Cibercrimen: Tendencias y desafíos actuales

Coordinadores:

Marina Mínguez Rosique
David Gallego Arribas

Derecho Penal
y Procesal Penal

BOE

CIBERCRIMEN Y USO ILÍCITO DE LA INTELIGENCIA ARTIFICIAL: RETOS Y DESAFÍOS DEL DERECHO PENAL

Ivan Salvadori*

I. INTRODUCCIÓN

Algunos de los investigadores que, en los años ochenta y noventa del siglo pasado, empezaron a analizar, desde un punto de vista criminológico y jurídico-penal, las primeras manifestaciones de la criminalidad informática *(computer crime),* definieron las agresiones cometidas a través (o en contra) de los nuevos medios u «objetos» informáticos (datos, programas y sistemas informáticos) como «vino viejo en botellas nuevas» *(old wine in new bottles)* [1]. En este sentido, no habría sido necesario introducir, en las legislaciones penales nacionales, ningún tipo delictivo nuevo para luchar contra la criminalidad informática: los hechos llevados a cabo mediante el uso indebido de los medios informáticos habrían podido ser subsumidos sin particulares dificultades en los delitos tradicionales (hurto, robo, daños, estafa, violaciones a la intimida, de los secretos empresariales, etc.). Al fin y al cabo, según los partidarios

* Profesor Titular de Derecho penal, Derecho penal del medio ambiente y Derecho penal internacional. Departamento de Ciencias Jurídicas, Universidad de Verona, Italia. Dirección de contacto: ivan.salvadori@univr.it. Esta contribución es uno de los resultados del Proyecto PID2022-136548NB-I00 «Los retos de la inteligencia artificial para el Estado social y democrático de Derecho», financiado por el Ministerio de Ciencia e Innovación en la Convocatoria Proyectos de Generación de Conocimiento 2022.

[1] En este sentido, véase, p. ej., Grabosky, P., «Virtual Criminality: Old Wine in New Bottles», *Social&Legal Studies,* vol. 10(2), 2001, pp. 243 y ss. Este artículo ha sido traducido al castellano por Cano Paños, M. Á., «Criminalidad virtual: ¿vino viejo en botellas nuevas? Traducción y nota previa», *REC: Revista Electrónica de Criminología,* vol. 2, 2019. En sentido parecido, véase ya, en la doctrina estadounidense, Easterbrook, G. H., «Cyberspace and the Law of the Horse», *The University of Chicago Legal Forum,* 1996, pp. 207 y ss.; Clarke, C. T., «From CrimiNet to Cyber-perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet», *Oregon Law Review,* vol. 75, 1996, pp. 191 y ss.

de esta toma de postura, el *computer crime* habría favorecido solamente la creación de nuevos medios o instrumentos *(new bottles)* para delinquir, mientras que el desvalor de las conductas llevadas a cabo mediante dichos medios y, por consiguiente, su calificación jurídico-penal, habría quedado básicamente la misma *(old wine)* [2].

Sin embargo, la rápida evolución de las nuevas tecnologías de la información y de la comunicación (TIC) dejó claro cómo iban surgiendo nuevos bienes informáticos (datos y programas informáticos) que no podían ser equiparados ni al concepto tradicional de «cosa», como objeto material de los delitos tradicionales contra el patrimonio (hurto, robo, apropiación indebida, etc.), ni al de «documento», en relación con los delitos de falsedades documentales [3]. Ya no era posible reconducir la criminalidad informática al concepto de «vino viejo en botellas nuevas», siendo más adecuado hablar de «vino nuevo en botellas nuevas», es decir, nuevas agresiones en contra de bienes jurídicos nuevos (confidencialidad informática, integridad y disponibilidad de datos y programas informáticos, seguridad informática, etc.) que necesitaban una protección penal especial [4].

Debido a la falta de una respuesta legal adecuada y a la existencia de objetivas lagunas normativas, a los sistemas judiciales de muchos países de nuestro entorno (Alemania, Italia, Francia, etc.) no les quedó más remedio que intentar subsumir los usos ilícitos de los instrumentos informáticos y las agresiones a los nuevos objetos informáticos en los delitos tradicionales. Sin embargo, los resultados jurisprudenciales logrados por esa vía no fueron satisfactorios. Las dificultades para extender el ámbito de aplicación de los tipos

---

[2] En este sentido, véase, p. ej., O'Neill, M. E., «Old Crimes in New Bottles: Sanctioning Cybercrime», *George Mason Law Review,* vol. 9, 2000, pp. 237 y ss.

[3] Sobre esta cuestión, véase Sieber, U., *The International Handbook on Computer Crime,* Chichester (Wiley), 1986; OECD, *Computer-related crime. Analysis of Legal Policy,* Paris (OECD), 1986. En la doctrina española, véase Corcoy Bidasolo, M., «Protección penal del sabotaje informático. Especial consideración de los delitos de daños», *La Ley,* núm. 1/1990, 1990, pp. 1000 y ss.; González Rus, J. J., «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», *Revista de la Facultad de Derecho de la Universidad Complutense,* núm. 12, 1986, pp. 107 y ss.; y «Protección penal de sistemas, elementos, datos, documentos y programas informáticos», *Revista Electrónica de Ciencia Penal y Criminología,* núm. 1, 1999. En la doctrina italiana, véase Sarzana, C. «Criminalità e tecnologia: il caso dei «computer crimes»», *Rassegna Penitenziaria e Criminologica,* núm. 1/2-1979, 1979, pp. 53 y ss.; y «Note sul diritto penale dell'informatica», *La Giustizia Penale,* Fasc. I, 1984, pp. 21 y ss.; Picotti, L., «La rilevanza penale degli atti di «sabotaggio» ad impianti di elaborazione dati», *Il Diritto dell'informazione e dell'informatica,* núm. 3 (anno II), 1986, pp. 971 y ss.; Alessandri, A., «Criminalità informatica», *Rivista trimestrale di Diritto penale dell'economia,* 1990, pp. 653 y ss.; Lanzi, A., «Sviluppo e prospettive nella disciplina dei computer crimes», *L'Indice Penale,* 1992, pp. 531 y ss.

[4] Brenner, S. W., «Cybercrime Metrics: Old Wine, New Bottles?», *Virginia Journal of Law & Technology,* vol. 9, núm. 13, 2004. En sentido bastante similar, Miró Llinares, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* Madrid (Marcial Pons), 2012, pp. 144 y ss.

delictivos tradicionales sin violar los principios de legalidad y de prohibición de analogía *in malam partem* pusieron de manifiesto la urgente necesidad de reformar la legislación penal tradicional. Como subrayó también destacada doctrina, era necesario tipificar expresamente los nuevos comportamientos ilícitos cometidos a través de medios informáticos (intrusismo informático, interceptación de datos informáticos, sabotaje informático, estafas mediante manipulaciones informáticas, etc.) [5]. Así, para cubrir estos mencionados vacíos de punibilidad, a partir de la última década del siglo pasado muchos legisladores europeos, siguiendo (en todo o en parte) la Recomendación R (89) 9 sobre delitos informáticos del Consejo de Europa, empezaron a introducir nuevos tipos delictivos para sancionar las preocupantes manifestaciones de la criminalidad informática [6].

La rápida evolución de las TIC y, en particular, la difusión de Internet, abrió el paso a una verdadera revolución cibernética, que, además de ofrecer muchas ventajas a los internautas y a la sociedad, favoreció la extensión de los comportamientos ilícitos en el ciberespacio, creando nuevas oportunidades criminales para los delincuentes [7]. Dicha revolución tuvo un gran impacto, tanto desde el punto de vista criminológico como jurídico-penal, determinando un cambio de paradigma y el surgimiento de la criminalidad cibernética.

La interconexión de los sistemas de información y el acceso libre a la red determinó la superación de la criminalidad informática *(computer crime)* como categoría que incluye hechos ilícitos cometidos en contra de ordenadores no estaban interconectados *(stand-alone)* o que formaban parte de una intranet, y la expansión del cibercrimen *(cyber crime),* que, en sentido amplio, abarca todo tipo de comportamiento ilícito (tradicional o nuevo) que puede llevarse a cabo en el ciberespacio (injurias, violaciones del derecho de autor, espionaje empresarial, sabotaje informático, etc.) [8]. Asimismo, los cibercrimi-

---

[5] Brenner, S. W., «Cybercrime Metrics: Old Wine, New Bottles?», *Virginia Journal of Law & Technology,* vol. 9, núm. 13, 2004.

