II

2023 N.º 140

cuadernos de política criminal

segunda época

Dykinson, S.L.

II

2023 N.º 140

cuadernos de política criminal

segunda época

Edita

Dykinson, S.L.

AVISO IMPORTANTE A NUESTROS SUSCRIPTORES

Si desea suscribirse a **Cuadernos de Política Criminal**, llame por teléfono o envíe un e-mail a info@dykinson.com, indicando la forma de pago y el número o números a los que quiere suscribirse, e inmediatamente recibirá su pedido.

CPC se adhiere a las Core Practices del Committee on Publication Ethics (COPE) disponibles en: *https://publicationethics.org/core-practices*; y especialmente a los *Principios de Buenas Prácticas y Transparencia en las Publicaciones Académicas* desarrollados por el Committee on Publication Ethics (COPE), Open Access Scholarly Publishers Association (OASPA), Directory of Open Access Journals (DOAJ) y World Association of Medical Editors (WAME) disponibles en: *https://publicationethics.org/ resources/guidelines-new/principles-transparency-and-best-practice-scholarly-publishing*. La Declaración de ética y malas prácticas completa de CPC puede ser consultada en sus versiones en español e inglés: *https://www.dykinson.com/revistas/cuadernos-de-politica-criminal/*

La Revista no se responsabiliza de las opiniones contenidas en los artículos

Edita: Dykinson, S.L.
C/ Meléndez Valdés, 61 — 28015 Madrid
Tels. 91 544 28 46 / 91 544 28 69
Fax 91 544 60 40
info@dykinson.com / www.dykinson.com

Imprime: Safekat, S. L.
Laguna del Marquesado, 32 - 28021 Madrid
www.safekat.com

ISSN: 0210-4059
Depósito Legal: M. 7533-1977
DOI: 10.14679/2247

CONTENIDO

SECCIÓN ESTUDIOS CRIMINOLÓGICOS

NUEVAS FORMAS DE FINANCIACIÓN DEL TERRORISMO. RETOS Y SOLUCIONES PARA COMBATIRLA UTILIZANDO SISTEMAS INTELIGENTES

New forms of terrorist financing. Challenges and solutions to combat it using intelligent systems[*]

JAVIER VALLS PRIETO**

Fecha de aceptación: 22/06/2023
Fecha de aprobación: 06/09/2023

DOI: 10.14679/2252

RESUMEN: Los grupos terroristas han adaptado sus formas de actuación a las nuevas tecnologías emergentes. Esto ha supuesto cambios no solo en las formas de comisión de sus delitos, sino también en sus formas de financiación. Se ha observado que el terrorismo también está utilizando criptomonedas para su financiación debido a sus características para proteger la identidad y su alcance global. Por todo ello, las nuevas formas de financiación del terrorismo suponen un reto para las autoridades ya que dificultan su detección y su persecución. Se requieren de herramientas tecnológicas que les permitan aumentar sus capacidades

* Este artículo es fruto del proyecto de investigación "La gobernanza de la inteligencia artificial (GOIA) TED2021-129402B-C22 financiado por Ministerio de Ciencia e Innovación.

** Profesor Titular. Universidad de Granada (España).

en la investigación y lucha contra este fenómeno y situarles al mismo nivel operativo que los grupos terroristas. El objetivo de este trabajo ha sido analizar si sería posible en esta situación la aplicación de los sistemas inteligentes en la lucha contra la financiación del terrorismo. Para ello, se realizó un acercamiento jurídico y criminológico a esta materia mediante la revisión de las directivas y los informes policiales pertinentes. Una vez analizada la cuestión, los resultados mostraron que la financiación del terrorismo es mayormente digital, por lo que el empleo de herramientas basadas en inteligencia artificial sería de utilidad para resolver estos problemas. Estas pueden ayudar a igualar las capacidades de las Fuerzas y Cuerpos de Seguridad del Estado a las nuevas exigencias de la lucha contra el terrorismo. No obstante, hay que señalar que no se dispone de un marco jurídico en materia de seguridad en lo que se refiere a la utilización de sistemas inteligentes. Por lo tanto, será necesario considerar un uso ético de la inteligencia artificial a través de una serie de criterios que respeten los derechos humanos.

PALABRAS CLAVE: Terrorismo, financiación, criptomonedas, derechos humanos, Inteligencia Artificial.

ABSTRACT: Terrorists have adapted their methods to new and emerging technologies. This has meant changes not only in the ways in which they commit their crimes, but also in their forms of financing. It has been observed that terrorism is also using cryptocurrencies for its financing due to their identity protection features and their global reach. Therefore, new forms of terrorist financing challenge authorities as they make it difficult to detect and prosecute. Technological tools are required to increase their capacity to investigate and combat this phenomenon and to place them at the same operational level as terrorist groups. The aim of this research has been to analyse whether the application of intelligent systems in the fight against terrorist financing would be possible in this situation. To this end, a legal and criminological approach to this issue was carried out by reviewing the relevant directives and police reports. Once the issue was analysed, the results showed that terrorist financing is largely digital, so the use of tools based on artificial intelligence would be useful to solve these problems. These can help to match the capabilities of law enforcement agencies to the new requirements of the fight against terrorism. However, it should be noted that there is no legal security framework for the use of intelligent systems. It will therefore be necessary to consider an ethical use of artificial intelligence through a set of criteria that respect human rights.

KEYWORDS: Terrorism, financing, cryptocurrencies, human rights, Artificial Intelligence.

ciación contra el terrorismo. III. El uso de la inteligencia artificial para combatir el terrorismo. IV. La utilización de criptomonedas como sistema de financiación. V. Cómo combatir el terrorismo y su financiación. VI. Problemas relacionados con el uso de la inteligencia artificial para luchar contra la financiación de grupos terroristas. VII. Conclusiones.

I. INTRODUCCIÓN

La flexibilidad y la facilidad con la que los grupos terroristas adaptan sus actuaciones a los nuevos objetivos suponen un reto en la lucha contra esta lacra. Con carácter internacional, el terrorismo utiliza la estructura y los métodos de gestión que emplean las corporaciones internacionales adaptadas a las nuevas tecnologías. Surge así un terrorismo descentralizado cuya persecución resulta compleja empleando únicamente las herramientas que de forma tradicional se han venido utilizando por las Fuerzas y Cuerpos de Seguridad del Estado.

La lucha contra el terrorismo actual plantea diversos retos que lo convierte en un fenómeno de especial complejidad. El primero de ellos, es la dificultad para establecer una única definición de terrorismo, que se ve afectada por un continuo cambio en los objetivos políticos, por el Estado que ayuda en las actividades que van a realizar o por sus diferentes formas de financiación, entre otras cosas por la hiperactividad de las instituciones internacionales y nacionales a la hora de crear instrumentos jurídicos para establecer una política de consenso a nivel internacional. Para los fines de este artículo, vamos a considerar terrorismo a los "actos de violencia dirigidos contra la población civil con fines políticos o ideológicos"[1].

Aun tomando está postura, no podemos no entrar en otras definiciones de importancia. Así, la Asamblea General de Naciones Unidas planeta un concepto de Derecho internacional de terrorismo considerándolo como actos criminales destinados o calculados para provocar un estado de terror en la población en general, en un grupo de personas o en personas determinadas con fines políticos[2]. El Consejo de Seguridad de Naciones Unidas, tras el atentado terrorista del 11 de septiembre de 2001, elaboró una nueva definición de terrorismo en la que señaló que los actos criminales podrían ser dirigidos también contra civiles, con la

[1] ACNUDH (2008). *Los Derechos Humanos, el Terrorismo y la Lucha contra el Terrorismo*. Naciones Unidas, p. 5.

[2] GENERAL ASSEMBLY (1995). 49/60. *Measures to eliminate international terrorism* [artículo en línea]. United Nations, p. 4. *https://documents-dds-ny.un.org/doc/UNDOC/GEN/N95/768/22/PDF/N9576822.pdf?OpenElement*

intención de causar la muerte o lesiones corporales graves o la toma de rehenes con el propósito de provocar un estado de terror en el público en general o en un grupo de personas o personas particulares, intimidar a una población u obligar a un Gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo[3].

