, sin contar con el consentimiento libre, expreso e informado, de la persona o usuario del dispositivo, inclusive en circunstancias médicas. Aun cuando la neurotecnología posea la capacidad de intervenir en ausencia de la conciencia misma de la persona.
g) En general, el derecho a no ser sujeto involuntario o no informado, de cualquier proceso o actividad que pueda de alguna manera interferir en los procesos cognitivos del individuo. Esto incluye otras prácticas no necesariamente relacionadas directamente con las neurotecnología, como la hipnosis y la sugestión (Parlatino, 2023, p.5).

Más adelante, el artículo 6 y 7 crea una "Autoridad Competente" que deberá ser definida por cada país y que deberá cumplir una lista de 17 funciones. Hacia el final del documento del Parlatino (2023), el artículo 8 establece la aplicación universal para todos los habitantes; el artículo 9 crea una nueva acción de protección rápida y expedita, cuando no exista otro medio judicial más idóneo, para que se actúe de manera inmediata ante una potencial lesión a los neuroderechos; el artículo 10 establece el reconocimiento de amplios derechos a la reparación por parte del Estado Nacional; el artículo 11 establece que cada país deberá ajustar la Ley Modelo a su ordenamiento; el artículo 12 consagra el procedimiento administrativo para sancionar a infractores; y el artículo 13 establece que la vigencia de la ley en caso de adoptarse.

Por otra parte, el Anexo Marco Teórico Conceptual General, establece notas importantes sobre la ciencia, tecnología e innovación, consagra los antecedentes conceptuales y su justificación, empezando por el concepto de neuroderechos, las vulnerabilidades neuropsicológicas del humano y los avances en neurotecnologías que representan amenazas. Adicionalmente, establece la ética global en la base de la ley, los principios básicos y derechos esenciales y consagra un glosario sobre definiciones de la aumentación cognitiva, la cognición, el dato neuronal, la distorsión cognitiva, la gobernanza de la inteligencia artificial, la hipnosis y la sugestión, la neurocriminología, la neuroética, el neuromarketing, la neurotecnología, la reserva cerebral y cognitiva, el sesgo y otro tipo de conceptos (Parlatino, 2023).

VI. El preocupante clausulado de la Ley Modelo del Parlatino

En el presente apartado señalaremos, de manera sumaria, las observaciones críticas puntuales a la Ley Modelo de Neuroderechos del Parlatino. En primer lugar, el documento de Ley Modelo aprobado por el Parlatino contiene un preámbulo, que, según el

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

artículo 5 del "Procedimiento para la Elaboración, Discusión y Aprobación de Proyectos de Leyes Modelo", del Parlatino (2017):

> Previo al desarrollo del texto normativo, se redactará un preámbulo el cual contendrá una explicación sucinta del contenido de la norma, las razones que han llevado a su elaboración y la finalidad tenida en cuenta para su tratamiento por parte del Parlatino (p.4).

De esa manera, el documento empieza a señalar que la palabra *neuroderechos* es fungible, intercambiable o equivalente a *los derechos del cerebro*, cosa que, valga la pena desde ya advertir, implica incurrir en la conocida falacia mereológica, muy común en el campo "neuro", que "consistente en atribuir a las partes propiedades que sólo son atribuibles al todo" (Sánchez de las Matas Martín, 2016, p.13). En esencia, el error conceptual aquí señalado, es pretender afirmar que los *neuroderechos* son derechos atribuibles al *cerebro*, cuando lo son, realmente, a la persona como un todo.

En dicho sentido, sugieren que *neuroderechos* es un concepto que se puede entender en dos aspectos: la privacidad mental y el derecho a la identidad. Es propio indicar que tal afirmación es, cuanto menos, imprecisa como definición conceptual. Los neuroderechos van mucho más allá y no pueden entenderse en esos dos aspectos seleccionados sin mayor razón. Quizás por eso, luego, acuden a enumerar los cinco neuroderechos de la NeuroRights Foundation.

Más adelante, señalan que actualmente, millones de personas se someten inconscientemente a la entrega de contenido a los algoritmos que decodifican la mente humana. En el texto esta afirmación usa como ejemplo los sistemas de recomendación que se alimentan de las preferencias del usuario para entregar el contenido adecuado; utilizando un lenguaje fatalista muy alejado de la gravedad que los sistemas de recomendación implican. En general el lenguaje utilizado en esta ley modelo tiende a hablar mucho más sobre las catastróficas consecuencias del avance tecnológico sin argumentar qué del avance actual podría resultar tan problemático.

No sin antes ser nuestro deber advertir que, en Borbón, Borbón y Laverde (2020), se sintetizan varios de los más problemáticos usos y desarrollos, a nivel experimental, de la neurotecnología, sí debemos señalar que esta forma de expresión resuena con palabras de Joseph Fins (2022) quien señala que, en general, estas iniciativas malinterpretan el futuro neurotecnológico al promover una postura de precaución sobre los neuroderechos que podría reducir el progreso, anticipando un resultado distópico de los desarrollos en neurociencia sin tener reales bases para sustentarlo.

Más adelante, señalan que la ciencia, la tecnología y la innovación, incluyendo especialmente la neurotecnología, "son el sustrato cada vez más determinante de las actividades humanas, y esto no es una cuestión del futuro sino del presente" (Parlatino, 2023, p.3). Al respecto, también valdría la pena cuestionarse sobre los alcances reales de la neurotecnología a niveles comerciales actuales, considerando que la mayoría de las personas si acaso entran en contacto una vez a lo largo de su vida con la neurotecnología para escáneres cerebrales, por ejemplo, con fines de diagnóstico clínico.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

El hecho de que el contacto presente con la neurotecnología sea tan reducido, sería otra variable al considerar la rapidez con la cual se pretende legislar, especialmente, si se pretende regular de manera apresurada e imprecisa, como sostenemos que lo han hecho las actuales iniciativas. En su lugar, los Estados deberían tomarse en serio las discusiones y plantear, con la debida cautela, mejores regulaciones. En tal sentido, no es cierto que la neurotecnología sea un sustrato determinante en la vida actual de los humanos, contrario, por ejemplo, a los celulares o a las aplicaciones digitales, que muchos países no han regulado aún.

Por tal razón, luego de citar una conferencia realizada en el Parlatino, concluyen que dichas razones hicieron que en el Parlatino (2023) se considere "un imperativo impostergable producir una ley modelo sobre la materia" (p.3). Además, precisan que dicha ley está redactada de manera amplia, sin ser específica, remitiendo al anexo conceptual, para que los países la adapten a sus contextos, cosa que se reitera en el artículo 2 de la Ley Modelo. La vaguedad de la ley modelo plantea una preocupación sustancial puesto a que justifica la amplitud normativa con el pretexto de simplificar su aplicabilidad y promover su adopción, pero no podemos pasar por alto que esta vaguedad también podría resultar en ambigüedad y falta de claridad en su implementación.

En dicho sentido, la redacción amplia es justificada en el artículo 2 de la Ley Modelo argumentando que se hace "de tal manera que se puedan incorporar permanentemente los avances que se produzcan" (Parlatino, 2023, p.4). No sobra decir que parece por lo menos problemático proponer una ley que tendrá que ser reformada "permanentemente" por lo amplia que es.

Más adelante, en el artículo 4, sobre el objetivo, afirman que pretenden posibilitar la implementación progresiva de los neuroderechos, con una visión sociocultural. Valga la pena resaltar las observaciones de Herrera-Ferrá et al. (2022) y de Borbón, Borbón y León (2021) sobre las diferencias culturales, incluso dentro del mismo territorio nacional, que harían que varios conceptos de neuroderechos sean problemáticos de cara a las diferencias culturales. Adicionalmente, se señala que esto se realiza "dentro del criterio fundamental de la neuroética". En tal sentido, no estamos convencidos de que la neuroética sea más un *criterio fundamental* que una disciplina interdisciplinaria con múltiples visiones y perspectivas que varían por cada autor y región.

Esto lo vuelven a reafirmar en el artículo 5 donde señalan que la ley de neuroderechos está basada en los principios éticos de validez universal, entre ellos la neuroética. Al respecto, valga la pena reiterar, en primer lugar, que los conceptos empleados por las iniciativas de neuroderechos están lejos de tener validez o aceptación universal; véase, tan sólo, la discusión sobre lo ético o no de las mejoras cognitivas sin fines terapéuticos (Borbón, Borbón y León; Herrera-Ferrá et al. 2022; Muñoz y Borbón, 2023). En segundo lugar, es necesario reiterar que no estamos convencidos en que sea adecuado entender que la *neuroética* sea un *principio universal* más que una disciplina.

Posteriormente, dentro del mismo artículo 5, establecen la siguiente lista de neuroderechos:

a) Derecho a la privacidad mental (los datos cerebrales de las personas)
b) Derecho a la identidad y autonomía personal

c) Derecho al libre albedrío y a la autodeterminación
d) Derecho al acceso equitativo a la aumentación cognitiva o al desarrollo cognitivo.
e) Derecho a la protección de sesgos de algoritmos o procesos automatizados de toma de decisiones
f) El derecho inalienable a no ser objeto de cualquier forma de intervención de las conexiones neuronales o cualquier forma de intrusión a nivel cerebral mediante el uso de neurotecnología, interfaz cerebro computadora o cualquier otro sistema o dispositivo, sin contar con el consentimiento libre, expreso e informado, de la persona o usuario del dispositivo, inclusive en circunstancias médicas. Aun cuando la neurotecnología posea la capacidad de intervenir en ausencia de la conciencia misma de la persona.
g) En general, el derecho a no ser sujeto involuntario o no informado, de cualquier proceso o actividad que pueda de alguna manera interferir en los procesos cognitivos del individuo. Esto incluye otras prácticas no necesariamente relacionadas directamente con las neurotecnología, como la hipnosis y la sugestión (Parlatino, 2023, p.5).

Al respecto, vale la pena recordar las críticas que se han hecho en contra de cada uno de los cinco neuroderechos propuestos por la Neurorights Foundation. En primer lugar, el derecho a la privacidad mental pretende asegurar que todos los datos provenientes de actividad neuronal se deben mantener privados NeuroRights Initiative (2021). Si bien la intención de proteger al usuario es pertinente, limitar el acceso a datos podría dificultar el desarrollo de algoritmos menos sesgados y limitar el avance e innovación en materia de las neurotecnologías, ya que el valor de estos dispositivos proviene de la capacidad para crear modelos sólidos al comparar grandes cantidades de datos (Borbón y Borbón, 2021).

En segundo lugar, el derecho a la identidad personal aborda la importancia de establecer límites para evitar que la tecnología altere la identidad personal a través de intervenciones en el cerebro. Anteriormente en Borbón y Borbón (2021), se resaltó la alta probabilidad de que una intervención en el cerebro pueda causar alteraciones en la mente y potencialmente amenazar la identidad personal; de tal modo que prohibir las tecnologías que alteren estos rasgos personales podría implicar prohibir las neurotecnologías en general. También es importante resaltar el gran desafío que implica establecer los límites en la definición de la identidad personal y su alteración.

Al respecto del neuroderecho al libre albedrío, esta etiqueta posee amplios problemas conceptuales y filosóficos (Muñoz, 2019), cuando la misma neurociencia y filosofía incompatibilista parece negar que algo llamado "libre albedrío" realmente exista (Borbón y Borbón, 2021). De la misma manera, parecería importante precisar por qué la *autonomía personal* se incluye con el derecho a la identidad, y no con el libre albedrío, y cómo dichos conceptos se diferencian de la *autodeterminación*. En lugar de desarrollar adecuadamente categorías con validez legal, introducen problemas de la filosofía de la mente, de la ciencia y del lenguaje que vuelven problemática la interpretación de la norma.

Por otra parte, en el literal d) proponen un "derecho al acceso equitativo a la aumentación cognitiva o al desarrollo cognitivo" (Parlatino, 2023, p.5). Al respecto, como fue resaltado en Borbón y Borbón (2021), la creación de un nuevo derecho que promueva

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

el acceso a tecnologías de mejora sin fines terapéuticos es problemática, ya que podría llevar a aplicaciones transhumanistas que deben tratarse con cautela. La alteración de la naturaleza humana podría afectar significativamente la libertad de quienes no desean mejorar, creando nuevas normas sociales, laborales y académicas que presionen a quienes no puedan soportar ser tratados como inferiores (Borbón y Borbón, 2021). Además, un derecho positivo a la mejora podría implicar una nueva carga financiera para el Estado y ser considerado obsoleto en países en desarrollo, donde no se puede garantizar ni siquiera los derechos fundamentales más básicos: ¿acaso el Estado ahora tendrá que asumir la financiación y subsidios equitativos para tecnologías recreativas de mejora sin fines de salud pública?

El literal e) enuncia el derecho a la protección de sesgos de algoritmos o procesos automatizados de toma de decisiones. No todos los sesgos algorítmicos son malos, algunos podrían incluso ayudar a que un sistema esté más acorde con los estándares sociales, éticos y legales de un país. Además, si bien se resalta la necesidad de incluir bases de datos más representativas de grupos vulnerables o minoritarios, reunir un conjunto de datos imparcial no siempre es posible o sostenible; principalmente porque suelen estar protegidos por temas de privacidad o incluso derechos de autor (Borbón y Borbón, 2021). Adicional al derecho a la protección contra sesgos de algoritmos, el literal e) incluye el derecho a la protección contra procesos automatizados de toma de decisiones, sin aclarar el alcance de la norma.

Posteriormente, en el literal f), más que un derecho, se presenta un párrafo sobre no ser objeto de intervenciones cerebrales sin consentimiento libre, inclusive en circunstancias médicas, "aún cuando la neurotecnología posea la capacidad de intervenir en ausencia de la conciencia misma de la persona" (Parlatino, 2023, p.5) Al respecto permítasenos traer a colación, nuevamente, las críticas de Fins (2022) y de Ruiz et al. (2021) respecto del consentimiento en estados de incapacidad e inconsciencia, pues, al parecer, la propuesta de la Ley Modelo detendría cualquier tipo de intervención médica beneficiosa para pacientes que no pueden expresar, por su estado de incapacidad, su consentimiento *expreso*.

En tal sentido, la forma en la cual se ha consagrado la exigencia del consentimiento en la Ley modelo merece las siguientes apreciaciones. El consentimiento informado, entendido como "el derecho a ser informado y en el derecho a decidir sobre la ejecución del acto médico" (Porfírio De Sá Lima, 2017, p. 474), surge como derecho y como principio de la bioética en el ámbito de la investigación médica en la Declaración de Helsinki, que se ha ido consagrando en normas internas de cada ordenamiento, también en instrumentos y normas internacionales, teniendo un abordaje suficiente como derecho e incluso su consagración expresa en el artículo 7 del Pacto Internacional de Derechos Civiles y Políticos en el sentido de que nadie será sometido sin su consentimiento a experimentos médicos o científicos.

Los cambios en materia de la relación médico-paciente y el avance desde el modelo paternalista al modelo personalista en el que se ha ido reconociendo la libertad y autonomía del paciente (Posteraro, 2019), han implicado la necesidad de ampliar la noción e incluso reconsiderar la naturaleza jurídica del consentimiento informado, de modo

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

tal que debe entenderse como derecho de los pacientes y a su vez como obligación de los galenos. Sin embargo, al menos en materia clínica, el consentimiento como derecho de los pacientes que materializa el principio de autonomía ya cuenta con normas que brindan precisión en el ámbito clínico; precisión que no se evidencia en la Ley modelo del Parlatino.

En tal dirección, cuando el literal f del artículo 5 de la Ley modelo, se indica que "Aun cuando la neurotecnología posea la capacidad de intervenir en ausencia de la conciencia misma de la persona" (Parlatino, 2023, p.5), ¿cómo es posible acaso solicitar el consentimiento informado de la persona que necesita de un tratamiento médico ante ausencia de su consciencia?

En la especialidad médica de neurología suelen emplearse tecnologías que implican intervenciones que resultan indispensables para el tratamiento clínico del paciente. En muchos de los casos, los pacientes en estado de inconsciencia requieren diagnóstico y tratamiento por neurología ¿resultaría lógico que aun en ausencia de consciencia se solicite el consentimiento del paciente al que se requiere realizar algún examen diagnóstico? Es claro que se deben consultar las preferencias del paciente, y cuando tenga alterada su capacidad o consciencia, debe hacerse por medio de su representante. También es claro que, si el paciente recupera su estado de consciencia, el médico debe obtener el consentimiento informado antes de realizar otras intervenciones, pero ante la imposibilidad de conocer las preferencias del paciente, incluso en casos de emergencia donde tampoco sea posible obtener el consentimiento, el médico deberá tomar las decisiones teniendo en cuenta el interés superior del paciente y con base en sus representantes o familiares.

Ante estos casos y obedeciendo a los principios bioéticos de beneficencia y no maleficencia, parece evidente que el médico podría realizar los exámenes o intervenciones necesarias aplicando las neurotecnologías necesarias, aun sin el consentimiento del paciente. Reconocer la importancia de la autonomía materializada en el consentimiento informado no puede implicar otorgarle de suyo un valor superior al de otros principios de la bioética, los cuales también resultan de la estricta observancia en todo acto médico y requerirán un análisis para cada caso en concreto. Por tales razones, es evidente la inconveniencia del mencionado literal f) del artículo 5.

Finalmente, la lista de neuroderechos del artículo 5 cierra con el literal g) que establece, nuevamente, una versión alternativa del consentimiento y el derecho a ser informado, pero incurre, de manera errática, a establecer una *protección* frente a otras formas de *manipulación* por fuera del área neurotecnológica. En tal sentido, mencionan, como ejemplo, una protección frente a la "hipnosis y la sugestión" (Parlatino, 2023, p. 5). Además de ser reiterativo el mencionado literal, parece profundamente extraño que la Ley Modelo propuesta pretenda abordar, adicionalmente, los temas de hipnosis o de sugestión. Al respecto, preferimos reservar los comentarios, tan solo señalando que no parece haber mayor conexidad temática.

Más adelante, el artículo 6 y 7 detalla las misiones y funciones de una nueva *Autoridad Competente* en relación con los neuroderechos. En dicho sentido, establecen que será la encargada de incluir la vinculación de los planteamientos de la ley con los preceptos

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

constitucionales relacionados con la educación, cultura, derechos ciudadanos, ciencia, tecnología e innovación. Además, se deben incluir en los planes nacionales, sectoriales y subnacionales, planificar y conducir políticas públicas y programas, establecer medidas, ejecutar programas de capacitación, expedir regulaciones, juzgar infracciones, coordinar acciones, promover la enseñanza y práctica de los principios y derechos, realizar actividades de promoción del conocimiento de los neuroderechos, informar sobre nuevas tecnologías, propender por la reformulación de derechos, incentivar la protección, definir tratamientos con técnicas de imagen cerebral, capacitar a los servicios penitenciarios, estimular el desarrollo de la inteligencia artificial, vincularse con redes y plataformas internacionales, crear espacios para el crecimiento y desarrollo personal en campos relacionados, y establecer modalidades de asesoramiento científico tecnológico a las diferentes áreas de gobierno (Parlatino, 2023).