[6] Recomendación Núm. R (89)9 del Comité de Ministros a los Estados Miembros sobre delitos informáticos, 1989. Véase también CONSEIL DE L'EUROPE, *La criminalitè informatique (Reccomandation n.º R (89) 9),* Strasbourg (Conseil del'Europe), 1990. Sobre esta cuestión, véase también, a nivel doctrinal, Sieber, U., *The International Emergence of Criminal Information Law,* Köln (Carl Heymanns Verlag KG), 1992.

[7] Véase, en este sentido, Miró Llinares, F., «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», *Revista Electrónica de Ciencia Penal y Criminología,* núm. 13, 2011, pp. 1 y ss.; García González, J., «Oportunidad criminal, internet y redes sociales. Especial referencia a los menores de edad como usuarios más vulnerables», *Indret,* núm. 4/2015, 2015, pp. 1 y ss.

[8] En este sentido, véase, p. ej., Picotti, L., «Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme», en Cadoppi, A. *et al* (dirs.), *Cybercrime,* 2.ª ed., Torino (UTET), 2023, pp. 31 y ss. y pp. 46 y ss.

nales ya no actuaban únicamente de manera individual, sino también de forma organizada, y, poco a poco, empezaron a ofrecer y poner a la venta de terceros, sobre todo en la *Dark web,* sus herramientas y su *know-how* para delinquir *(Cybercrime as a Service o CaaS),* favoreciendo de esta manera la comisión de ciberdelitos [9].

En los últimos tiempos, los ciberdelincuentes se han aprovechado de las enormes potencialidades de las tecnologías de la IA con fines ilícitos, desarrollando nuevas formas de agresiones y ciberataques cada vez más peligrosos *(spear-phishing, AI-generated malware attacks,* etc.). Gracias a los avances de la IA, del *machine learning,* de las redes neuronales y de la inteligencia artificial generativa, los criminales pueden llevar a cabo ataques más sofisticados y múltiples agresiones a bienes jurídicos fundamentales (vida, integridad física o sexual, honor, patrimonio, la seguridad y el orden público, etc.) [10]. Esta nueva categoría de delitos cometidos a través de la IA, que suele denominarse con la expresión anglosajona *«AI-Crime»,* abarca una multiplicidad de hechos ilícitos llevados a cabo a través de algoritmos, agentes artificiales, robots o sistemas de información inteligentes [11]. Se trata de nuevos hechos ilícitos, caracterizados por su complejidad tecnológica, que plantean nuevos problemas tanto a nivel interpretativo y hermenéutico –en relación con la posibilidad de subsumirlos en los tipos penales vigentes– como dogmáticos –al incidir sobre los fundamentos de la responsabilidad penal y la teoría del delito– [12]. No queda

[9] Véase Leukfeldt, E. R. / Lavorgna, A. / Kleemans, E. R., «Organised Cybecrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime», *European Journal on Criminal Policy and Research,* vol. 23 (3), 2017, pp. 287 y ss.; FBI, *Internet Crime Report 2023,* disponible en: www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[10] Caldwell, M. / Andrews, J. T. A. / Tanay, T., Griffin, L. D., «AI-Enabled Future Crime», *Crime Science,* vol. 9, 2020, pp. 1 y ss.; King, T. C. / Aggarwal, N. / Taddeo, M. / Floridi, L., «Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions», *Science and Engineering Ethics,* vol. 26, 2020, pp. 1 y ss.

[11] King, T. C. / Aggarwal, N. / Taddeo, M. / Floridi, L., «Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions», *Science and Engineering Ethics,* vol. 26, 2020, pp. 1 y ss.; Salvadori, I., «Agentes artificiales, opacidad tecnológica y distribución de la responsabilidad penal», *Cuadernos de Política Criminal,* núm. 133, 2021, pp. 137 y ss.

[12] En relación con los problemas político-criminales y dogmáticos que plantea la IA, véase, en el debate español e italiano, Quintero Olivares, G., «La Robótica ante el Derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas», *Revista Electrónica de Estudios Penales y de la Seguridad,* núm. 1, 2017, p. 9; Blanco Cordero, I., «Homo Sapiens y ¿machina sapiens? Un Derecho penal para los robots dotados de inteligencia artificial», en Mallada Fernández, C. (coord.), *Nuevos retos de la ciberseguridad en un contexto cambiante,* Navarra (Aranzadi), 2019, pp. 63 y ss.; Valls Prieto, J., *Inteligencia artificial, Derechos Humanos y bienes jurídicos,* Navarra (Aranzadi), 2021; Romeo Casabona, C. M. / Rueda Martín M. A. (eds). *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial,* Granada (Comares), 2023; Cappellini, A., «Machina delinquere potest? *Brevi appunti su intelligenza artificiale e responsabilità penale», Criminalia*, 2019, pp. 499 y ss.; Manes, V., «L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocracia», *discrimen.it,* 15.05.2020; Piergallini, C., «Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?», *Rivista italiana di diritto e procedura penale*, vol. 63,

claro, por lo tanto, de si se trata, en este caso, de «vino viejo en botellas nuevas» o, más bien, de una forma de criminalidad completamente nueva, que necesita nuevas respuestas penales.

En este trabajo se analizará, en primer lugar, la evolución de la legislación penal española e italiana contra la criminalidad informática *(computer crime)* y el proceso de aproximación en la regulación de los ciberdelitos (apartados 2 y 2.1). En segundo lugar, se centrará la atención en el cibercrimen y en las manifestaciones más frecuentes del *AI-Crime* (apartado 3). De esta manera, será posible comprobar si (algunos de) los delitos cibernéticos vigentes en España e Italia pueden aplicarse a las más recientes amenazas llevadas a cabo mediante el uso ilícito de la inteligencia artificial. En este sentido, se analizará la relevancia penal que puede tener el uso de la IA como modalidad de ejecución de un hecho ilícito (apartado 3.1) y las agresiones a los sistemas de inteligencia artificial (apartado 3.2). Como conclusión, se formularán algunas consideraciones finales sobre los nuevos retos del Derecho penal en la lucha contra el *AI-Crime* (apartado 4).

II. LA EVOLUCIÓN DEL DERECHO PENAL DE LAS NUEVAS TECNOLOGÍAS EN ESPAÑA E ITALIA

Italia fue uno de los primeros países europeos en introducir medidas penales *ad hoc* para luchar contra la criminalidad informática *(computer crime)* [13]. Con la Ley 23 diciembre 1993, n. 547, de modificaciones e integraciones de las normas del Código Penal y del Código Procesal Penal en el ámbito de la

---

núm. 4, 2020, pp. 1743 y ss.; Salvadori, I., «Agentes artificiales, opacidad tecnológica y distribución de la responsabilidad penal», *Cuadernos de Política Criminal,* núm. 133, 2021, pp. 137 y ss.; Salvadori, I., «Interazione uomo-agente artificiale, eventi lesivi e allocazione della responsabilità penale», en Picotti, L. (coord.), *Automazione, diritto e responsabilità,* Napoli (Edizioni Scientifiche Italiane), 2023, pp. 153 y ss.

[13] Lo mismo hizo Alemania con la segunda ley de lucha contra la criminalidad económica (*Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität - 2. WiKG),* de 15 de mayo de 1986, que se publicó en el *Bundesgesetzblatt,* n. 21 del 23 de mayo de 1986 (BGBI 1986, I, 721). Mediante dicha ley, el legislador alemán introdujo en el §263a StGB el delito de estafa informática *(Computerbetrug),* en el § 269 StGB el delito de falsedades informáticas *(Fälschung beweiserheblicher Daten),* en el § 303a StGB los delitos de daños de datos informáticos *(Datenveränderung),* en el §303b StGB el sabotaje informático *(Computersabotage)* y, en el §202a el delito de espionaje de datos informático. Sobre los delitos informáticos introducidos mediante el 2. *WiKG,* véase Weber, U., «Aktuelle Probleme bei der Anwendung des Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, Recht und Kriminalität», en Schlüchter, E. / Laubenthal, K. (coords.), *Recht und Kriminalität: Festschrift für Friedrich-Wilhelm Krause zum 70. Geburtstag,* Köln (Heymann), 1990, pp. 427 y ss.; Meuerer, D., «Die Bekämpfung der Computerkriminalität in der Bundesrepublik Deutschland, Wege zum japanischen Recht», en Leser, H. G. / Isomura, T. (coords.), *Wege zum japanischen Recht Festschrift für Zentaro Kitagawa zum 60. Geburtstag am 5. April 1992,* Berlin (Dunker & Humblot), 1992, pp. 971 y ss.

criminalidad informática, el Parlamento italiano introdujo, en el Código Penal de 1930 (que hoy en día sigue estando vigente), un abanico muy amplio de delitos informáticos. Así, siguiendo la mencionada Recomendación del Consejo de Europa, el legislador italiano pasó a castigar, de manera expresa, las falsedades informáticas (art. 491 bis CP), el acceso no autorizado a un sistema informático o telemático (art. 615 ter CP), la interceptación, obstaculización o interrupción ilícita de comunicaciones informáticas o telemáticas (art. 617 quater CP), la instalación de aparatos destinados a interceptar, impedir o interrumpir las comunicaciones informáticas o telemáticas (art. 617 quinquies CP), la falsificación, alteración o supresión del contenido de comunicaciones informáticas o telemáticas (art. 617 sexies CP), los daños a sistemas informáticos o telemáticos (art. 635 bis CP) y el fraude informático (art. 640 ter CP). Asimismo, yendo más allá de lo establecido por el Consejo de Europa en su Recomendación, el Parlamento italiano, adelantando las barreras de protección penal, estableció, además, la relevancia penal de la difusión ilícita de códigos de acceso a sistemas informáticos o telemáticos (art. 615 quater CP) y de programas dirigidos a dañar o interrumpir el funcionamiento de un sistema de información (art. 615 quinquies CP) [14].