Fuera de Naciones Unidas no podemos olvidar que la definición más actual la proporciona la OTAN y define el terrorismo como el uso ilegal o la amenaza de uso de la fuerza o la violencia, infundiendo miedo y terror, contra personas o bienes en un intento de coaccionar o intimidar a gobiernos o sociedades, o de obtener el control sobre una población, para lograr objetivos políticos, religiosos o ideológicos[4].

Dentro del marco de la Unión Europea también se ha realizado un esfuerzo considerable para establecer qué se considera como terrorismo. La Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre lucha contra el terrorismo, fue pionera en la lucha contra el terrorismo, definió como grupo terrorista a un grupo estructurado de más de dos personas establecido durante un periodo de tiempo y que actúa de forma concertada para cometer delitos de terrorismo. Esta definición de mantiene en la actual Directiva (UE) 2017/541[5] que, además, define como "organización estructurada" a una "organización no formada fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se ha asignado a sus miembros funciones formalmente definidas ni hay continuidad en la condición de miembro o una estructura desarrollada"[6].

Finalmente podemos recurrir a las definiciones aportadas por la literatura científica, como la elaborada por Fortna, Lotito y Rubin que consideran el terrorismo como el uso sistemático de la violencia intencionadamente indiscriminada contra objetivos civiles públicos (…) para enviar un mensaje político a un público más amplio[7]. Otros como Cronin, en lugar de aportar una definición han señalado cuáles serían los elementos clave del terroris-

[3] SECURITY COUNCIL (2004). *Resolution 1566 (2004) / adopted by the Security Council at its 5053rd meeting, on 8 October 2004* [artículo en línea]. United Nations, p. 2. *https://digitallibrary.un.org/record/532676?ln=en*

[4] NORTH ATLANTIC TREATY ORGANIZATION (2021). *AAP-06. NATO Glossary of Terms and Definitions*, p. 130.

[5] 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* (31 de marzo de 2017), L 88, pp. 1-32.

[6] Ibid, p.12

[7] PAGE FORTNA, V; J. LOTITO, N. and A. RUBIN, M. (2018). "Don't Bite the Hand that Feeds: Rebels Funding Sources and the Use of Terrorism in Civil Wars". *International Studies Quarterly*. Vol. 62, núm.4, pp. 782-794.

mo como su carácter político, el uso de la violencia de carácter no estatal y su ataque deliberado contra inocentes. Por último, los grupos terroristas no están sometidos al cumplimiento de leyes o normas internacionales en sus actividades y eso es para maximizar el efecto psicológico del ataque[8].

Por otro lado, otro de los retos de la lucha contra el terrorismo ha sido la adaptación de los grupos terroristas a la utilización de las nuevas tecnologías en la preparación y desarrollo de sus actividades delictivas. Esto ha quedado demostrado con la aparición del ciberterrorismo, que consiste en el ataque contra redes informáticas –en su mayoría infraestructuras estatales–, con una motivación política, religiosa o ideológica[9].

Todo ello nos indica que una comprensión total del terrorismo en el siglo XXI requiere de una consideración amplia de su *modus operandi* que incluya las redes informáticas como herramienta para facilitar sus actividades o para atentar contra ellas. Así, se ha observado que redes sociales encriptadas como Telegram, WhatsApp y Facebook se utilizan para captar nuevos miembros en los grupos terroristas, así como para establecer contactos entre diferentes grupos y difundir propaganda con un alto alcance y bajo coste[10].

El Informe de la Unión Europea sobre Situaciones y Tendencias Terroristas (TESAT)[11] señala que la propaganda en línea y la creación de redes a través de las redes sociales siguen siendo esenciales para los intentos terroristas de llegar al público de la Unión Europea con el objetivo de reclutamiento, la radicalización y la recaudación de fondos.

La financiación de terrorismo se presenta como uno de los ámbitos de este fenómeno en el que han tenido especial relevancia la inclusión de las nuevas tecnologías. Existe cierta tendencia a utilizar campañas de recaudación de fondos mediante *crowdfunding* y financiarse a través de la comisión de delitos económicos. Pero al mismo tiempo, también ha adquirido importancia la financiación a través de criptomonedas como el

---

[8] CRONIN, A. K. (2002). "Behind the curve: globalization and international terrorism". *International Security*. Vol. 27, núm. 3, p. 30–58.

[9] CLOUGH, J. (2012). *Principles of Cybercrime*. 2ª ed. Victoria: Cambridge University Press.

[10] EUROPOL (2022). *Internet Organized Crime Threat Assessment 2019 (IOCTA)* [informe en línea]. European Union Agency for Law Enforcement Cooperation [Fecha de consulta: 9 de noviembre de 2019]. *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019*

[11] EUROPOL (2022). *European Union Terrorism Situation and Trend Report 2022 (TE-SAT)* [informe en línea]. European Union Agency for Law Enforcement Cooperation [Fecha de consulta: 2 de junio de 2023]. *https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf*

Bitcoin debido a sus características como la facilidad de acceso, el anonimato, la seguridad de las transacciones, el bajo coste y la alta velocidad de las transferencias internacionales. Esto ha dificultado la persecución de la actividad delictiva, siendo uno de los grandes retos a los que se enfrentan las Fuerzas y Cuerpos de Seguridad del Estado.

El estudio de las formas de financiación del terrorismo se ha convertido en un aspecto clave para tener en cuenta en la lucha contra este fenómeno como veremos más adelante. La nueva estrategia de intercambio de información entre instituciones y la libre circulación de capitales en todo el mundo permiten la obtención de pruebas económicas que permita la detección y persecución de los grupos terroristas, principalmente cuando estas tienen un formato digital. La orden europea de investigación, establecida por la 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, ha proporcionado un nuevo sistema de cooperación en materia de persecución penal que permite solicitar pruebas a otros Estados miembros basándose en la confianza entre ellos, acelerando de esta forma el intercambio de información relevante para las investigaciones penales. De esta forma, el intercambio de información financiera y económica se convierte en un factor clave en la lucha contra el terrorismo, dada la facilidad de recopilación de pruebas y de su cesión a los países donde se realizan la investigación.

Uno de los escollos a superar en este tipo de investigaciones es que las estrategias de persecución y lucha contra el terrorismo han de desarrollarse al mismo nivel que los avances realizados por los grupos terroristas. Por eso, el último de los retos que se señala en este trabajo para la lucha contra el terrorismo es la dotación a las Fuerzas y Cuerpos de Seguridad del Estado de las herramientas necesarias para perseguir este fenómeno criminal. En este sentido, se considera que la inteligencia artificial, que ha demostrado ser muy beneficiosa en diversas áreas, sería de gran utilidad también en la persecución de los grupos terroristas. El uso de estas herramientas permitiría a las Fuerzas y Cuerpos de Seguridad del Estado la elaboración de nuevas técnicas de investigación en dos aspectos que se consideran clave en la lucha contra el terrorismo como son la vigilancia y el seguimiento del dinero.

Sin embargo, su utilización deberá respetar los derechos fundamentales presentes en una sociedad democrática. La utilización de la vigilancia y el seguimiento masivo de transacciones financieras puede poner en peligro estos derechos, principalmente la intimidad y privacidad de los ciudadanos, por lo que el reto sería conseguir un sistema de legitimación internacional de esta tecnología utilizada por los servicios de inteligencias y las Fuerzas y Cuerpos de Seguridad del Estado.

Por todo ello, el objetivo de este trabajo es analizar si sería posible la utilización de los sistemas inteligentes en la lucha contra la financiación del terrorismo, determinando dónde habría que establecer el equilibrio entre los derechos a la libertad y la seguridad de los ciudadanos.

II. FINANCIACIÓN DEL TERRORISMO

Un factor clave en la lucha contra el terrorismo es cómo obtienen los grupos terroristas los recursos para el desarrollo de sus operaciones. Estos grupos necesitan financiar dos actividades principales de cualquier grupo criminal estable: los atentados terroristas (recursos operativos) y la infraestructura del grupo (necesidades organizativas generales)[12].