Respecto de la propuesta de crear dicha poderosa y novel autoridad parece, por lo menos, cuestionable la creación de una entidad específica para los temas relacionados con la neurociencia, creando una amplísima lista de más de 17 funciones disímiles desde la educación, la regulación, la sanción, el juzgamiento de infracciones, la promoción de información, la definición de tratamientos, entre muchas otras cosas. En tal sentido, los Estados miembros del Parlatino deberán ponderar si la creación de esta entidad omnicomprensiva tiene sentido dentro de sus ordenamientos internos, o si algunas de dichas funciones deberán, mejor, redistribuirse entre entidades ya existentes.

Por su parte, el artículo 8, establece que el Estado nacional declara que los neuroderechos son de ejercicio obligatorio. Vale la pena cuestionarse, por ejemplo, si es apropiado declarar que un derecho al aumento cognitivo con tecnologías de mejora sin fines terapéuticos es algo que merece ser de ejercicio obligatorio, o preguntarse por el acceso a neurotecnologías para menores de edad.

Posteriormente, en el artículo 9, se crea una Acción de Protección y Garantía, para reconocer una acción de protección legal expedita, siempre que no exista otro medio más idóneo, para proteger contra todo "acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, en forma antijurídica su indemnidad y privacidad cerebro mental" (Parlatino, 2023, p.8). Al respecto, nos parece una propuesta sensata que podría, en la práctica material, ser positiva, aunque en algunas legislaciones ya existen mecanismos similares, como la acción de tutela, amparo o de protección, podría ser una buena señal para otros Estados que aún no contemplen estos mecanismos. Al respecto, se debe recordar la obligación convencional del artículo 2 de la Convención Americana sobre Derechos Humanos de ajustar los ordenamientos para consagrar recursos judiciales efectivos para la protección de derechos humanos, como lo exige el artículo 25 de la CADH.

Por su parte, el artículo 10, sobre la reparación, consagra que el "Estado Nacional reconocerá amplios derechos para la reparación integral de los daños causados por la aplicación no consentida o mal informada de neurotecnologías" (Parlatino, 2023, p.8). Podría ser relevante precisar que dichos alcances a la reparación integral no deberían provenir, exclusivamente, del Estado, sino que conllevan la importante corresponsabilidad de las empresas neurotecnológicas, bajo los Principios Rectores de las Naciones

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

Unidas sobre Empresas y Derechos Humanos. Esto en atención a que también son las empresas las que están llamadas, especialmente, a conservar estándares de debida diligencia y a reparar daños a los derechos humanos.

Por otra parte, el artículo 11 establece que cada país conserva la autonomía para adecuar la Ley a su ordenamiento y el artículo 12 establece una muy extraña reglamentación de *Procedimiento administrativo para la instrucción del sumario* y la aplicación de las *sanciones*. Dicho artículo, por lo menos en criterio de los suscritos, es complejo de interpretar y adecuar normativamente. Con todo, el artículo 13 finaliza estableciendo la entrada en vigor.

VII. El también preocupante Anexo Marco Teórico Conceptual General

Si las anteriores observaciones no fueron lo suficientemente ilustrativas de las problemáticas de la Ley Modelo de Neuroderechos del Parlatino, el Anexo *Marco Teórico Conceptual General*, adjunto al articulado, puede ser igual o aún más problemático.

La importancia del mencionado Anexo surge de su fuerza vinculante consagrado en el artículo 2 de la Ley Modelo, estableciendo que el amplio margen de acción está restringido a "las bases filosóficas y conceptuales que se encuentran en el Anexo, el cual forma parte inseparable de la ley" (Parlatino, 2023, p.4). Así, una de las primeras afirmaciones del anexo es que:

> Las definiciones que constan en esta ley modelo son tomadas de fuentes fidedignas; sin embargo no se trata de definiciones universales y concluyentes, porque se inscriben en el ámbito de las humanidades y de las ciencias sociales, no de las ciencias exactas. Pero para la cabal comprensión de esta ley modelo, siempre deben tomarse como referente necesario las definiciones que constan en el presente documento (Parlatino, 2023, p.11).

Sin embargo, de las más de noventa citas a pie de página que se pueden extraer del documento Anexo, la inmensa mayoría de ellas son fuentes de internet, entre los que cuentan, notas de prensa, entrevistas en medios, enciclopedias en línea, incluyendo, además, Wikipedia, grabaciones del Senado de Chile, conferencias del Profesor Rafael Yuste, blogs en línea y videos de YouTube. Además, en algún apartado, se citan fuentes de internet y se incluye la expresión "otras varias" (Parlatino, 2023, p.4).

De las pocas fuentes bibliográficas que podrían tener algún contenido académico, la mayoría son libros de divulgación de hace varias décadas, y otras rozan con la literatura de ciencia ficción. Por otra parte, de los escasos artículos de investigación consultados para formular el Anexo, en general, se tratan de textos que no revelan el estado del arte y se encuentran desactualizados.

Por supuesto, al tratarse de un documento de contenido político, no sería leal exigirles a los redactores un estándar científico que revelase una verdadera revisión sistemática del estado del arte. Lo que pretendemos señalar, por lo menos, es que lo aquí mencionado nos permite advertir, de entrada, que el *Anexo Marco Teórico Conceptual*

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

General, lejos de ser un documento con bases filosóficas y conceptuales, académicamente sustentadas, es un texto de recopilación y divulgación de fuentes sin carácter académico ni investigativo.

Por las anteriores razones, rogaríamos que, si algún Estado incorpora normas provenientes de la Ley Modelo del Parlatino, puedan ajustarlas al escrutinio de la academia, y que el Anexo técnico, a pesar de lo manifestado en el artículo 2, no sea tomado en cuenta como una fuente válida de conocimiento técnico, ni se emplee para la interpretación de las normas, ni se le otorgue credibilidad irreflexiva a las fuentes que componen dicho Anexo.

En dicho sentido, el Anexo contiene afirmaciones, argumentos, y conceptos que, incluso, reconocen que carecen de definiciones precisas o inequívocas, por lo que, además, se podría cuestionar hasta qué punto las múltiples definiciones extendidas en el documento son adecuadas o se podrían extraer de principios universalmente válidos. Lo anterior considerando que existen profundas discusiones filosóficas, que desde la academia se han promovido de tiempo atrás, frente a los conceptos empleados textualmente para convertirse en normas de derecho positivo.

De la misma manera, gran parte del contenido se encuentra transcrito textualmente de las fuentes de internet consultadas, por lo que, si el documento es sometido al escrutinio de un Software de detección de plagio, el resultado de coincidencias es elevado, precisando que, por regla general los redactores sí identifican las fuentes de consulta[1].

VIII. Reflexiones finales sobre la Ley Modelo del Parlatino

Por las anteriores razones, podemos señalar, como primera conclusión, que las definiciones y la conceptualización de los "neuroderechos", incurren en imprecisiones y errores potenciales. La ley modelo, además, parecería estar impregnada de un fatalismo tecnológico, pero manteniendo una preocupante vaguedad y amplitud, así como la suposición de validez universal de ciertos conceptos. En tal sentido, la necesidad de una revisión cuidadosa para asegurar precisión conceptual, sensibilidad cultural y aplicabilidad práctica es relevante, y se debe subrayar la importancia de abordar los complejos temas en juego con cautela.

Por otra parte, con la enumeración y descripción de los neuroderechos en la Ley Modelo se plantean una serie de cuestiones complejas y problemáticas que requieren de mayor análisis y reflexión. Desde la privacidad mental hasta la protección contra *la hipnosis y la sugestión*, la ley presenta desafíos conceptuales, éticos y prácticos. La pro-

1. En particular, sometimos los 18 folios del Anexo "Marco Teórico Conceptual General", sin incluir las referencias, al análisis del Software "Turnitin", encontrando un puntaje elevado de coincidencias. En ocasiones, no se citan las fuentes, se citan fuentes equivocadas, o no se cita con base en un sistema de referenciación adecuado. En concreto, el porcentaje de coincidencias alcanzó un 69%, excluyendo, por supuesto, la Web de las páginas del Parlatino para que no identificase el documento con un 100% de coincidencia. El porcentaje de coincidencias, permítasenos señalar nuevamente, no implica, per se, un hallazgo de plagio.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

puesta de una Autoridad Competente y la declaración de obligatoriedad de los neuroderechos también son complejas.

Además, del análisis del Anexo *Marco Teórico Conceptual General* se pueden revelar serias deficiencias y problemáticas en su validez y utilidad como guía conceptual para la ley modelo. Desde la fuerza vinculante hasta las definiciones imprecisas, el Anexo es criticable por su falta de solidez académica, rigor y precisión. La dependencia de fuentes no académicas y desactualizadas, junto con la falta de rigor en su elaboración, lo convierte en un documento cuestionable. En tal sentido, recomendamos que cualquier Estado que incorpore normas de la Ley Modelo ajuste estas al escrutinio de la academia y no tome el Anexo como una fuente válida de conocimiento técnico.

En conjunto, estas conclusiones ofrecen una evaluación crítica y comprensiva de la Ley Modelo de Neuroderechos del Parlatino, subrayando la necesidad de una revisión y reconsideración cuidadosas para asegurar que la ley sea conceptualmente sólida, éticamente responsable y prácticamente aplicable en el complejo y dinámico campo de la neuroética y el neuroderecho. En tal sentido, la ambigüedad terminológica, la fundamentación técnica insuficiente, la inadecuada consideración del consentimiento informado, los problemas en el acceso a tecnologías de mejora, la ausencia de claros lineamientos de responsabilidad legal, así como la carencia de consideraciones académicamente sustentadas, convierten a estos documentos en problemáticos puntos de partida.

IX. La falacia del falso dilema de los neuroderechos

Considerando lo problemático que han sido estas propuestas, bien uno podría pensar que la alternativa a no incorporar las iniciativas de neuroderechos sería un futuro distópico y apocalíptico, basado en una postura fatalista de la tecnología. Sin embargo, en este punto particular, consideramos que estamos ante un falso dilema. Contrario a lo que se suele plantear, la regulación de la neurotecnología no está limitada a las propuestas de crear nuevas categorías de derechos fundamentales, como si dicha regulación, o la ausencia de tal, fuesen las únicas opciones posibles.

En cambio, como se ha propuesto desde Borbón, Borbón y Laverde (2020), como lo han argumentado López-Silva y Madrid (2021), Moreu Carbonell (2021), y Bublitz (2022), en lugar de propuestas generales, con contenidos ambiguos, que reformen constituciones y creen nuevos derechos abstractos, podría ser muchísimo más provechoso y efectivo crear legislaciones concretas y precisas que regulen problemas inminentes, basados en la evidencia.

En tal sentido, nos parece que la experiencia de Argentina, y la propuesta de reforma del Código Procesal Penal Federal de la Nación, es diciente de las reales reformas que podrían necesitarse. Al respecto, como se mencionó con anterioridad, en Argentina, en lugar de crear nuevos derechos constitucionales, ambiguos y conceptualmente complejos, el proyecto de ley 0339-D-2022, contempla salvaguardias y exige el consentimiento previo, así como una orden judicial, antes de utilizar la neurotecnología en procesos penales. Véase la redacción propuesta:

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

> ARTÍCULO 1°.- Modifíquese el artículo 134 del Código Procesal Penal Federal de la Nación y sus modificatorias, el que quedará redactado de la siguiente manera:
> […]
> Entre estos medios se incluyen las técnicas de imagen cerebral y cualquier otro tipo de neurotecnologías que, a partir de los datos relativos a la estructura y/o función cerebrales, permitan de algún modo inferir la actividad mental, en todos sus aspectos. Sólo podrán ser empleados por orden judicial y con el consentimiento explícito de la persona, que previamente deberá ser informada sobre sus finalidades y alcances.
> ARTÍCULO 2°.- Modifíquese el artículo 1° de la Ley 24.660 y sus modificatorias, el que quedará redactado de la siguiente manera:
> […]
> Los tratamientos que incluyen técnicas de imagen cerebral y cualquier otro tipo de neurotecnologías que, a partir de los datos relativos a la estructura y/o función cerebrales, permitan de algún modo inferir la actividad mental, en todos sus aspectos, sólo podrán ser empleados por orden judicial y con el consentimiento explícito de la persona, que previamente deberá ser informada sobre sus finalidades y alcances (Diputados Argentina, 2022, p.1-2).

En tal sentido, Argentina, en lugar de crear una regulación ambigua, abstracta y poco precisa, plantea una reforma concreta, aplicada de manera precisa en temas procesal-penales y penitenciarios, de modo que se protejan los sustratos de los derechos constitucionales de libertades de la persona y su consentimiento informado. Con dicha reforma, entonces, el mencionado país estaría, verdaderamente, protegiendo a sus ciudadanos de los usos coercitivos de la neurotecnología en materia penal.

En un sentido similar, por ejemplo, en Díaz-Soto y Borbón (2023), se señaló que los neuroderechos no eran propuestas idóneas para proteger a las personas de los usos coercitivos de neurotecnologías en materia de neuropredicción, detección de mentiras o de intervención con fines de *mejora moral*. En tal dirección, como principios de rango constitucional, los neuroderechos serían relativos, a tal punto que en el artículo seminal de Ienca y Andorno (2017), se reconoce que estos se podrían relativizar en nombre de la seguridad pública en ciertos casos específicos. Por el contrario, creemos que la propuesta de reforma legal es suficientemente fuerte para no ser ponderada y relativizada. Por lo tanto, acogemos la propuesta de Argentina como un ejemplo claro de una debida regulación.

Lo cierto es que estas iniciativas no requirieron crear una nueva categoría de derechos fundamentales, sino que, por el contrario, precisaron alcances para problemas concretos. Por lo anterior, consideramos que supone un falso dilema sostener que, sin crear nuevos "neuroderechos" no sería posible regular la neurociencia humana. Propuestas legislativas, con base en los actuales derechos fundamentales, parecen ser las más idóneas para enfrentar los retos del futuro neurotecnológico. De la misma manera, las actuales listas de derechos humanos deben interpretarse de manera que puedan proteger a las personas de los retos neurotecnológicos y también podría resultar una idea adecuada crear convenios internacionales que aborden, de manera precisa y exhaustiva, las regulaciones con perspectiva global.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

X. Conclusiones

En este artículo hemos realizado una aproximación crítica a las iniciativas de neuroderechos y, en particular, a la Ley Modelo de Neuroderechos del Parlatino. Reconocemos que, aunque supone un paso significativo en el reconocimiento de los desafíos planteados por el avance de la neurotecnología, la propuesta adolece de serias deficiencias en su fundamentación teórica, conceptual y científica. La imprecisión en la definición de neuroderechos y la posible ambigüedad en su implementación, junto con una preocupante falta de rigor académico en el Anexo *Marco Teórico Conceptual General*, subrayan la necesidad de una revisión cuidadosa y considerada. En tal sentido, la rapidez con la que se pretende legislar en un campo complejo y dinámico puede resultar en aplicaciones problemáticas e inconvenientes.

Por lo tanto, las observaciones críticas a la Ley Modelo no se limitan a cuestiones teóricas y conceptuales; también se extiende a aspectos prácticos y éticos que se inscriben en un debate más amplio y global sobre la necesidad y conveniencia de los neuroderechos. La oposición académica, la falta de consenso y la complejidad en torno a los neuroderechos, reflejada en las críticas y preocupaciones planteadas, subrayan la necesidad de un enfoque cauteloso y reflexivo. La adaptación y protección de los derechos existentes, en lugar de la creación prematura de nuevos derechos abstractos y ambiguos, parecen ser caminos más idóneos para enfrentar los retos del futuro neurotecnológico. De la misma manera, es sugerible la creación de convenios internacionales que aborden, de manera precisa y exhaustiva, las regulaciones con perspectiva global.

En última instancia, este artículo hace un llamado al debate académico, científico y político, sin incurrir en proposiciones normativas apresuradas e inadecuadas. La recomendación es no incorporar la Ley Modelo propuesta en su forma actual, y en lugar de crear normas ambiguas y abstractas, legislar materias concretas con base en los riesgos reales, actuales e inminentes de la neurotecnología. En tal sentido, ejemplos como la propuesta de reforma legal en materia penal en Argentina demuestran que es posible desarrollar legislaciones concretas y precisas que protejan a los ciudadanos sin caer en la complejidad conceptual de las listas de *neuroderechos*.