Por su parte, el mismo legislador español, con la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, superando las objetivas lagunas normativas que había en el anterior Código Penal, decidió sancionar el apoderamiento de correos electrónicos ajenos (art. 197.1 CP), el apoderamiento, utilización o modificación, en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos (art. 197.2 CP), el uso no autorizado de cualquier equipo terminal de telecomunicación (art. 256 CP), el fraude informático (art. 248.2 CP) [15] y el sabotaje informático (art. 264.2 CP) [16]. Contrariamente a lo que solicitaba el Consejo de Europa, no consideró necesario introducir un

[14] Sobre las novedades más importantes introducidas con la Ley 23 diciembre 1993, n. 547, véase Mucciarelli, F. / Picotti, L. / Rinaldi, L. / Uguccioni, L., «Legge 547 del 1993», en *Legislazione penale,* 1996, pp. 57 y ss.; Borruso, R. / Buonuomo, G. / Corasaniti, G. / D'aietti, G., *Profili penali dell'informatica,* Milano (Mondadori), 1994; Pica, G., *Diritto penale delle tecnologie informatiche,* Torino (UTET), 1999, *passim*.

[15] Con la Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, se añadió un apartado 3 al artículo 248 para castigar, con la misma pena establecida, *«a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo»*.

[16] Morón Lerma, E., *Internet y Derecho penal: hacking y otras conductas ilícitas en la Red,* Navarra (Aranzadi), 2002.

nuevo tipo delictivo para castigar el intrusismo informático *(hacking)* [17]. Tal y como puede observarse, la técnica de formulación normativa de los delitos informáticos introducidos en el Código Penal español de 1995 fue distinta a la de los países de su entorno. En lugar de crear tipos delictivos autónomos, como hicieron, por ejemplo, Alemania y, en parte, Italia, el legislador español consideró suficiente extender el ámbito de aplicación de los delitos tradicionales (estafa, daños, violaciones a la intimidad, etc.), que presentaban analogías con los nuevos actos ilícitos cometidos a través de las nuevas tecnologías. En particular, la extensión de los delitos tradicionales se llevó a cabo mediante la previsión, por un lado, de nuevas conductas típicas y, por otro lado, la introducción de nuevos objetos materiales [18].

A la hora de eliminar las lagunas normativas que dificultaban la incriminación de las nuevas manifestaciones criminales, tanto el legislador italiano como el legislador español no recurrieron a una ley penal especial [19], evitándose así el peligro de dejar la normativa penal sobre la criminalidad informática fuera del Código Penal. Por otro lado, tampoco se agruparon los delitos informáticos dentro de un título específico del Código Penal (como sí hicieron los legisladores de Francia o Bélgica), al considerarse que tanto la legislación penal informática como los bienes jurídicos protegidos no revestían un carácter tan novedoso o peculiar que justificara la creación de un título autónomo. Así, en España e Italia, los delitos informáticos se introdujeron, dentro del mismo

---

[17] En relación con las dificultades de castigar el hacking en falta de un tipo delictivo expreso véase Gutiérrez Francés, M. L., «El intrusismo informático (hacking): ¿represión penal autónoma?». *Informática y derecho: Revista iberoamericana de derecho informático,* núm. 12-15, 1996, pp. 1163 y ss. Sobre la necesidad de castigar de manera expresa el intrusismo informático, véase también Matellanes Rodríguez, N., «El intrusismo informático como delito autónomo», *Revista General de Derecho Penal,* núm. 2, 2004, pp. 79 y ss.; Matellanes Rodríguez, N., «Algunas razones para la represión autónoma del intrusismo informático», *Derecho Penal y Criminología,* vol. 26, núm. 77, 2005, pp. 131 y ss.; Rueda Martín, M. Á., «Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político- criminales», *Revista penal,* núm. 1, 2008, pp. 65 y ss.

[18] Ejemplo de la primera técnica de tipificación es el delito de fraude informático, que originariamente se encontraba en el art. 248.2 CP. Contrariamente al delito de estafa del art. 248.1 CP, el fraude informático, en su originaria formulación de 1995, castigaba al que consigue un acto de disposición patrimonial mediante una manipulación informática o un artificio semejante, en lugar del engaño bastante para inducir a error a otro. Un ejemplo de extensión del ámbito de aplicación de los delitos tradicionales mediante la previsión de nuevos objetos materiales fue el originario delito de daños de datos, programas y documentos informáticos del art. 264.2 CP: «*La misma pena* [pena de prisión de uno a tres años y multa de doce a veinticuatro meses)] *se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos».*

[19] Distinta fue la decisión del legislador portugués que, en lugar de incluir los delitos informáticos dentro del Código Penal, decidió reunirlos, debido a sus peculiaridades técnicas, dentro de la Ley 17 agosto 1991, n. 109. En este sentido, véase Faria Costa, J., «Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique au Portugal», *International Review of Penal Law,* vol. 64, núm. 1-2, 1993, pp. 517 ss.

Código Penal, junto a aquellos delitos tradicionales que presentaban, en opinión del legislador, aspectos parecidos (estafa, daños, etc.). Sin embargo, el esfuerzo para adaptar estos delitos informáticos, tanto desde el punto de vista de su formulación como de su consecuencia jurídica, a los tipos penales tradicionales, como si con las nuevas tecnologías hubiesen cambiado solamente las modalidades de agresión a los bienes jurídicos tradicionales, llevó ambos legisladores a tipificarlos de manera no siempre satisfactoria.

1. **Aproximación a la regulación penal de los delitos cibernéticos**

Gracias a los esfuerzos del Consejo de Europa y de la Unión Europea para mejorar las estrategias en la lucha contra la criminalidad informática y, sobre todo, contra el cibercrimen, en los últimos años ha tenido lugar, afortunadamente, un proceso de convergencia y aproximación de la legislación penal de los Estados miembros [20]. Esto explica por qué el Derecho penal de las nuevas tecnologías tanto en Italia como en España ha sido objeto de múltiples reformas, que, poco a poco, han producido el acercamiento de muchos tipos penales de ambos países.

Para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, el legislador español, con la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, modificó varios delitos informáticos. Tal y como se hizo en 1995, los nuevos tipos penales se han introducido al lado de aquellos delitos tradicionales que presentan algunas (supuestas) analogías. En este sentido, la Ley Orgánica 5/2010 introdujo un nuevo apartado tercero en el artículo 197 CP, para castigar de manera expresa el acceso sin autorización, y vulnerando las medidas de seguridad, a datos o programas informáticos contenidos en un sistema de información o en parte

[20] A nivel de la ONU se está elaborando, por parte de un comité internacional de expertos, una propuesta de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos. De acuerdo con la Resolución 75/292, de 26 de mayo de 2021, de la Asamblea General de Naciones Unidas, la propuesta de Convención tendría que presentarse con ocasión de la sesión número 78 de la Asamblea General, que debería haberse celebrado entre septiembre de 2023 y septiembre de 2024. Sin embargo, de momento, los Estados miembros no han encontrado todavía un acuerdo sobre el texto de la Convención que, de aprobarse, favorecería la cooperación judicial entre los Estados de la ONU para prevenir y combatir la utilización de las TIC con fines delictivos. La Asamblea General, en su decisión 78/549, ha establecido que la mencionada propuesta tendrá que presentarse en una nueva sesión, que se celebrará entre el 29 de julio y el 9 de agosto de 2024 en Nueva York.

del mismo [21]. Al mismo tiempo, con la LO 5/2010 se tipificó, dentro del apartado tercero del art. 248 CP, tras la estafa tradicional (art. 248.1) y el fraude informático (art. 248.1), la cada vez más extendida modalidad de defraudar utilizando tarjetas ajenas o los datos obrantes en ellas, y, de esta manera, llevar a cabo operaciones de cualquier clase en perjuicio de su titular o de un tercero [22].