El primer acto jurídico internacional contra la financiación del terrorismo fue el Convenio Internacional para la Represión de la Financiación del Terrorismo del año 1999, que tuvo lugar sin demasiada repercusión[13]. No fue hasta los atentados terroristas del 11 de septiembre cuando surgió un intento real por regular y combatir la financiación del terrorismo. En el año 2001, en una Sesión Plenaria Extraordinaria, la Organización de las Naciones Unidas (ONU) creó las ocho Recomendaciones Especiales contra la Financiación del Terrorismo. Este fue el inicio de la firma de las resoluciones que se esperaban desde el año 1999 y que terminaron con la Resolución 1373 del Consejo de Seguridad, incluyendo las ocho Recomendaciones un mes después de su adopción.

De la misma forma que la ONU, la Unión Europea reaccionó a estos sucesos, de forma que el Consejo Europeo creó una batería de acciones en su reunión extraordinaria del 21 de septiembre del 2001 que incluía una lista de organizaciones terroristas y un plan contra la financiación del terrorismo[14]. Como resultado de este plan se adoptó la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo, que trataba sobre la responsabilidad de las personas jurídicas en la financiación de estos grupos, consideraba a las víctimas de los atentados terroristas e incluía el robo agravado y la extorsión como delitos vinculados a la financiación de las actividades terroristas. Todos estos cambios sugieren que la estructu-

[12] TOFANGSAZ, H. (2015). "Rethinking terrorist financing; where does all this lead?" *Journal of Money Laundering Control*. Vol.18, núm.1, pp.113-114.

[13] RIDLEY, N. and ALEXANDER, D. C. (2012). "Combating terrorist financing in the first decade of the twenty-first decade". *Journal of Money Laundering Control*. Vol.15, núm.1, pp. 38-40.

[14] RODRÍGUEZ-IZQUIERDO, M. (2010). "El terrorismo en la evolución del espacio de libertad, seguridad y justicia". *Revista de Derecho Comunitario Europeo*, núm. 36, pp. 531-559.

ra financiera de las actividades terroristas requiere también de recursos legales y de la necesidad de que las personas jurídicas gestionen su financiación para suplir las necesidades del grupo.

Si bien esta Decisión Marco se dedica también a la persecución del blanqueo de capitales[15], con esta nueva regulación lo que se impone es la introducción de un sistema de seguimiento del dinero y de intercambio de información que dificulte las posibilidades de financiación de las actividades delictivas. Aunque la motivación de los grupos no es económica, sino política, requieren de la obtención de una financiación que pueda permitir el desarrollo de sus operaciones y propósitos criminales. De esta forma se daba un gran paso en la lucha contra el terrorismo, ya que se contemplaba la transferencia de información entre el sector privado, en particular el sistema financiero y bancario y las Fuerzas y Cuerpos de Seguridad del Estado. La última actualización de la regulación europea sobre terrorismo se produce en la Directiva (EU) 2017/541 que determina cuáles van a ser los delitos relacionados con el terrorismo, añade nuevos delitos al catálogo y define el terrorismo sobre la base de un objetivo de intimidar gravemente a la población, obligar a las instituciones públicas nacionales o internacionales a realizar u omitir un acto y desestabilizar gravemente o destruir las estructuras políticas, constitucionales, económicas o sociales fundamentales de un país o de una organización internacional. Por último, se desarrollan los delitos relacionados con la financiación del terrorismo, castigando el proporcionar o recaudar fondos, directa o indirectamente, para cometer o contribuir a la comisión de un atentado terrorista.

Paralelamente a este desarrollo normativo, el Reglamento (CE) No 1889/2005 del Parlamento europeo y del Consejo de 26 de octubre de 2005 relativo a los controles de la entrada o salida de dinero efectivo de la Comunidad, introdujo el ámbito de la financiación del terrorismo, definida como la "provisión o recogida de fondos, por cualquier medio, directa o indirectamente, con la intención de que sean utilizados a sabiendas de que van a ser utilizados, en todo o en parte, para cometer cualquiera de los delitos" establecidos en la Decisión Marco 2002/475/JAI. Esta normativa imponía un sistema de diligencia debida y seguimiento de la información de las transferencias de dinero que permite a las autoridades seguir las transacciones de dinero con la ayuda de personas, instituciones de financiación, casinos y transferencias de dinero. Esta Decisión Marco

[15] En relación al blanqueo de capitales y financiación del terrorismo Cfr. BLANCO CORDERO, I. (2022). "Cooperación jurídica internacional en materia penal en la Unión Europea contra el blanqueo de capitales y la financiación del terrorismo" *Revista Jurídica de Castilla y León*, núm. 57, pp. 178 y 179.

tuvo una actualización en 2015 en la Directiva (UE) 2015/849 en particular, adaptando la cantidad de dinero y algunas instituciones como los servicios de juegos de azar como los casinos. Durante estos doce años el dinero de los juegos de azar se ha trasladado a otras plataformas como los sitios web de apuestas en línea. Por lo tanto, estos nuevos sistemas de juego tienen que ser incluidos y tomados como posibles objetivos.

Aunque el concepto de financiación del terrorismo no ha cambiado, sí que se han introducido cambios en cuanto a la evaluación de riesgos que los estados tienen que implementar en sus sistemas de control del dinero. La normativa europea sobre la financiación del terrorismo en su última actualización aborda la transferencia electrónica de dinero como las monedas virtuales, los proveedores de monederos y las actualizaciones de dinero electrónico y promueve la tipificación de la financiación del terrorismo[16].

En definitiva, la lucha contra la financiación de terrorismo requiere de la colaboración entre instituciones que intercambien datos y les permita obtener información relevante en el control y la lucha contra este fenómeno criminal. La agencia Europol en su informe sobre Evaluación de la Amenaza del Crimen Organizado en Internet de 2019 señala la utilización de las nuevas tecnologías por parte de los grupos terroristas para sus operaciones de propaganda y reclutamiento online, incluyendo como parte de esta tecnología la utilización de criptodivisas en sus formas de financiación[17]. En las últimas décadas, las instituciones legislativas de la Unión Europea han dirigido sus actuaciones hacia la lucha contra la financiación de terrorismo que se está ocurriendo con la utilización de estas nuevas tecnologías, no obstante, el uso de las monedas virtuales con este propósito sigue siendo bajo[18].

1. Medios de prueba con información económica

El nuevo instrumento de cooperación en materia penal, desarrollado por la Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia

[16] Artículo 7 de la Directiva (UE) 2015/849.

[17] EUROPOL (2022). *Internet Organized Crime Threat Assessment 2019 (IOCTA)* [informe en línea]. European Union Agency for Law Enforcement Cooperation [Fecha de consulta: 3 de junio de 2023]. *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019*

[18] EUROPOL (2022). *European Union Terrorism Situation and Trend Report 2022 (TE-SAT)* [informe en línea]. European Union Agency for Law Enforcement Cooperation [Fecha de consulta: 2 de junio de 2023]. *https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf*

penal, da un paso más en la lucha contra la financiación del terrorismo. La orden europea de investigación (OEI) supone un gran cambio respecto al sistema original de cooperación judicial penal, basado en la Decisión Marco 2003/577/JAI del Consejo, de 22 de julio de 2003, relativa a la ejecución en la Unión Europea de las resoluciones de embargo preventivo de bienes y de aseguramiento de pruebas y la Decisión Marco 2008/978/JAI del Consejo, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal. El nuevo instrumento jurídico pretende agilizar el proceso de solicitud de pruebas en algunos delitos con la orden de que todos los Estados miembros implicados faciliten las pruebas solicitadas por uno de ellos. Los datos solicitados por una OEI son: el nombre y la dirección del titular de la cuenta, los datos de cualquier poder que se tenga sobre la cuenta y cualquier otro dato y documento relacionado con la cuenta.

De todos los tipos de pruebas recogidos en esta norma, en este trabajo será de interés la solicitud de cuentas bancarias o financieras e información bancaria y financiera. Según lo establecido en los números 27, 28 y 29, se puede emitir una OEI para obtener pruebas relativas a las cuentas con independencia de cuál sea su naturaleza o si se han mantenido en un banco o en otra institución financiera no bancaria por una persona sujeta a ella. Sin embargo, esto se debe entender en sentido amplio, ya que comprende no sólo a las personas sospechosas o acusadas, sino también a cualquier otra persona respecto de la cual las autoridades competentes consideren necesaria dicha información en el curso de un procedimiento penal, de conformidad con el artículo 3 de la Directiva 2005/60/CE relativa al blanqueo de capitales y a la financiación del terrorismo.