La necesidad de una revisión y reconsideración cuidadosa, para asegurar que las propuestas que se planteen sean conceptualmente sólidas, éticamente responsables, legalmente consistentes y prácticamente aplicables en el complejo campo de la neuroética y el neuroderecho, es imperativa. Hasta entonces, los comentarios críticos que desde la academia se han planteado, son una necesaria crítica que disputa el papel de los neuroderechos en el entorno político global.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

Bibliografía

Biblioteca del Congreso Nacional de Chile. (2021). Decreto 100 fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=242302&idVersion=2021-10-25

BORBÓN RODRÍGUEZ, D. A., & BORBÓN RODRÍGUEZ, L. F., (2021) A Critical Perspective on Neuro-Rights: Comments Regarding Ethics and Law. *Frontiers in Human Neuroscience*. 15:703121. https://doi.org/10.3389/fnhum.2021.703121

BORBÓN RODRÍGUEZ, D. A., BORBÓN RODRÍGUEZ, L. F., & LAVERDE PINZÓN, J. (2020). Análisis crítico de los NeuroDerechos Humanos al libre albedrío y al acceso equitativo a tecnologías de mejora. *IUS ET SCIENTIA*, *6*(2), 135–161. https://doi.org/10.12795/IETSCIENTIA.2020.i02.10

BORBÓN RODRÍGUEZ, D. A., BORBÓN RODRÍGUEZ, L. F., & León Bustamante, M. A. (2021). Neuro-Right to equal access to mental augmentation: analysis from posthumanism, law and bioethics. *Revista Iberoamericana de Bioética*, (16), 6. https://doi.org/10.14422/rib.i16.y2021.006

BUBLITZ, J.C. (2022). Novel Neurorights: From Nonsense to Substance. *Neuroethics* (15), 7. https://doi.org/10.1007/s12152-022-09481-3

CÁCERES NIETO, E., y LÓPEZ OLVERA, C. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. Cuestiones constitucionales, (46), 65-92. Epub 03 de marzo de 2022.https://doi.org/10.22201/iij.24484881e.2022.46.17048

Câmara dos Deputados de Brasil. (2022). Proyecto de Ley PL 522/2022 Modifica la Ley N° 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos Personales), a fin de conceptualizar los datos neuronales y regular su protección. Disponible en: https://www.camara.leg.br/propostas-legislativas/2317524

Comité Jurídico Interamericano. (2021). Declaración del Comité Jurídico Interamericano sobre Neurociencias, Neurotecnologías y Derechos Humanos: Nuevos Desafíos Jurídicos para las Américas. IAJC/DEC. 01 (XCIX-O/21). Organización de los Estados Americanos. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-DEC_01_XCIX-O-21.pdf

Comité Jurídico Interamericano. (2023). Declaración Interamericana de Principios sobre Neurociencias, Neurotecnologías y Derechos Humanos CJI/RES. 281 (CII-O/23) corr.1. Disponible en: https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf

Consejo de Derechos Humanos. (2022). Resolución A/HRC/RES/51/3 Neurotecnología y derechos humanos. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/525/04/PDF/G2252504.pdf?OpenElement

CORNEJO-PLAZA, M. I., & Saracini, C. (2023). On pharmacological neuroenhancement as part of the new neurorights' pioneering legislation in Chile: a perspective. *Frontiers in psychology*, 14, 1177720. https://doi.org/10.3389/fpsyg.2023.1177720

DE ASÍS, R. (2022). Sobre la propuesta de los neuroderechos. *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, (47), 51-70. https://doi.org/10.20318/dyl.2022.6873

DÍAZ SOTO, J. M., & BORBÓN, D. (2022). Neurorights vs. neuroprediction and lie detection: The imperative limits to criminal law. Frontiers in Psychology, 13, 1030439. https://doi.org/10.3389/fpsyg.2022.1030439

Diputados Argentina. (2022). Ley 24660 -. Modificaciones sobre la inclusión de técnicas de imagen cerebral y cualquier otro tipo de neurotecnología como prueba. Expediente 0339-D-2022. Disponible en: https://www.hcdn.gob.ar/proyectos/proyecto.jsp?exp=0339-D-2022

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

FINS, J. J. (2022). The Unintended Consequences of Chile's Neurorights Constitutional Reform: Moving beyond Negative Rights to Capabilities. Neuroethics, 15(26), 1-3. https://doi.org/10.1007/s12152-022-09504-z

FYFE, S., LANPHIER, E., & PETERSON, A. (2022). Neurorights for Incarcerated Persons: Should We Curb Inflation? *AJOB Neuroscience*, 13(3), 165-168. https://doi-org.basesbiblioteca.uexternado.edu.co/10.1080/21507740.2022.2082585

Gobierno de España. (2021). Carta de Derechos Digitales. Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Gobierno de Francia. (2021). LEY n° 2021-1017 de 2 de agosto de 2021 relativa a la bioética. Disponible en: https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000043884401

HERRERA-FERRÁ, K., Muñoz, J. M., NICOLINI, H., SARUWATARI ZAVALA, G., & MARTÍNEZ BULLÉ GOYRI, V. M. (2022). Contextual and Cultural Perspectives on Neurorights: Reflections Toward an International Consensus. *AJOB Neuroscience*. https://doi.org/10.1080/21507740.2022.2048722

IENCA, M. (2021). On Neurorights. Front. Hum. Neurosci. 15:701258. doi: 10.3389/fnhum.2021.701258

IENCA, M., & ANDORNO, R. (2017). Towards new human rights in the age of neuroscience and neurotechnology. *Life sciences, society and policy,* 13(1), 5. https://doi.org/10.1186/s40504-017-0050-1

LEVY, N. (2008). Introducing Neuroethics. Neuroethics, 1, 1–8. https://doi.org/10.1007/s12152-008-9007-7

LIGTHART, S., IENCA, M., MEYNEN, G., MOLNAR-GABOR, F., ANDORNO, R., BUBLITZ, C.,... KELLMEYER, P. (2023). Minding Rights: Mapping Ethical and Legal Foundations of 'Neurorights'. *Cambridge Quarterly of Healthcare Ethics,* 1-21. https://doi.org/10.1017/S0963180123000245

LÓPEZ-SILVA, P., & Madrid, R. (2021). Sobre la conveniencia de incluir los neuroderechos en la Constitución o en la ley. *Revista Chilena De Derecho Y Tecnología*, *10*(1), 53–76. https://doi.org/10.5354/0719-2584.2021.56317

MEYNEN G. (2019). Forensic psychiatry and neurolaw: Description, developments, and debates. *International journal of law and psychiatry*, *65*, 101345. https://doi.org/10.1016/j.ijlp.2018.04.005

MOREU CARBONELL, E. (2021). The Regulation of Neuro-Rights. *European Review of Digital Administration & Law - Erdal*, 2(2), 149-162. doi:9791259947529

MUÑOZ J. M. (2019). Chile - right to free will needs definition. *Nature*, *574*(7780), 634. https://doi.org/10.1038/d41586-019-03295-9

MUÑOZ, J. M., & Borbón, D. (2023). Equal access to mental augmentation: Should it be a fundamental right? *Brain Stimulation, 16*(4), 1094-1096. https://doi.org/10.1016/j.brs.2023.05.003

NeuroRights Foundation. (s.f.). The Neurorights Foundation. Human Rights for the Age of Neurotechnology. Disponible en: https://neurorightsfoundation.org/

NeuroRights Initiative (2021). The Five Ethical NeuroRights. Disponible en: https://neurorights-initiative.site.drupaldisttest.cc.columbia.edu/sites/default/files/content/The%20Five%20Ethical%20NeuroRights%20updated%20pdf_0.pdf

PARLATINO. (2003). Lineamientos Metodológicos Para la Realización de Estudios de Armonización Legislativa. São Paulo, Brasil: PARLATINO.

PARLATINO. (2017). Procedimiento para la elaboración, discusión y aprobación de proyectos de leyes modelo. Parlatino.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

PARLATINO. (2023). Ley Modelo de Neuroderechos para América Latina y El Caribe. Disponible en: https://parlatino.org/wp-content/uploads/2017/09/leym-neuroderechos-7-3-2023.pdf

PARLATINO. (s.f.) Historia y Objetivos. Disponible en: https://parlatino.org/historia-y-objetivos/

PETOFT A. (2015). Neurolaw: A brief introduction. Iranian journal of neurology, 14(1), 53–58.

PORFÍRIO DE SÁ LIMA, ÉFREN PAULO. (2017). Naturaleza jurídica del consentimiento informado a la luz de los modelos español y brasileño de protección al paciente. Revista de Derecho Privado, (32), 473-489. https://doi.org/10.18601/01234366.n32.16

POSTERARO, N. (2019). El problema del consentimiento informado de los derechos del enfermo a la despersonalización de la relación médico-paciente. *Medicina Y Ética*, *30*(1), 67–92. Recuperado a partir de https://revistas.anahuac.mx/index.php/bioetica/article/view/438

Prensa Diputados Morena. (2023). Plantea María Eugenia Hernández Garantizar Entornos Seguros Ante Transformación Digital. Recuperado de: https://diputadosmorena.org.mx/blog/2023/08/12/plantea-maria-eugenia-hernandez-garantizar-entornos-seguros-ante-transformacion-digital/

RUIZ, SERGIO, RAMOS-VERGARA, PAULINA, CONCHA, RODRIGO, ALTERMATT, FERNANDO, VON-BERNHARDI, RoMMY, CUELLO, MAURICIO, GODOY, JAIME, VALERA, LUCA, ARAYA, PABLO, CONDE, EDGARDO, TORO, PABLO, & CANEO, CONSTANZA. (2021). Negative effects of the patients' rights law and neuro-rights bill in Chile. *Revista médica de Chile*, 149(3), 439-446. https://dx.doi.org/10.4067/s0034-98872021000300439

SÁNCHEZ DE LAS MATAS MARTÍN, M. DEL C. (2016). Confusión Mereológica y Praxis Psiquiátrica: Aspectos de la Insuficiencia Teórica y Empírica. *InterSedes*, 17(35). http://dx.doi.org/10.15517/isucr.v17i35.25564

SENADO DE CHILE. (2021). Boletín N° 578/SEC/21. Ley de Neuroprotección. 2021. Disponible en: https://www.senado.cl/appsenado/index.php?mo=tramitacion&ac=getDocto&iddocto=14385&tipodoc=mensaje_mocion

TAYLOR, J. S., HARP, J. A., & ELLIOTT, T. (1991). Neuropsychologists and neurolawyers. *Neuropsychology*, 5(4), 293–305. doi:10.1037/0894-4105.5.4.293

UNESCO. (2021). Reporte sobre Cuestiones Éticas de la Neurotecnología. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000383559

YUSTE, R., GOERING, S., ARCAS, B., et al. (2017). Four ethical priorities for neurotechnologies and AI. *Nature*, 551, 159-163. https://doi.org/10.1038/551159a

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 228-260
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

Derecho y ciencia: entre la dignidad humana y la inteligencia artificial

LAW AND SCIENCE: BETWEEN HUMAN DIGNITY AND ARTIFICIAL INTELLIGENCE

Jorge Antonio Breceda Pérez
Universidad Autónoma de Ciudad Juárez
jorge.breceda@uacj.mx 0000-0001-5280-6936
Clara Castillo Lara
Universidad Autónoma Metropolitana
ccl@azc.uam.mx 0000-0003-3031-2091

Recibido: 14 de junio de 2023 | Aceptado: 04 de diciembre de 2023

RESUMEN

La inteligencia artificial (IA) impacta todos los ámbitos y resalta su enorme potencial para transformar la vida diaria en este siglo XXI. No obstante, a medida que se integra cada vez más en nuestras vidas, resulta crucial reflexionar sobre su influencia en la dignidad humana. Este ensayo aborda precisamente la IA y la dignidad humana, examinando los desafíos y riesgos que plantea, así como las múltiples posibilidades y oportunidades en la vida. Aparte de explorar la ética y su regulación en la gobernanza de la IA, los cambios sociales y económicos que puede forjar. El objetivo principal aquí es el debate crítico sobre el uso de la ciencia, en el derecho para garantizar la dignidad humana.

PALABRAS CLAVE

Inteligencia artificial
Siglo XXI
Derecho
Dignidad
Ética

ABSTRACT

Artificial intelligence (AI) impacts all areas and highlights its enormous potential to transform daily life into this 21st century. However, as it becomes increasingly integrated into our lives, it is crucial to reflect on its influence on human dignity. This test addresses precisely AI and human dignity, examining the challenges and risks it poses, as well as the many opportunities and opportunities in life. Apart from exploring ethics and regulation in AI governance, the social and economic changes it can bring about. The main objective here is the critical debate on the use of science, in law, to guarantee human dignity.

KEYWORDS

Artificial intelligence
21st century
Law
Dignity
Ethics

I. Introducción

En el panorama contemporáneo, la interacción entre la Inteligencia Artificial (IA) y la dignidad humana ha cobrado una relevancia sin precedentes. La IA, definida como la habilidad de máquinas y sistemas informáticos para ejecutar tareas tradicionalmente reservadas a la inteligencia humana, abarca competencias como el aprendizaje automático, el procesamiento del lenguaje natural y la toma de decisiones avanzadas. Con el avance acelerado de la IA y su creciente integración en múltiples facetas de la vida cotidiana, emergen interrogantes fundamentales sobre su impacto en la dignidad humana, un pilar central en los campos de la ética y los derechos humanos que subraya el valor intrínseco y la merecida consideración de todos los individuos.

Este trabajo explora el desafío clave de cómo garantizar que los sistemas de IA honren y respeten la dignidad humana. A medida que la IA se desarrolla, enfrentamos riesgos significativos como la falta de transparencia, la ausencia de responsabilidad en las decisiones automatizadas, la discriminación y el sesgo en los sistemas, así como la protección de datos personales. Sin una gestión adecuada, estos factores pueden menoscabar gravemente la dignidad humana.

Sin embargo, la IA también ofrece un vasto espectro de posibilidades para enriquecer y mejorar aspectos cruciales de la existencia humana, tales como la calidad de vida, la asistencia sanitaria, la eficiencia en el trabajo, la productividad y la accesibilidad en términos de movilidad. Para capitalizar estas oportunidades de manera efectiva, es imprescindible la adopción de principios éticos sólidos en el desarrollo y uso de la IA, así como la implementación de políticas y regulaciones gubernamentales que garanticen su aplicación responsable y provechosa para la sociedad.

Por consiguiente, la interacción entre la dignidad humana y la Inteligencia Artificial (IA) se presenta como una relación extraordinariamente compleja y de múltiples dimensiones, exigiendo un análisis detallado y considerado. Esta dinámica intrincada demanda un enfoque que no solo sea reflexivo, sino también profundamente crítico y basado en un entendimiento comprensivo de ambas entidades. En este contexto, el presente artículo tiene como objetivo primordial promover un uso de la IA que sea no solo responsable y ético, sino también conscientemente alineado con los principios fundamentales de respeto y valor hacia la dignidad humana.

Este cometido implica un balance cuidadoso entre aprovechar los beneficios potenciales de la IA, como su capacidad para mejorar la calidad de vida, optimizar procesos y facilitar soluciones innovadoras a problemas complejos, y al mismo tiempo, reconocer y mitigar los riesgos que podría acarrear. Estos riesgos incluyen, pero no se limitan a, la invasión de la privacidad, el aumento de la desigualdad, la erosión de la autonomía humana y la perpetuación de sesgos y discriminaciones preexistentes.

El objetivo es avanzar hacia un futuro donde la tecnología y la humanidad no solo coexistan, sino que también se complementen y enriquezcan mutuamente, en un marco de respeto mutuo y entendimiento. Esto implica un esfuerzo colaborativo para integrar la tecnología de IA en la sociedad de una manera que honre y refuerce la dignidad intrínseca

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

de cada individuo, sin sacrificar los valores humanos esenciales en el altar de la innovación y el progreso tecnológico.

Es por esta razón que el presente artículo busca ser un catalizador para un diálogo más amplio y profundo sobre cómo la tecnología de IA puede ser diseñada, regulada y utilizada de manera que sustente y fomente un respeto genuino por la dignidad humana, asegurando así un futuro donde la tecnología sirva al bienestar y al enriquecimiento de toda la humanidad.

II. Contexto y justificación

La era de la Inteligencia Artificial (IA) ha marcado un punto de inflexión significativo en múltiples sectores, incluyendo la atención médica, la logística y el transporte. Esta revolucionaria tecnología no solo ha mejorado la eficiencia y precisión en numerosas tareas laborales, sino que también ha abierto un panorama de posibilidades para empresas y organizaciones en la búsqueda de soluciones innovadoras a los desafíos contemporáneos. La capacidad de la IA para procesar grandes volúmenes de datos y aprender de ellos ha permitido avances sustanciales en áreas como el diagnóstico médico precoz, la optimización de rutas de transporte y la automatización de procesos complejos.

Sin embargo, paralelamente a estos avances, el desarrollo acelerado de la IA ha desencadenado una serie de preocupaciones éticas y morales, particularmente en relación con su impacto en la dignidad humana. Un aspecto crítico de esta preocupación se centra en la programación de la IA para tomar decisiones en sectores tan sensibles como el laboral, médico o de seguridad. La posibilidad de que estas decisiones automatizadas, si no son rigurosamente supervisadas y reguladas, podrían resultar en la violación de derechos humanos, es un tema de debate creciente.

Además, la creciente capacidad de la IA para recopilar, almacenar y analizar información personal plantea serios interrogantes sobre la privacidad y seguridad de los datos. Existe el riesgo real de que estos datos se utilicen de manera indebida o para propósitos discriminatorios, lo que podría tener consecuencias adversas no solo para los individuos afectados, sino también para la sociedad en general. En este contexto, se vuelve imperativo reflexionar sobre cómo garantizar que la IA esté al servicio de la dignidad humana, evitando que su uso indebido o no regulado resulte en consecuencias negativas.

Esta discusión entre la dignidad humana y la IA es crucial para asegurar que los avances tecnológicos se utilicen de manera que beneficien y enriquezcan la sociedad. Es esencial establecer un marco ético y legal que guíe el desarrollo y la implementación de la IA, de manera que se respeten los valores humanos fundamentales y se promueva un progreso tecnológico que sea inclusivo, justo y respetuoso con los derechos de todos los individuos. La tarea de integrar la IA en nuestra sociedad de una manera que fomente la dignidad humana y el bienestar colectivo representa uno de los desafíos más significativos y urgentes de nuestra época.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

2.1. Marco jurídico internacional, regional y nacional sobre la inteligencia artificial

Actualmente, nos encontramos en un escenario donde aún no se ha establecido un marco jurídico internacional específico y exhaustivo para la regulación de la Inteligencia Artificial (IA). A pesar de esta ausencia de un estándar global unificado, diversos países y regiones han empezado a desarrollar y aplicar sus propios marcos legales y éticos para abordar los desafíos y oportunidades que presenta esta tecnología emergente. Estas iniciativas varían en alcance y naturaleza, reflejando las diferentes prioridades y contextos de cada región. Incluyen desde regulaciones sobre privacidad y uso de datos hasta directrices éticas que buscan orientar el desarrollo responsable de la IA. Estos esfuerzos representan pasos importantes hacia la creación de un entorno normativo que pueda guiar de manera efectiva la evolución y aplicación de la IA, asegurando que su impacto en la sociedad sea positivo y alineado con los principios de justicia, equidad y respeto por los derechos humanos.

La Primera Revolución Industrial (entre 1760 y 1830) marcó la transición de la producción manual a la mecanizada, la Segunda– cerca de 1850– introdujo la electricidad y la manufactura en masa, la Tercera, a mediados del siglo XX, conocida como Revolución Digital, por el uso de tecnologías de información que automatizó más la producción, y la Cuarta Revolución Industrial, definida por la integración de tecnologías de procesamiento de datos. Recurriendo a Internet, a los sistemas ciber físicos y a las redes virtuales, enlazando lo físico a lo digital, utilizando el *Internet of things* (IOT) como medio de comunicación (*Big Data*) (González-Páramo, 2018, 96).

Al respecto, el Comité Económico y Social Europeo, argumentó que el mercado digital, producción, consumo, empleo y la sociedad, entre otros ámbitos más referentes a la tecnología digital, física y biológica, se utilizará el Internet de las Cosas como el terreno de aplicación de IA, cuya base es el principio del control de los seres humanos sobre dichos objetos (Porcelli, 2020, 60).

En el ámbito internacional la Declaración Universal de los Derechos Humanos de la ONU (1948) reconoce los derechos inalienables a las personas. El Convenio Europeo de Derechos Humanos (1950), establece la protección de los datos personales. El Pacto Internacional de Derechos Civiles y Políticos (1966) y el Pacto Internacional de Derechos Económicos, Sociales y Culturales (1966), reconocen el derecho a la vida, trabajo y educación (Valdez, 2018, 37).

La Directiva de la Unión Europea UE sobre Protección de Datos Personales (GDPR, por sus siglas en inglés) en vigor desde 2018, establece protección de los datos personales en la Unión Europea (De Juan, 2018, 40). La Organización para la Cooperación y el Desarrollo Económicos (OCDE) se compone de 38 estados con la coordinación de sus políticas económicas y sociales, creado en París en 1961. AI Principles (Principios de la OCDE sobre IA) establece un marco ético para el uso de la IA, al igual que algunos países han adoptado legislaciones específicas al respecto, como la Ley de Inteligencia Artificial de la República Popular China, en vigor desde 2021 (Gerencia de Promoción y Difusión (INDECOPI), 2018).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

En Latinoamérica, el marco jurídico de la IA varía de país en país y aún está en proceso de desarrollo en la mayoría de ellos. Algunos países han comenzado a regular su uso mientras que otros están en las primeras etapas de discusión sobre el tema (Vélez et al., 2022, 15). Países como México, Brasil, Colombia, Chile, y Argentina ya comenzaron a desarrollar políticas públicas y marcos regulatorios relativas a IA. Por ejemplo, en México, se ha creado el Instituto Nacional de Inteligencia artificial (INIA) para fomentar el desarrollo y su uso responsable. La iniciativa también busca establecer la Red Nacional de Estadística de Uso y Monitoreo de la Inteligencia Artificial y la Robótica. También se plantea regular la inteligencia artificial con una ley de ética. Mientras que en Brasil se crea una ley de IA para garantizar la ética y transparencia en el uso de la tecnología (Crovi, 2017, 30).