Sin embargo, a diferencia de lo que hizo el legislador en 1995, el legislador de 2010 decidió colocar los daños informáticos en apartados diferentes: un primer apartado, relativo a los daños de datos y programas informáticos (art. 264.1 CP), y un segundo apartado, relativo al hecho de obstaculizar o interrumpir el funcionamiento de un sistema de información ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave (264.2 CP). El legislador español de 2010 superó, además, el principio *societas delinquere non potest,* introduciendo en el Código Penal la responsabilidad penal de las personas jurídicas. Su aplicación fue limitada a un número cerrado de delitos, dentro de los cuales se incluyeron también los delitos informáticos, en línea con el artículo 9 de la Decisión Marco 2005/222/JAH.

Asimismo, para cumplimentar el Convenio de Lanzarote del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, el legislador español, con la mencionada LO 5/2010, introdujo, en el art. 183 bis CP, un precepto de nuevo cuño para castigar el embaucamiento de menores *(child-grooming)* [23]. Se trata, en este caso, de un paradigmático ejemplo de delito cibernético en sentido estricto, puesto que castiga solamente las conductas de embaucamiento de menores que se llevan a cabo «a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación» [24].

Años más tarde, para transponer la Directiva 2011/93/UE, 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, el legislador español modificó distintos delitos sexuales con la Ley Orgánica 1/2015. En particular, merece la pena destacar aquí el nuevo

---

[21] Sobre la reforma del Derecho penal informático de 2010, véase Salvadori, I., «Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de Derecho comparado», *Anuario de Derecho Penal y Ciencias Penales,* vol. LXIV, 2011, pp. 221 y ss.

[22] Galán Muñoz, A., «El nuevo delito del artículo 248.3 CP: ¿un adelantamiento desmedido de las barreras de protección penal del patrimonio?», *La Ley,* núm. 3-2004, 2004, pp. 1859 y ss.

[23] Tras la reforma de la Ley Orgánica 10/2015, el delito de embaucamiento de menores se encuentra ahora tipificado en el art. 183 CP.

[24] Sobre las distintas técnicas de incriminación del embaucamiento de menores empleadas en los países de *civil law* y de *common law,* véase Salvadori, I., *L'adescamento di minori. Il contrasto al child-grooming tra incriminazione di atti preparatori ed esigenze di garanzia,* Torino (G. Giappichelli), 2018.

delito cibernético (en sentido estricto) introducido en el nuevo apartado quinto del artículo 189 CP, que, adelantando la protección penal, castiga la mera visualización de pornografía infantil, es decir, el hecho de acceder a sabiendas a este tipo de material o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección por medio de las TIC [25].

En virtud de esta misma Ley Orgánica 1/2015, el legislador español llevó a cabo también la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información. De acuerdo con el planteamiento recogido en la mencionada Directiva, se tipificó, dentro del nuevo art. 197 bis CP, el mero intrusismo informático, castigando, de manera parecida al art. 615*ter* del Código Penal italiano, tanto el hecho de acceder al conjunto o una parte de un sistema de información como el de mantenerse en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo [26]. Asimismo, con esta reforma se introdujo también un nuevo precepto, en el segundo apartado del nuevo art. 197 bis CP, para castigar la interceptación (mediante *spyware, keylogger,* etc.) de transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos. De esta manera, en conformidad con el art. 6 de la Directiva europea 2013/40/UE, se sanciona oportunamente la interceptación no autorizada de cualquier tipo de transmisión de datos informáticos que no tenga el carácter de comunicación interpersonal y que se lleve a efecto por redes privadas. Las mencionadas conductas no tienen por lo tanto que afectar a la intimidad o a los datos informáticos de personas concretas y determinadas [27].

Esta reforma también implicó la introducción en el Código Penal del art. 197 ter, con el objeto de castigar la facilitación y la producción de programas informáticos o equipos específicamente diseñados o adaptados para la comisión

---

[25] Sobre las dificultades probatorias que entraña el mencionado delito, véase la Circular de la Fiscalía General del Estado 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015. Subraya los múltiples aspectos críticos de la introducción del mencionado delito Fernández Teruelo, J. G., «Expansión de la represión penal de la pornografía infantil: La indemnidad sexual de los adultos que parecen menores y la de los personajes 3D», *Revista penal,* núm. 42, 2018, pp. 67 y ss.

[26] Sobre la nueva formulación del delito de intrusismo informático del art. 197 bis CP y los problemas interpretativos que plantea, véase Pedreira González, F. M., *El delito de hacking,* Valencia (Tirant lo Blanch), 2023. En relación con el controvertido ámbito de aplicación del art. 615 *ter* del Código Penal italiano, véase Salvadori, I., «¿El delito de acceso abusivo a un sistema informático se puede aplicar también a los *insider?», Revista de Derecho Penal Contemporáneo,* núm. 43, 2013, pp. 5 y ss.; Salvadori, I., «Il delitto di accesso abusivo ad un sistema informatico o telematico. Sono maturi i tempi per un suo restyling?», en AIPDP, *La riforma dei delitti contro la persona,* Milano (DiPLaP), 2023, pp. 579 y ss.

[27] Véase la Circular de la Fiscalía General del Estado 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, párrafo 1.3.2.

del delito de intrusismo informático del art. 197 bis CP. Se trata de un delito de emprendimiento, que adelanta la protección del bien jurídico de la intimidad informática [28]. Asimismo, se procedió a realizar una reorganización sistemática de los delitos de daños informáticos, tipificando y sancionando oportunamente por separado las interferencias en datos, documentos y programas informáticos ajenos (art. 264 CP) y en los sistemas de información (art. 264 bis CP), con el fin de diferenciar la respuesta penal con base en la diferente gravedad de los hechos, como exige la mencionada directiva europea [29]. También en relación con los daños informáticos, se tipificó la facilitación y la producción de programas informáticos o equipos específicamente diseñados o adaptados para la comisión de un delito de daños informáticos (art. 264 ter CP). Para los mencionados delitos cibernéticos se estableció además la responsabilidad de las personas jurídicas (arts. 197 quinquies y art. 264 quater CP).

La necesidad de proceder a la transposición al ordenamiento jurídico de la Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, llevó a que en el año 2022 el legislador español separara, por un lado, en el artículo 249 del Código Penal, el delito de fraude informático de la estafa común, que permanece en el artículo 248 CP, y, por otro lado, a ampliar sus conductas típicas. Además de las modalidades tradicionales del «*valerse de cualquier otra manipulación informática o artificio semejante*», el nuevo delito de fraude informático puede ahora llevarse a cabo mediante el hecho de *«obstaculizar o interferir indebidamente en el funcionamiento de un sistema de información»* o de *«introducir, alterar, borrar, transmitir o suprimir indebidamente datos informáticos»* [30]. Se trata de una transposición literal del art. 6 de la directiva 2019/713 que no era necesaria en relación

[28] En relación con la incriminación de los programas informáticos de doble uso *(dual-use software),* en cuya categoría hay que incluir el art. 197 *bis*.2 CP, véase Salvadori, I., «La incriminación de software «de doble uso» en el Derecho penal europeo e italiano», *Revista General de Derecho Penal,* núm. 28, 2017, pp. 1 y ss.

[29] Sin embargo, este objetivo parece que no se ha conseguido por completo, puesto que el tipo básico del delito de daños de datos informáticos del art. 264.1 CP se castiga con la misma pena (prisión de seis meses a 3 años) que la que se establece por el tipo básico del delito más grave de daños de sistemas informáticos del art. 264 *bis*.1 CP. En relación con los delitos de daños informáticos y su relevancia penal, véase Rueda Martín, M.Á., «Los ataques de denegación de servicios como ciberdelito en el Código Penal español», *Revista Penal,* núm. 49, 2022, pp. 183 y ss.