2. Realidad de la lucha contra la financiación del terrorismo

Desde el punto de vista jurídico disponemos de instrumentos legales para la lucha contra la financiación del terrorismo, pero en su aplicación surgen algunas dificultades.

Tras los atentados del 11-S la investigación de la financiación del terrorismo se centró en los bancos y en los sistemas financieros islámicos, pero la respuesta de las instituciones fue débil por la ausencia de información o por falta de disposición[19]. Aunque existen algunas irregularidades y cierta falta de control que permiten que el dinero ilícito se mueva a través de las

[19] RIDLEY, N. and ALEXANDER, D. C., cit., p. 49.

instituciones bancarias islámicas, la actuación de los organismos encargados de hacer cumplir la ley en EE.UU. y la UE fue considerada como una intrusión de los países occidentales[20]. El interés por los sistemas bancarios y financieros clásicos tenía su razón de ser en cómo Al-Qaeda era financiada por Osama Bin Laden a través del empleo de diferentes cuentas bancarias con nombres falsos desde que vivía en Sudán[21]. La respuesta por parte de las entidades que financiaban a los grupos terroristas tras los primeros intentos de controlar la financiación del terrorismo consistió en cambiar el sistema de financiación mediante la banca, por un sistema informal de transferencia de fondos, como el Hawala en las sociedades islámicas, el Hundi en la India o Fei ch'ien en China[22]. Otra solución fue la transferencia del dinero mediante el movimiento físico de los fondos, pero este sistema tenía el inconveniente de que limitaba la cantidad de dinero que se podía transferir, por lo que no funcionaba para grandes sumas de dinero. Por último, el comercio también permitía transferir objetos de valor y bienes a través de los flujos comerciales, dando a los grupos terroristas el acceso a materiales y bienes que necesitan para sus operaciones[23].

Pero la financiación no es un tema relevante únicamente en el terrorismo islámico. El acceso a fuentes naturales y a financiación externa determinan la probabilidad de creación de un grupo terrorista mucho más que el apoyo civil[24]. Por lo tanto, la fortaleza financiera de un grupo dependerá de la situación geográfica de las actividades del grupo terrorista. Un ejemplo de ello ha sido el tráfico de drogas[25], que ha sido popular en la financiación de grupos terroristas como el "Ejército de Liberación de Kosovo" o Euskadi Ta Askatasuna (ETA) en España[26].

La financiación externa ha sido un factor importante en algunos casos de terrorismo nacional, sobre todo en aquellas regiones con intereses geoestratégicos como Centroamérica y Oriente Próximo. La realidad de las nuevas formas de terrorismo como el terrorismo islámico internacional y las acciones de extrema derecha demuestran que el actor externo tiene una influencia considerable al alentar sus atentados y financiarlos como hemos visto anteriormente.

---

20 Ibid.

21 TOFANGSAZ, H., cit., pp.113-114.

22 KISER, S. (2005). *Financing Terror. An Analysis and Simulation for Affecting Al Qaeda's Financial Infrastructure* [informe en línea]. RAND Corporation. 245.

23 TOFANGSAZ, H., cit., pp. 117-118.

24 PAGE FORTNA, V. J., LOTITO, N. and A. RUBIN, M., cit., p. 789.

25 CLARKE, C. P. (2016). Drugs & Thugs: Funding Terrorism through Narcotics Trafficking. *Journal of Strategic Security*. Vol. 9, núm. 3, pp.1-15.

26 Ibid, 3.

Los grupos terroristas necesitan dinero para sus actividades operativas, como es el caso del atentado terrorista, que tendrá costes derivados de la logística de este. Pero los grandes grupos también tienen amplias necesidades organizativas creando, manteniendo y desarrollando su infraestructura[27]. En este caso, la necesidad de dinero es considerable ya que una organización con una infraestructura es más costosa que la gestión de las actuaciones que llevaría a cabo "un lobo solitario"[28].

Además, el método de financiación también puede cambiar la forma en la que puede desarrollarse un atentado terrorista. Así, existen fuentes de financiación ilegales y legales. Las primeras, a través de actos delictivos como el narcotráfico, la extorsión, los delitos económicos, el crimen organizado o el secuestro[29] y ahora también la ciberdelincuencia a través de la utilización de Internet por parte de las organizaciones criminales[30]. La globalización de los sistemas monetarios internacionales ha abierto nuevas vías de financiación a escala mundial[31], lo que ha ocasionado el empleo de nuevas formas de financiación, como las transacciones con criptomonedas[32]. Por otro lado, las formas legales de financiación son muy diversas, pudiendo consistir, por ejemplo, en donaciones, obras de caridad o a través de organizaciones no gubernamentales[33].

Al mismo tiempo, el tipo de financiación determina el tipo de grupo de terrorista del que se trata, existiendo hasta seis grupos. El primero sería el grupo patrocinado por un Estado, en el que ambos compartirían objetivos políticos[34]. En segundo lugar, se encuentra el Estado "tapadera" considerado como una zona en la que el grupo terrorista ejerce su poder dentro de un Estado nacional, financiándose a través de los recursos naturales o con actos delictivos dentro de su territorio, como los grupos terroristas vinculados al narcotráfico[35]. El tercer grupo es una evolución del primero en el que los recursos proceden de un Estado pero también de patrocinadores individuales, lo que permite al grupo mantener su

[27] TOFANGSAZ, H., cit. pág. 113-114.

[28] MARRERO ROCHA, I. (2017). Nuevas dinámicas en las relaciones entre crimen organizado y grupos terroristas. *Revista española de derecho internacional*. Vol. 69, núm. 2, pp. 145, 169.

[29] Ibid, 115.

[30] EUROPOL, cit., pág. 48.

[31] VITTORI, J. (2011). *Terrorist Financing and Resourcing*. 1ª ed. Palgrave Macmillan, p. 244.

[32] IRWIN, A. S. M. and MILAD, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control*. Vol.19, núm. 4, pp. 407-425.

[33] TOFANGSAZ, H., cit. pp. 115-116.

[34] VITTORI, J., cit., p. 8.

[35] TOFANGSAZ, H., cit., p. 118.

continuidad en caso de que una de las fuentes ponga fin a su financiación[36]. En cuarto lugar, de una forma más sofisticada, se encuentra el apoyo agrupado, en el que el número de simpatizantes es mayor, siendo la mayoría pequeños donantes privados con un vínculo nacional o étnico con el grupo[37]. En quinto lugar, el aumento de las dimensiones estructurales y de financiación de un grupo terrorista, ha dado lugar al modelo de empresa transnacional[38]. Esta es la estructura que Al Qaeda utilizó implantando un modelo de negocio de empresa transnacional en un grupo terrorista. Por último, una vez disuelto este modelo por la legislación internacional la siguiente estandarización ha sido el "lobo solitario"[39], un terrorismo de bajo coste en el que la necesidad de suministros de dinero y recursos es muy modesta.

El éxito de la aplicación del reglamento internacional sobre el blanqueo de dinero y la financiación del terrorismo ha ocasionado una evolución de los grupos terroristas hacia formas de financiación basadas en la ciberdelincuencia[40]. El uso de las tecnologías ha facilitado y aumentado la eficacia de las tareas administrativas en las organizaciones transnacionales, así como la coordinación de las operaciones, el reclutamiento de miembros potenciales[41], la comunicación con los adeptos, la captación de simpatizantes[42] y la transferencia de dinero.

El éxito de la ciberdelincuencia se basa en seis factores clave. El primero de ellos es el alcance que tiene Internet, que permite poner en contacto a personas en cualquier localización y con bajo coste. Esto ha favorecido la consecución de simpatizantes de los grupos terroristas. En segundo lugar, la accesibilidad de Internet, siendo actualmente una herramienta al alcance de casi cualquier persona en el mundo. El tercero es el anonimato, que dificulta la detección de actividades de los grupos como la transferencia de dinero para su financiación. Se puede conseguir a través de servidores *proxy*, servidores de correo electrónico encriptado o falsas direcciones IP. En cuarto lugar, las tecnologías de encriptación son fácilmente accesibles y permiten dificultar el rastreo del dinero.