La UNESCO aborda la ética en la IA (UNESCO, 2019). El informe reconoce el desarrollo social con los riesgos y desafíos éticos de su uso. Propone un marco ético para su diseño, desarrollo y uso basado en cuatro principios éticos: la autonomía, justicia, beneficencia y no maleficencia. Así como también, la necesidad de desarrollar capacidades éticas y de alfabetización digital en todas las etapas de la educación, esto es, desde la educación básica hasta la superior. Contribuyen al debate sobre la ética en la IA que proporciona un marco ético sólido y una guía práctica para el diseño, desarrollo y uso responsable de esta tecnología en beneficio de la sociedad.

Colombia, creo la Comisión de Inteligencia Artificial, Ética y Transformación Digital, encargada de promover el uso responsable de la IA en el país, (Ministerio de tecnología de la información y las comunicaciones) mientras que en Chile se ha creado una iniciativa público-privada llamada "AIChile" para desarrollar y aplicarla de manera ética y responsable. En Argentina, se ha creado la Agencia Nacional de Inteligencia Artificial (ANIA) para impulsar la investigación en ese campo (EMOL, 2022). En general, aunque todavía falta mucho por hacer en términos de marco jurídico en Latinoamérica, los países están empezando a reconocer la importancia de regular la IA para garantizar su uso responsable y ético.

En México, actualmente no existe una regulación en la materia. Sin embargo, existen algunas leyes y normas que abordan la protección de datos personales, tecnologías de la información, y responsabilidad civil y penal por daños causados por su uso (Senado de la República, 2023). También se cuenta con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que establece las obligaciones de los responsables del tratamiento de datos personales y los derechos de los titulares. El Código Penal Federal, tipifica delitos relacionados con el acceso, uso y divulgación no autorizados de datos informáticos, así como la producción y distribución de programas maliciosos o virus informáticos.

Asimismo, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) publicó lineamientos, sobre el uso de tecnologías y su protección. Actualmente se encuentra en proceso la discusión de una iniciativa de ley en IA en México, la cual, ha de establecer un marco legal para regular su uso y desarrollo (El Economista, 2023).

Luciano Floridi (Floridi, 2019, 100) presenta una teoría de la filosofía como diseño conceptual. Argumenta que la información es clave en la comprensión de la realidad.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

Pues, la información es una propiedad fundamental del universo, y también es un medio para construir modelos para comprender el mundo. Establece las bases teóricas sobre la información y la filosofía, luego aplica esta teoría a la ética, la política, la epistemología y la ontología. Posteriormente, discute algunas de las implicaciones de su teoría, como la relación entre la información y la realidad, y la naturaleza de la inteligencia artificial y la tecnología. Propone una nueva forma de pensar sobre la filosofía y la ciencia, centrada en la información y el diseño conceptual. Ofrece una visión de la información, desde la filosofía, la ciencia y la tecnología.

Entre las teorías que respaldan el uso de la IA en el mundo se encuentra el Utilitarismo que sostiene que el uso de la inteligencia artificial debe basarse en su capacidad para maximizar la felicidad y minimizar el sufrimiento humano. En este sentido, se argumenta que puede ser utilizada para resolver problemas en la sociedad. Lo mismo que la Ética de las virtudes, centrada en la formación del carácter, y sostiene que su uso ha de ser en base a valores éticos y morales que fomenten el desarrollo humano y la virtud.

La Deontología se enfoca en el deber y la responsabilidad, sostiene que la IA ha de basarse en principios éticos universales y los derechos humanos. La Ética del cuidado se centra esencialmente en las relaciones interpersonales y el cuidado de los demás, sustenta que su uso debe fundamentarse en la empatía y la consideración a los demás. Estas teorías tienen diferentes interpretaciones y enfoques, según el contexto y los valores y principios éticos de cada sociedad (Rouyet, 2021).

El uso de la IA puede llegar a violentar la privacidad, al utilizar datos personales. Lo mismo que el derecho a la no discriminación, puesto que estos sistemas pueden tener sesgos discriminatorios incorporados (Naciones Unidas, 2021). La seguridad, puede ser vulnerable a ciberataques. Estos sistemas deben ser transparentes en su funcionamiento y en las decisiones que toman (México Transparente, 2023, 12). En el caso del derecho a la autonomía, puede tomar decisiones y actuar en nombre de las personas. Por ello, se debe garantizar que éstas tengan el control sobre las decisiones. Y con respecto al derecho a la igualdad, puede afectarles a las personas en sociedad, así como también en el mercado laboral (Granados, 2022, 15). Por lo cual, se deben proteger los derechos y garantizar que no se amplíen las desigualdades (Martínez, 2017, 60) existentes, ni se tomen decisiones que comprometan la seguridad ni la autonomía de las personas.

Estos son solo algunos de los derechos que deben ser protegidos en los posibles casos de violaciones por la IA, pero la lista puede variar dependiendo del contexto y la situación específica (Morán, 2022, 300). Aunque debemos subrayar que en sí misma no puede cometer delitos, somos las personas las que pueden utilizarla para llevar a cabo actividades ilegales o dañinas.

Entre los delitos que se pueden cometer con la ayuda de la IA se encuentra el Fraude: puesto que se puede utilizar para cometer fraudes en línea, como el *phishing* o la suplantación de identidad. Puede ser utilizada para engañar a las personas y obtener beneficios económicos o de otra índole. Por ejemplo, se puede utilizar para crear *bots* que se hacen pasar por humanos en redes sociales para promover productos o servicios falsos o engañosos (Parada, 2021, 130). También está el Robo de información, donde los ciberdelincuentes pueden utilizarla para robar información de sistemas informáticos.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

Lo mismo ocurre con el Ciber espionaje, donde los gobiernos o empresas pueden utilizar la IA para espionaje cibernético, o los ataques cibernéticos, como el *ransomware* o el *malware* (Sánchez, 2012, 80).

Otra cuestión es cuando la IA es programada con sesgos discriminatorios, o sea, sus algoritmos pueden discriminar a ciertos grupos de personas al tomar decisiones (Asquerino, 2022). Por ejemplo, un sistema utilizado en la selección de currículums puede programarse para rechazar automáticamente los currículums de ciertas etnias o géneros. También se puede usar la manipulación de la opinión pública, para difundir desinformación y manipularla en las redes sociales. El Robo de identidad, sucede cuando es utilizada para recopilar información personal, y utilizarlo para el robo de identidad (Ruiz, 2018). Por ejemplo, se pueden crear *bots* que se hacen pasar por personas reales en línea, con el objetivo de obtener información personal de otras personas.

Brent Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter y Luciano Floridi, (Mittelstadt et al., 2019, 10) realizan un análisis crítico de las implicaciones éticas de algoritmos, examinando diferentes perspectivas y enfoques en el debate sobre algoritmos en política, justicia, atención médica, marketing, y educación, entre otros. Proponen un marco ético para la evaluación de los algoritmos, que incluye la transparencia, equidad, responsabilidad y la justicia. También discuten la necesidad de un enfoque interdisciplinario para abordar la ética con la participación de los expertos en tecnología, derecho y otras disciplinas. Su contenido proporciona una base para la reflexión crítica de su uso en diversos ámbitos.

La IA puede ser utilizada para acosar y amenazar a personas en línea, como en el caso de los *bots* creados para el ciberacoso en redes sociales. También puede ser utilizada para la vigilancia y el espionaje de personas sin su conocimiento o con consentimiento, y utilizar su información para controlar y manipularlas (UNICEF, 2022). Estos son solo algunos ejemplos de los delitos que pueden ser cometidos con el uso de la IA en nuestras vidas, se plantean importantes desafíos éticos y legales que deben ser abordados, para garantizar la protección de la dignidad.

En algunos Tribunales se han presentado casos (Cahun, 2017) que involucran la violación de la dignidad humana por parte de la IA. Por ejemplo, en 2018, en EUA, un conductor de un automóvil Tesla falleció en un accidente mientras usaba la función de piloto automático del automóvil. La familia del conductor presentó una demanda contra Tesla, argumentando que la compañía había creado un sistema de piloto automático defectuoso que no detectaba peligros en la carretera. El caso planteó cuestiones sobre la responsabilidad de los fabricantes de tecnología de IA seguros y confiables.

Existen preocupaciones éticas y legales en el uso de sistemas de IA para tomar decisiones en el empleo, salud, (Live, J.G, 2020, 24) seguridad y la administración de justicia. En algunos casos, estos sistemas han demostrado ser propensos a errores y sesgos, que han llevado a cuestionarse la responsabilidad de las empresas y gobiernos.

En 2018, se presentó en California el caso de un hombre que afirmara que la empresa IBM lo había discriminado por edad al despedirlo y reemplazarlo por un empleado más joven que usaba la IA de la empresa para realizar tareas similares (Becares, 2023) (Pastor, 2023). El demandante argumentó que el sistema había sido programado para buscar

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

a candidatos más jóvenes, lo que constituía una forma de discriminación por edad. Si bien el caso fue desestimado por un juez, planteó preguntas interesantes sobre la responsabilidad de las empresas en la programación y uso de sistemas de IA.

En 2019, se informó que la Policía de Detroit, estaba utilizando un sistema de reconocimiento facial de IA para identificar sospechosos. Sin embargo, el sistema identificó erróneamente a varias personas inocentes, eso generó expectativas sobre la fiabilidad de estos sistemas y su impacto en los derechos humanos (Red en Defensa de los Derechos Digitales, 2020).

En 2020, Amnistía Internacional, (publicó un informe que denunciaba la manera en que las empresas de tecnología estaban violentando los derechos humanos, al proporcionar herramientas de vigilancia a gobiernos autoritarios. El informe trataba sobre la venta de sistemas de IA que permitían la vigilancia masiva de la población, y la identificación de personas señaladas como disidentes políticos, lo que podía poner en peligro su seguridad y privacidad. Incluso, su vida (Amnistía Internacional, 2020).

Los ejemplos referidos muestran cómo la aplicación de la IA puede plantear muchas preguntas importantes sobre la dignidad en los diferentes contextos. Los casos que han sido presentados ante los diferentes tribunales de varias partes del mundo involucran violaciones de derechos humanos sobre cuestiones de discriminación algorítmica, monitoreo masivo y uso de datos personales sin consentimiento.

Aunque los casos tienen que ver con cada situación particular. Algunos han sido resueltos mediante acuerdos extrajudiciales, mientras que otros se han llevado a juicio y han resultado en sentencias condenatorias o acuerdos de conciliación. En general, si aumenta el uso de la IA también las violaciones a los derechos humanos, lo que genera más presión para garantizarlos.

En México, aún no se han presentado ningún caso en los tribunales en los que se haya acusado directamente a la IA como responsable de un delito. Sin embargo, se tiene conocimiento que en algunos asuntos en los que se si han utilizado sistemas de IA, se ha cuestionado la responsabilidad, tanto de los creadores como de los usuarios de estos sistemas, especialmente en casos de discriminación o violaciones a la privacidad de datos. Es un tema que está en la mesa de debates en donde se definirán responsabilidades claras y precisas para el uso de estas tecnologías.

Pensemos por un momento, el supuesto caso donde intervenga una persona, dotada de un sistema gano-nano-robo-tecno, llevando a cabo una acción (subir a la plataforma una fotografía que muestre a la persona en un estado que no quisiera que nadie lo viera), aquí la interrogante seria, si sigue siendo una persona o se califica como una máquina. Lo cual, nos lleva a reflexionar, puesto que implica cuestiones éticas y filosóficas sobre lo que define a una persona como tal. En general, se considera que una persona es un ser humano dotado de conciencia, inteligencia y capacidad de tomar decisiones autónomas (Arbeláez-Campillo et al., 2021, 510). Sin embargo, si esa persona estuviera bajo el sistema o condición ya descrita líneas arriba, (Ovalle, 2007, 260) significaría la integración de tecnología avanzada en su cuerpo y mente, y podríamos preguntarnos si sigue siendo completamente humana o si se ha convertido en algo diferente. En este sentido, algunos filósofos y científicos opinan que la identidad humana no está limitada

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

a características biológicas específicas, sino que puede ampliarse para incluir la tecnología que se integra en el cuerpo y la mente.

> Es evidente que el post-humanismo se presenta como un indeterminismo jurídico que no sustenta suficiente exhaustividad normativa en la mencionada declaración de derechos humanos urgiéndose un sistema colegislador que delimite los fronterismos tuitivos regulatorios con un imperativismo categórico que impida el uso irracional de sus contenidos.
>
> Por un segundo orden expone Ovalle se comprenden: "personas con identidad genética-cognitiva informacional alterada por la modificación geno-nano-robo-tecno", se alude que se está en presencia de seres mutantes cuya naturaleza significa la incorporación de elementos tecnológicos integrando organización con funcionamiento humano lo cual cambia la concepción de la vida justificando redefiniciones en la concepción del derecho (Márquez, 2022, 2).

Por ejemplo, Andy Clark (Clark, 1997, 180) argumenta que la mente humana es una entidad extendida que incluye tanto el cerebro como las herramientas tecnológicas que utilizamos para procesar información y tomar decisiones. Así, una persona dotada de un sistema gano-nano-robo-tecno seguiría siendo una persona, aunque con una identidad expandida que incluiría tecnología avanzada. En cualquier caso, es importante tener en cuenta que la integración de tecnología en el cuerpo y la mente plantea una serie de cuestiones éticas y sociales que deben ser abordadas cuidadosamente, para garantizar la dignidad.

2.2. La dignidad y su relación con la inteligencia artificial

La dignidad humana debe ser considerada en todas las áreas de la vida, además del desarrollo y uso de la IA. Entendiendo a la dignidad humana como principio ético y a su aplicación en el contexto de la IA (Martínez, 2020, 30). Estudiaremos la relación entre la IA y la autonomía humana, y cómo aquella puede afectar la capacidad para tomar decisiones informadas y libres. Igualmente, analizaremos su impacto en la identidad humana y la no discriminación en su uso. Considerando los desafíos y riesgos de un enfoque ético, centrado en la dignidad humana en su diseño, desarrollo y uso.

La dignidad humana es un concepto filosófico, y se refiere al valor inherente de cada ser humano, que debe ser respetado y protegido en todas las circunstancias (Habermas, 2010, 15). Considerando que no depende de factores externos como la riqueza, el poder o el estatus social, sino que es intrínseca a la condición humana. Como tal, se le considera un principio fundamental que debe guiar todas las acciones y políticas relacionadas con los derechos y el bienestar humanos en general.

La IA ha traído grandes avances y beneficios a la humanidad, pero también ha planteado preocupaciones éticas y sociales. Uno de los mayores desafíos es el impacto que puede tener en la dignidad humana (Aparisi, 2013, 210) por eso, se analizará la discriminación algorítmica, puesto que dichos algoritmos pueden perpetuar y amplificar prejuicios y discriminación si se basan en datos históricos y patrones que reflejan la discriminación

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

pasada. Por ejemplo, los sistemas de IA utilizados en la selección de personal, pueden perpetuar la discriminación de género o raza si se basan en datos históricos que reflejan la discriminación en el mercado laboral.

Otra de las implicaciones de la IA es la dignidad en el trabajo, con la automatización y robotización de ciertas tareas, se pueden desplazar a los trabajadores humanos con un gran impacto negativo para su dignidad y bienestar. Además, de que la monitorización constante del rendimiento con la IA puede llevar a una presión excesiva y a la invasión de la privacidad (Cañigueral, 2022, 280). La IA puede llevar a la pérdida de autonomía y control en la vida de las personas al tomar decisiones y acciones sin la intervención humana. Un ejemplo preocupante es su uso en la medicina, donde pueden decidir sobre el tratamiento que se aplicara sin la supervisión de un médico. (De Lecuona, 2020, 150).

En este sentido, Bostrom, N. (Bostrom, 2014, 250) argumenta la creación de una IA superinteligente que supere ampliamente la inteligencia humana, podría ser una amenaza para la humanidad. Explica cómo la inteligencia artificial se ha desarrollado y cómo se espera que progrese en el futuro. Luego, examina los diferentes escenarios que podrían ocurrir si se desarrolla una inteligencia artificial superinteligente. Los escenarios prevén que la inteligencia artificial se vuelva hostil hacia los humanos, y que pierdan el control sobre la IA y de que ésta ignore a los humanos. Y supone que la mejor manera de evitar estos peligros potenciales es desarrollar una estrategia coordinada y cuidadosa para el progreso de la inteligencia artificial.

Los desarrolladores de IA deben considerar estos riesgos y trabajar en minimizar su impacto en la dignidad humana (Habermas, 2010, 18) con políticas y regulaciones adecuadas para el abordaje de estas cuestiones y garantizar que se utilice de manera ética y responsable. En el entendido que la dignidad es fundamental por considerar el desarrollo y uso de la inteligencia artificial, puesto que plantea numerosos desafíos éticos, sociales y legales que se han de abordar para garantizar su desarrollo responsable y sostenible. Es así como la dignidad humana (Corvalán, 2018, 300) debe ser un principio rector en el desarrollo de la IA. Significa que en su diseño y uso se debe respetar y promover (Aparisi, 2013) en todas sus dimensiones, incluyendo la autonomía, privacidad, integridad física y mental y la no discriminación.

La dimensión comunicacional plantea la privacidad y confidencialidad de las comunicaciones electrónicas (Zinguer, 2014, 26). La dimensión decisional es la capacidad para tomar decisiones libres e independientes, sin interferencias. La dimensión informativa se centra en el control sobre los datos personales y su utilización. La dimensión asociativa aborda el derecho de asociarse sin temor a ser vigilados o perseguidos. La dimensión contextual se refiere al impacto del entorno sociocultural en la privacidad y sostiene que no es un valor absoluto, sino que debe equilibrarse con otros derechos y valores. Esta tipología puede ser útil en las políticas públicas y las decisiones éticas respecto de la tecnología digital. Para ello, es necesario que los responsables del desarrollo de la IA adopten un enfoque ético y multidisciplinario que considere los aspectos técnicos, económicos, éticos, sociales y legales. Esto implica la participación de los expertos en ética y derechos humanos (Valdés, 2022, 116), reguladores y responsables políticos. Igualmente, la transparencia y la rendición de cuentas. Igual que la publicación de información clara

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

y accesible sobre los algoritmos utilizados, así como la responsabilidad de los desarrolladores y usuarios, en caso de violentar algún derecho.

Por eso, la dignidad humana (Habermas, 2010, 10) debe ser un principio rector en el desarrollo y uso de la IA. Lo que implica que los derechos humanos, podrá garantizar que contribuya al bienestar humano y respete la dignidad en el diseño, la transparencia y la participación del proceso de construcción de la IA.