[30] Bastante parecida es, desde el punto de vista del hecho típico, la formulación del delito de fraude informático en Italia. El art. 640 *ter* del Código Penal italiano castiga con la pena de prisión de 6 meses a 3 años y multa, a quien consiga para sí mismo o para un tercero un beneficio injusto en prejuicio ajeno alterando de cualquier modo el funcionamiento de un sistema informático o de telecomunicaciones o interviniendo sin derecho de cualquier modo en los datos, informaciones o programas contenidos en un sistema informático o de telecomunicaciones o perteneciente al mismo.

con el delito de fraude informático, puesto que la originaria formulación del art. 248.2 CP ya se encontraba en línea con lo establecido en la mencionada directiva [31]: el concepto de «manipulación informática», previsto en la originaria formulación del art. 248.2 CP, era ya lo suficientemente amplio como para abarcar, tal y como había sido reconocido por la doctrina y la jurisprudencia, cualquier alteración o modificación no autorizada de datos o programas informáticos, así como de sistemas de información [32]. En este sentido, mejor habría hecho el legislador español en eliminar la referencia, dentro del tipo penal, de la expresión «artificio semejante», al tratarse de una cláusula general que no respeta el principio de taxatividad y de legalidad [33]. Al mismo tiempo, el legislador de 2022 extendió la relevancia penal de las conductas que implican el uso de forma fraudulenta de cualquier medio de pago distinto del efectivo, que ahora abarcan los mecanismos de pago tanto materiales como inmateriales y digitales, así como su sustracción, apropiación o adquisición de forma ilícita con finalidad de utilización fraudulenta.

El legislador italiano, contrariamente a lo que ha hecho en algunas ocasiones el legislador español, no ha traspuesto de manera (casi) literal las disposiciones europeas e internacionales sobre el cibercrimen. Sin embargo, dicha transposición se ha llevado a cabo casi siempre fuera del plazo establecido y mediante técnicas de incriminación que no siempre se corresponden con las obligaciones de incriminación establecidas en la directivas europeas o recomendadas por los convenios del Consejo de Europa. En este sentido, debe remarcarse cómo solo en 2008, el Parlamento italiano, con mucho retraso respecto a los demás países de Europa (Francia, Alemania, Austria, etc.), ratificó y dio actuación al Convenio sobre la ciberdelincuencia del Consejo de Europa, hecho en Budapest el 23 de noviembre de 2001 [34]. Así, con la Ley de 18 de

[31] En sentido parecido, Bustos Rubio, M., «La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal», *Revista de Derecho, Internet y política,* núm. 38, 2023, pp. 1 y ss. (pp. 6 y ss.).

[32] En este sentido, véase Mata y Martín, R. M., *Delincuencia informática y Derecho Penal,* Madrid (Edisofer), 2001, pp. 48 y ss.; Faraldo Cabana, P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico,* Valencia (Tirant lo Blanch), 2009, pp. 89 y ss.; Miró Llinares, F., «La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del *phishing», Revista Electrónica de Ciencia Penal y Criminología,* núm. 15, 2013, pp. 12 y ss.

[33] En este sentido, véase también Faraldo Cabana, P., «Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática», *Eguzkilore,* núm. 21, 2007, p. 43, quien subraya que la única manera de reducir la excesiva extensión de la mencionada conducta típica consistiría en exigir un carácter informático al «artificio» para que sea semejante a la conducta de manipulación informática.

[34] El Convenio sobre Ciberdelincuencia fue ratificado por España en el año 2010 (BOE de 17 de septiembre). En relación con el contenido del mencionado Convenio, véase Morón Lerma, E. / Rodríguez Puerta, M. J., «Traducción y breve comentario del convenio sobre cibercriminalidad», *Revista de Derecho y Proceso Penal,* núm. 7, 2002, pp. 167 y ss.

marzo de 2008, n. 48, de ratificación y ejecución del Convenio de Budapest de 2001, el legislador italiano reformó, en primer lugar, los delitos de falsedades informáticas (art. 491 bis CP) y de daños informáticos (art. 635 bis CP). En segundo lugar, introdujo nuevos ciberdelitos, alejándose por completo de lo establecido en el mencionado Convenio del Consejo de Europa. Paradigmáticos, en este sentido, son los delitos de declaración o afirmación falsa al certificador de firma electrónica (art. 495 bis CP), de daños de datos informáticos y de sistemas informáticos pertenecientes a particulares (arts. 635 bis y 635 ter CP) y a entidades públicas (arts. 635 quater y 635 quinquies CP) [35], y de fraude informático por parte del sujeto que lleva a cabo servicios de certificación de firma electrónica (art. 640 quinquies CP) [36].

Tras un procedimiento de infracción abierto contra Italia por parte de la Comisión Europea por no transponer, dentro del plazo establecido, la directiva 2013/40/UE, relativa a los ataques contra los sistemas de información, el Parlamento italiano, con el art. 19 de la Ley 23 de diciembre 2021, n. 238, relativa a las disposiciones para actuar las obligaciones que consiguen de la pertenencia de Italia a la Unión Europea, reformó parte de la legislación penal sobre el cibercrimen y, en particular, los delitos contra la intimidad y la seguridad informática (arts. 615 quater, 615 quinquies, 617 quater y 617 quinquies CP) [37]. De esta manera, con la Ley 8 noviembre 2021, n. 184, de actuación de la directiva 2019/713/UE del Parlamento europeo y del Consejo, del 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la decisión marco 2021/413/GAI del Consejo, el Parlamento italiano reformó el art. 493 ter CP, incluyendo en el objeto material del delito de utilización indebida y de falsificación de medios de pago, además de las tarjeas de débito y crédito, cualquier instrumento de pago distinto del efectivo [38]. Asimismo, el Parlamento italiano introdujo, dentro de los delitos contra la fe pública del título VII del libro segundo del Código Penal,

[35] Sobre los daños informáticos en la legislación penal italiana, véase Salvadori, I., «La regulación de los daños informáticos en el Código Penal italiano», *Revista de Internet, Derecho y Política,* núm. 16, 2013, pp. 44 y ss.

[36] Sobre las novedades introducidas en el Código Penal italiano con la Ley n.º 48/2008, véase Picotti, L., «La ratifica della Convenzione cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale», *Diritto Penale e Processo,* núm. 6, 2008, pp. 700 y ss.

[37] Sobre las principales novedades introducidas en 2021 en el ámbito del Derecho penal de las nuevas tecnologías, véase Crescioli, C., «Le recenti modifiche ai reati cibernetici, tra tardivo recepimento delle direttive europee e nuove incriminazioni: riflessioni critiche», *Archivio Penale,* núm. 2, 2022, pp. 1 y ss.; Salvadori, I., «I reati contro la riservatezza informática», en Cadoppi, A. *et al* (dirs.), *Cybercrime,* 2.ª ed., Torino (UTET), 2023, pp. 694 y ss.

[38] En este sentido, véase Crescioli, C., «Le recenti modifiche ai reati cibernetici, tra tardivo recepimento delle direttive europee e nuove incriminazioni: riflessioni critiche», *Archivio Penale,* núm. 2, 2022, pp. 3 y ss.

un precepto penal de nuevo cuño para castigar la tenencia y la difusión de aparatos, dispositivos o programas informáticos dirigidos a cometer delitos relacionas con los sistemas de pago distintos de los efectivos (art. 493 quater CP). Las conductas sancionadas por dicho precepto son las mismas mencionadas en el artículo 7 de la Directiva 2019/713/UE, es decir la producción, la importación, la exportación, la venta, el transporte, la distribución, la puesta a disposición de terceros y la obtención para uno mismo o para otra persona de aparados, dispositivos o programas informáticos que, por sus características técnicas o de construcción, están *«construidos principalmente o adaptados específicamente»* para cometer cualquiera de los delitos relacionados con los medios de pagos.

En conclusión, se puede afirmar que las recientes leyes de transposición de las directivas europeas han acercado la legislación penal sobre el cibercrimen de España e Italia. Quedan, por supuesto, importantes diferencias, sobre todo en relación con la normativa en materia de intrusismo informático y de daños informáticos. De todos modos, con estas reformas se han cubierto varias lagunas normativas y, al mismo tiempo, se ha superado la obsolescencia de algunos tipos penales que, como habían puesto de manifiesto la doctrina y la jurisprudencia, no permitían castigar las manifestaciones más recientes del cibercrimen.