---

36 VITTORI, J., cit., p. 8.

37 TOFANGSAZ, H., cit., p. 118.

38 CRONIN, A. K., cit.

39 TOFANGSAZ, H., cit., p. 118.

40 NIETO MARTÍN, A., GARCÍA MORENO, B. (2021) "Criptomonedas y derecho penal: más allá del blanqueo de capitales" en *Revista Electrónica de Ciencias Penales y Criminología*, núm. 23, pp. 18 y ss.

41 CANO PAÑOS, M.A. (2016) "Odio e incitación a la violencia en el contexto del terrorismo islamista: Internet como elemento ambiental", *Indret*, núm. 4, passim.

42 CRONIN, A. K., cit., p. 47.

Además, las tecnologías digitales son fáciles de transportar y permiten almacenar una gran cantidad de datos en un espacio reducido. El quinto factor es el alcance global, que en el caso del terrorismo las redes han facilitado la internacionalización de los grupos criminales. Finalmente, el sexto punto, es la ausencia de guardianes capaces de permitir que estas nuevas formas de financiación sean detectadas y perseguidas[43].

Los datos electrónicos necesitan técnicas forenses complejas para su obtención mediante un sistema que garantice que puedan utilizarse como prueba en un juicio. Al mismo tiempo, la vigilancia en la red del movimiento de dinero también es muy complicada. El hecho de que la infraestructura, en la que se realizan estos movimientos de dinero, pertenezca al sector privado y la comunicación esté enrutada de manera que pase por distintas jurisdicciones nacionales, hace que el intercambio de información entre policías sea un gran reto[44].

III. EL USO DE LA INTELIGENCIA ARTIFICIAL PARA COMBATIR EL TERRORISMO

Internet se presenta como el lugar en el que suceden una gran variedad de actividades de los grupos terroristas, desde suministro de información, captación de terroristas a financiación de actividades. Por lo tanto, serán necesarias el uso de tecnologías que permitan la recopilación de pruebas electrónicas e inteligencia que permita la lucha contra este fenómeno criminal.

La inteligencia artificial puede aportar importantes herramientas en este ámbito que permitan interceptar comunicaciones, encontrar pruebas, detectar la captación de nuevos miembros o la utilización de propaganda terrorista y el intercambio de dinero para su financiación. Así, existen programas basados en inteligencia artificial para el seguimiento de las criptomonedas desde el monedero de origen hasta el de destino[45]. Al mismo tiempo, las investigaciones sobre financiación permite recopilar información, enriqueciendo los datos obtenidos mediante sistemas automáticos de gestión, permitiendo enriquecer las pruebas que se obtengan dentro de un caso concreto. Esto se puede utilizar desde el punto de vista estratégico u operacional.

No obstante, en este último caso, su utilización se centrará en adquirir y utilizar información sobre acontecimientos, tendencias y relaciones

[43] CLOUGH, J., cit., p. 5-9.

[44] Ibid.

[45] Véase *https://www.ait.ac.at/en/research-topics/datascienceartificialintelligence/projects/virtcrime?no_cache=1*

en un entorno determinado para apoyar la toma de decisiones y la planificación[46]. En concreto, cuando utilizamos sistemas inteligentes como herramienta en la lucha contra el terrorismo es necesario establecer indicadores e identificar facilitadores del desarrollo presente y futuro de estas actividades delictivas. Existen señales que anticipan el posible desarrollo de los escenarios y estas deben relacionarse con algún indicador estadístico de eventos que se toman como claves en el fenómeno terrorista. Con estos modelos estadísticos la inteligencia artificial "aprende" dónde buscar y qué tipo de pruebas son relevantes o no[47].

La propuesta de Reglamento europeo sobre inteligencia artificial de la Comisión Europea hace distinción en tres niveles para determinar si esta tecnología se puede utilizar o no. La primera son los casos prohibidos en los que no se permiten su uso[48]. Así, en cuestiones relacionadas con la seguridad y con la lucha contra el crimen quedan taxativamente prohibidas las técnicas de puntuación social, la utilización de datos biométricos de forma generaliza y la manipulación psicológica. En ninguno de estos casos se encuentra la propuesta que proponemos para su utilización.

El segundo nivel son los usos denominados como de alto riesgo[49]. En esta figura entran la mayoría de los usos de los sistemas inteligentes utilizados en materia policial. Para su uso será necesaria la realización de una evaluación de impacto en los derechos fundamentales, que veremos, más adelante. Aunque no tendría cabida en el estudio de la financiación del terrorismo hay que considera un acierto, desde nuestro punto de vista, de un control judicial para su utilización con datos biométricos en investigaciones en curso. Solución que se asemeja a la adoptada con la utilización de otras tecnologías en investigaciones policiales como puede ser las escuchas telefónicas o la entrada en domicilios de sospechosos.

Finalmente, están los usos que no se consideran de riesgo en los que se recomienda que se realicen esas evaluaciones de impacto, pero no son obligatorias.

---

[46] CHOO, C. W. (2005). The Art of Scanning the Environment. *Bulletin of the American Society for Information Science and Technology*. Vol.25, núm. 3, pp. 21-24.

[47] VALLS-PRIETO, J. y GÓMEZ-ROMERO, J. (2016). Use of Big Data and the Prediction of Organized Crime. En: BALCELLS PADULLÉS, J. et al. (coords.). *Building a European Digital Space*. Barcelona: Huygens Editorial, p. 369.

[48] Artículo 5 de 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, 2021.

[49] Anexo III de 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, 2021.

De forma general, podemos considerar que la inteligencia artificial aplicada a la lucha contra el crimen puede formularse en cinco etapas. La primera es la adquisición de datos. Esta tarea se realiza rastreando tanto la web superficial como la *Darknet* en busca de información específica en chats, webs y foros donde, en nuestro caso de estudio, se pueda encontrar información sobre actividades terroristas, así como fuentes de datos abiertas que puedan estar vinculadas al caso[50]. Para este cometido es necesario procesar el lenguaje natural con el fin de extraer información que pueda ser analizada por una máquina.

Una vez almacenados los datos, como segunda fase, hay que hacer un estudio de la información para detectar patrones y extraer inteligencia. Al mismo tiempo, será necesaria información adicional que pueda complementar los resultados obtenidos. Esta fase de enriquecimiento de la información obtenida se realiza también mediante la ayuda de sistemas inteligentes. Si por ejemplo se han obtenido datos de chats en los que se conversaba sobre terrorismo, será de utilidad la obtención de datos adicionales como las conexiones geográficas de los usuarios y su vinculación con otras actividades en línea. Esta fase de descubrimiento permite a las Fuerzas y Cuerpos de Seguridad del Estado superar el anonimato de determinados usuarios y encontrar información operacional que sin el uso de esta tecnología estaría oculta.

Posteriormente, se deberá iniciar una fase de evaluación para analizar la información proporcionada por la herramienta de Inteligencia artificial en la que el analista estudiará la veracidad de la información obtenida. En este paso la inteligencia artificial permite facilitar la visualización de los contenidos presentándolos de una forma cómoda, mayormente a través de un interfaz hombre-máquina personalizado.

Finalmente, se lleva a cabo una fase de previsión en la que las herramientas basadas en inteligencia artificial ofrecen la posibilidad de prever futuros actos terroristas a través del análisis de la información de casos anteriores. Esto tiene una gran relevancia en la anticipación de futuras acciones, permitiendo la prevención de estos eventos y tomando medidas para disminuir las posibilidades de que se produzcan.

IV. LA UTILIZACIÓN DE CRIPTOMONEDAS COMO SISTEMA DE FINANCIACIÓN

El avance tecnológico que suponen las criptomonedas permite transferir dinero entre las partes interesadas de forma descentralizada a tra-

[50] Ibid., pp. 370-371.

vés de redes *peer-to-peer*. Este intercambio de dinero entre miembros de las organizaciones terroristas y sus simpatizantes, sin la intervención del Estado de un estado como intermediario, es utilizado por los grupos terroristas como un sistema descentralizado de financiación que facilita el anonimato y el movimiento transfronterizo de los recursos monetarios necesarios para la comisión de estos atentados. Las características de las criptomonedas han dificultado la detección y la persecución de la financiación terrorista que emplea estas monedas virtuales.