2.3. Los desafíos y riesgos de la inteligencia artificial para la dignidad humana

A medida que la IA avanza, surgen desafíos y riesgos importantes para la dignidad humana (Habermas, 2010, 20). Algunos de los principales desafíos y riesgos están presentes en la discriminación algorítmica, al ser utilizados en la IA pueden ser sesgados y discriminativos, lo que lleva a tomar decisiones que violenten la dignidad humana (Aparisi, 2013, 208). Lo mismo ocurre con la Privacidad, al recopilar grandes cantidades de datos personales que pueden violentar la dignidad humana. Igual sucede con el desplazamiento laboral, donde los trabajadores humanos sufren consecuencias negativas como el desempleo y la pérdida de la identidad laboral.

Es así como, Koops (Koops, 2016, 550) propone una tipología de la privacidad que pueda ser aplicable en el contexto digital, pues la privacidad ha evolucionado para incluir nuevas dimensiones, por eso, es necesario contar con una tipología actualizada. Es una tipología de siete dimensiones de la privacidad: territorial, personal, comunicacional, decisional, información, asociativa y contextual. La dimensión territorial, es el derecho a estar protegidos en su propio hogar o lugar de trabajo, mientras que la personal abarca aspectos como la integridad corporal y la identidad.

La IA puede afectar la autonomía, cuando toma decisiones importantes en lugar de los seres humanos, lo que puede reducir la capacidad para ejercer su libre albedrío. También se plantean desafíos importantes en cuanto a la Responsabilidad por las decisiones tomadas por las máquinas, lo que puede derivar en un serio problema para la dignidad humana, (Aparisi, 2013, 215) si no se aborda adecuadamente. La IA puede ser utilizada para fines maliciosos, como la guerra cibernética y el espionaje, peligrando así la seguridad (Habermas, 2010, 23). Estos desafíos y riesgos deben ser abordados responsablemente para garantizar que se proteja y respete la dignidad humana en todo momento.

La transparencia es un problema que atañe a la dignidad humana. Pues es de esperarse que la IA se utiliza en situaciones en donde se toman decisiones importantes para la selección de candidatos para empleo o en cuestiones médicas. Sin embargo, las decisiones que toma no siempre son transparentes. Además, no siempre se puede responsabilizar a alguien por los resultados negativos de una decisión equivocada tomada por la IA.

Lo anterior, plantea serios problemas de dignidad humana, pues las personas deben de entender y cuestionar las decisiones. Además, de poder buscar responsabilidad y reparación cuando las decisiones tomadas por la IA tienen consecuencias negativas para ellas. La falta de transparencia y responsabilidad socava la dignidad humana al privar a las

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

personas de estas capacidades esenciales. Por lo tanto, es esencial que la IA sea diseñada y utilizada de manera transparente y responsable, lo que significa que las decisiones tomadas deben ser explicadas de manera clara y accesible para las personas afectadas, quienes deberán poder impugnar estas decisiones y buscar responsabilidad y reparación cuando sea necesario. Solo así la IA puede ser compatible con la dignidad humana.

La discriminación y el sesgo en los sistemas de IA son otro de los desafíos y riesgos para los derechos humanos (Habermas, 2010, 15) considerando que aquella recupera y analiza datos, y si estos están sesgados o son discriminatorios, los sistemas también lo serán. Por ejemplo, si la IA contiene datos que muestran una discriminación histórica contra ciertos grupos de personas, es probable que el sistema perpetúe esa discriminación en el futuro, lo que puede llevar a decisiones injustas en áreas como la contratación, servicios financieros, de salud, (Live, J.G., 2020, 30) y de administración de justicia, entre otros. Este problema se debe abordar mediante la recopilación de datos más equilibrados y diversos, así como el diseño de algoritmos y sistemas de IA sensibles de la discriminación y el sesgo potenciales. Y que las empresas y organizaciones responsables de desarrollar y utilizarla sean transparentes en sus procesos y decisiones, para que se pueda detectar y corregir cualquier discriminación o sesgo.

Uno de los principales desafíos para la dignidad humana son los datos personales, en la IA. La recolección y el almacenamiento de datos de los usuarios son fundamentales para su funcionamiento, puesto que necesitan información para aprender y mejorar su desempeño. Sin embargo, esto puede representar una amenaza para los datos respecto a la privacidad y seguridad que puede violentar la dignidad. Considerando a la privacidad (Turégano, 2020, 270) un derecho fundamental, incluyendo el control de datos personales. Con la IA la privacidad se ve amenazada por su recopilación y uso sin el consentimiento del usuario, o la falta de seguridad para la protección de datos recopilados. Esto puede resultar en la exposición de información personal, utilizada para el acoso, la discriminación o la vigilancia.

Desde ese enfoque, Jobin, Ienca y Vayena (Jobin et al., 2020, 360) examinan 84 guías éticas desarrolladas en el mundo en respuesta al rápido despliegue de la inteligencia artificial (IA). Provienen de diferentes países y organizaciones internacionales para crear una tipología de las áreas de preocupación ética en la IA, e identifican cuatro categorías principales: (1) seguridad, privacidad y responsabilidad, (2) transparencia e interpretación, (3) equidad e inclusión, y (4) valores y gobernanza. Luego, examinan las diferencias y similitudes entre las distintas guías éticas y concluyen que, aunque hay una gran variabilidad en las recomendaciones específicas, si hay un amplio consenso sobre los temas generales de preocupación ética. También destacan la importancia de la gobernanza global y la colaboración internacional para abordar las preocupaciones éticas en la IA de manera efectiva.

Los sistemas de IA almacenan datos, y si estos son robados o perdidos, pueden ser utilizados para actividades ilegales. Además, la seguridad de los datos puede ser comprometida por errores en los algoritmos que pueden llevar a decisiones incorrectas y perjudiciales. La IA debe respetar la dignidad en el tratamiento de los datos personales. Esto implica la necesidad de implementar medidas de privacidad y seguridad

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

adecuadas para garantizar la transparencia al usar los datos. Su regulación y supervisión adecuadas son esenciales para abordar estos desafíos y garantizar que se utilice con ética (González, 2017, 30).

2.4. Las posibilidades y oportunidades de la IA para mejorar la calidad de vida

La IA también presenta oportunidades y posibilidades en la mejora la calidad de vida (Live. J.G., 2020, 40) al proporcionar diagnósticos más precisos y rápidos, detectar enfermedades en una etapa temprana y personalizar los tratamientos médicos. Lo mismo que en la seguridad y prevención del crimen, igual que las amenazas a la seguridad, la identificación de los patrones de comportamiento sospechosos y el monitoreo de las áreas de alta actividad criminal (Llinares, 2018, 100). En la misma tesitura, la IA puede mejorar la educación y el aprendizaje al personalizar la enseñanza, con retroalimentación y evaluar el progreso del estudiante, monitorear la calidad del aire y agua, prevenir incendios forestales y mejorar su gestión. La aplicación de la IA en estas áreas debe ser cuidadosamente considerada para garantizar que se aborden los problemas de manera ética y equitativa, y que se eviten posibles impactos negativos, por lo que también debe ser acompañada de políticas y regulaciones claras y efectivas para proteger la dignidad humana.

Es dable menciona que la Bioética, es la atención médica y el bienestar donde la IA puede ser positivo en el análisis de datos y localización de patrones en la detección de enfermedades, como el PNUMA ("organismo de las Naciones Unidas cuya misión es catalizar, defender, educar y facilitar la promoción del uso sensato y del desarrollo sostenible del medio ambiente global") (RAE, 2023) O en la Biotecnología, que es la "aplicación tecnológica que utiliza sistemas biológicos y organismos vivos o sus derivados para la creación o modificación de productos o procesos …". Los algoritmos de aprendizaje ayudan a identificar signos tempranos de cáncer, aumentando la eficacia del tratamiento lo que mejoraría la tasa de supervivencia. También puede ser útil en la atención de pacientes crónicos o ancianos. Los robots, (Zabala, 2021, 488) o sea, la IA, la cual es una "disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico" (RAE, 2023) de asistencia pueden ayudar a las personas mayores a realizar tareas cotidianas y monitorear su salud, (Live.J.G., 2020, 66) lo que les permitiría más independencia, con la reducción de la carga de cuidados médicos y asistenciales en sus familiares. En general, la IA puede mejorar la vida en muchos aspectos. Sin embargo, se deben abordar los desafíos y riesgos que plantea su implementación para garantizar su utilización responsable.

En este sentido, Patrick Lin, Keith Abney y George BEKEY, (Lin et al., 2011, 16) abordan las implicaciones de la robótica y su impacto en la sociedad. Trata de cuestiones éticas y sociales relacionadas con los robots, como la privacidad, seguridad, responsabilidad legal y la justicia, así como los intereses de la sociedad. Presentan diferentes perspectivas

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

sobre cada tema y exploran los argumentos a favor y en contra de diversas posiciones. También ofrecen recomendaciones prácticas para los diseñadores, ingenieros y responsables políticos que trabajan en el campo de la robótica. Resulta esencial su consulta (Ordoñez, 2021, 20) pues proporciona una sólida base para el diseño y la implementación responsable de robots en nuestra sociedad.

El avance de la IA también puede aumentar la eficiencia en el trabajo, porque puede ayudar en la automatización de tareas repetitivas, para que los empleados dediquen su tiempo a tareas más complejas y creativas, lo que podría mejorar la satisfacción laboral y aumentar la calidad y productividad del trabajo realizado. Además, de ayudar a mejorar la seguridad laboral, al detectar posibles riesgos y alertar a los trabajadores y empleadores, reduciendo los accidente y mejorando la seguridad (Benhamou, 2022).

Los sistemas de IA pueden predecir las necesidades de los consumidores, personalizar los productos y servicios según sus preferencias y mejorar la satisfacción del cliente. El tema sobre el impacto relativo a la movilidad y la accesibilidad en los Vehículos autónomos impactan a las personas con discapacidad y/o movilidad reducida, así como los desafíos en cuanto a la seguridad y responsabilidad en caso de accidentes. Lo mismo puede ocurrir con los llamados Sistemas inteligentes de transporte público: donde existe la posibilidad de que la IA mejore su eficiencia y accesibilidad, así como garantizar la privacidad de datos. Respecto a las Tecnologías de asistencia para la accesibilidad la IA es útil para mejorar la movilidad y accesibilidad de las personas con discapacidad (Martínez et al., 2020). En tal contexto, el monitoreo y control de tráfico puede mejorar la seguridad en las carreteras, y la privacidad de los datos. En cuanto a las personas con discapacidad, la accesibilidad digital sería de gran ayuda para igualar sus oportunidades.

2.5. El papel de la ética y su regulación en la gobernanza de la inteligencia artificial

La IA requiere se regulada para que se utilice dentro de marcos éticos adecuados para garantizar su uso seguro y responsable (González, 2017, 156). Con lo cual, se han de establecer leyes y normas que definan los límites y responsabilidades de sus desarrolladores, fabricantes y usuarios. La transparencia y la responsabilidad son fundamentales para garantizar la confianza en la IA, por lo mismo, habrá que establecer mecanismos para que los desarrolladores y los proveedores de servicios sean responsables de las decisiones tomadas por sus sistemas.

La necesidad de una evaluación ética es importante para garantizar que la IA se utilice sin discriminación. En esa tesitura, habrá que establecer comités de ética y mecanismos de revisión que garanticen los derechos humanos y valores éticos (P. Quirós, 2022, 155). El diálogo social amplio y transparente sobre la sociedad y el impacto de la IA en los derechos humanos es necesario, igual que el involucramiento de la sociedad civil, expertos en tecnología, empresas y los gobiernos, para establecer un marco ético y de regulación adecuado.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

Es así como la ética y la regulación son fundamentales para utilizar la IA de manera responsable y efectiva, conforme a derechos humanos. Los principios éticos garantizan que se utilice en beneficio a la sociedad. Algunos de los principios éticos que se han propuesto incluyen la transparencia, la responsabilidad, privacidad, no discriminación y seguridad. Por lo cual, habrá que integrarlos en el diseño de la IA (P. Quirós, 2022, 160).

Además de los principios éticos, la regulación gubernamental también es crucial para garantizarla el uso de la IA de manera responsable y beneficiosa. Las políticas gubernamentales pueden establecer límites en su uso en la seguridad pública, y requerir la transparencia en la toma de decisiones al respecto, así como establecer estándares de seguridad y privacidad de datos personales. De esta manera queda claro que la ética y la regulación son decisivas en la gobernanza, (Pita, 2021, 289) los principios éticos deben integrarse a su diseño y uso, mientras que las regulaciones gubernamentales pueden establecer límites y estándares para garantizar que se utilice en beneficiosa de la sociedad.

Las políticas y regulaciones gubernamentales son esenciales para garantizar que el desarrollo y uso se realicen de manera responsable y ética (Ausín, 2021, 16). Los gobiernos de todo el mundo comienzan a reconocer la importancia de regular la IA y están estableciendo normas y leyes para abordar los desafíos y riesgos asociados. Entre las políticas y regulaciones gubernamentales, destacan los comités y grupos de trabajo encargados de investigar y evaluar su impacto. Estos comités y grupos de trabajo también proponen recomendaciones y directrices para su desarrollo y uso.

También la creación de estándares técnicos y éticos para la IA es decisiva, pues establecen las mejores prácticas para la recopilación y el uso de datos, la transparencia, la privacidad de los datos, y la responsabilidad en su diseño y desarrollo. Algunos gobiernos están implementando políticas de educación y capacitación para garantizar que todos comprendan su impacto en la sociedad y tengan la capacidad de desarrollar y utilizar sistemas responsablemente. Los gobiernos deben crear políticas y regulaciones que fomenten su desarrollo ético (Ausín, 2021, 5).

En este sentido, Aimee van Wynsberghe, Marcello Ienca y Effy Vayena, (Jobin et al., 2019, 390) examinan 80 guías éticas para la IA diferentes, publicadas por organizaciones gubernamentales, empresas y sociedad civil, analizan sus similitudes y diferencias para evaluar su efectividad y garantizar un desarrollo ético. Examinan las áreas de la privacidad, responsabilidad, transparencia y la justicia, y analizan sus similitudes y diferencias que abordan las guías. También analizan la efectividad de las guías éticas de IA para garantizar un desarrollo ético de la tecnología. Identifican varias limitaciones como la falta de aplicación efectiva, de supervisión y de mecanismos de responsabilidad. El señalamiento se centra sobre la búsqueda de una mayor colaboración entre las organizaciones que publican guías éticas de IA y una mayor aplicación y supervisión para garantizar un desarrollo ético tecnológico.

La responsabilidad social y corporativa es una cuestión clave en el desarrollo de la IA. Las empresas y organizaciones que la desarrollan y utilizan deben tener en cuenta el impacto social y humano de sus aplicaciones. Por eso, las empresas deben seguir principios éticos y adoptar medidas como la transparencia, promoción e inclusión en sus

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

equipos de trabajo. Los gobiernos y los organismos reguladores han de establecer políticas y regulaciones claras para garantizar que se desarrolle responsable y ética mente (Becerra et al., 2021, 10). Al establecer estándares de seguridad y privacidad para los datos personales, así como requisitos para la transparencia. La ética y la regulación garantizan la calidad de vida sin socavar la dignidad humana.

La IA impacta los aspectos éticos, técnicos, y económicos de toda sociedad, y la manera en que las personas trabajamos y nos relacionamos. Algunos cambios se reflejan en la automatización de trabajos y la robótica, lo que deja fuera ciertos puestos de trabajo. Esto puede afectar especialmente a trabajos que implican tareas repetitivas o de baja cualificación (Lahera, 2019, 258). Aunque también pueden crearse nuevos trabajos en el diseño, programación, mantenimiento y reparación. La automatización y la capacidad de procesamiento de la IA pueden lograr mayor eficiencia y productividad que optimizan la cadena de suministro además de prever la demanda de productos en las empresas.

La introducción de la IA requerirá una formación y capacitación diferente a la que se requiere actualmente. Esto puede implicar cambios significativos en la educación y la formación, incluyendo la necesidad de una mayor formación en tecnología y habilidades digitales. También puede mejorar la calidad sanitaria, en el sector de la medicina, al analizar datos y diagnosticar con más precisión e identificar tratamientos más efectivos (Lahera, 2019, 269).

Igualmente, puede proporcionar nuevas formas de interacción social, como asistentes virtuales y robots (Zabala, 2021, 489) de compañía. Estas tecnologías pueden ser especialmente útiles para personas mayores o personas con discapacidades. Estos cambios requerirán de tiempo para ser implementados de manera adecuada y efectiva. Además, pueden no afectar a todas las sociedades de la misma manera, y es necesario considerar la diversidad cultural y económica en su regulación y uso.

Es así como, Calvo, R. A., & Peters, D. (Calvo y Peters, 2013, 177) realizaron un estudio de interacción humano-robot en donde los participantes interactuaron con un robot durante varias semanas en su hogar. Los resultados mostraron que los participantes, inicialmente tenían altas expectativas sobre el robot, pero que éstas disminuían con el tiempo a medida que se acostumbraban a su presencia. Sin embargo, los participantes aún encontraban útil al robot en su hogar y estaban dispuestos a seguir interactuando con él. Los autores concluyen que la habituación es un factor esencial para el diseño y la creación de robots domésticos, y se requieren más estudios para comprender la forma en que los humanos se adaptan a la presencia de robots a largo plazo.

Por un lado, la automatización de ciertas tareas y procesos puede llevar a la pérdida de empleos en ciertos sectores. Sin embargo, también puede llevar a la creación de nuevos empleos en otros sectores relacionados con la IA. Además, puede tener un impacto significativo en la economía a mejorar la eficiencia y la productividad, puede ayudar a reducir costos y aumentar la producción. Lo mismo que a identificar oportunidades y a mejorar las decisiones empresariales. Pero la implementación de la IA también puede generar desigualdades económicas, porque las empresas con más recursos pueden tener una ventaja en su desarrollo y uso. Por lo tanto, resulta esencial abordar estas posibles consecuencias sociales y económicas al regularla.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

La IA avanza y produce cambios significativos en los sectores industriales, desde la fabricación hasta la logística, pasando por el comercio y los servicios financieros. La automatización de procesos y el procesamiento de datos pueden mejorar la eficiencia y reducir costos en estas industrias. Estos cambios también pueden tener un impacto en el empleo y requerir nuevas habilidades y competencias para los trabajadores. Habrá cambios sociales en la educación, salud transporte y la movilidad en las ciudades. Hay que tener presente los posibles efectos negativos en la privacidad, la seguridad y la desigualdad social que surgirán de estos cambios.

La IA transforma la operación de las empresas e industrias y como resultado, se producen cambios en la economía y en el terreno laboral. La automatización y la robótica aumentarán la eficiencia y reducirán los costos, pero también pueden afectar a la cantidad y calidad de los trabajos disponibles (Wilson, 2018, 60). La IA también causa impacto en la educación y la formación de habilidades que prepara a las personas para trabajar con la tecnología. Por lo tanto, se ha de analizar y comprender los cambios sociales y económicos que puede generar y desarrollar estrategias para adaptarse a ellos de manera efectiva (González, 2018, 100).