III. CIBERCRIMEN Y USO ILÍCITO DE LA INTELIGENCIA ARTIFICIAL

En la actualidad no existe, ni a nivel europeo ni supranacional, una definición común de cibercrimen [39]. La doctrina suele incluir en este concepto aquellos comportamientos ilícitos que pueden realizarse exclusivamente en el entorno digital (cibercrimen en sentido estricto) o que pueden llevarse a cabo tanto en el mundo «real» (off-line) como en el ciberespacio (cibercrimen en sentido amplio). Son ejemplos del cibercrimen en sentido estricto las conductas de *phishing, vishing, pharming* o los ciberataques, al tratarse de agresiones que no podrían llevarse a cabo fuera de un contexto digital o de la red. Por otro lado, dentro de la categoría del cibercrimen en sentido amplio deben incluirse

[39] No consta ninguna definición de «cibercrimen» en ninguno de los instrumentos de la Unión Europea o del Consejo de Europa, ni tampoco en el Tratado de Naciones Unidas. En la doctrina, véase Philipps, K. / Davidson, J. C. / Farr, R. R. / Burkhardt, C. / Caneppele, S. / Aiken, M. P., «Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies», *Forensic Sciences,* núm. 2, 2022, pp. 379 y ss.; Curtis, J. / Oxburgh, G., «Understanding Cybercrime in 'Real World' Policing and Law Enforcement», *The Police Journal,* vol. 96, 2023, pp. 573 y ss.

todos aquellos delitos que, pese a no tener en su formulación normativa elementos de naturaleza informática, pueden llevarse a cabo tanto en el mundo real *(off-line)* como en el ciberespacio, como pueden ser, por ejemplo, las estafas online (mediante falsos anuncios de empleo, de compraventa, etc.), las injurias o el ciber-acoso *(stalking).*

En los últimos años, el rápido desarrollo de la inteligencia artificial, de las redes neuronales y de la inteligencia artificial generativa (AIG) ha favorecido la creación de algoritmos y, en particular, de agentes inteligentes (o robots) que poseen un nivel de autonomía cada vez más alto, y que permiten sustituir, en todo o en parte, muchas actividades humanas. El empleo en distintos ámbitos de la IA y de los robots lleva consigo muchos beneficios para la sociedad, pero la IA constituye un típico ejemplo de tecnología de «doble uso» *(dual-use technology),* pues puede ser empleada no solamente para llevar a cabo actividades lícitas, sino también ilícitas [40]. En relación con los comportamientos ilícitos realizados mediante la IA, la doctrina de habla inglesa ha creado el concepto de *Artificial Intelligence Crime* [41].

La difusión de la IA y su uso ilícito lleva consigo la generación de nuevas formas de agresión a bienes jurídicos tanto tradicionales (patrimonio, vida, integridad física, dignidad, etc.) como modernos (intimidad informática, seguridad informática, etc.). Recientes noticias de actualidad ponen de manifiesto cómo los ciberdelincuentes han empezado a emplear las múltiples tecnologías de IA para hacerse con las contraseñas que protegen los sistemas de información y, de esta manera, introducirse en los mismos con finalidades ilícitas (manipular, sustraer o dañar datos o programas informáticos), para llevar a cabo nuevas formas de estafas o de fraudes informáticos (como, p. ej., el *spear phishing),* para manipular la opinión pública mediante *fake news* y *deep fake,* para producir y difundir nuevos contenidos ilícitos (p. ej. pornografía infantil mediante *deep nude),* etc. En este sentido, se estima que dentro de unos años los ciberataques lanzados con IA *(AI-Driven malware)* serán algo muy común [42].

Las agresiones y las amenazas relacionadas con el uso ilícito de la IA pueden manifestarse en muchos y muy diversos ámbitos. El AIC puede afectar, en primer lugar, a la seguridad informática, es decir, la intimidad, la dispo-

[40] Yamin M. / Ullah M. / Ullah H. / Katt B., «Weaponized AI for Cyber Attacks», Journal of Information Security and Applications, vol. 57, 2021, pp. 1 y ss.

[41] En este sentido, véase, p. ej., King, T. C. / Aggarwal, N. / Taddeo, M. / Floridi, L., «Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions», *Science and Engineering Ethics,* vol. 26, 2019, pp. 1 y ss.

[42] Guembe, B. / Azeta, A. / Misra S. / Chukwudi Osamor, V. / Fernández-Sanz, L. / Pospelova, V., «The Emerging Threat of AI-Driven Cyber Attacks: A Review», *Applied Artificial Intelligence,* vol. 36, 2022, pp. 1 y ss.

nibilidad e integridad de datos y sistemas informáticos tanto de sujetos particulares como de entidades públicas. En este sentido, son especialmente vulnerables los sistemas de información que son esenciales para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad y la protección y el bienestar económico y social de la población. El AIC también constituye un riesgo relevante para los sistemas de información ciberfísicos [43], cuyo empleo es muy frecuente hoy en día en el sector de las telecomunicaciones, de la industria 4.0, de la energía y de los transportes. Piénsese, por ejemplo, en los coches sin conductor.

Actualmente parece difícil que un agente artificial pueda llevar a cabo de forma completamente autónoma un hecho que, en el caso de que lo realizara un ser humano, se consideraría como un hecho típico, penalmente antijuridico y culpable. En este sentido, la doctrina mayoritaria considera hoy en día que un agente artificial, pese a su autonomía, no puede considerarse todavía, a efectos del Derecho penal, como el verdadero autor de un delito, al no tener un nivel suficiente de conciencia para entender el sentido de sus comportamientos y, por consiguiente, no ser imputable [44].

1. **La inteligencia artificial como medio de ejecución de un hecho ilícito**

En un contexto ilícito, la IA puede emplearse, en primer lugar, como medio de ejecución de un delito tanto tradicional (estafa, injurias) como cibernético o, más en general, con fines ilícitos. Paradigmático en este sentido es el fenómeno del *spear phishing* [45]. Se trata de una modalidad muy peculiar de *phishing,* dirigida contra un objetivo específico (una persona o una empresa), que normalmente se lleva a cabo mediante correos electrónicos que parecen legítimos para el destinatario y que lo inducen a proporcionar datos confidenciales (credenciales de inicio de sesión, datos de tarjetas de crédito, etc.) al sujeto atacante. La diferencia principal con el *phishing* es que el sujeto atacan-

[43] En este sentido, véase MIT Technology Review, *Preparing for AI-enabled Cyberattacks,* 2021.

[44] Abbott, R. / Sarch, A. F., «Punishing Artificial Intelligence: Legal Fiction or Science Fiction», *UC David Law Review,* vol. 53, 2019, pp. 323 y ss.; Gless, S. / Silverman, E. / Weigend, T., «If Robots Cause Harm, who is to blame? Self-driving Cars and Criminal Liability», *New Criminal Law Review,* vol. 19, 2016, pp. 412 y ss.; Pagallo, U., « Vital, Sophia, and Co.–The Quest for the Legal Personhood of Robots», *Information,* vol. 9, 2018, pp. 1 y ss.

[45] Bethaby, M. / Galiopoulos, A. / Bethany, E. / Karkevandi, M. B. / Vishwamitra, N. / Najafirad, P., «Large Language Model Lateral Spear Phishing: A Comparative Study in Large-Scale Organizational Settings», *ArXiv, Bethany, M., Galiopoulos, A., Bethany, E., Karkevandi, M. B., Vishwamitra, N., & Najafirad, P. (2024). Large Language Model Lateral Spear Phishing: A Comparative Study in Large-Scale Organizational Settings. ArXiv,* abs/2401.09727, 2024.

te, en lugar de dirigirse a miles de posibles víctimas mediante *phishing* masivo, se dirige a personas o grupos específicos con correos electrónicos personalizados.

Para hacerse con las contraseñas que protegen un sistema informático o que sirven para acceder a una cuenta bancaria online, los criminales suelen emplear, en el marco de los ataques de *spear phishing,* técnicas de ingeniería social, cada vez más sofisticadas [46]. En primer lugar, los ciberdelincuentes pueden suplantar de forma ilícita la identidad del remitente y, de esta manera, engañar a la víctima sobre su verdadera identidad, logrando que esta le proporcione las informaciones que necesita (contraseñas, datos personales o sensibles, etc.). La suplantación de identidad normalmente se lleva a cabo mediante el envío de un correo desde una dirección falsa para hacer creer al destinatario que el mensaje proviene de una persona o de una entidad que conoce o en la que puede confiar. Sin embargo, hoy en día, con el desarrollo de las tecnologías del *deepfake* y de la IA generativa, los criminales logran suplantar la identidad ajena mediante la creación de imágenes o videos que reproducen de forma perfecta el rostro o la misma voz de un sujeto [47]. Esto es, precisamente, lo que le ocurrió hace unos meses al empleado de una empresa multinacional de Hong Kong que hizo una transferencia millonaria a quien él creía que era la filial de su empresa en el Reino Unido, sin darse cuenta de que fue engañado para que asistiera a una videoconferencia en la que realmente no estaban, como él pensaba, el director financiero de su empresa u otros miembros del personal, al ser todos ellos en realidad recreaciones hiperrealistas falsas creadas mediante tecnología *deepfake* [48].