Uno de los problemas que se han observado en la financiación del terrorismo es que las pequeñas donaciones entre particulares y las transferencias en efectivo, como el Hawala, restringen el dinero a los grupos terroristas internacionales y para financiar células terroristas fuera del control geográfico de los grupos. El Hawala, por ejemplo, es un sistema que funciona a través de comerciantes de confianza en el que el responsable de la red entrega el dinero de sus recursos y tiene un crédito con el otro comerciante del país del que procede la orden de transferencia.

Las criptodivisas permiten a las organizaciones terroristas gestionar los fondos con más opacidad y menos riesgos, dando a los grupos terroristas más flexibilidad y operatividad. En primer lugar, para utilizarlas se deberá obtener un monedero o cartera, que otorga al individuo de una clave pública y otra privada. La primera será compartida con el resto de los usuarios para poder recibir las transacciones y la segunda será el equivalente a la contraseña de la cartera. Este funcionamiento permite realizar la transacción entre las partes interesadas sin compartir la identidad de los usuarios, dotando al sistema de anonimato. Sin embargo, el funcionamiento de las criptomonedas es posible gracias a la creación de la tecnología *Blockchain*, que constituye una cadena de bloques descentralizada en la que los mineros almacenan, verifican y confirman las transacciones realizadas en el sistema. Esta tecnología tiene un carácter público, por lo que cualquier persona interesada puede acceder y consultar las transacciones realizadas y a su vez permite rastrear los movimientos de los fondos. De esta forma, se estaría hablando en realidad de un pseudoanonimato, porque las criptomonedas podrían ser rastreadas[51].

El punto débil de este sistema tiene lugar cuando el sujeto desea convertir los fondos que dispone en criptomonedas a dinero fiduciario. En este caso, se requiere de la utilización de una entidad bancaria u otro sistema centralizado sometidos a la regulación financiera que podría poner en peligro la ocultación de su identidad. Existen opciones más

[51] IRWIN, A. S. M. and MILAD, G., cit. p. 412.

seguras, como la utilización de cajeros automáticos de criptomonedas, que en algunas ocasiones no requieren de la aportación de documentos identificativos y que también permiten el cambio de dinero fiduciario a criptomonedas[52].

Las organizaciones terroristas, por tanto, buscarán la forma de obtener y cambiar criptomonedas sin que esto suponga una revelación de su identidad. Una opción es a través del comercio directo con otro individuo a través de un intermediario que facilite la conexión en un país *off-shore*. Pero la opción más habitual es a través de la utilización de la moneda virtual en la compra de algún bien o servicio. Los grupos terroristas pueden obtener suministros para el desarrollo de sus actividades a través de la compra en la *Darknet* utilizando criptomonedas.

Ante esta situación, la inteligencia artificial ofrece herramientas que permiten gestionar toda esta cantidad de información y establecer conexiones en poco tiempo. La rapidez de actuación en este fenómeno criminal es muy importante, especialmente en la evitación de los atentados terroristas. Aunque la toma de decisiones debería llevarse a cabo por humanos, la ayuda de las máquinas puede ser determinante en la lucha contra el terrorismo.

V. CÓMO COMBATIR EL TERRORISMO Y SU FINANCIACIÓN

Conscientes de las dificultades para combatir un fenómeno cambiante que evoluciona con gran rapidez, los expertos han aportado distintas soluciones para luchar contra el terrorismo.

Desde el punto de vista estadounidense, Ridley y Alexander afirman que se necesita más mano de obra, recursos financieros y atención, pero también mayor colaboración, intercambio de información y menos guerras territoriales[53]. El gobierno debe considerar que los miembros de los grupos terroristas también participan de las actividades legales de la sociedad. Por lo tanto, se debería incrementar la cantidad de información financiera que se comparte entre las Fuerzas y Cuerpos de Seguridad del Estado y las instituciones financieras, así como solicitar la colaboración con el sector privado[54].

De forma similar, Abeyratne pide la adopción de medidas prácticas para desalentar la comisión de actos terroristas[55]:

---

52 Ibid., p. 414.
53 RIDLEY, N. and ALEXANDER, D. C., cit. p. 52.
54 Ibid.
55 ABEYRATNE, R. cit., p. 67.

> *Se trata de a) la mejora del sistema de inteligencia que informará al Estado en cuestión sobre el riesgo de un atentado terrorista; b) el establecimiento de mecanismos antiterroristas centrados en la recogida de armas, municiones y armamento; c) la adopción de medidas prácticas de autoayuda y ataque en caso de atentado terrorista; d) la existencia de la maquinaria necesaria para conservar en todo momento la confianza y la simpatía del público; y e) la persuasión para convencer al público de que no debe tolerarse ningún tipo de terrorismo de cualquier tipo*[56].

Desde un punto de vista económico, otra medida para combatir la financiación consiste en gravar aquellos productos que son necesarios para esta financiación, como por ejemplo, los instrumentos de la producción de narcóticos y la exportación[57]. Desde una perspectiva económica, Hausken señala que, en un balance de costes y beneficios, esto supondría el aumento de los costes de los terroristas y la disminución de los costes del gobierno. La disminución de los beneficios para el terrorismo podría producirse mediante la aplicación de la ley, la vigilancia y la detección que hicieran menos lucrativos los esfuerzos criminales impidiendo que grandes organizaciones eficientes lo financien y animando a los benefactores a no financiar. Para aumentar el coste del terrorismo los gobiernos pueden hacer que los delitos de terrorismo incrementen esta variable animando a los benefactores a castigar el delito, disminuyendo los recursos de los terroristas y confiscando, congelando e impidiendo la acumulación de recursos, bloqueando la financiación del terrorismo por parte de los benefactores, criminalizando su financiación e impidiendo la producción efectiva de delitos[58].

El terrorismo es un problema multifactorial para el que no hay una única solución. Sin embargo, la evolución en las formas delictivas del terrorismo ha ocasionado que las formas clásicas de persecución de esta delincuencia sean insuficientes e incluso peligrosas y se necesiten nuevas propuestas para resolver el problema[59]. Un ejemplo del uso de nuevas técnicas para luchar contra la financiación del terrorismo es el proyecto "MIDAS" de la empresa IBM, en el que desarrollaron una máquina que tiene capacidad para extraer información de las multas adoptadas por

---

[56] Ibid.

[57] BERCK, P. and LIPOW, J. (2012). Trade, tariffs and terrorism. *Applied Economics Letters*. Vol. 19, núm. 18, pp. 1847-1849.

[58] HAUSKEN, K. (2017). Government Protection against Terrorists Funded by Benefactor and Crime: An Economical Model. *International Journal of Conflict and Violence*.Vol.11, pp. 1-37.

[59] CRONIN, A. K., cit., p. 31.

los organismos de control de EE.UU. en casos de blanqueo de capitales y financiación del terrorismo[60]. La reutilización de esta información con herramientas de inteligencia artificial permite mejorar el seguimiento de las empresas implicadas y proporcionar una metodología sobre cómo encontrar información financiera de relevancia.

Por todo ello, se puede señalar que uno de los factores clave en la lucha contra el terrorismo es la actividad de vigilancia, que para que realmente sea eficaz se deberá conseguir un equilibrio entre los costes de las acciones gubernamentales y el coste ocasionado para los grupos terroristas. Para conseguir este objetivo, la aplicación de la inteligencia artificial es un factor clave ya que puede reducir estos costes. La vigilancia de Internet es compleja y la utilización de los recursos humanos no es barata, por lo que el desarrollo de sistemas de vigilancia efectivos supondría una mejora en la lucha contra el terrorismo. Sin embargo, no todos son ventajas. La utilización de sistemas inteligentes por la policía implica otra serie de riesgos por su utilización.