La dignidad humana y la IA puede tener un impacto significativo en los derechos humanos. En este ensayo, se explora la dignidad humana, su evolución histórica y la relación entre ambas. También se analizan los desafíos y riesgos en la toma de decisiones con transparencia, discriminación, sesgo y privacidad de datos personales. Destaca las posibilidades y oportunidades de la IA en la calidad de vida, atención médica, productividad en el trabajo, movilidad y accesibilidad. La ética y la regulación son fundamentales en la gobernanza de la IA, estableciendo principios éticos claros y políticas y regulaciones gubernamentales adecuadas para fomentar la responsabilidad social y corporativa en su desarrollo.

La IA puede generar cambios en la sociedad, economía, mercado laboral y la transformación de las industrias. Por eso, debemos prepararnos para estos cambios y adaptarnos a ellos, especialmente en términos de educación y formación de habilidades. Puesto que puede impactar la dignidad humana y habrá que abordar los desafíos y riesgos mientras se aprovechan sus oportunidades y se promueva una gobernanza ética y responsable. Si bien puede mejorar la calidad de vida, también puede poner en peligro algunos derechos. Por eso, debe haber un equilibrio entre el avance tecnológico, la protección de la dignidad y el beneficio social.

El Grupo Europeo de Ética en la Ciencia y las Nuevas Tecnologías (EGE) (European Group on Ethics in Science and New Technologies, 2018, 150) en este informe aborda la ética en la IA autónoma. Los desafíos éticos de su desarrollo y propone la transparencia, responsabilidad, justicia, privacidad y la seguridad, entre otros más, como principios éticos y valores fundamentales que deberían guiar el diseño. Refieren su impacto en todas las áreas del conocimiento humano como el empleo, educación, democracia y la autonomía individual, y sugiere formas de abordar estos desafíos desde la ética. Contribuye al debate sobre la ética en la IA autónoma, proporcionando una base para el uso responsable de la tecnología.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

2.6. Desarrollos de inteligencia artificial en el proceso judicial

PROMETEA (Procesos, Medidas y Tecnología Asistida por IA) es un proyecto de inteligencia artificial implementado en Argentina en el ámbito judicial (Grosso, 2020, 15). Fue desarrollado por el Ministerio de Justicia y Derechos Humanos de Argentina, con el objetivo de mejorar la eficiencia y la transparencia en el sistema judicial con el uso de IA, además de agilizar los procesos judiciales, reducir la carga de trabajo de los operadores judiciales y mejorar el acceso a la administración de justicia. Se enfoca en áreas de análisis automatizado de documentos legales, generación de informes y apoyo en la toma de decisiones. Utiliza lenguaje natural y aprendizaje automático para clasificar documentos legales, identificar información relevante y generar resúmenes y análisis de estos (Robledo, 2022, 54).

Por otra parte, VICTOR (Sistema Inteligente de Videoconferencia y Operación Remota) es una iniciativa de IA implementada en Brasil. Fue desarrollado por el Tribunal de Justicia de Río Grande do Sul. El objetivo de VICTOR es facilitar la realización de audiencias judiciales a través de videoconferencias y permitir la operación remota de los procedimientos judiciales. Además de agilizar los procedimientos judiciales, reducir los costos asociados a los desplazamientos y mejorar la accesibilidad de la administración de justicia. También utiliza el reconocimiento facial y vocal para verificar la identidad de las personas que participan en las audiencias y garantizar la seguridad del proceso, así como, utiliza procesamiento de lenguaje natural que transcribe y genera automáticamente documentos a partir de las audiencias (Robledo, 2022, 50).

Es dable menciona que China se encuentra avanzando en el desarrollo de IA en el ámbito judicial. Han surgido plataformas de inteligencia artificial que ayudan en la resolución de casos, proporcionando asesoramiento legal automatizado, predicción de fallos judiciales y análisis de riesgos. Además, se han establecido tribunales inteligentes en ciudades como Beijing, Shanghai y Guangzhou, donde se utilizan tecnologías de IA, como reconocimiento facial y análisis de *big data* para agilizar los procedimientos y mejorar la eficiencia de los procesos judiciales. También han desarrollado sistemas de inteligencia artificial que pueden analizar grandes cantidades de datos legales y ayudar a los jueces en la toma de decisiones, al proporcionar recomendaciones sobre fallos judiciales basados en casos y precedentes anteriores (Robledo, 2022, 56).

En el Reino Unido, también se están llevando a cabo diversos proyectos de inteligencia artificial en el ámbito judicial. Por ejemplo, se están desarrollando sistemas de IA para analizar contratos y documentos legales, facilitando así el trabajo de los abogados. Asimismo, se están utilizando algoritmos de IA que calcula la reincidencia delincuencial y apoya la toma de decisiones en la libertad condicional y sentencias. Estos sistemas utilizan algoritmos de lenguaje natural que identificar cláusulas, analiza riesgos legales y ayuda a los abogados en la revisión de documentos (Robledo, 2022, 64). También se están utilizando algoritmos de IA para predecir la reincidencia delincuencial. Esto ayuda a los jueces en la toma de decisiones relacionadas con la libertad condicional y las sentencias, permitiendo una evaluación más objetiva y basada en datos (Granero, 2020, 128).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

El gobierno de Singapur anuncio un proyecto para explorar cómo la IA puede mejorar los servicios legales y la administración de justicia. Esto incluye el uso de *chatbots* y asistentes virtuales para proporcionar información y orientación jurídica a los ciudadanos. También se están utilizando sistemas de IA para analizar y clasificar casos legales, así como para ayudar a los jueces en la toma de decisiones al hacer recomendaciones basadas en precedentes legales con datos para identificar patrones y tendencias (Robledo, 2022, 60).

Así como, Argentina, Brasil, Estados Unidos; China; Reino Unido y Singapur son solo algunos ejemplos de países que están implementando desarrollos de IA en los procesos judiciales, aumentar la eficiencia y facilitar el acceso (Solar, 2021, 25). Estas iniciativas aprovechan el potencial de la IA para apoyar a los operadores del sistema judicial y mejorar la calidad y la rapidez de los procesos legales. La IA en el ámbito legal es ya una realidad que va evolucionando con tecnologías que propician la eficiencia en la administración de justicia (González, 2020, 32). Aunque la IA en el proceso judicial plantea desafíos éticos, como la transparencia de los algoritmos, la equidad y el sesgo algorítmico, se debe garantizar su uso responsable y asegurar los derechos humanos.

Actualmente, en la abogacía, ya es común que tanto en los asuntos relativos a la investigación revisión, redacción y análisis de dictámenes, contratos y demás documentos legales, asesoramiento, material documental para el litigio, y las decisiones en una demanda o estrategia procesal, sean elaboradas por sistemas de IA o por especialistas que se apoyan en estos sistemas. La automatización de las tareas legales tiene un gran impacto en el trabajo de los profesionales de servicios jurídicos, resultando nuevos modelos de negocio y ejercicio de la abogacía (Solar, 2021, 28).

2.7. Planteamiento de un caso hipotético: Kimi

Kimi es una película estadounidense dirigida por Steven Soderbergh, estrenada el 10 de febrero de 2022. La protagonista es Zoë Kravitz. El argumento trata sobre Bradley Hasling, chief executive officer (CEO) de Amygdala, es una corporación tecnológica. Bradley concede una entrevista para hablar sobre Kimi, producto nuevo que están promocionando, es un altavoz inteligente que, utiliza la supervisión humana para mejorar el algoritmo de búsqueda del dispositivo. Amygdala lanzara una oferta pública y Hasling ganara mucho dinero.

Angela Childs, empleada de Amygdala en Seattle se decida a monitorear los flujos de datos entrantes de los dispositivos Kimi, y corrige el software. Angela padece ansiedad y agorafobia, porque fue víctima de una agresión en el pasado, sus padecimientos se han exacerbado por la pandemia de COVID-19 debido a la cuarentena que guardamos en el hogar.

Su único contacto es con su pareja romántica Terry, su vecino del otro lado de la calle. En cierta ocasión Angela escucha una grabación con tintes de agresión sexual. Un compañero de trabajo llamado Darius, la ayuda y accede a la información de Samantha titular de la cuenta. Se percata que existen otras grabaciones y que "Brad" fue quien asesinó a Samantha. Es muy revelador porque al parecer 'Brad' es Bradley Hasling, quien ordenó a Rivas la muerte de Samantha. Por seguridad, Angela transfiere las grabaciones

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

a una unidad flash e informa el incidente a su superior, quien la remite con una ejecutiva de Amygdala llamada Natalie Chowdhury, Angela llama a la Dra. Chowdhury pero no logra comunicarse y se dirige a su oficina, la idea es que informe el caso al FBI.

Angela se percata que la Dra. Chowdhury no quiere hablar con las autoridades y trae a colación la anterior licencia de Angela por salud mental. Mientras está esperando a que la Dra. Llame al FBI, recibe noticias de Darius, quien le informa que alguien ha eliminado las grabaciones de voz de Samantha que estaban guardados en los servidores de Amygdala, y se da cuenta que dos desconocidos entran a la oficina. Ella huye y Rivas la rastrea a través de su teléfono.

Los maleantes encuentran a Angela e intentan secuestrarla, pero una manifestación de un grupo de personas lo evita. Sin embargo, Yuri, un hacker que trabaja para Rivas, registra su historial de búsqueda y con eso deduce hacia dónde se dirige. Por fin, encuentran a Angela la drogan y la llevan a su apartamento para asesinarla.

Cuando se dirigen al departamento de Angela, Kevin, un vecino que también pasa todo el tiempo encerrado le sale al paso para saber de Ángela porque la vio salir de la casa. Al pobre Kevin lo apuñalan los hombres de Rivas. Rivas ya se encontraba en el departamento de Angela para confiscar la unidad flash y borrar las grabaciones, pero ella usó su dispositivo Kimi y los distrajo, luego escapó a un piso más alto e improvisó una pistola de clavos que dejaron unos trabajadores de construcción, Ángela logra matar a los intrusos. Terry, llega justo cuando ella está marcando al 911. Bradley Hasling es detenido por el asesinar a Samantha, y Angela desayuna con Terry.

Aunque sería difícil (pero no imposible) que los jueces, autoridades administrativas, policía investigadora ministerial, operadores penales y demás autoridades tuvieran el panorama completo sobre el asesinato de una mujer, o cualquier otra persona bajo las circunstancias descritas, sin el apoyo de la ciencia por la complejidad para reunir las pruebas del ilícito y esclarecer los hechos en un proceso judicial. Porque se requiere de un conocimiento especializado sobre los indicios, pruebas y demás cuestiones relacionadas con el análisis científico del ilícito perpetrado.

En el caso particular, las grabaciones, el conocimiento y la ciencia ayudaron a que Angela descubriera el delito, porque tuvo la capacidad de intuir que algo estaba mal, e investigó con apoyo de la inteligencia artificial. En este supuesto, la IA es útil para el análisis de documentos, costumbres personales, detección de voz, identificación de huellas dactilares o cualquier otra prueba relacionada con el hecho delictivo.

III. Conclusiones

A partir de los hallazgos de esta investigación, llegamos a la conclusión de que es crucial implementar medidas que aseguren un desarrollo y uso ético y responsable de la Inteligencia Artificial (IA), con el fin de salvaguardar la dignidad humana. Este objetivo se logra fomentando la transparencia y garantizando una comprensión y documentación adecuadas de los algoritmos empleados en la toma de decisiones.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

Asimismo, es esencial que los gobiernos aborden la discriminación y el sesgo en los sistemas de IA, estableciendo estrategias que prevengan estas problemáticas en la recopilación y uso de datos. Paralelamente, deben implementarse medidas de seguridad y privacidad robustas. Estas acciones son fundamentales en sectores clave como la atención médica, el bienestar social, la eficiencia laboral, la movilidad y la accesibilidad.

Se hace imperativo diseñar y desarrollar principios éticos en el uso de la IA que respeten los derechos humanos. Para esto, se deben implementar políticas y regulaciones gubernamentales que supervisen adecuadamente el desarrollo y uso de la IA, asegurando el cumplimiento de estos principios éticos y la protección de la dignidad humana.

Es vital promover la responsabilidad social y corporativa, instando a empresas y desarrolladores a comprometerse con un uso ético y responsable de la tecnología. Dada la naturaleza evolutiva de la tecnología, las regulaciones y políticas deben ser dinámicas y adaptativas, capaces de abordar los desafíos y riesgos emergentes.

La estrategia global para el manejo de la Inteligencia Artificial (IA) debe abarcar no solo la investigación en torno a la seguridad de estos sistemas, sino también fomentar la cooperación internacional y la integración de valores humanos fundamentales en su diseño y operación. Este enfoque holístico implica un desafío significativo para nuestra comprensión actual de la IA y su relación intrínseca con la humanidad. Nos obliga a reflexionar críticamente sobre el papel que deseamos que la IA juegue en nuestro futuro, no solo como una herramienta o un medio para alcanzar fines específicos, sino también como un actor que podría, en cierta medida, influir o incluso determinar aspectos cruciales de nuestra vida cotidiana y decisiones morales.

Debemos considerar que la mente humana no es un ente aislado o limitado a procesos internos a nivel cerebral. Más bien, debe ser entendida como una entidad ampliada que incluye el cerebro, el cuerpo y el entorno externo. En esta era digital, las herramientas tecnológicas, como los smartphones y las computadoras, se han convertido en extensiones de nuestra cognición.

Estos dispositivos y sistemas no solo mejoran nuestras capacidades para realizar tareas complejas, sino que también transforman la manera en que procesamos la información, tomamos decisiones y interactuamos con nuestro entorno. Esta interacción simbiótica entre el humano y la tecnología redefine los límites de nuestras capacidades cognitivas y plantea preguntas fundamentales sobre la autonomía, la dependencia tecnológica y la evolución de nuestra propia identidad.

En el marco de los recientes avances en inteligencia artificial, la teoría de la mente extendida propuesta por Clark adquiere una relevancia crucial. Según esta teoría, robots y otros sistemas inteligentes deben ser considerados no como entidades aisladas, sino como extensiones funcionales de nuestras propias capacidades cognitivas. Estos sistemas, equipados con herramientas y sensores externos avanzados, no se limitan a amplificar nuestras habilidades humanas; también tienen el potencial de modificar significativamente nuestra percepción y comprensión del mundo que nos rodea.

Esta interacción entre humanos y máquinas plantea preguntas fundamentales sobre la naturaleza de la cognición y la identidad. Al integrar la IA en nuestras actividades diarias, desde la toma de decisiones hasta el análisis de datos complejos, estamos externalizando

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

procesos que tradicionalmente se consideraban exclusivamente humanos. Este fenómeno sugiere una simbiosis emergente entre el ser humano y la tecnología, lo que lleva a una reevaluación de lo que significa ser cognitivamente humano.

Más allá de ser simples herramientas, estos sistemas inteligentes actúan como colaboradores en nuestra interpretación y respuesta al entorno. Esto desafía la idea tradicional de la mente como una entidad cerrada y autosuficiente, proponiendo en su lugar un modelo más dinámico y fluido, donde las fronteras entre la mente humana y la tecnología se vuelven cada vez más borrosas. En este modelo, la cognición se extiende más allá de los límites físicos del cerebro para abarcar los dispositivos y sistemas que utilizamos, indicando una evolución en nuestra forma de procesar información y tomar decisiones.

Este cambio paradigmático conlleva implicaciones profundas, no solo en términos de cómo entendemos la mente y la cognición, sino también en cómo abordamos la relación entre humanos y máquinas. Al reconocer la interdependencia entre la cognición humana y la inteligencia artificial, nos vemos obligados a reconsiderar los límites éticos, legales y sociales de esta interacción, así como a reflexionar sobre el futuro de nuestra coexistencia con estas tecnologías cada vez más integradas en nuestra vida cotidiana.

En este sentido, la incursión de la Inteligencia Artificial (IA) en roles tradicionalmente humanos, especialmente en el análisis legal sobre la inocencia o culpabilidad de individuos, abre un campo de interrogantes éticos y prácticos. Si consideramos un escenario donde una IA, equipada con avanzadas capacidades de análisis y razonamiento legal, es capaz de influir o determinar la responsabilidad penal, nos enfrentamos a un cambio paradigmático en el sistema jurídico. Este desarrollo plantea la cuestión de si un sistema artificial, por más sofisticado que sea, puede entender la complejidad y las sutilezas del derecho, que a menudo implican interpretaciones contextuales y consideraciones morales. Además, ¿cómo podríamos asegurarnos de que estas máquinas estén libres de los sesgos inherentes en los datos con los que han sido entrenadas?

Por otro lado, existe la preocupación de que la participación de la IA en la toma de decisiones legales podría llevar a un distanciamiento de la empatía y la comprensión humana, elementos cruciales en muchos aspectos de la jurisprudencia. Mientras que los algoritmos pueden procesar información con una eficiencia y precisión que supera la capacidad humana, carecen de la capacidad de comprender las emociones humanas y los matices éticos que a menudo son fundamentales en la toma de decisiones judiciales. Este desequilibrio entre la lógica algorítmica y el razonamiento emocional humano plantea la pregunta de cómo se podrían integrar estas dos formas de juicio para alcanzar veredictos justos y equitativos.

La participación de la IA en los procesos judiciales nos lleva a reflexionar sobre el alcance y los límites de su integración en el sistema legal. ¿Cómo podemos garantizar que su uso esté alineado con los principios éticos y los derechos fundamentales? ¿Qué mecanismos de supervisión y revisión podrían implementarse para asegurar que las decisiones tomadas por sistemas de IA sean justas, imparciales y transparentes? Estas preguntas son cruciales en un momento en que la tecnología avanza a un ritmo sin precedentes y su integración en la sociedad se vuelve cada vez más profunda y compleja.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

Esta confluencia de la IA con el derecho y la jurisprudencia exige un debate continuo y multidisciplinario. Juristas, científicos de datos, filósofos, éticos y la sociedad en general deben colaborar para explorar estas cuestiones complejas y desarrollar un marco que equilibre la innovación tecnológica con la integridad moral y legal. Es imperativo que este diálogo sea inclusivo y diverso, considerando una amplia gama de perspectivas y experiencias para comprender plenamente las implicaciones de integrar la IA en nuestro sistema legal. Solo mediante un esfuerzo colectivo y considerado podremos navegar por estas aguas inexploradas y garantizar que la evolución de la IA sirva al bienestar y la justicia para toda la humanidad.