El hecho de suplantar sin autorización la identidad de otra persona tiene relevancia penal en el ordenamiento jurídico italiano. El art. 494 del Código Penal italiano castiga con pena de prisión de hasta un año a quien, con el fin de procurarse a sí mismo o a otros un provecho o causar un perjuicio ajeno, induzca a error a otro sustituyendo ilícitamente su propia persona por la de otro, o atribuyéndose a sí mismo o a otros un nombre falso, una condición falsa o una capaci-

---

[46] Sobre la evolución de las técnicas de ingeniería social, véase Washo, A. H., «An Interdisciplinary View of Social Engineering: A Call to Action for Research», *Computers in Human Behavior Reports,* vol. 4, 2021, pp. 1 y ss.; Gallo, L. / Gentile, D. / Ruggiero, S. / Botta, A. / Ventre, G., «The Human Factor in Phishing: Collecting and Analyzing User Behavior When Reading Emails», *Computers & Security,* vol. 139, 2024, pp. 1 y ss.

[47] Sobre los riesgos relacionados con el *deep fake,* véase EUROPOL, *Facing reality? Law enforcement and the challenge of deepfakes. An observatory report from the Europol Innovation Lab,* Luxembourg (Publications Office of the European Union), 2022.

[48] Véase, en este sentido, CNN, «Trabajador de finanzas paga US$ 25 millones después de una videollamada con un 'director financiero' falso», 4 de febrero de 2024, disponible en: 'https://cnnespanol.cnn.com/2024/02/04/trabajador-paga-us-25-millones-tras-videollamada-director-financiero-falso-trax'

dad a la que la ley atribuye efectos jurídicos. La jurisprudencia italiana, en distintas ocasiones, ha aclarado que este se aprecia en los casos en los que el autor crea y emplea un perfil falso en redes sociales, utilizando de manera no autorizada el nombre y apellidos de otra persona, al tratarse de una conducta idónea para representar una identidad digital que no se corresponde a la realidad [49].

Este delito requiere un ánimo subjetivo del injusto: el hecho típico tiene que llevarse a cabo con el propósito de conseguir un provecho, que no tiene que ser necesariamente de carácter económico, o, alternativamente, de causar un daño a otro [50]. Se trata, asimismo, de un delito de resultado y se perfecciona mediante cualquier conducta que consista en suplantar a otra persona. En este sentido, el tipo delictivo puede apreciarse también en los casos en que un sujeto, mediante tecnología *deepfake,* se hace pasar por otra persona y, de esta manera, logra engañar la víctima con la intención de conseguir un provecho (p. ej., conseguir la contraseña de acceso a un sistema informático o los datos de acceso a una cuenta bancaria online) o causarle un daño. Al tratarse de un delito mutilado de dos actos, no será necesario, para la consumación del tipo penal, que el criminal, mediante la ejecución del primer acto, consiga efectivamente una ventaja.

Mas complejo resulta castigar las conductas de suplantación de identidad, tradicional o llevada a cabo mediante el empleo de la IA, en España, puesto que no hay en el Código Penal español un tipo penal específico, como sucede en Italia. En este sentido, tanto la doctrina penal como la jurisprudencia mayoritaria no considera aplicable el delito de usurpación del estado civil del art. 401 CP a los supuestos de suplantación de identidad online [51]. Y es que, come ha reconocido en distintas ocasiones la jurisprudencia, no es suficiente la continuidad o la repetición en el tiempo del uso indebido del nombre y apellidos de otro para integrar el tipo de usurpación del art. 401 CP, requiriendo el tipo algo más, es decir, *«hacer algo que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden»* [52]. Sin embargo, en la mayoría de los casos de suplantación de identidad digital, y, en

[49] Véase, p. ej., Cass. pen., sez. V, 28 de noviembre de 2012, n.º 18826; Cass. pen., sez. V, 4 de noviembre de 2022, n. 41801.

[50] En este sentido, véase, p. ej., Cass. pen., 6 de julio de 2020, n.° 22409; Cass. pen., 23 de abril de 2014, n.º 25774. En la doctrina, véase Crescioli, C., «La tutela penale dell'identità digitale», *Diritto penale contemporaneo,* 5/2018, 2018, pp. 1 y ss.

[51] En este sentido, véase, p. ej., Sánchez Domingo, M. B., «Robo de identidad personal a través de la manipulación o el acceso ilegítimo a sistemas informáticos: ¿necesidad de una tipificación específica?», Revista General de Derecho Penal, núm. 26, 2016, pp. 1 y ss. (pp. 10 y ss.).

[52] En este sentido, véase, p. ej., STS 635/2009, de 15 de junio; SAP Madrid 461/2017, de 25 de mayo; SAP Valladolid 78/2017, de 22 de febrero.

particular, en relación con los casos de *spear phishing,* la conducta se lleva a cabo para conseguir de manera fraudulenta datos personales de las víctimas para luego utilizarlos con fines ilícitos (acceder a su sistema informático, difundirlos en redes sociales, venderlos, extorsionar a la víctima, etc.).

Tampoco resulta aplicable el nuevo tipo delictivo del art. 172 ter.5 CP, que el legislador español ha introducido en el Código Penal con la LO 10/2022 de 6 de diciembre, y que castiga con pena de prisión de tres meses a un año o multa de seis a doce meses a quien, *«sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación».* Se trata de un delito de resultado, puesto que el hecho típico tiene que causar humillación, acoso u hostigamiento a la víctima, si bien no requiere que dicho resultado sea causado directamente por el autor del delito (quien ha utilizado la imagen para abrir perfiles falsos), pudiendo haber sido causado por terceras personas que, engañadas, se dirigen a la víctima en la creencia de que ella misma es quien solicita el contacto [53]. Por esta razón, el precepto no podría aplicarse a los casos de suplantación relacionados con el *spear phishing,* puesto que el sujeto atacante que crea falsos perfiles sociales no lo hace para causar un acoso a la víctima, sino para hacerse de manera fraudulenta con sus datos personales.

En la medida en que el criminal, mediante técnicas de ingeniería social o suplantación de identidad, consiga efectivamente datos e informaciones de la víctima, tanto en Italia como en España, podrán apreciarse, dependiendo de la naturaleza de dichos datos, distintos delitos:

a) La conducta de procurarse, de manera no autorizada, códigos, contraseñas u otros medios idóneos para acceder a un sistema informático (o a una cuenta bancaria online) con la finalidad de conseguir para sí o para un tercero un beneficio económico, es castigada por el Código Penal italiano con la pena de prisión de hasta dos años y multa de hasta 5.164 euros (art. 615 quater) [54]. En el concepto «otros medios idóneos»» pueden incluirse también las creden-

[53] En este sentido, véase Jareño Leal Á., «El derecho a la imagen íntima y el Código Penal. La calificación de los casos de elaboración y difusión del deepfake sexual», *Revista Electrónica de Ciencia Penal y Criminología,* núm. 26, 2024, pp. 1 y ss. (pp. 20 y ss.).

[54] Art. 615 quater: *«Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164 (3). La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui al quarto comma*

ciales que el autor de un ataque de *spear phishing* necesita para acceder a la cuenta bancaria online de la víctima. La misma conducta tiene relevancia penal también en el ordenamiento jurídico español, que, en el art. 197 ter CP castiga el hecho de «adquirir para su uso», con la intención de facilitar la comisión de un delito de intrusismo informático del art. 197 bis CP, una *«contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información»* (art. 197 ter.2.b CP).

b) Si el ciberdelincuente, mediante «robo» de identidad o técnicas de ingeniería social consigue que la víctima le proporcione los datos de su tarjeta de crédito o débito, se aplicará le pena de prisión (de tres meses a tres años) establecida por el art. 249.2.b CP, que castiga el hecho de apropiarse o adquirir de forma ilícita los datos de las tarjetas de crédito.

c) Si el ciberdelincuente, tras conseguir, mediante el envío de correos electrónicos fraudulentos (escritos mediante IA generativa, utilizando de manera engañosa el nombre y apellidos de otra persona, con un enlace que puede redirigir a un sitio web falso del banco o de un comercio electrónico, etc.), las claves de acceso a la cuenta bancaria de la víctima o, valiéndose de una manipulación informática o artificio semejante, consigue acceder a *su home banking* y llevar a cabo directa o indirectamente una transferencia no autorizada de cualquier activo patrimonial en perjuicio de la víctima, podrá apreciarse el delito más grave de fraude informático (del art. 249.1 CP o del art. 640 ter del Código Penal italiano).