VI. PROBLEMAS RELACIONADOS CON EL USO DE LA INTELIGENCIA ARTIFICIAL PARA LA LUCHA CONTRA LA FINANCIACIÓN DE GRUPOS TERRORISTAS

Aunque la utilización de la Inteligencia artificial puede ser beneficiosa en la lucha contra la financiación del terrorismo, también puede suponer algunos inconvenientes. Por un lado, permitiría el rastreo del dinero y de las criptomonedas través de los sistemas financieros, y la posibilidad de vigilar la información terrorista en Internet. Pero, por otro lado, estas actuaciones podrían afectar a los derechos a la intimidad, a la presunción de inocencia y a la no discriminación de la población afectada.

Como han demostrado Raso et al., el uso de la inteligencia artificial tiene un impacto positivo en el derecho a la seguridad, ya que facilita el tratamiento de una gran cantidad de información y la búsqueda de pruebas en Internet, algo que puede resultar complejo para los humanos. Sin embargo, estos autores señalan que su uso en la justicia penal tiene un impacto negativo en el derecho a la intimidad, a ser considerado inocente y a la audiencia pública[61]. Además, a medio plazo, podría tener un im-

[60] PLACHOURAS, V. and LEIDNER, J. L. (2015). "Information Extraction of Regulatory Enforcement Actions: From Anti-Money Laundering Compliance to Countering Terrorism Finance". *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 950-953.

[61] RASO, F.; HILLIGOSS, H.; KRISHNAMURTHY, V.; BAVIZ, C. and KIM, L. (2018). *Artificial Intelligence & Human Rights: Opportunities and Risks* [informe en línea].

pacto en derechos como la no discriminación. La máquina puede tener un sesgo en su desarrollo, pero al mismo tiempo, esa misma máquina, puede evitar la discriminación por el sesgo de los humanos, por lo que puede ser positivo o negativo, y esto puede ocurrir con el derecho a no ser arrestado, detenido o exiliado arbitrariamente[62].

Al tratarse de una tecnología relativamente nueva y con una corta trayectoria de aplicación en esta materia, será necesario evitar los riesgos ligados a su uso. Esa es la idea fundamental de las directrices éticas para una inteligencia artificial digna de confianza[63]. Estas directrices tienen siete puntos principales que se han de respetar de forma general en el uso de cualquier inteligencia artificial, también, en nuestro caso concreto, para su uso en materia de seguridad.

El primero es la agencia y la supervisión humanas. Con ello se pretende que la inteligencia artificial ayude y capacite a los humanos, pero no los sustituya. Además, los sistemas deben ser técnicamente robustos y seguros, lo que significa que deben ser resistentes y seguros, y garantizar un plan de emergencia en caso de que ocurra algún incidente. Debe respetar la privacidad y trabajar con datos íntegros y de calidad. El sistema debe construirse pensando en la diversidad y la no discriminación. Tiene que ser sostenible y respetuoso con el medio ambiente, pensando en las generaciones futuras. Por último, tiene que haber mecanismos que garanticen la responsabilidad y la rendición de cuentas de los resultados.

Para abordar esta configuración es necesario hacer una evaluación de los derechos humanos. Esto es importante porque existe un riesgo elevado de sesgo contra determinados grupos de población. Virginia Eubanks describe un ejemplo de esto que tuvo lugar en la ciudad de Los Ángeles, donde las personas pobres (en su mayoría negros) fueron señaladas como peligrosos cuando la inteligencia artificial utilizó datos de los servicios sociales, como el código postal, los ingresos generales del barrio, el nivel educativo o las enfermedades psicológicas en el barrio de Skid Row[64].

En cuanto al campo de la seguridad, no hay demasiados trabajos al respecto. Una posibilidad para realizar la evaluación de los derechos es

---

Berkman Klein Center for Internet & Society Research Publication. [Fecha de consulta: 9 de enero de 2020]. *http://nrs.harvard.edu/urn-3:HUL.InstRepos:38021439*

[62] Ibid.

[63] HIGH-LEVEL EXPERT GROUP ON AI (2019). Ethics Guidelines for Trustworthy Artificial Intelligence [informe en línea]. European Comission. [Fecha de consulta: 9 de enero de 2020]. *https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai*

[64] EUBANKS, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*. St. Martin's Press, p. 272.

partir de la base de la evaluación de la vigilancia realizada por Wright et al., que en un intento de legitimar la vigilancia por parte de las instituciones estatales creó una evaluación según los actores: instituciones estatales, sector privado, ciudadanos, ONG y sociedad.

Para ello, ofrecen una lista de preguntas genéricas que todo trabajador del sector debería hacerse antes de utilizar las herramientas de vigilancia. Se trata de un total de quince preguntas que son las siguientes[65]:

1. *¿Cuál es la finalidad del sistema?*
2. *¿Es realmente necesario? ¿Es legal? ¿Es proporcionada al fin perseguido?*
3. *¿Qué alternativas menos intrusivas existen?*
4. *¿Quién lo desarrollará, explotará y autorizará?*
5. *¿Quién tendrá acceso a los datos recogidos?*
6. *¿Durante cuánto tiempo se almacenarán los datos recogidos? ¿Cuándo se suprimirán? ¿Qué medidas se tomarán para almacenar o transmitir los datos de forma segura?*
7. *¿En qué medida se consultará a las partes interesadas, incluidos los ciudadanos, sobre el proyecto y sus efectos?*
8. *¿Qué supervisión externa existe, incluida una auditoría periódica, independiente, realizada por terceros y a disposición del público?*
9. *¿Cómo se formará a los operadores del sistema para que sean sensibles a cualquier consecuencia perjudicial?*
10. *¿Permite el sistema identificar a las personas? En caso afirmativo, ¿es necesario? ¿Ofrece a las personas la posibilidad de excluirse?*
11. *¿Trata el sistema datos personales "sensibles"? En caso afirmativo, ¿es necesario?*
12. *¿A qué intereses sirve el sistema?*
13. *¿Crea el sistema daños identificables, por ejemplo, daños sociales, medioambientales, económicos o relacionados con los derechos humanos?*
14. *Si no se puede evitar la vigilancia o mitigar sus efectos, ¿cómo se puede capacitar a la sociedad para que desarrolle las capacidades necesarias para hacer frente a sus consecuencias?*

[65] WRIGHT, D.; RODRIGUES, R.; RAAB, C.; JONES, R.; SZÉKELY, I.; BALL, K.; BELLANOVA, R. and BERGERSEN, S. (2015). Questioning surveillance. *Computer Law & Security Review*. Vol. 31, núm. 2, p. 280-292.

15. *¿Se han tenido en cuenta las posibles repercusiones negativas y los riesgos de la aplicación o continuación del sistema de vigilancia en cuestión? ¿Qué relación guardan con los beneficios?*[66]

A esto, hay que añadir una pregunta sobre qué derechos fundamentales se va a ver afectados. Los derechos procesales de los acusados, tales como el derecho de presunción de inocencia o el derecho a ser oído por parte del tribunal deberán estar asegurados. Al mismo, tiempo los derechos de privacidad y de no discriminación también juegan un papel importante que se debe de analizar en toda la vida de uso de estos sistemas. Como vemos, para garantizar la legitimación de su uso es preciso un análisis escrupuloso de los derechos afectados para garantizar que el Estado no se extralimita en su utilización y da garantías a los ciudadanos.

Igualmente, los principios éticos de supervisión humana, transparencia y rendición de cuentas deberán se tenidos en cuenta para su implementación. En casos de investigaciones en curso, estos derechos pueden ser limitados para garantizar el buen fin de la investigación. Es por ello que un sistema de información a la ciudadanía adecuado al uso concreto y el contexto en el que se realiza es pertinente.

La respuesta a estas preguntas no podrá consistir únicamente en un "sí" o un "no", sino que el objetivo es hacer reflexionar a los sujetos implicados en su integración práctica sobre la repercusión que podría tener la vigilancia tecnológica en la sociedad. Esto sirve para los organismos encargados de hacer cumplir la ley, los servicios de inteligencia, pero también para los desarrolladores de tecnología en el sector privado.