Bibliografía

Amnistía Internacional. (2020, 21 de septiembre). Empresas de la UE venden herramientas de vigilancia a responsables de abusos contra los derechos humanos en China. *Amnistía Internacional*. https://www.amnesty.org/es/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/

APARISI MIRALLES, Á., (2013). El principio de la dignidad humana como fundamento de un bioderecho global. *Cuadernos de Bioética*, XXIV(2), pp. 201-221. https://www.redalyc.org/articulo.oa?id=87528682006

ARBELÁEZ-CAMPILLO, D.F., VILLASMIL ESPINOZA, J.J. y ROJAS-BAHAMÓN, M. J. (2021). Inteligencia artificial y condición humana: ¿Entidades contrapuestas o fuerzas complementarias? *Revista de Ciencias Sociales (Ve),* XXVII (2), pp. 502-513, https://www.redalyc.org/journal/280/28066593034/html/

ARDILA, R. (2011). Inteligencia. ¿qué sabemos y qué nos falta por investigar? *Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales*, 35 (134). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0370-39082011000100009

ASQUERINO LAMPARERO, M. J. (2022, 30 de abril). Algoritmos y Discriminación. *Trabajo, persona, derecho y mercado. Nuevos retos del mercado laboral: Pobreza en el trabajo, economía colaborativa y envejecimiento*. Https://grupo.us.es/iwpr/2022/04/30/algoritmos-y-discriminacion/

AUSÍN, T. (2021). ¿Por qué ética para la Inteligencia Artificial? Lo viejo, lo nuevo y lo espurio. *Sociología y tecnociencia*, 11(Extra_2), pp. 1-16.

BACHELET, M. (2021, 15 de septiembre). Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes. *Naciones Unidas*. https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet

BÉCARES, B. (2023, 2 de mayo). IBM puede llegar a sustituir a casi 8.000 personas por inteligencia artificial. Comienza paralizando las contrataciones. *GENBETA*. https://www.genbeta.com/actualidad/ceo-ibm-dice-que-inteligencia-artificial-podria-reemplazar-a-7-800-sus-trabajadores-empiezan-pausando-contrataciones

BECERRA, M. D. C., ABALLAY, A., ROMAGNANO, M. R., y TORAL SARMIENTO, A. (2021). *Análisis de nuevos problemas éticos y legales al aplicar business intelligence en los sistemas de información organizacionales*. FCEF http://sedici.unlp.edu.ar/bitstream/handle/10915/141295/Documento_completo.pdf-PDFA.pdf?sequence=1

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

BENHAMOU, S. (2022). *La transformación del trabajo y el empleo en la era de la inteligencia artificial: análisis, ejemplos e interrogantes*. CEPAL. https://repositorio.cepal.org/bitstream/handle/11362/47985/S2200188_es.pdf?sequence=1

BOSTROM, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press

CAHUN, A. (2017, 20 Junio). El conductor del Tesla fallecido en accidente con piloto automático ignoró las advertencias del sistema, según el gobierno USA. *Xataka* https://www.xataka.com/automovil/el-fatal-accidente-del-tesla-model-s-con-piloto-automatico-pudo-haberse-evitado-segun-el-gobierno-de-ee-uu

CALLEJA LOPEZ, A., CANCELA, E., y CAMBRONERO GARBAJOSA, M. (2022). *Desplazar los ejes: alternativas tecnologicas, derechos humanos y sociedad civil a principios del siglo XXI*. Universitat Oberta de Catalunya. http://hdl.handle.net/10609/147765

CALVO, R. A., & PETERS, D. (2013). Living with robots: Investigating the habituation effect in participants' preferences during a longitudinal human–robot interaction study. *International Journal of Social Robotics*, 5(2), pp. 173-181.

CAÑIGUERAL, A. (2020). *El trabajo ya no es lo que era: Nuevas formas de trabajar, otras maneras de vivir*. Conecta.

CASADEVALL, J. (2018). *La Directiva de la Unión Europea contra la elusión fiscal*. Aranzadi.

CLARK, A. (1997). *Being There: Putting Brain, Body, and World Together Again*. Bradford Books.

CORVALÁN, J. G. (2018). Inteligencia artificial: retos, desafíos y oportunidades-Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia. *Revista de Investigações Constitucionais*, 5, pp. 295-316.

CROVI DRUETTA. D. (2017). "Prácticas de apropiación e interacción en la cultura digital". En *Teoría, debates y nuevas perspectivas sobre la apropiación de tecnologías digitales* (coord. Martínez, S. L., Méndez, A., y Gendler, M) (pp. 25-32). Ediciones del Gato Gris.

DE LECUONA, I. (2021). Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia. *Revista internacional de pensamiento político*, 15, pp. 139-166.

EMOL. (2022, 11 de octubre). Estudio de NTT DATA refleja que Inteligencia Artificial incrementa la productividad en empresas: Conoce sus ventajas y desafíos. *EMOL*. https://www.emol.com/noticias/Tendencias/2022/10/11/1075238/estudio-de-ntt-data.html

– (2018). *European Group on Ethics in Science and New Technologies*. Ethics of autonomous artificial intelligence.

FLORIDI, L. (2019). *The Logic of Information: A Theory of Philosophy as Conceptual Design*. Oxford University Press.

GOV.CO. (2022, 9 de marzo). Ministerio de tecnologías de la información y las comunicaciones. Colombia adopta de forma temprana recomendaciones de ética en Inteligencia Artificial de la Unesco para la región. GOV.CO. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208109:Colombia-adopta-de-forma-temprana-recomendaciones-de-etica-en-Inteligencia-Artificial-de-la-Unesco-para-la-region

GONZÁLEZ-PÁRAMO, J. M. (2018). *Cuarta revolución industrial, empleo y estado de bienestar.* Ministerio de Justicia. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-M-2018-10008900113

GONZÁLEZ, A. F. (2021, abril). *El procesamiento de textos jurídicos: natural language processing & legal tech*. Universidad Pontificia https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/46784/TFG%20-%20201607852.pdf?sequence=-1&isAllowed=y

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

GONZÁLEZ, M. J. S. (2017). Regulación legal de la robótica y la inteligencia artificial: retos de futuro. *Revista Jurídica de la Universidad de León*, 4(4), pp. 25-50. https://pdfs.semanticscholar.org/ea29/4cbf53fd151134f1d949382dc89d8af120ab.pdf

GRANADOS FERREIRA, J. (2022). Análisis de la inteligencia artificial en las relaciones laborales. *Revista CES Derecho,* 13 (1), pp. 111-132. https://doi.org/10.21615/cesder.6395

GRANERO, H. R. (2020). "Inteligencia Artificial y Justicia Predictiva (¿puede la inteligencia artificial determinar si tengo razón o no en un juicio?)". En *Inteligencia artificial y derecho, un reto social* (coord. Veltani, D. y Lozano, R.). Albremática. http://159.65.240.138/bitstream/handle/uvscl/1261/EBOOK%20Inteligencia%20Artificial%20y%20Derecho%2C%20un%20reto%20social.pdf?sequence=1&isAllowed=y

GROSSO, C. P. (2020) "Apuntes acerca del jurista y las nuevas tecnologías". En *Inteligencia artificial y derecho, un reto social* (coord. Veltani, D. y Lozano, R.). Albremática. http://159.65.240.138/bitstream/handle/uvscl/1261/EBOOK%20Inteligencia%20Artificial%20y%20Derecho%2C%20un%20reto%20social.pdf?sequence=1&isAllowed=y

HABERMAS, J. (2010). El concepto de dignidad humana y la utopía realista de los derechos humanos. *Diánoia*, 55(64), pp. 3-25. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-24502010000100001&lng=es&tlng=es

JOBIN, A., IENCA, M., y VAYENA, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), pp. 389-399.

JOBIN, A., IENCA, M., y VAYENA, E. (2020). Artificial intelligence: The global landscape of ethics guidelines. En *Advanced Multimedia and Ubiquitous Engineering* (eds. Lee, J. H. S., Kim, Y. S., Kim, H. K., Kang, K. C. y Lee J. W.)(pp. 357-365). Springer.

KARDOUDI, O. (2023). Empieza la carnicería: IBM elimina 8.000 trabajos humanos por la inteligencia artificial. *El confidencial*. https://www.elconfidencial.com/tecnologia/novaceno/2023-05-02/ibm-inteligencia-artificial-perdida-trabajos-humanos_3621469/

KOOPS, B. J. (2016). A typology of privacy. *University of Pennsylvania Journal of International Law*, 38(2), pp. 483-575.

LABORDE, A. (2020, 26 de junio). Detenido injustamente un afroamericano en EE UU por un error en el sistema de reconocimiento facial. *El País*. https://elpais.com/tecnologia/2020-06-26/un-afroamericano-es-detenido-injustamente-por-un-error-en-el-sistema-de-reconocimiento-facial.html

LAHERA SÁNCHEZ A. (2019). Digitalización, robotización, trabajo y vida: cartografías, debates y prácticas. *Cuadernos de Relaciones Laborales*, 37(2), pp. 249-273. https://doi.org/10.5209/crla.66037

LIN, P., ABNEY, K., & BEKEY, G. A. (2011). *Robot ethics: The ethical and social implications of robotics*. MIT Press.

LIVE, J. G. (2020) Inteligencia Artificial en Salud. *Revista Innova*, salud digital.

LLINARES, F. M. (2018). Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología*, (20), pp. 87-130.

MÁRQUEZ, B. (2022). Los neodeterminismos jurídicos evolutivos en la tutelación universal de los seres trans-humanos. *UBAIUS*, 11(1), pp. 9-15 https://revistasuba.com/index.php/UBAIUS/article/view/321/217

MARTÍNEZ CRUZ, J. (2020, 13 de julio) Inteligencia artificial debe respetar la dignidad humana. *INFOEM*. https://www.infoem.org.mx/es/contenido/noticias/inteligencia-artificial-debe-respetar-la-dignidad-humana

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

MARTÍNEZ, R., PALMA, A., y VELÁSQUEZ, A. M. (2020). *Revolución tecnológica e inclusión social: reflexiones sobre desafíos y oportunidades para la política social en América Latina*. CEPAL. https://repositorio.cepal.org/bitstream/handle/11362/45901/S2000401_es.pdf

MARTÍNEZ, S. L., MÉNDEZ, A., y GENDLER, M. (2017). "Teoría, debates y nuevas perspectivas sobre la apropiación de tecnologías digitales". En *Contribuciones al estudio de procesos de apropiación de tecnologías*. Ediciones del Gato Gris.

México transparente (mayo de 2023). *Revista digital del sistema nacional de transparencia*, (3) https://www.itei.org.mx/v3/documentos/estudios/mexico_transparente_3_mayo2022_ok.pdf

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2019). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 6(2).

MORÁN ESPINOSA, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *Revista IUS*, 15(48), pp. 289-323. https://doi.org/10.35487/rius.v15i48.2021.706

ORDOÑEZ LEÓN, P. (2021) Derecho a la consulta previa, libre e informada y acceso a la información de los pueblos y comunidades indígenas. *México Transparente Revista digital del sistema nacional de transparencia*, 2, 22. https://snt.org.mx/wp-content/uploads/formado-Mexico-transparente-no.2-diciembre-2021-final.pdf

OVALLE GÓMEZ, C., (2007). La bioética en la concepción, reivindicación y reconocimientos emergentes en los derechos humanos. *Revista Colombiana de Bioética*, 2(2), pp. 247-266. https://www.redalyc.org/articulo.oa?id=189217250011

P. QUIRÓS, J. J. M. (2022). Derechos humanos e inteligencia artificial. *Dikaiosyne: revista semestral de filosofía práctica*, (37), pp. 140-163. http://www.ulpiano.org.ve/revistas/bases/artic/texto/DIKAIOSYNE/37/dikaiosyne_2022_37_139-163.pdf

PARADA SÁNCHEZ, D. A. y DÍAZ LEÓN, I. H. (2021). "La identidad digital como garantía constitucional y un medio para la prevención del delito". En *Tópicos de Política Criminal 2. Ciencia y Tecnología* (coord. Álvarez León J.A.). Universidad Nacional Autónoma de México. http://derecho.posgrado.unam.mx/site_cpd/public/publis_cpd/topicos2_digital.pdf

PASTOR, J. (2023, 3 de mayo). IBM ya ha paralizado sus contrataciones por la IA. El despido de 7.800 trabajadores es el siguiente paso. *Xataka*. https://www.xataka.com/robotica-e-ia/ibm-ha-paralizado-sus-contrataciones-ia-despido-7-800-trabajadores-siguiente-paso

PITA, E. V. (2021). La UNESCO y la gobernanza de la inteligencia artificial en un mundo globalizado. La necesidad de una nueva arquitectura legal. *Anuario de la Facultad de Derecho. Universidad de Extremadura*, (37), pp. 273-302.

PORCELLI, A. M. (2020). La inteligencia artificial y la robótica: sus dilemas sociales, éticos y jurídicos. *Derecho global. Estudios sobre derecho y justicia*, 6(16), pp. 49-105. https://www.scielo.org.mx/scielo.php?pid=S2448-51362020000300049&script=sci_arttext

RAE. (2023). Inteligencia. *Real Academia Española*. https://dle.rae.es/inteligencia#2DxmhCT

RAMOS, R. (2023, 23 de mayo). Urgen a legislar en materia de Inteligencia Artificial en México. *El Economista*. https://www.eleconomista.com.mx/arteseideas/Urgen-a-legislar-en-materia-de-Inteligencia-Artificial-en-Mexico-20230507-0035.html

Red en defensa de los derechos digitales. (2020, 7 de julio). La policía de Detroit admite que su tecnología de reconocimiento facial se equivoca 96% de las veces. *Red en defensa de los derechos digitales*. https://r3d.mx/2020/07/07/la-policia-de-detroit-admite-que-su-tecnologia-de-reconocimiento-facial-se-equivoca-96-de-las-veces/

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

ROBLEDO, D. (2022). Proceso judicial y inteligencia artificial. *Revista Electrónica de Derecho Procesal*, 23(3). https://www.e-publicacoes.uerj.br/index.php/redp/article/viewFile/70391/43567

ROUYET, J.I. (2021, 26 de mayo). Ser éticos con la inteligencia artificial. *ESGLOBAL*. HTTPS://WWW.ESGLOBAL.ORG/SER-ETICOS-CON-LA-INTELIGENCIA-ARTIFICIAL/

RUIZ MARULL, D. (2018) La manipulación en las redes sociales no para de crecer a escala mundial. *La Vanguardia*. https://www.lavanguardia.com/vida/20180720/45977023154/manipulacion-redes-sociales-mundo-politicos.html

RYAN-MOSLEY, T. (2012, 20 de abril). La demanda que podría lograr el fin del reconocimiento facial policial. *MIT technology review*. https://www.technologyreview.es/s/13238/la-demanda-que-podria-lograr-el-fin-del-reconocimiento-facial-policial

SÁNCHEZ MEDERO, G. (2012). Ciberespacio y el crimen organizado. los nuevos desafíos del siglo xxi. Revista Enfoques: Ciencia Política y Administración Pública, X(16), pp. 71-87. https://www.redalyc.org/comocitar.oa?id=96024266004

Senado de la República (2023, 23 de enero). Piden acciones para tratamiento de datos personales derivado del uso de inteligencia artificial. *Senado de la República*. https://comunicacionsocial.senado.gob.mx/informacion/comunicados/4827-piden-acciones-para-tratamiento-de-datos-personales-derivado-del-uso-de-inteligencia-artificial

SOLAR CAYÓN, J. I. (2021). *Reflexiones sobre la aplicación de la inteligencia artificial en la administración de justicia*. Universidad de Cantabria. https://repositorio.unican.es/xmlui/bitstream/handle/10902/24149/ReflexionesSobreLaAplicaci%C3%B3n.pdf?sequence=1

TURÉGANO, I. (2020). Los valores detrás de la privacidad. *Doxa. Cuadernos de Filosofía del Derecho*, 43 https://rua.ua.es/dspace/bitstream/10045/106968/1/Doxa_2020_43_10.pdf

UNESCO. (2019). *Recommendation on the ethics of artificial intelligence*.

UNICEF. (2022, enero) Ciberacoso: Qué es y cómo detenerlo. Lo que los adolescentes quieren saber acerca del ciberacoso. *UNICEF*. https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

VALDÉS, L. F. A., Gómez, G. M., y Limón, J. E. (2022). La tutela judicial efectiva en México. *Prospectiva Jurídica*, 12(23), pp. 105-127.

VALDÉS, M. (2018). La dignidad humana como parámetro de interpretación en fuentes de Derecho Internacional de los Derechos Humanos y Bioética ¿La definición inexistente? Inmanencia. *Revista Del Hospital Interzonal General De Agudos (HIGA)*, 6 (1).

VÉLEZ, M. I., Gómez Santamaría, C., y Osorio Sanabria, M. A. (2022). *Conceptos fundamentales y uso responsable de la inteligencia artificial en el sector público*. Informe 2.

WILSON, A. (2018). *El ascenso de la automatización: la tecnología y los robots reemplazarán a los humanos*. Babelcube Inc.

ZABALA LEAL, T. D., & ZULUAGA ORTIZ, P. A. (2021). Los retos jurídicos de la inteligencia artificial en el derecho en Colombia. *Jurídicas cuc*, 17(1), pp. 475–498. https://doi.org/10.17981/juridcuc.17.1.2021.17

ZINGUER, M. A. (2014). Libertad de expresión y derecho a la información en las redes sociales en Internet. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (12), 5.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 261-287
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.12

RESEÑA DE LIBROS

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

BUENO DE MATA, Federico: *Investigación y prueba de delitos de odio en redes sociales: técnicas OSINT e inteligencia policial*. Tirant lo Blanch, Valencia, 2023, 328 páginas, ISBN: 9788411696197

Celia Carrasco Pérez
Contratada Predoctoral (FPI). Universidad de Burgos
ccperez@ubu.es 0000-0003-0540-3477

Recibido: 24 de noviembre de 2023 | Aceptado: 06 de diciembre de 2023

En una época en la que el derecho requiere de un pensamiento jurídico comprometido con la respuesta a las nuevas necesidades y exigencias que plantea la era digital, se reclama de los juristas una actitud reflexiva, crítica y responsable ante los nuevos problemas que suscita la tecnología. Una especie de consciencia tecnológica que sea capaz de calar en las diferentes generaciones de operadores jurídicos y permita sentar las bases de la apertura del derecho a la tecnología.

En este nuevo marco interdisciplinar que se reclama, destaca la labor del Catedrático de Derecho Procesal de la Universidad de Salamanca, el profesor Federico Bueno de Mata. Cuya andadura en el marco de la investigación y enjuiciamiento procesal, a la vanguardia en la implementación tecnológica al proceso penal, se consagra en este año 2023 a partir de la publicación de su última monografía *Investigación y Prueba de Delitos de Odio en Redes Sociales: técnicas OSINT e inteligencia policial* en la editorial Tirant lo Blanch.

La obra que en estas páginas se presenta, parte de una problemática real: nuestro estilo de vida fomenta un ambiente propicio para las manifestaciones basadas en el odio y la intolerancia. Una actitud que se ha visto favorecida por la expansión de las redes sociales, donde fácilmente se puede difundir contenido violento, ofensivo y discriminatorio, dificultando a su vez el control, investigación y enjuiciamiento de estas conductas que sobrepasan la libertad de expresión.

El papel que juegan las nuevas tecnologías en la comisión de este tipo de comportamientos hace que la respuesta frente a los mismos requiera de instituciones procesales adecuadas que puedan ofrecer una respuesta completa, desde la investigación tecnológica de la comisión de estos hechos en redes abiertas o cerradas, hasta el posterior tratamiento de las pruebas obtenidas.