Por otro lado, la IA también permite desarrollar nuevas técnicas para facilitar el espionaje de datos informáticos (ciberespionaje), el acceso no autorizado a sistemas de información, y para llevar a cabo ataques contra datos y sistemas informáticos (ciberataques), estafas o fraudes informáticos [55]. En este sentido, cada vez hay más evidencias sobre el empleo, por parte de los criminales cibernéticos, de los denominados *AI-generated malware,* es decir, programas informáticos maliciosos basados en la IA que resultan particularmente difíciles de detectar y de bloquear por parte de los sistemas antivirus [56]. Estos

dell'articolo 617-quater». El mencionado artículo ha sido modificado por el art. 19, par. 1, let. C) de la Ley 23 de diciembre de 2021, n. 238.

[55] Sobre el impacto que el uso ilícito de la IA puede tener en relación con las estafas y los fraudes informáticos, véase el informe de PwC «Impact of AI on fraud and scams», 2023, que se puede consultar aquí: www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf.

[56] En este sentido, véase, p. ej., HYAS, «Blackmamba: AI-Sybthesized, Polymorphic Keylogger with on-the-fly Program Modification», 2023, que se puede consultar aquí: 'https://www.hyas.com/hubfs/Downloadable%20Content/HYAS-AI-Augmented-Cyber-Attack-WP-1.1.pdf'; National Cyber Security Center, «The Near-term Impact of AI on The Cyber Threat», 2024, que se puede consultar aquí: www.ncsc.gov.uk/pdfs/report/impact-of-ai-on-cyber-threat.pdf

tipos de *malware,* que se emplean para llevar a cabo ataques o para extorsionar a los usuarios (mediante *ransomware)* pueden conseguirse fácilmente a través de la *deep web* o canales online (como *Telegram).* En este sentido, la conducta del sujeto que, sin autorización, tenga a su disposición los mencionados programas informáticos maliciosos *(malware, ransomware,* etc.) o que, de forma ilícita, se procure o adquiera los mencionados objetos con el propósito de dañar datos o sistemas de información, tiene relevancia penal tanto en Italia como en España: en Italia dicha conducta puede ser subsumida en el art. 615 quinquies del Código Penal, que se reformó con el art. 19, párrafo 2, letra b), de la Ley n.º 238/2021; en España podrá aplicarse el art. 264 ter CP.

El hecho que los *AI-generated malware* sean objetos informáticos nuevos, desarrollados mediante la IA, no plantea particulares problemas jurídico-penales, puesto que los mencionados delitos, que castigan actos preparatorios a la ejecución de hechos ilícitos más graves, tienen por objeto cualquier programa informático *(software)* concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores [57].

IV. LA RELEVANCIA PENAL DE LAS AGRESIONES A LAS TECNOLOGÍAS DE IA

En el Derecho penal vigente en España e Italia, los agentes inteligentes y los sistemas de IA no son mencionados en ningún tipo penal y, por lo tanto, no constituyen, de manera expresa, el objeto material de ningún delito cibernético. Sin embargo, esto no significa que no gocen de protección penal. En este sentido, no hay particulares problemas hermenéuticos e interpretativos para equiparar, a efectos penales, los agentes artificiales, que funcionan sobre la base de algoritmos, a un programa informático *(software).*

El art. 2, letra b, de la directiva europea 2023/40/UE define los programas informáticos como un conjunto de datos informáticos que sirven para hacer que un sistema de información realice determinadas funciones. En este sentido, es evidente que cualquier hecho no autorizado que cause la alteración, la supresión, el borrado, o que haga inaccesible los datos informáticos que integran un agente artificial o el programa informático que determina su funcionamiento, podrá ser subsumido en los tipos penales vigentes de daños de datos y

[57] En relación con los problemas político-criminales y dogmáticos que plantean los tipos penales que castigan actos preparatorios, véase Alonso Rimo, A., *El tipo subjetivo de los actos preparatorios del delito,* Valencia, 2023; Salvadori, I., *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata,* Napoli (Edizioni Scientifiche Italiane), 2016, pp. 253 y ss.

de sistemas de información (arts. 264 del Código Penal español; arts. 635 bis y 635 ter del Código Penal italiano). Y es que los agentes artificiales y robots, compuestos de uno o más dispositivos lógicos *(software)* y físicos *(hardware),* pueden ser considerados como un sistema de información de conformidad con el art. 2, letra a de la misma directiva europea, que incluye en este concepto *«todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización protección y mantenimiento»*. Por consiguiente, el hecho no autorizado de dañar, obstaculizar o interrumpir el funcionamiento de un sistema de IA o de un robot podría tener ya relevancia penal tanto en España (art. 264 bis CP) como en Italia (art. 635 quater y 635 quinquies).

Tampoco plantea relevantes problemas jurídico-penales la conducta del *hacker* que accede sin autorización a un sistema ciberfísico (como podría ser el sistema de información que controla diferentes aspectos de un *smart car)* o de un sistema informático que controla el correcto funcionamiento de una infraestructura crítica, al existir un delito de acceso no autorizado a un sistema de información (art. 197 bis CP español y art. 615 ter CP italiano).

Debe también tenerse en cuenta que un programa de ordenador puede considerarse, de cumplirse todos los requisitos normativos, un objeto de propiedad intelectual[58]. En este sentido, la reproducción o la distribución, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, de un programa informático que constituye un objeto de propiedad intelectual, que sirva para hacer que un sistema de información de IA realice determinadas funciones, son conductas con relevancia penal tanto en España (art. 270 CP), como en Italia (art. 171 bis y siguientes de la Ley sobre propiedad intelectual).

V. CONSIDERACIONES FINALES

Un sector doctrinal considera que el incesante y rápido desarrollo de la IA favorecerá, en un futuro cada vez más cercano, la creación de agentes artificia-

[58] Véase el art. 10, letra i) del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

les completamente autónomos que podrán determinar su propio comportamiento de manera autónoma sin ninguna intervención humana, comprender el sentido de sus comportamientos y, al mismo tiempo, llevar a cabo conductas con relevancia penal [59]. Si dentro de unos años esto, finalmente, sucede, los organismos internacionales (Naciones Unidas, Consejo de Europa, Unión Europea, etc.) y los legisladores nacionales tendrán que tomar seriamente en cuenta la posibilidad de tomar nuevas medidas penales para castigar las agresiones llevadas a cabo mediante agentes artificiales y sistemas de IA a bienes jurídicos tradicionales y a los nuevos intereses jurídicos, merecedores y necesitados de protección penal, que surgirán como consecuencia de los avances tecnológicos. Así, tendrán que plantearse la posibilidad de establecer consecuencias penales para aquellos agentes artificiales que hayan cometido de manera consciente y libre un hecho típico y penalmente antijurídico [60].

A la espera de averiguar si la ciencia penal tendrá que aceptar que no solamente las personas jurídicas pueden delinquir y cometer delitos y, en consecuencia, castigadas *(societas delinquere et puniri potest),* sino que también pueden hacerlo los agentes artificiales y los robots *(maquina delinquere et puniri potest),* el análisis del Derecho penal de las nuevas tecnologías de España e Italia demuestra que una correcta interpretación y aplicación de los vigente delitos cibernéticos (en sentido estricto y en sentido amplio) permite evitar, *de lege lata,* peligrosos vacíos normativos y sancionar aquellos sujetos que intentan explotar las tecnologías de IA para finalidades ilícitas.

[59] Defiende esta posición HALLEVY, G., «The Criminal Liability of Artificial Intelligence Entities. From Science Fiction to Legal Social Control», *Akron Intellectual Property Journal,* vol. 4, 2010, pp. 171 y ss.

[60] Admiten, con distintas argumentaciones, la posibilidad de mover el reproche penal a los robots, HALLEVY, G., «The Criminal Liability of Artificial Intelligence Entities. From Science Fiction to Legal Social Control», *Akron Intellectual Property Journal,* vol. 4, 2010, pp. 171 y ss.; HALLEVY, G., «*Liability for Crimes Involving Artificial Intelligence Systems,* Cham (Springer), 2014; LAGIOIA, F. / SARTOR, G., «AI Systems Under Criminal Law: A Legal Analysis and A Regulatory Perspective», *Philosophy & Technology,* vol. 33, 2019, pp. 1 y ss.; SIMMLER M. / MARKWALDER N., «Guilty Robots? Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence», *Criminal Law Forum,* vol. 30, 2019, pp. 1 y ss.