Los responsables políticos y los reguladores deben responder a otras preguntas, que son las siguientes[67]:

1. *¿Es la vigilancia necesaria, legítima, transparente y proporcionada? ¿Cómo se realizan estos juicios? ¿Existen alternativas menos intrusivas?*
2. *¿Cómo se han sopesado en la decisión de utilizar la vigilancia los costes, beneficios y riesgos, incluidas las consecuencias de la vigilancia para los derechos humanos, las libertades y la democracia? ¿Está documentado públicamente el proceso de toma de decisiones?*
3. *¿Qué deliberaciones han tenido lugar sobre la necesidad y proporcionalidad de la intrusión en la vida privada de las personas*

[66] WRIGHT, D.; RODRIGUES, R.; RAAB, C.; JONES, R.; SZÉKELY, I.; BALL, K.; BELLANOVA, R. and BERGERSEN, S., cit., p. 283.

[67] Ibid., p. 284.

mediante la medida o política de vigilancia? ¿Está documentado públicamente el proceso de toma de decisiones?

4. *¿Cómo se han tenido en cuenta las opiniones de las distintas partes interesadas, especialmente del público?*
5. *¿Han identificado los responsables políticos los posibles daños, a quién perjudica y a quién beneficia la vigilancia, cuáles son los posibles efectos en cadena, cuáles son las consecuencias sociales? Después de intentar identificar todas las consecuencias, ¿han pensado los responsables políticos qué pueden hacer razonablemente para combatir los daños?*
6. *¿Qué sistemas existen para una supervisión, revisión y control adecuados de las prácticas de vigilancia?*
7. *¿Se ha informado a los destinatarios de la vigilancia (que puede ser el público en general) de la existencia del sistema de vigilancia y de su objetivo general? ¿Cómo pueden obtener más información sobre el alcance del sistema? ¿Cómo pueden solicitar una reparación personal por los daños sufridos? ¿Cómo pueden cuestionar o, fundamentalmente, cuestionar el sistema de vigilancia?*
8. *¿Cuál es la mejor manera de controlar la proliferación de la vigilancia en el proceso político y de elaboración de políticas?*
9. *Si no se puede evitar la vigilancia, ¿cómo se puede capacitar a la sociedad para que desarrolle las capacidades necesarias para hacer frente a sus consecuencias?*
10. *¿Cómo se evaluarán o controlarán continuamente los efectos de la vigilancia?*
11. *¿Cómo pueden la cooperación y la normalización reglamentarias internacionales responder mejor al reto del flujo mundial de información personal?*
12. *¿Cuál es la mejor manera de controlar la proliferación de la vigilancia en el proceso político y de elaboración de políticas?*

Estos autores proponen también seis medidas políticas y reglamentarias. Aunque se trata de un planteamiento general para otras tecnologías distintas de la inteligencia artificial, muchas de ellas pueden ampliarse o adaptarse a este sistema informático. La primera es la rendición de cuentas y la supervisión, que deben introducirse a través de procesos políticos. La rendición de cuentas requiere de procedimientos y normas que informen públicamente y se comprometan en posibles impugnaciones de las cuentas rendidas. La supervisión debe correr a cargo de organismos independientes que tengan en cuenta el servicio público. El consentimiento, en este proceso de investigación, obviamente no puede ser

dado por individuos. En este caso tiene que ser un acuerdo social entre el Estado y la sociedad. El tercer punto es reforzar la protección jurídica de la privacidad. 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 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 personas, es una buena forma de proteger y legitimar el uso de la inteligencia artificial en la financiación de investigaciones sobre terrorismo. Desgraciadamente, no ha tenido tanto éxito como el Reglamento de protección de datos del mismo año, pero es cierto que en él se incluye la evaluación de impacto y, si se hace como hemos dicho antes, podría ser un sistema de legitimación fuerte, así como una línea base para un estándar internacional como es el reglamento de protección de datos. Pero lo que es cierto, como hemos visto en este trabajo, es que la lucha contra la financiación del terrorismo sin el uso de las nuevas tecnologías, como están haciendo los terroristas, es una quimera hoy en día.

VII. CONCLUSIONES

Como hemos visto en este trabajo, las nuevas formas de terrorismo desafían no sólo a los Estados nacionales, sino también a la comunidad internacional. La forma en la que los grupos terroristas han evolucionado en su *modus operandi* es clave en el desarrollo de sus acciones y en su supervivencia, por lo que las Fuerzas y Cuerpos de Seguridad del Estado han de disponer de la capacidad suficiente para hacer frente a estos avances.

Como se ha podido observar en las soluciones que los expertos proponen para la lucha contra el terrorismo, hay dos puntos en los que es posible avanzar: cambiar la percepción que los ciudadanos tienen del terrorismo, y los apoyos financieros, y controlar el dinero. Ambos se están desarrollando en Internet porque la utilización de la red tiene un bajo coste, ofrece gran flexibilidad, acceso global y anonimato.

Para hacer frente a las nuevas formas de terrorismo y, en particular, para luchar en Internet, necesitamos utilizar la inteligencia artificial para estar, al menos, al mismo nivel que los terroristas. De lo contrario, las posibilidades de evitar el control policial y aumentar los riesgos para la sociedad serán fáciles para cualquier persona que quiera tener un impacto político en una sociedad.

En nuestra opinión, el uso de estas herramientas es necesario. Pero es cierto que podría suceder que el miedo al terrorismo se convirtiera en miedo al control estatal[68]. Esa es la razón por la que se requiere de un sistema legítimo para utilizar este tipo de herramientas entre la sociedad civil, el sector privado y el Estado[69]. En este trabajo se propone el primer paso para este nuevo contrato social: la evaluación del impacto. Como se ha observado con el trabajo de Wright et al., se ponen sobre la mesa algunas cuestiones que deberían ser consideradas por toda persona implicada en el desarrollo y uso de estas máquinas.

Las herramientas basadas en inteligencia artificial presentan un gran potencial en la lucha contra el terrorismo, pero su uso inadecuado puede poner en riesgo la Democracia de los países. Por lo tanto, será necesario seguir unos pasos que permitan su utilización de forma adecuada. En primer lugar, se requiere de un uso ético de estas herramientas. En segundo lugar, se debe replantear la protección de la intimidad en particular y de los derechos humanos en general, desde los puntos de vista administrativo y penal[70]. Por último, desde el derecho internacional, será necesario un acuerdo internacional para tratar la vigilancia en línea y el seguimiento financiero.

Todo ello podría suponer el inicio de una regulación del uso de la inteligencia artificial en el sector de la seguridad. Los avances de la Unión Europea para regular esta materia podrían tener un gran impacto en la sociedad internacional y en el sector privado. Las *Ethics Guidelines for Trustworthy Artificial Intelligence* elaboradas por el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial apuestan por un desarrollo humano en este campo, basado en el respeto a los derechos humanos. Esto supone un reto para los juristas, ya que saber traducir los principios del análisis ético en nuevos derechos para los ciudadanos requiere probablemente un replanteamiento de todo el sistema jurídico.

El impacto de esta tecnología en la vida es enorme, para bien y para mal. Si la vida normal va a estar regida por ella en muchos ámbitos, su uso en seguridad, inteligencia y delincuencia tendrá un fuerte impacto en los derechos de los ciudadanos.

Por lo tanto, se debe debatir al respecto y reaccionar rápidamente ante el impacto que estas tecnologías pueden tener. Por un lado, la no uti-

---

[68] SCHNEIER, B. (2015). *Data and Goliath*. W. W. Norton and Company, p. 448.

[69] Ibid., p. 259.

[70] VALLS-PRIETO, J. (2018). *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*. Madrid: Dykinson, p. 162.

lización de estas herramientas significaría que el terrorismo y el crimen organizado tendrán un espacio de impunidad y, por otro, su uso sin ningún límite destruiría la confianza de los ciudadanos en las instituciones del Estado. La labor las autoridades judiciales que desarrollan la investigación es crucial para mantener el debido equilibrio entre las necesidades de la investigación y el respeto de los derechos fundamentales de los ciudadanos.

Trabajando juntos, ciudadanos, sector privado y Estado, podemos producir un nuevo contrato social en el que el respeto de los derechos humanos ocupe el primer lugar entre las prioridades, que produzca nuevas formas de seguridad en nuestras sociedades, y que base la confianza en las instituciones para una "democracia inteligente". Está en nuestras manos combatir al terrorista con el Estado de Derecho, pero los derechos humanos deben ser nuestra primera y principal prioridad.