A lo largo de tres capítulos, se afronta el desafío que debe asumir el Derecho Procesal como un derecho de garantías, necesario para proteger los derechos y libertades fundamentales de

los ciudadanos en el espacio cibernético. Se proporciona un completo y riguroso estudio interdisciplinar, bajo un marcado carácter tecnológico a partir de tres premisas que sirven de introducción a la obra: la actividad delictiva relacionada con el odio va en claro aumento; los casos que mayor incidencia presentan, son justamente los cometidos a través de redes sociales; y la existencia de una clara percepción de que es necesaria una mejora en el tratamiento procesal de los delitos de odio en redes sociales desde una triple perspectiva: victimológica, investigativa y probatoria.

La presente monografía, aborda de manera práctica y precisa un auténtico desafío para la ciencia procesal, como es la incorporación de las técnicas de inteligencia en la búsqueda y obtención de fuentes de datos a través de fuentes y canales abiertos. Un reto para el autor, que consideramos superado dada la ausencia de doctrina específica en la materia.

El estudio se divide en tres capítulos interrelacionados entre sí, en el que la técnica OSINT, se presenta como una herramienta fundamental en la localización de discurso de odio en las redes sociales.

De esta forma, trataremos de exponer las principales ideas que desarrolla el autor a lo largo de más de 300 páginas de estudio, que convierten esta obra en una valiosa fuente bibliográfica para la ciencia procesal.

I. El primer capítulo titulado *Inteligencia, proceso penal y delitos de odio en redes sociales: especial referencia a la investigación en fuentes abiertas,* le sirve al autor para contextualizar el fenómeno de la sociedad en red ligada a la tecnología, origen de los delitos de odio en Internet. Claro ejemplo de cómo la constante generación de información en Internet puede tener efectos negativos en la sociedad. Y es que la ubicuidad intrínseca a las conductas que constituyen los delitos de odio requiere de acciones de investigación concretas que permitan determinar al autor y proceder a enjuiciar los hechos. Para el autor, dicho cometido parte de un contenido generado en redes sociales, que se podría denominar información electrónica. Es en este momento, en el que se plantea el tratamiento más adecuado que se debe otorgar a esta información, de cara a su aplicabilidad como prueba en un plano jurídico.

En este sentido, el análisis de la información facilitaría la identificación de patrones con importantes implicaciones de cara a un proceso penal. Sin embargo, muy acertadamente, considera necesario diferenciar en el proceso de conformación de pruebas a partir de información contenida en medios tecnológicos, entre información e inteligencia. Una diferencia conceptual clave que apoya toda la argumentación que prosigue la monografía. La inteligencia como generador de conocimiento, el cual, alimentado de información, sirva al proceso como una valiosa fuente de prueba. Esta premisa, le sirve al autor para abordar la aplicación de técnicas de inteligencia en la investigación de delitos de odio en la era de la sociedad en red. Lo que le lleva a situar el ciclo de la inteligencia en el centro del proceso penal cuya finalidad sea la de lograr una prueba que, generada a través de la aplicación de técnicas de inteligencia sirva para enervar la presunción de inocencia.

De esta forma diferencia de un lado la inteligencia criminal, y de otro, la inteligencia de fuentes abiertas. Dentro de esta última se inserta OSINT como modelo de inteligencia idóneo para investigar delitos de odio en redes sociales.

La inteligencia criminal se caracterizaría, por tener un carácter preventivo que poco encajaría en la investigación de los delitos de odio por cuanto la línea que sigue conforma una finalidad preventiva. La inteligencia de fuentes es el tipo de inteligencia que para el autor se presenta como idónea para el proceso penal por delitos de odio. La metodología electrónica de este tipo de tecnología lleva al autor a asentar el concreto estudio de la técnica de inteligencia OSINT, que, pese a sus limitaciones legales, facilita la investigación en las redes sociales abiertas del investigado.

El planteamiento que se propone en este primer capítulo de la técnica OSINT, se basa en abordar su origen y fundamentos, así como su componente principal: los datos, recopilados en espacios virtuales abiertos. OSINT ejemplifica un modelo de inteligencia adaptado a la realidad tecnológica, en el que los datos abiertos marcan una nueva línea para investigar hechos delictivos por odio. El estudio de los datos es fundamental para el autor, quien centra su enfoque en las redes sociales. Un espacio en el que contar con técnicas especificas se vuelve fundamental. Es por ello por lo que se ofrece el análisis de SOCMINT como variante de OSINT, en tanto analiza el método por el cual, mediante esta técnica, es posible la recopilación de datos en redes sociales, en calidad de fuentes accesibles, cuyo análisis conformarían un factor de polarización radical de la comisión de delitos de odio. Armonizando así una herramienta fundamental en la localización del discurso de odio en las redes sociales.

II. Las redes sociales se convierten en el medio ideal de comisión de delitos de odio, lo que inevitablemente lleva al debate de las técnicas de investigación más adecuadas para afrontar el desafío del odio en línea en fase de instrucción. El segundo capítulo, titulado *Las técnicas OSINT como diligencias para la investigación de delitos de odio en redes sociales*, parte de una idea que consideramos fundamental: la expectativa de privacidad. La presente monografía, se presenta como una propuesta innovadora y clave en el reto investigativo del delito de odio cometido por redes sociales de una manera concreta, pero también respecto de las diligencias de investigación tecnológica. La recopilación de información en el marco de la investigación del delito de odio es fundamental, sobre todo desde el momento en el que estos datos pueden obtenerse de las redes sociales. Como acertadamente señala el autor a lo largo de la obra, apenas se conocen estudios doctrinales en la materia, de ahí la importancia del estudio que ofrece el profesor Bueno de Mata.

¿Debería tener control judicial la obtención de datos a través de fuentes y canales abiertos? ¿Hay divergencia entre lo que se considera dato abierto y la funcionalidad de este?

El autor, ofrece un riguroso examen procesal de la inteligencia de fuentes abiertas como técnica aplicada a la investigación en un proceso penal, por cuanto el carácter extensivo y abierto de las redes sociales condiciona las herramientas de investigación criminal. En este sentido, las técnicas OSINT vienen a materializar, desde el punto de vista de las fuentes abiertas, la mejor o más adecuada forma de configurar inteligen-

temente el dato para producir una prueba. El autor retoma la inteligencia de fuentes para conformar el tratamiento procesal de las técnicas OSINT, poniendo su énfasis, de manera acertada, en la diferenciación entre fuente abierta y fuente accesible, y el correspondiente dato accesible y dato abierto, planteando la posibilidad del uso de técnicas OSINT sobre fuentes accesibles, esto es sobre aquellas fuentes en las que hay una expectativa de privacidad frente a las fuentes abiertas, en las que no tiene por qué.

Uno de los desafíos principales que aborda el autor respecto de estas técnicas, es la posible vulneración de los derechos fundamentales en la obtención del dato electrónico. Para tal cuestión, se plantea desde el punto de vista del marco regulatorio, si la técnica OSINT es una diligencia de investigación tecnológica que, como tal, requiera de autorización judicial para romper la expectativa de privacidad y obtener así el dato electrónico como prueba valida. El tratamiento procesal de esta tan innovadora técnica de investigación presenta desafíos que son abordados por el autor, pues ciertamente la recopilación de datos electrónicos puede afectar a derechos fundamentales, hecho que dependerá de la capa de Internet en la que se encuentren estos datos.

De tal manera que este segundo capítulo, presenta una metodología que parte de analizar el marco legal aplicable en la obtención de datos electrónicos en redes sociales para la investigación de delitos de odio. Examinando a su vez, los posibles derechos fundamentales que pueden lesionarse según el tipo de dato que se pretenda obtener. De ahí, la importancia que cobra para el autor la diferenciación entre datos electrónicos abiertos y accesibles, vinculados a cuentas en redes sociales abiertas y cerradas del investigado.

Junto a ello se plantean los presupuestos procesales que deberán tenerse en cuenta, así como el cumplimiento de los principios procesales que actuarán como límite a la actuación práctica.

Son analizadas de una manera rigurosa, las diferentes medidas para la obtención de los datos electrónicos en redes sociales por medio de técnicas OSINT. De un lado aquellas medidas, que, sin ser consideradas diligencias de investigación con amparo en la LECrim, podrán ser usadas para canales abiertos en los que no se necesite autorización judicial: el ciberpatrullaje, o las cuentas títere. De otro, aquellas medidas que encajarían en canales virtuales cerrados: interceptación de comunicaciones y el registro de repositorios telemáticos de datos alojados en la nube. A lo que se añade el estudio de figuras concretas, aplicadas a contenido de odio en redes sociales como la herramienta del agente encubierto o el uso de virus espía. Figuras clave sobre las que, de manera posterior, se puedan aplicar técnicas de inteligencia y configurar así una verdadera prueba de delitos vinculados a odio.

III. Finaliza la obra con el tercero de los capítulos titulado *Prueba de inteligencia policial y delitos de odio en redes sociales***.** En este capítulo el autor se desliga de los anteriores, al pasar del ámbito de la investigación, al desafío que supone desde una óptica procesal la construcción probatoria de los delitos de odio en Internet. Abordar los delitos de odio, requiere de una especial atención a la motivación e intencionalidad que hay detrás de la conducta delictiva. En concreto, la particularidad del delito de odio recae en demostrar que el delito fue motivado por el odio o la discriminación contra un

grupo específico o uno de sus miembros. Sin duda requiere de un enfoque subjetivo que debe contar con las herramientas y garantías procesales adecuadas.

El desarrollo del capítulo se centra concretamente en la prueba de inteligencia policial, para la que el autor propone una teoría general en base a la falta de tratamiento procesal de esta figura. La lectura y estudio de este capítulo termina por corroborar la excelente técnica procesal del profesor Bueno de Mata. Una particular habilidad que ha dejado ver a lo largo de la obra que se presenta, por la que ha dirigido la política jurídica en reglas claras de aplicación tecnológica, ante un derecho penal sustantivo tan complejo como es la concreción de una conducta de odio en un comportamiento típico, antijurídico y culpable en sede procesal.

Hasta el momento, el autor no se había centrado específicamente en determinar la validez probatoria del contenido de los datos recabados, sin embargo, el último de los capítulos resuelve el desafío de la prueba de los delitos de odio en las redes sociales centrado en: la intención y la motivación. El autor parte de los indicadores de polarización radical para probar estas dos facetas detrás del delito de odio, que pese a conformarse como una institución que no cuenta con un reconocimiento legal y jurisprudencial expreso, permite articularse como prueba indiciaria. Se propone un verdadero análisis del tratamiento del delito de odio en Internet, por cuanto la prueba de la motivación e intencionalidad que subyace en los delitos de odio debe revestirse de las garantías propias del Estado de Derecho.

En este sentido, los denominados factores de polarización radical son analizados como parámetros indiciarios que sirvan a la construcción probatoria del odio. La figura de la prueba de inteligencia policial se plantea desde su construcción mediante la prueba de indicios, pero ¿una prueba de inteligencia construida por indicios debe tener el valor de prueba indiciaria? Esta es la pregunta base que da forma al último de los capítulos.

A partir de lo que plantea la Circular 7/2019, de 14 de mayo, de la Fiscalía General del Estado sobre pautas para interpretar los delitos de odio, tipificados en el artículo 510 del Código Penal, se proyecta la utilidad probatoria asociada a la prueba pericial de inteligencia. Manteniéndose crítico respecto de los indicadores de polarización propuestos por la Fiscalía General española, propone otros tantos, concretamente aplicables en el análisis de las redes sociales abiertas del investigado, bajo la denominación de "Decálogo de indicadores de polarización de las redes sociales abiertas", entre los que se incluye el análisis de los algoritmos de recomendación asociados al perfil o en análisis de hashtags.

El autor, Catedrático de Derecho Procesal, apuesta por la prueba de inteligencia policial y la virtualidad probatoria que de la misma se desprende. La metodología de esta debe reunir un proceso de evaluación, de análisis de la información. Para lo que se deberán utilizar técnicas de inteligencia. Aspecto clave por cuanto la diferenciarían de las simples diligencias de investigación; y es que la complejidad de este tipo de delitos junto al contexto tecnológico requiere de herramientas útiles, las cuales deben ser empleadas por especialistas en inteligencia. Un planteamiento que logra relacionar los delitos de odio, con el uso de inteligencia en la investigación y prueba de estos en el marco de un contexto cada vez más tecnológico.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 289 -294
ISSN 2444-8478

Nos encontramos ante una obra de máxima actualidad, de carácter crítico y reflexivo, con numerosas indicaciones prácticas, fruto del trabajo del Catedrático de Derecho Procesal Federico Bueno de Mata. La obra *Investigación y prueba de delitos de odio en redes sociales: técnicas OSINT e inteligencia policial* se presenta como lectura obligada para los incipientes y ya aventajados estudiosos de la ciencia procesal, así como para autoridades policiales y judiciales, por cuanto se ofrecen desde una vertiente humanista, líneas clave en la implementación de herramientas tecnológicas de investigación al proceso penal, que permitan en este concreto ámbito, atajar el odio tecnológico.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 289 -294
ISSN 2444-8478

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

PÉREZ ESTRADA, Miren Josune: *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*. Tirant lo Blanch, Valencia, 2022. ISBN: 978-84-1113-761-4

Francisco Javier Fernández Galarreta
Profesor Doctor del Área de Derecho Procesal
Universidad del País Vasco. UPV/EHU
franciscojavier.fernandez@ehu.eus 0000-0001-7402-4863

Recibido: 27 de noviembre de 2023 | Aceptado: 06 de diciembre de 2023

La transformación digital y la incorporación de tecnologías avanzadas de Inteligencia Artificial (IA) en el ámbito de la Administración de Justicia es ya un hecho. Los últimos avances tecnológicos han llegado para quedarse y para provocar una profunda transformación, no sólo en la Administración de Justicia, sino también en el conjunto de nuestra sociedad. En este contexto, la obra, que en estas líneas reseñamos, aborda de manera valiente el estudio del impacto del uso de estas nuevas tecnologías en distintos ámbitos de la administración de justicia. La obra es fruto de diferentes proyectos de investigación nacionales en los que ha colaborado de manera activa, así como consecuencia de su trayectoria profesional.

En lo que respecta a la estructura de la obra, cabe señalar que la misma está dividida en cinco partes, en las que de manera sucesiva y coherente va analizando los distintos aspectos fundamentales de la IA y la repercusión que ésta puede llegar a tener sobre las garantías del proceso, afectando a derechos tan fundamentales como el de la tutela judicial efectiva.

Así, en la primera parte, aborda una aproximación al concepto de IA y al funcionamiento de los distintos sistemas de IA en el campo de la administración de justicia, como son los sistemas de aprendizaje automático, los sistemas de aprendizaje profundo y el uso de los *Big Data* al servicio de dichos sistemas algorítmicos.

La segunda parte, acomete el estudio concreto de los distintos sistemas de IA aplicables al ámbito de la justicia, como es el caso de los llamados Sistemas Jurídicos Expertos. En este sentido, nos recuerda la autora que la digitalización y la algoritmización de la justicia adopta muchas formas, como es el uso de herramientas de IA en la predicción de decisiones judiciales y en la

ayuda de resolución de conflictos, a través de algoritmos de aprendizaje automático, aprendizaje profundo, redes neuronales y robótica inteligente.

La tercera parte, aborda el análisis de las experiencias del uso de diferentes sistemas y aplicaciones de la IA en el Derecho Comparado, así como su implementación por parte de los distintos operadores jurídicos al cargo de la administración de justicia en los países analizados.

La cuarta parte, realiza un estudio sobre la implementación de estos sistemas de IA en el ámbito jurisdiccional, como es el caso de la automatización de los procesos judiciales y la repercusión que dicha implementación puede llegar a tener en la configuración de las oficinas judiciales y en la tramitación de los distintos expedientes judiciales. Analiza, por ejemplo, el impacto de las aplicaciones de la inteligencia artificial en la estructura de la oficina judicial. Estudia los desafíos a los que se enfrenta la misma, con motivo de la digitalización de archivos jurídicos y actos procesales, así como con la toma de decisiones automatizadas, consecuencia del cambio de un modelo de tramitación guiada a un modelo de tramitación automatizada. Asimismo, analiza distintas tecnologías directamente aplicables en el proceso judicial, como son las tecnologías de reconocimiento facial y las tecnologías de procesamiento de lenguaje. Finalmente, el capítulo aborda el estudio del marco normativo a nivel nacional y comunitario de la IA, el cual, deviene necesario para garantizar una incorporación correcta de este tipo de aplicaciones, evitando que las mismas puedan llegar a suponer una merma de las garantías procesales de los justiciables.

La quinta, y última parte, nos presenta los efectos y los posibles riesgos a los que estamos expuestos con motivo de la incorporación de la IA en el proceso judicial, haciendo hincapié en la afectación que se deriva de su uso en derechos fundamentales tan importantes como: el derecho a la protección de datos de carácter personal, el derecho a la garantía de imparcialidad judicial, el derecho de defensa, entendido como el derecho a un proceso debido y sin indefensión. En definitiva, la autora nos avanza los desafíos a los que se enfrenta la administración de justicia con motivo de la incorporación de la IA. Asimismo, finaliza esta quinta parte realizando una serie de recomendaciones y proponiendo la necesidad de establecer una serie de principios rectores que rijan el uso de la IA en el ejercicio de la actividad jurisdiccional.

Para cerrar la obra termina realizando una serie de conclusiones respecto de los temas abordados a lo largo de misma.

En la elaboración de la obra se lleva a cabo un amplio y exhaustivo análisis de las monografías doctrinales más relevantes en este campo, y de diversos artículos especializados, publicados en revistas nacionales e internacionales relacionados con el tema objeto de estudio. Todo ello, partiendo de las publicaciones más recientes que analizan todas las cuestiones relacionadas con la incorporación de las nuevas tecnologías en la administración de justicia, así como aquellas dedicadas al análisis de las últimas modificaciones operadas con motivo de la irrupción de las nuevas tecnologías y de la implantación de la inteligencia artificial en los distintos ámbitos de la justicia. Por lo tanto, la obra recoge una extensa y actualizada bibliografía, haciendo referencia a la doctrina

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 295 -297
ISSN 2444-8478

más reputada en este campo, lo cual es un claro ejemplo del rigor científico con el que la obra ha sido abordada.

Amén de la metodología ya mencionada, y toda vez que el objeto de la obra está estrechamente relacionado con la práctica forense, la autora ha incorporado conocimientos de primera mano, de su anterior condición de operadora jurídica, como Juez de provisión temporal y como Letrada de la administración de Justicia.

El tema que se desarrolla además de estar de constante actualidad con motivo de los avances de la ciencia la autora lo aborda con rigor y sistemática, pero sin alejarse del contexto en el que debe aplicarse, el ámbito jurisdiccional. Creemos que, por su actual temática y, en especial, por su tratamiento, la obra puede ser de enorme interés para el lector.

En definitiva, se trata de una obra valiente, bien redactada, y con una estructura lógica y coherente, que facilita mucho su lectura y comprensión. No sólo realiza una exposición clara de los problemas que enfrenta la Administración de Justicia con motivo de la incorporación de la IA sino que presenta una serie de propuestas claras para resolver dichos desafíos, dotando, de ese modo, de consistencia a la obra.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 295 -297
ISSN 2444-8478